UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO

TESIS PARA OPTAR EL TÍTULO DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR (A)

CELIS FIGUEROA, LEONARDO ANDRE

Chiclayo, 06 de diciembre de 2018

PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO

PRESENTADA POR:
CELIS FIGUEROA, LEONARDO ANDRE

A la Facultad de Ingeniería de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR:

_____
Mgtr. Reyes Burgos, Karla Cecilia
PRESIDENTE

_____
Mgtr. Imán Espinoza, Ricardo David
SECRETARIO

_____
Mgtr. León Tenorio, Gregorio Manuel
ASESOR

DEDICATORIA

A Dios por darme la vida, existir y hacerme un instrumento de su amor.
A mi esposa Juliana y a mi hija Flavia, que son y siempre serán el motor de mi vida; mis ganas para salir adelante con mis metas y objetivos.
A mis padres Hugo y Maritza, ejemplo de vida, amor y familia.
A mis hermanas Estefani y Valeria por su gran apoyo moral.

EPÍGRAFE

“No importa cuántas veces te equivocas o con que lentitud progresas, sigues estando muy por delante de los que ni lo intentan”
Anthony Robbins

“Cuando todo parezca estar en tu contra, recuerdas que los aviones despegan con el aire en contra, no a favor”
Henry Ford

AGRADECIMIENTO

Al Ing. Gregorio León Tenorio, asesor de la tesis, a quien admiro, respeto y agradezco por su tiempo y apoyo; así como por la sabiduría que supo transmitirme en la ejecución del presente Informe de Tesis.

A los Directivos de la Central Hidroeléctrica Carhuaquero por las facilidades brindadadas para que fuera posible la realización del Trabajo de Investigación.

Agradecimiento especial a la Facultad de Ingeniería de nuestra Universidad. Al Director de Carrera y Plana Docente, por su tiempo compartido e impulsar el desarrollo de nuestra formación profesional.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación denominada "Plan de Seguridad de la Información aplicado a la Central Hidroeléctrica Carhuaquero", surge como alternativa de solución frente al problema de seguridad de la información que tiene la Unidad de Producción Hidráulica de la referida organización.

El Plan de Seguridad compromete la organización de los procesos de la citada Unidad, puesto que la correcta gestión de seguridad de la información puede marcar la diferencia entre la eficacia y la inoperancia.

En cuanto a la metodología utilizada debemos señalar que después de una sutil comparación con las ya existentes en este campo, se optó por aquella denominada MAGERIT; la misma que permitió el análisis y gestión de riesgos. También, se utilizó la herramienta EAR-PILAR que ayudó en la toma de las mejores decisiones frente al problema de seguridad de la información.

Finalmente, después de haber recogido información fidedigna producto de una exhaustiva investigación, se concluyó que el Sistema de Gestión de Seguridad de la Información (SGSI) es un soporte importante que ayuda a organizar los procesos, controles y salvaguardas de la Unidad de Producción Hidráulica de la Central Hidroeléctrica Carhuaquero; y al mismo tiempo hace posible mantener la información bajo medidas de seguridad, garantizando su integridad, confidencialidad y autenticidad.

Palabras clave: Seguridad, Información, MAGERIT, Norma ISO, Confidencialidad, Autenticidad, Integridad, Procesos, Controles, Salvaguardas

ABSTRACT

Current research called “Information Security Plan applied to the Central Hydroelectric Carhuaquero” it emerges as an alternative of solution that allows you to deal with the problem of information security which has production hydraulic unit.

The Security Plan compromises the organization of the processes of the aforementioned Unit, since the correct management of information security can make the difference between efficiency and inoperability.

Regarding the methodology used, we should point out that after a subtle comparison with those already existing in this field, we chose the one called MAGERIT; the same that allowed the analysis and risk management. Also, the EAR-PILAR tool was used, which helped in making the best decisions regarding the security of information problem.

Finally, after having collected reliable information resulting from an exhaustive investigation, it was concluded that the Information Security Management System (ISMS) is an important support that helps organize the processes, controls and safeguards of the Hydraulic Production Unit of the Hydroelectric Plant Carhuaquero; and at the same time it makes it possible to keep the information under security measures, guaranteeing its integrity, confidentiality and authenticity.

Keywords: Security, Information, MAGERIT, ISO Standard, Confidentiality, Authenticity, Integrity, Process, Controls and Safeguards

I. INTRODUCCIÓN

"Las tecnologías de la información actualmente son elementos fundamentales para la superación y desarrollo de un país, la información que en ellas se maneja es considerada un activo cada vez más valioso el cual puede hacer que una organización triunfe o quiebre, es por eso que debemos brindarle seguridad." (M. Hernández 2006)

En ese sentido, el principal activo de toda organización, la seguridad, no puede ser concebida solo como un accionar defensivo y reactivo para preservar los activos de negocio, sino que requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo, así como lo ha expuesto (Pallas 2009) "los sistemas tecnológicos deben permitir resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma".

Según (Córdova 2003) menciona: "La mayoría de las empresas han invertido tiempo y dinero en la construcción de una infraestructura para la tecnología de la información que soporte su compañía. Esta infraestructura de TI (Tecnología de la Información) podría resultar ser una gran debilidad si se ve comprometida. Es por ello, que para que las organizaciones que funcionan en la era de la informática interconectadas y con comunicación electrónica, las políticas de información bien documentadas que se comunican, entienden e implementen en toda la empresa, son herramientas comerciales esenciales en el entorno actual para minimizar los riesgos de seguridad".

Sin embargo, existen otras organizaciones que no cuentan con el suficiente capital para protegerla de los diversos riesgos que afectan la seguridad de su información, y según lo expuesto por (M. Hernández 2006), "debemos tener identificadas y controladas esas vulnerabilidades y esto se logra con un adecuado plan de seguridad elaborado basándose en un análisis de riesgo previo".

Vulnerabilidades que "de acuerdo a unas encuestas internacionales, el mayor riesgo a la seguridad de la información son el factor humano, específicamente errores, conductas inapropiadas y/o negligencias generadas internamente". (Pallas 2009) Razón por la que es necesario considerar que "Implementar una política de seguridad completa, le da valor intrínseco a su empresa, asimismo la credibilidad y reputación aumentará la confianza de los accionistas principales, lo que dará una ventaja estratégica" (Córdova 2003)

El presente trabajo de investigación, se llevó a cabo en la CENTRAL HIDROELÉCTRICA CARHUAQUERO, ubicada en la sierra norte del país, distrito de Llama, provincia de Chota, región Cajamarca. Es una empresa de tipo minería energética, cuyo producto es la generación de energía que utiliza como materia prima el agua del río Chancay, por encontrarse certificada como 100% limpia al emplear fuentes eficientes, renovables y responsables (Duke Energy 2014)

Al observar la realidad existente con respecto a la seguridad de la información en la Unidad de Producción Hidroeléctrica de la misma Central, se constató la presencia de intrusos que pretenden penetrar los niveles de seguridad de la red, creando el llamado "hueco de seguridad" con la finalidad de desviar el flujo de información de un punto de transmisión a su debido destino. Esta forma de actuar de personas inescrupulosas permite darnos cuenta que la empresa carece de seguridad y poca previsión respecto a los riesgos de sus activos de información, situación que podría acarrear cuantiosas pérdidas económicas.

Otra de las dificultades de la empresa son las insuficientes medidas y procedimientos recogidos en los planes de seguridad informática que no responden a los estándares internacionales que norman los sistemas de gestión de seguridad informática tanto en la prevención como recuperación ante desastres o ataques.

Por otra parte, en entrevista sostenida con el encargado del área de Tecnologías de Información señaló que los problemas de seguridad de la información de la Unidad de Producción Hidroeléctrica de la misma Central son ocasionados entre otros factores por los siguientes:

- ✓ La ubicación de los servidores dentro de la organización, los mismos que se encuentran en una oficina que no corresponde al área de Tecnologías de la Información y están a la vista de todas las personas que pueden acceder a esta área. Además, no se encuentran protegidos por ningún tipo de seguridad, lo que trae como consecuencia que el personal pueda acceder fácilmente a la información de la empresa.

- ✓ Uso inadecuado de la información y el hecho de que terceros puedan utilizarla en contra de la empresa y del mismo trabajador. Situación que se confirma con los resultados obtenidos de la encuesta aplicada a trabajadores de la Central Hidroeléctrica Carhuaquero. En ella se observa que el 40,63% de los usuarios dejan sus computadoras desbloqueadas cuando van a trabajar al campo (Anexo 2 – Figura 65). En tanto que, el 56.25% de los trabajadores ha brindado su contraseña a algún compañero de trabajo. De estos, el 46,88% conoce sobre temas de seguridad y 9 de ellos, es decir 38% ha brindado su contraseña a algún compañero (Anexo 2 – Figura 70). Esto potencia el riesgo como lo manifiesta (Universidad Miutar Nueva Granada 2013) sobre la utilización de los sistemas de la empresa sin privilegios otorgados que traería como consecuencia suplantación de identidad, degradación, corrupción, divulgación de información, acceso no autorizado, ingreso de falsa información y robo.

- ✓ Existen colaboradores que se conectan a la red corporativa por medio de cable Ethernet. Esto además de estar prohibido por ética laboral, expone a los sistemas de la Central Hidroeléctrica Carhuaquero a una propensión del software de sus ordenadores con códigos maliciosos que pueden comprometer a la red, puesto que solo el 53.13% de los usuarios a veces utiliza el programa antivirus para salvaguardar la información del ordenador y el 6. 25% nunca lo utiliza (Anexo 2 – Figura 66).

Por otra parte, es preciso señalar que en la Central Hidroeléctrica Carhuaquero, la información es un activo fundamental para la prestación de servicios y la toma de decisiones eficientes, razón por la cual existe un Information Security Incident Management o Gestión de la Información de Incidentes de Seguridad (ANEXO 3) de sus activos más significativos como parte de una estrategia orientada a la prestación de servicios, la administración de riesgos y la consolidación de una cultura de seguridad; la misma que solo queda como un referente que forma parte del protocolo pero que no es tomado en cuenta como ya se ha detallado líneas arriba.

Conocedores de las necesidades en lo que respecta la seguridad de la información en la Central Hidroeléctrica se propuso la implementación de una metodología de análisis y gestión de riesgos de la información (MAGERIT) como herramienta que permitió analizar el impacto que tiene para la empresa la omisión de seguridad de la información; y sensibilizó a los colaboradores sobre la importancia de saber a qué riesgos están expuestos los sistemas de

información de la empresa y como ayudarían ellos a gestionarlos, dando un tratamiento oportuno para mantenerlos bajo control. De esta manera se ayudó a la reducción de costos operativos y financieros, y se estableció una cultura de seguridad.

Por todo lo anteriormente expuesto, se planteó la siguiente problemática: ¿De qué manera se puede prevenir posibles riesgos y vulnerabilidades de los activos de la información de la empresa Central Hidroeléctrica Carhuaquero?

Para dar respuesta anticipada al problema se formuló la siguiente hipótesis: Si se implementa un plan de seguridad acorde con MAGERIT la cual se basa en la ISO 31000 y 27001 que elevará los niveles de seguridad entonces se posibilitará la identificación, evaluación de riesgos y posibles vulnerabilidades en el acceso a la información de la Unidad de Producción Hidráulica.

Asimismo, como objetivo general se planteó: Proponer un plan de seguridad de la información en la Central Hidroeléctrica de Carhuaquero utilizando la metodología MAGERIT para el análisis y gestión de riesgos. (Versión 3). Entre los objetivos específicos planteados podemos señalar:

- Identificar y evaluar los activos que existen en la organización, además de las amenazas que afectan a estos activos.
- Establecer los mecanismos de protección apropiados para minimizar los riesgos críticos de la organización en estudio.
- Proponer proyectos adecuados para tratar y minimizar los riesgos críticos encontrados.

En lo concerniente a su justificación, la presente tesis es importante en lo tecnológico, porque la información es el activo más importante para una empresa, y porque el análisis e implementación del Plan de Seguridad Informática traerá consigo mejoras en el entorno de la empresa, beneficiándose desde el punto de vista económico, ya que evitará la baja productividad por la pérdida de información y de dinero, logrando asegurar así la continuidad del negocio.

También se justifica en lo científico, puesto que se considera información teórica científica acerca de los recursos informáticos y metodologías apropiadas para salvaguardar la información de una empresa.

Y, por último, en lo personal contribuyó a conocer a través de lo facto perceptible la realidad existente en un tema tan complejo como la seguridad de la información y de esta manera contrastar el conocimiento teórico aprendido en aulas con la práctica a fin de ser un profesional con experiencia.

II. MARCO TEÓRICO

2.1. ANTECEDENTES

Para este punto, los antecedentes al problema se dividen en tres puntos:

2.1.1. ANTECEDENTES INTERNACIONALES:

Tabla 1: Antecedente Internacional N° 01

Año	Barcelona, 2013
Autores	José Aurela
Título	Plan de Implementación de la norma ISO/IEC 27001:2005
Resumen	Este proyecto de investigación expuesto por (Aurela Pereira 2013), nos menciona que en la actualidad el volumen y complejidad de la información, y la dependencia de las organizaciones hacia procesos y sistemas informáticos han llevado a los profesionales de TI a enfrentar grandes retos y amenazas. Estos retos han obligado a las compañías a organizarse y crear estrategias y estándares que permitan proteger el activo intangible más valioso: "La información". Con la realización de este trabajo se logró el objetivo de crear de manera practica un plan de trabajo que permita implementar la ISO/IEC 27001:2005. Así mismo, se desarrolló la información normativa y conceptos generales que deben conocerse antes de iniciar un proceso de implementación y correcto funcionamiento.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar riesgos y reducir costos, implementando la norma ISO 27002 en los hallazgos encontrados.

Tabla 2: Antecedente Internacional N° 02

Año	Cuenca, 2013
Autores	Karina del Rocío Gaona Vásquez
Título	Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravitos S.A. en la ciudad de Machala
Resumen	El proyecto de investigación expuesto por (Gaona Vasquez 2013), explica las fases que se deben de seguir para poder desarrollar la metodología MAGERIT, paso por paso, pero aplicado a una industria pesquera. Asimismo, también detalla cómo se analizan los procesos de la empresa y de cómo está constituida. De esta manera se encuentran las carencias de seguridad que posee
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información con la metodología MAGERIT, desarrollando sus fases y proponer la implementación de esta.

Tabla 3: Antecedente Internacional N° 03

Año	Sangolqui, 2015
Autores	Cristian Fabricio Viteri Silva
Título	Evaluación de riesgos tecnológicos del centro de datos de la Universidad nacional de Chimborazo usando los procesos de TI basados en COBIT y MAGERIT
Resumen	El proyecto de investigación de (Viteri Silva 2015), que la evaluación basada en riesgos permite a una institución considerar la dimensión con que los eventos potenciales influyan en la obtención de los objetivos, evaluándolos desde la perspectiva de la probabilidad y el impacto, es por ello que marcos de referencia como COBIT y la metodología MAGERIT, permiten determinar los riesgos al que está sometido un Centro de Datos. La mayoría de las amenazas no resaltan a la vista de la persona hasta que es demasiado tarde, mucho más si se hace referencia a los activos de la organización.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar riesgos ante las amenazas a los activos de la organización. A diferencia de este trabajo, no se utilizará COBIT, pero por cultura ayudará a tener un conocimiento más concreto sobre la gestión de riesgos en base a este marco de referencia.

2.1.2. ANTECEDENTES NACIONALES:

Tabla 4: Antecedente Nacional N° 04

Año	Lima, 2012
Autores	Barrantes Porras, Carlos Eduardo Hugo Herrera, Javier Roberto
Título	
Resumen	Este proyecto de investigación de (Barrantes Porras y Hugo Herrera 2013), que la característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una empresa; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar riesgos ante las amenazas a los activos de la organización.

Tabla 5: Antecedente Nacional N° 05

Año	Lima, 2014
Autores	Josefina Ríos Villafuerte
Título	Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos
Resumen	En este proyecto de investigación expuesto por (Ríos Villafuerte 2014), menciona que el diseño de un SGSI para una central de riesgo privada y esta pueda cumplir con las exigencias regulatorias a las que se haya sujeta, siguiendo los siguientes marcos de trabajo: ISO/IEC 27001, 27002 y 31000. Además expone definiciones según la ley y marco Legal.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación se basa en los marcos de trabajo: ISO/IEC 27001, 27002 y 31000 en la cual se basa MAGERIT para el desarrollo de sus fases. Además, ayudará mucho el tema de leyes, lo cual nos ayudará a saber bajo que reglamento se basa una organización para implementar la gestión de riesgos para los activos de TI

Tabla 6: Antecedente Nacional N° 06

Año	Ayacucho, 2016
Autores	Huerta Aranda, Melissa
Título	Procedimientos para la auditoría en seguridad física del Data Center de la Municipalidad Provincial de Huamanga
Resumen	En este proyecto de investigación expuesto por (Huerta Aranda 2016) proponer procedimientos para la realización de una auditoría en seguridad física al Data Center de la Municipalidad Provincial de Huamanga, basados en estándares internacionales como el TIER 1, en la normativa peruana NTP ISO/lEC 17799 y el marco de control COBIT5.0; con la intención de evaluar la Infraestructura del Dato Center y verificar la disposición de su seguridad física.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que habla sobre la seguridad física en la data centers, lo cual es un activo importante en la organización que se tiene como estudio en el actual proyecto de tesis. Utiliza Normas como TIA942 en los cuales clasifica a estos centros de datos en TIER, son 4 niveles y cada nivel refleja el porcentaje de disponibilidad que debería tener estos centros de datos, los cuales son conocimiento bases que se debe tener a la hora de aplicar las salvaguardas basados en una norma ANSI (TIA942)

2.1.3. ANTECEDENTES LOCALES:

Tabla 7: Antecedente Local N° 07

Año	Chiclayo, 2012
Autores	Santa María, Frank
Título	Buenas prácticas para auditor redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo
Resumen	El proyecto de investigación expuesto por (Santa María Becerra 2013), propone buenas prácticas para el desarrollo de auditorías de redes inalámbricas aplicadas a las empresas del rubro hotelero, con el fin de mejorar la disponibilidad, confiabilidad e integridad de la información, cotejando metodologías existentes que ayuden auditar redes inalámbricas y desarrollando la propuesta de las buenas prácticas. (Santa María Becerra 2013), Cotejó metodologías, manuales y buenas prácticas nacionales e internacionales, tales como ISO 27001, ISO 27002, NAGU, donde se pudo identificar 8 buenas prácticas en promedio, logrando desarrollar 5 nuevas prácticas para así obtener finalmente 13 buenas practicas agrupadas en tres demonios: Diseño, administración y seguridad, haciendo posible aplicar y logar mayor eficiencia y eficacia en el proceso de auditoría a las redes inalámbricas en el rubro hotelero.
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar riesgos y reducir costos, implementando la norma ISO 27002 en los hallazgos encontrados.

Tabla 8: Antecedente Local N° 08

Año	Chiclayo, 2016
Autores	Hilda Milagros Santa Cruz Quiroz
Título	Implementación de Gestión de Riesgos de TI para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque
Resumen	El proyecto de investigación expuesto por (Santa Cruz Quiroz 2016) dice que el entorno y dinámicas competitivas de la actualidad, contar con tecnología de información y comunicaciones no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede dar una ventaja o marcar factor diferencial para el éxito de éstas. De acuerdo a esto, apropiarse de un modelo de gobierno de TI, para esta gestión, es un elemento clave para el cumplimiento de los objetivos de la empresa. Los riesgos de las inversiones tecnológicas son hoy contingencias de nivel empresarial, y por lo tanto, no se puede hablar de riesgo de negocio sin haber contemplado antes estos mismos peligros para la Tecnologías de la Información.

Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar riesgos ante las amenazas a los activos de la organización. A diferencia de este trabajo, no se utilizará ISO 27001 como marco metodológico, pero por cultura ayudará a tener un conocimiento más concreto sobre la gestión de riesgos en base a este marco de referencia. MAGERIT se basa en esta ISO con relación a sus fases a implementar.

Tabla 9: Antecedente Local N° 09

Año	Chiclayo, 2015
Autores	Damaris Fernández
Título	Modelo de gestión de riesgos de ti de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, MAGERIT para la caja de ahorro y créditos SIPAN S.A:
Resumen	El proyecto de investigación expuesto por (Fernández Fernández 2015) menciona que la falta de acción con respecto a los riesgos se debe al temor de tomar decisiones negativas y señalen a un responsable ante la perdida por un derivado. Esta es una de las medidas más importantes que una empresa puede implementar para reducir de forma potencial los Riesgos de TI. Este proyecto se basa en la manera de cómo se puede mejorar la gestión de riesgos en base a los activos de TI con exigencias de la SBS (Superintendencia de Banca y Seguros) basadas en las ISO 27001 y 17799, además de la metodologías MAGERIT
Análisis de relación con la presente investigación	La relación que existe con el presente proyecto de investigación es que ambos buscan mejorar la gestión de riesgos IT, con el fin de minimizar riesgos ante las amenazas a los activos de la organización. A diferencia de este trabajo, no se utilizará ISO 27001 como marco metodológico, pero por cultura ayudará a tener un conocimiento más concreto sobre la gestión de riesgos en base a este marco de referencia. MAGERIT se basa en esta ISO con relación a sus fases a implementar.

2.2. BASES TEÓRICO CIENTÍFICAS

2.2.1. SEGURIDAD DE LA INFORMACIÓN.

La seguridad de los sistemas de información es un elemento central en todo desarrollo de la sociedad, pasando a ser una disciplina cada vez más crítica, necesaria y obligatoria y un componente clave en todo tipo de proyectos de sistemas de información. (Areitio, 2008: 2) siendo de vital importancia para la sobrevivencia de las organizaciones.

Así como lo mencionan Alegre y García, “por lo anterior se considera muy importante la seguridad informática, que se puede definir como un conjunto de procedimientos, dispositivos, herramientas encargadas de asegurar la

integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo"[1] Esta se clasifica según Alegre y García como:

- ✓ Activa: "Se entiende por seguridad activa todas aquellas medidas que se actualizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema".[2]

- ✓ Pasiva: "Comprende todo el conjunto de medidas utilizadas para que una vez que se produzca al ataque o el fallo en la seguridad de nuestro sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo".[3]

2.2.1.1. ELEMENTO DE SEGURIDAD DE LA INFORMACIÓN.

- **Riesgos:** "Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio".[4]

  Según Amutio y Candau "el riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización".[5]

- **Amenazas:** "Cualquier acción o evento que puede ocasionar consecuencias adversas"[6]

[1] Alegre y García. *Seguridad Informática*. (Madrid: Paraninfo, 2011).
[2] Véase la nota 4.
[3] Véase la nota 4.
[4] Ortiz y Villegas. *Seguridad de la Información*.(Guatemala: Universidad de San Carlos de Guatemala, 2014)101-117.
[5] Amutio y Candau. *MAGERIT - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I.* (Madrid: Ministerio de Haciendo y Administraciones Públicas, 2012).
[6] Véase la nota 8

Figura 1 Amenazas a los Sistemas de Información

Fuente: recuperado de (Candau y Amutio Gómez 2012)

- **Vulnerabilidad:** "Deficiencias que pueden ser explotadas por amenazas" [7]

- **Riesgo Residual:** "El riesgo que permanece después de que se han implementado contra medidas y controles." [8]

[7] Véase la nota 8
[8] Véase la nota 8

Figura 2: Relaciones entre los elementos de seguridad.

Fuente: Recuperado de (Frayssinet, 2011: 24)

2.2.2. NORMA ISO/IEC 27001

Según ADEA es la solución de mejora continua más adecuada para evaluar los riesgos físicos (Incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. [9]
Siendo ISO 27001 según Baldecchi es un SGSI10, la seguridad de la información queda definida por tres atributos (figura 8):[11]

- **Confidencialidad**: La información disponible exclusivamente a personas autorizadas. [12]
- **Integridad:** Es mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas.[13]
- **Disponibilidad**: Es el acceso y utilización de los servicios solo y en el momento de ser solicitado por una persona autorizada.[14]

La SI[15] según MAGERIT, es la protección de la información contra una amplia gama de amenazas respecto.[16]

---

[9] "ADEA: Ingeniería Documental", ADEA, acceso el 2 de enero de 2017, http://www.adea.es/seguridad.
[10] SGSI: Sistema de Gestión de la Seguridad de la Información
[11] Rodrigo Baldecchi. *Implementación efectiva de UN SGSI ISO 27001*. CiGRAS, acceso el 03 de enero de 2017. https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf. 3-30.
[12] Véase la nota 15
[13] Véase la nota 15
[14] Véase la nota 15
[15] SI: Seguridad De La Información
[16] MAGERIT. *Ministerio de Administración Públicas, Versión 2.* (Madrid: NIPO, 2006).

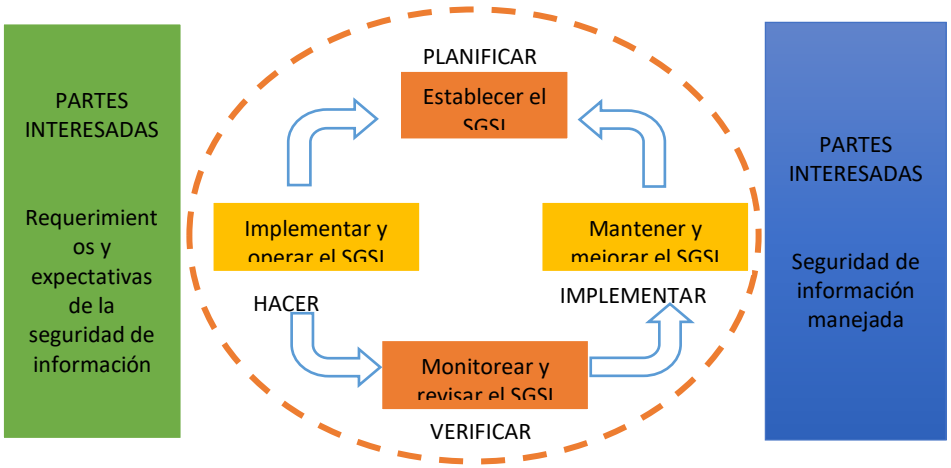
- Minimizar daños
- Oportunidades del negocio
- Retorno de la inversión
- Continuidad del negocio
- Cultura ética.

El SGSI según MAGERIT, garantiza la SI mediante una estructura de buenas prácticas, definidas por: [17]

- Gestión de riesgos
- Políticas
- Procesos
- Procedimientos
- Controles
- Revisiones
- Mejoras.

Esta Norma Internacional según Baldecchi menciona que para ISO (International Organization for Standardization) un sistema de gestión queda definido por un proceso de 4 etapas, creado por Walter Andrew Shewhart (1891 – 1967) y popularizado por William Edwards Deming (1900 – 1993). [18] Como se puede observar en la figura 10 y 11.

Figura 3: Modelos PDCA aplicado a procesos SGSI



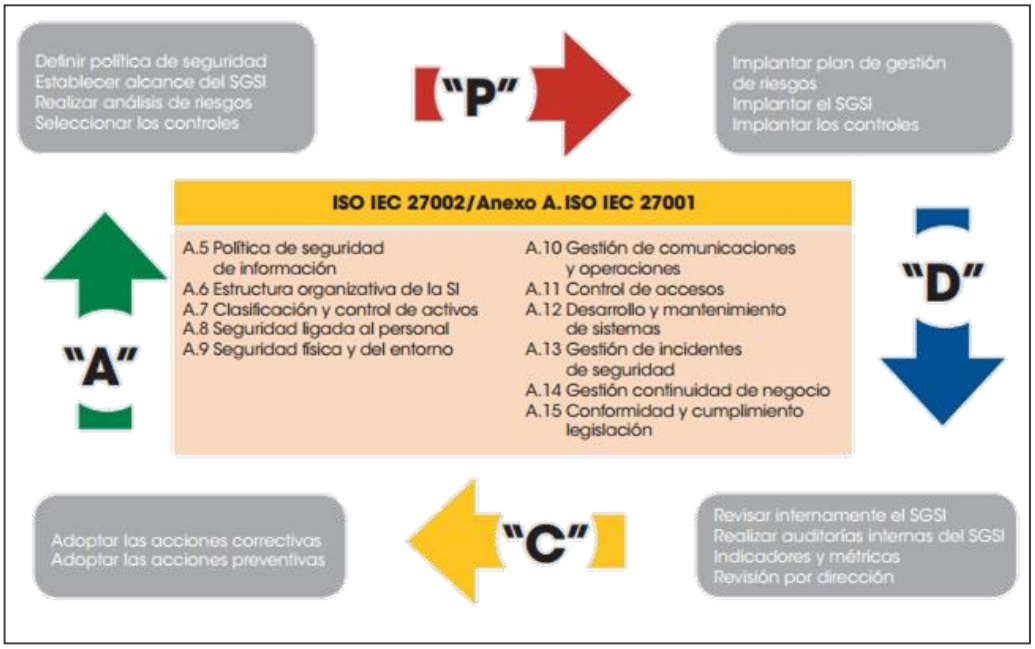
Fuente: (ISO/IEC 27001 2005)

Según AENOR el Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001:2007, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Panificar-Hacer-Verificar-Actuar, más conocido con

[17] Véase la nota 20
[18] Véase la nota 15

el acrónimo en inglés PDCA[19] (similar a la más extendida y reconocida norma ISO 9001). Asimismo, tiene también su fundamento en la norma UNE–ISO/IEC 27002:2009, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información. Como se muestra en la Figura 12. [20]

Figura 4: Sistema de Gestión de la Seguridad de la Información ISO 27001



Fuente: (AENOR 2012, 42)

2.2.2.1. BENEFICIOS DE ISO 27001

La información según ISO27000, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.[21] Como se puede observar figura 13.

[19] PDCA: Plan-DO-Check-Act)

[20] AENOR. *La norma ISO 27001 del Sistema de Gestión de la Seguridad de Información*. (2012). 40 - 44

[21] ISO27000. *Sistema de Gestión de la Seguridad de la Información.* Acceso el 02 de Septiembre de 2016 http://www.iso27000.es/download/doc_sgsi_all.pdf.

Figura 5: Beneficios de ISO 27001

Fuente: Recuperado de (ISO27000 2012, 4)

2.2.2.2. ¿QUÉ INCLUYE UN SGSI?

Según ISO27000 en el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles.[22] Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, de la siguiente forma:

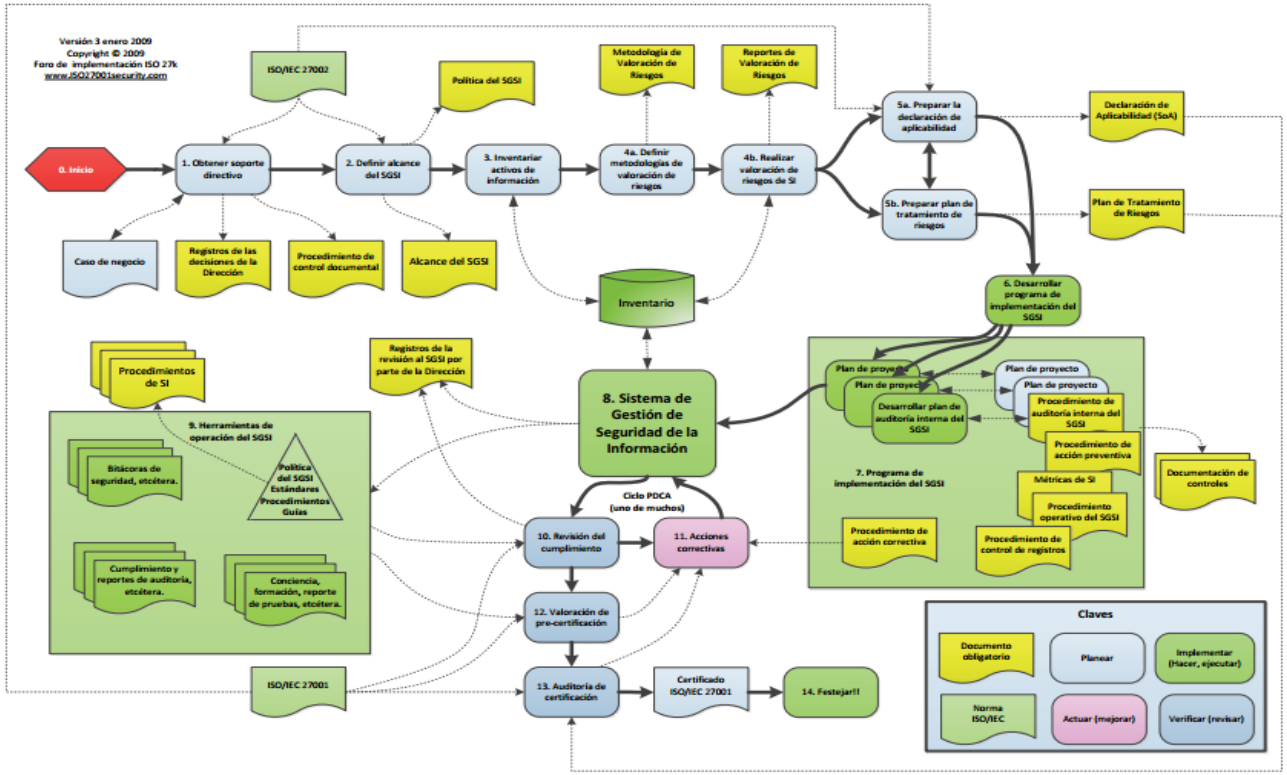
Figura 6: Modelo SGSI (Sistema De Gestión de la Seguridad.

Fuente: Recuperado de (ISO27000 2012, 4)

[22] Véase la nota 25

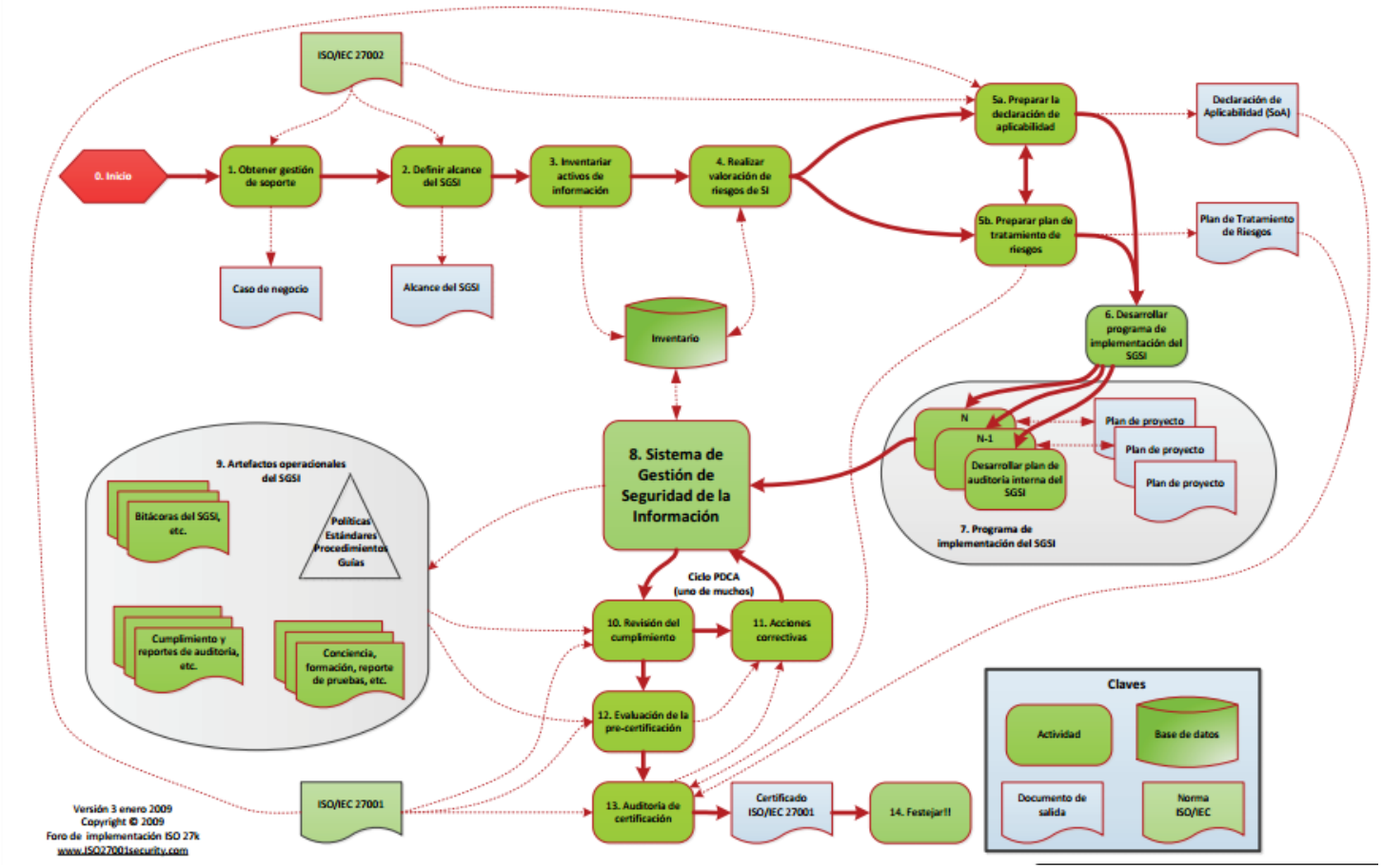
2.2.2.3. IMPLEMENTACIÓN ISO 27001

Figura 7: Implementación ISO 27001



Fuente: Recuperado de (ISO27001security 2009)

Figura 8: Implementación ISO 27001



Fuente: (ISO27001security 2009)

2.2.3. METODOLOGÍAS PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS.

Tabla 10 Metodologías para el análisis y gestión de riesgos

COMPARATIVA DE METODOLOGÍAS			
	MAGERIT	***OCTAVE***	***CRAMM***
NOMBRE DE LA METODOLOGÍA	*"Metodología de análisis y gestión de riesgos de los sistemas de información*	*"Operationally Critical Threat, Asset and Vulnerability Evaluation"*	*"CCTA Risk Assessment and Management Methodology"*
PAÍS DE PROCEDENCIA	*España*	*Estados Unidos*	*Reino Unido*
RESPONSABLE DEL PRODUCTO	*Ministerio de Hacienda y Administraciones Públicas*	*ERG*	*Centro de informática y la Agencia Nacional de Telecomunicaciones (CCTA)*
APLICACIÓN	*Gobierno, Organismos, Compañías grandes, PYMES, compañías comerciales y no comerciales*	*PYMES*	*Empresas comerciales, agencias del gobierno, organizaciones sin ánimo de lucro*
FASES	*- Análisis de riesgos* *- Caracterización de los activos* *- Caracterización de las amenazas* *- Caracterización de las salvaguardas* *- Estimación del estado del riesgo* *- Gestionar los riesgos*	*- Visión de organización* *- Visión tecnológica* *- Planificación de las medidas y reducción de riesgos*	*-Establecimiento del alcance (a través de la identificación y valoración de los activos)* *- Valoración de las amenazas y vulnerabilidades* *- Selección y recomendación de contramedidas (CRAMM contiene una gran librería de más de 3500 contramedidas organizadas en 70 grupos)*

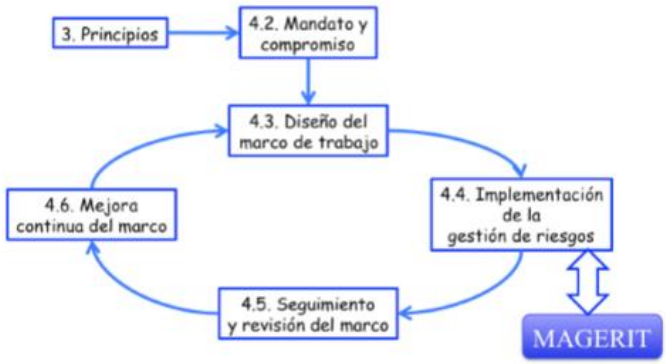
PRINCIPALES CARACTERÍSTICAS	*- Esta metodología fue creada por el Consejo Superior de Administración Electrónica de España.* *- Está orientada a los sistemas de información* *- Ofrece una método dinámico para analizar los riesgos.* *- A nivel internacional no es muy conocida, aunque su utilización puede ser interesante en cualquier tipo de empresa* *- Prepara a la organización para procesos de evaluación, auditoría, certificación o acreditación.* *- Consta de 03 libros: "Método", "Catálogo de elementos", "Guía de técnicas"* *- Es de acceso público* *- Posee un extenso archivo de inventarios en los referente a recursos de información, amenazas y tipo de activos.* *- Permite un análisis completo cualitativo y cuantitativo* *- Se le considera con un alcance completo, tanto en el análisis como en la gestión de riesgos*	*- Está dirigido a grupos pequeños de trabajo (personal de la organización y el área de TI) para que puedan dar ideas en conjunto sobre las necesidades de seguridad de la información.* *- Permite la comprensión del manejos de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización.* *- OCTAVE divide los activos en dos tipos:* *Sistemas: (hardware, software y datos)* *Personas* *- Existen tres métodos OCTAVE: Método OCTAVE, OCTAVE-S y OCTAVE ALLEGRO* *- Tiene un buen reconocimiento internacional, buena aceptación a nivel mundial, aunque las fases que la componen son diferentes de las metodologías habituales, lo cual suele implicar mayor dificultad en su utilización.*	*- Aplica los conceptos de una manera formal y estructurada.* *- Orientada a proteger las dimensiones: confidencialidad, integridad y disponibilidad de un sistema y de sus activos* *- Sirve para la evaluación del impacto empresarial* *- Evaluar los niveles de riesgo* *- Asimismo, CRAMM calcula los riesgos para cada grupo de activos contra las amenazas a las que es vulnerable en un escala de 1 a 7, utilizando una matriz de riesgo con valores predefinidos comparando los valores de activos a las amenazas y niveles de vulnerabilidad. En esta escala, "1" indica una línea de base de bajo nivel de exigencia de seguridad y el "7 " indica un requisito de seguridad muy alto.* *- Tiene reconocimiento a nivel internacional y su desarrollo es de lo más simple, identificación y valoración de activos, valoración de amenazas, vulnerabilidades y selección de contramedidas.*

COSTO	*No tiene costo, para el sector educativo.* *EAR/PILAR menciona lo siguiente:* *- La aplicación puede descargarse libremente* *- El uso libre para consultar análisis de riesgos realizados en soporte fichero (.mgr)(modo "read only")* *- Para generar nuevos análisis de riesgos se requiere un licencia comercial* *- Para utilizar PILAR sobre base de datos se requiere una licencia comercial extendida.* *Los costos van desde los 250 a 3,000 Euros.*	*Uso Interno: Gratuito* *Uso Externo: Se debe compra una a SEI si se quiere implementar una metodología a un tercero*	*Para una compañía comercial:* *2,800 euros + 850 euros al año de mantenimiento.* *Para agencias y departamentos del estado británico:* *1,600 euros + 850 euros al año de mantenimiento*
HERRAMIENTAS	*EAR/PILAR, SECITOR, R-BOX*	*No especifica un producto en concreto para el análisis*	*CRAMM tool, CRAMM express*
IDIOMA	*Español*	*Inglés*	*Inglés*

2.2.4. MAGERIT

"El CSAE[23] ha elaborado y promueve MAGERIT[24], y desde la publicación de la primera versión en 1997 hasta la fecha".[25]
Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina *Proceso de Gestión de Riesgos*, SECCIÓN 4.4 (Implementación de la gestión de riesgos) dentro del "Marco de Gestión de Riesgos".
En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de información." [26]

Figura 9: Relaciones entre los elementos de seguridad



Fuente: Recuperado de (Frayssinet, 2011: 24)

2.2.4.1. OBJETIVOS DE MAGERIT

MAGERIT persigue según Amutio y Candau los siguientes objetivos:[27]

Directos:

a) Se debe concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo
b) Se debe ofrecer un método sistemático para analizar tales riesgos
c) Se debe ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control
d) Se debe preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos según Amutio y Candau: [28]

[23] CSAE: Consejo Superior de Administración Pública
[24] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
[25] Véase la nota 20
[26] Véase la nota 20
[27] Véase la nota 8
[28] Véase la nota 8

- **Modelo de Valor:** Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.
- **Mapa de Riesgos:** Relación de las amenazas a que están expuestos los activos.
- **Evaluación de Salvaguardas:** Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- **Estado de Riesgo:** Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- **Informe de Insuficiencias:** Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.
- **Plan de Seguridad:** Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

2.2.4.2.CATÁLOGOS DE ELEMENTOS

2.2.4.2.1. ACTIVOS

"Es un elemento o una parte de un sistema global al que la organización asigna un valor y, por lo tanto, requiere protección. Posibles activos a identificar son: Activos de TIC, personal, entorno, actividades, información, datos y software." [29]

Los activan se clasifican en los siguientes tipos:

- **Datos:** "Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos." [30]
- **Software:** "Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios". [31]

- **Hardware:** "Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos." [32]

[29] Javier Areitio, *Seguridad de la información. Redes, informática y sistemas de información*. (Madrid: Paraninfo, 2008) 1-11.
[30] Véase la nota 8
[31] Véase la nota 8
[32] Véase la nota 8

- **Redes:** "Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro". [33]
- **Soportes:** "Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo". [34]
- **Instalaciones:** "Son lugares donde se hospedan los sistemas de información y comunicaciones". [35]
- **Personal:** "Aparecen las personas relacionadas con los sistemas de información". [36]
- **Servicios:** "Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema". [37]

2.2.4.2.1.1.DIMENSIONES DE VALORACIÓN.

"Son las características o atributos que hacen valioso un activo. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión". [38]

a) **Disponibilidad:** "La disponibilidad es una característica que afecta a todo tipo de activos. A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación". [39]
   egún lo expuesto por Segunda Cohorte del Doctorado en Seguridad Estratégica, "garantizar la disponibilidad implica también la prevención de ataque de denegación del servicio. [40]

   Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y

[33] Véase la nota 8
[34] Véase la nota 8
[35] Véase la nota 8
[36] Véase la nota 8
[37] Véase la nota 8
[38] Véase la nota 8
[39] Véase la nota 8
[40] Segunda Cohorte del Doctorado en Seguridad Estratégica. *Seguridad de la Información: Revista de la segunda Cohorte en Seguridad Estratégica.* (Guatemala: Universidad de San Carlos de Guatemala, 2014).

minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio".

b) **Integridad**: "Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados". [41]

c) **Confidencialidad de datos y de la información del sistema**: "Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados".[42] Según lo expuesto por Areitio, "es el requisito que protege la información privada o secreta, para que no se revele a individuos no autorizados, esta se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito. Para muchas de las organizaciones, la confidencialidad se encuentra, frecuentemente, detrás de la disponibilidad y de la integridad, en términos de importancia". [43]

d) **Autenticidad: "**Es la propiedad que permite identificar el generador de la información. Esta propiedad se puede considerar como un aspecto de la integridad (si está firmado por alguien), está realmente enviado por él mismo". [44]

e) **Trazabilidad:** Según lo expuesto por González, es el "perjuicio de no conocer a quien se le presta el activo, lo que se hace con él, cómo y cuándo. Así como desconocer quienes acceden a determinados archivos y para qué son utilizados". [45]

2.2.4.2.1.2.CRITERIOS DE VALORIZACIÓN

"Para valorar los activos vale, teóricamente, cualquier escala de valores. Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos". [46]

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor irrelevante para la organización, como se indica a continuación:

[41] Véase la nota 44
[42] Véase la nota 44
[43] Véase la nota 33
[44] Véase la nota 44
[45] Juan González. *Elaboración de un Plan de implementación de la norma ISO/IEC 27001:2013*. Tesis. (Barcelona: Universitat Oberta de Catalunya, 2015).
[46] Véase la nota 8

Tabla 11: Criterios de Valorización

VALOR	CRITERIO
10	Daño muy grave a la organización
7 – 9	Daño grave a la organización
4 – 6	Daño importante a la organización
1 – 3	Daño menor a la organización
0	Irrelevante para la organización

Fuente (Amutio y Candau 2012)

2.2.4.2.2. AMENAZAS

"Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño." [47]

2.2.4.2.2.1.VALORACIÓN DE LAS AMENAZAS

"Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: degradación: cuán perjudicado resultaría el [valor del] activo probabilidad: cuán probable o improbable es que se materialice la amenaza". [48]

Figura 10: Probabilidad de Ocurrencia

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 1. Degradación del valor

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia[15] como medida de la probabilidad de que algo ocurra. Son valores típicos:

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2. Probabilidad de ocurrencia

Fuente: recuperado de (Candau y Amutio Gómez 2012)

[47] Véase la nota 8
[48] Véase la nota 8

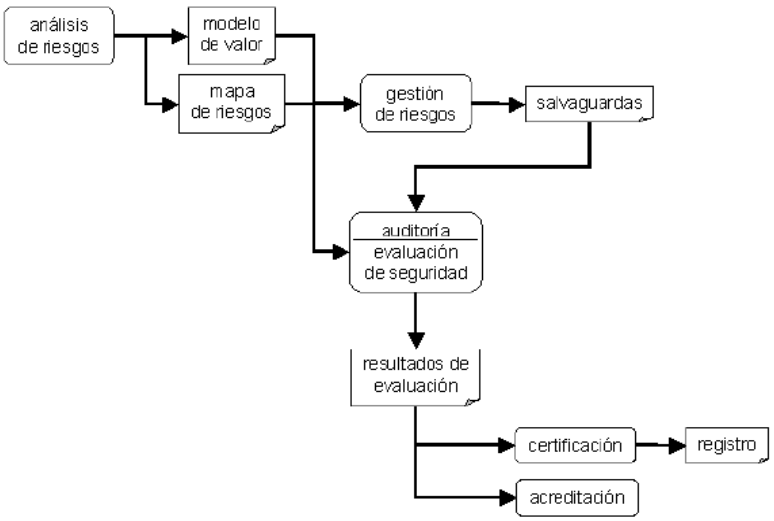
2.2.4.2.3. SALVAGUARDAS

"Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal". [49]

2.2.4.2.3.1.EVALUACIÓN, CERTIFICACIÓN, AUDITORÍA Y ACREDITACIÓN

Según Amutio y Candau "el análisis de riesgos es una piedra angular que formaliza la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporcionan una visión singular de cómo es cada sistema, que valor posee, a que amenazas está expuesto y de que salvaguardas se ha dotado". [50]
Es pues el análisis de riesgos pasó obligado para poder llevar acabo todas las tareas mencionadas, que se relacionan según el siguiente esquema (figura 7):

Figura 11: Evaluación, certificación, auditoría y acreditación



Fuente: Recuperado de (Amutio y Candau, 2012: 15)

a) **Evaluación: "**Es cada vez más frecuente la evaluación de la seguridad de los sistemas de información, tanto internamente como parte de los procesos de gestión, como por medio de evaluadores independientes externos. Las evaluaciones

[49] Véase la nota 8
[50] Véase la nota 8

permiten medir el grado de confianza que merece o inspira un sistema de información". [51]

b) Certificación: "Certificar es asegurar responsablemente y por escrito un comportamiento. Lo que se certifica, producto o sistema, se somete a una serie de evaluaciones orientadas por un objetivo ¿para qué lo quiere?, Un certificado dice que un sistema es capaz de proteger unos datos de unas amenazas con una cierta calidad (capacidad de protección). Y lo dice en base a que ha observado la existencia y el funcionamiento de una serie de salvaguardas. Es decir que detrás de un certificado no hay sino los conceptos de un análisis de riesgos". [52]

c) Acreditación: "Algunas certificaciones tienen como objetivo la acreditación del producto o sistema. La acreditación es un proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios. Se puede ver como una certificación para un propósito específico". [53]

d) Auditorías: Una auditoría puede servirse de un análisis de riesgos que le permita según Amutio y Candau en:[54]

a. Saber qué hay en juego
b. Saber a qué está expuesto el sistema
c. Valorar la eficacia y eficiencia de las salvaguardas.

"Frecuentemente, los auditores parten de un análisis de riesgos, implícito o explícito, que, o bien realizan ellos mismos, o bien lo auditan. Siempre en la primera fase de la auditoría, pues es difícil opinar de lo que no se conoce. A partir del análisis de riesgos se puede analizar el sistema e informar a la gerencia de si el sistema está bajo control; es decir, si las medidas de seguridad adoptadas están justificadas, implantadas y monitorizadas, de forma que se puede confiar en el sistema de indicadores de que dispone la gerencia para gestionar la seguridad de los sistemas".[55]

[51] Véase la nota 8
[52] Véase la nota 8
[53] Véase la nota 8
[54] Véase la nota 8
[55] Véase la nota 8

2.2.4.3.PROYECTO DE ANÁLISIS DE RIESGOS:

2.2.4.3.1. PROCESO P1: ACTIVIDADES PRELIMINARES:

Según MAGERIT "El objetivo principal de este proceso es establecer el marco general de referencia para todo el proyecto".[56]
Este proceso se desarrolla por medio de las siguientes actividades y tareas:

2.2.4.3.1.1. ACTIVIDAD A1.1: ESTUDIO DE OPORTUNIDAD

Se fundamenta la oportunidad de la realización, ahora, del proyecto AGR, enmarcándolo en el desarrollo de las demás actividades de la Organización. El resultado de esta actividad es el informe denominado "preliminar". (Amutio y Candau, 2012: 64)

- Tarea T1.1.1: Determinar la oportunidad

2.2.4.3.1.2.ACTIVIDAD A1.2: DETERMINACIÓN DEL ALCANCE DEL PROYECTO

"Se definen los objetivos finales del proyecto, su dominio y sus límites. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. Y por último se estima el coste que va a suponer. El resultado de esta actividad es un perfil de proyecto AGR". [57]

- Tarea T1.2.1: Objetivos y restricciones generales
- Tarea T1.2.2: Determinación del dominio y límites
- Tarea T1.2.3: Identificación del entorno
- Tarea T1.2.4: Estimación de dimensiones y coste

2.2.4.3.1.3.Actividad A1.3: Planificación del proyecto

Se determinan las cargas de trabajo que supone la realización del proyecto. Se planifican las entrevistas que se van a realizar para la recogida de información: quiénes van a ser entrevistados. [58]

Se elabora el plan de trabajo para la realización del proyecto. En esta actividad se determinan los participantes y se estructuran los diferentes grupos y comités para llevar a cabo el proyecto.

El resultado de esta actividad está constituido por:

- Un plan de trabajo para el proyecto AGR59
- Procedimientos de gestión de la información generada

- Tarea T1.3.1: Evaluar cargas y planificar entrevistas
- Tarea T1.3.2: Organizar a los participantes

[56] Véase la nota 28
[57] Véase la nota 28
[58] Véase la nota 28
[59] AGR: Análisis de Gestión de Riesgos)

- Tarea T1.3.3: Planificar el trabajo

2.2.4.3.1.4.Actividad A1.4: Lanzamiento del proyecto

Según MAGERIT, se adaptan los cuestionarios para la recogida de información adaptándolos al proyecto presente. Se eligen las técnicas principales de evaluación de riesgo a utilizar y se asignan los recursos necesarios para el comienzo del proyecto. El resultado de esta actividad está constituido por:[60]

- Los cuestionarios para las entrevistas
- El plan de entrevistas
- El catálogo de tipos de activos
- La relación de dimensiones de seguridad y
- Los criterios de valoración

- Tarea T1.4.1: Adaptar los cuestionarios
- Tarea T1.4.2: Criterios de evaluación
- Tarea T1.4.3: Recursos necesarios
- Tarea T1.4.4: Sensibilización

2.2.4.3.2. PROCESO P2: ANÁLISIS DE RIESGOS

Según lo expone el MAGERIT, "este proceso es el núcleo central de MAGERIT y su correcta aplicación condiciona la validez y utilidad de todo el proyecto. La identificación y estimación de los activos y de las posibles amenazas que les acechan representa una tarea compleja". Este proceso tiene los siguientes objetivos:[61]

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto).
- Mostrar al comité director las áreas del sistema con mayor impacto y/o riesgo.

El punto de partida según MAGERIT de este proceso es la documentación del anterior referente a los objetivos del proyecto, los

[60] Véase la nota 28
[61] Véase la nota 28

planes de entrevistas, la evaluación de cargas, la composición y reglas de actuación del equipo de participantes, el plan de trabajo y el informe de presentación del proyecto. Este proceso se desarrolla por medio de las siguientes actividades y tareas.[62]

2.2.4.3.2.1.Actividad A2.1: Caracterización de los activos

Según MAGERIT, "Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia". El resultado de esta actividad es el informe denominado "modelo de valor".[63]

- Tarea T2.1.1: Identificación de los activos
- Tarea T2.1.2: Dependencias entre activos
- Tarea T2.1.3: Valoración de los activos

2.2.4.3.2.2.Actividad A2.2: Caracterización de las amenazas

Según MAGERIT, "Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por la frecuencia estimada de ocurrencia y la estimación de daño (degradación) que causarían sobre los activos". El resultado de esta actividad es el informe denominado "mapa de riesgos".[64]

- Tarea T2.2.1: Identificación de las amenazas
- Tarea T2.2.2: Valoración de las amenazas

2.2.4.3.2.3.Actividad A2.3: Caracterización de las salvaguardas

Según MAGERIT, "Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar". El resultado de esta actividad es el informe denominado "evaluación de salvaguardas".[65]

- Tarea T2.3.1: Identificación de las salvaguardas existentes
- Tarea T2.3.2: Valoración de las salvaguardas existentes

[62] Véase la nota 28
[63] Véase la nota 28
[64] Véase la nota 28
[65] Véase la nota 28

2.2.4.3.2.4.ACTIVIDAD A2.4: ESTIMACIÓN DEL ESTADO DE RIESGO

Según MAGERIT, "Esta actividad procesa todos los datos recopilados en las actividades anteriores para:[66]

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo
- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

- Tarea T2.4.1: Estimación del impacto
- Tarea T2.4.2: Estimación del riesgo
- Tarea T2.4.3: Interpretación de los resultados

2.2.4.3.3. PROCESO P3: GESTIÓN DE RIESGOS

Según MAGERIT, "Se procesan los impactos y riesgos identificados en el proceso anterior, bien asumiéndolos, bien afrontándolos. Para afrontar los riesgos que se consideren inaceptables se llevará a cabo un plan de seguridad que corrija la situación actual. Un plan de seguridad se materializa en una colección de programas de seguridad. Algunos programas serán sencillos, mientras que otros alcanzarán suficiente nivel de Complejidad y coste como para que su ejecución se convierta en un proyecto propiamente dicho. La serie de programas (y, en su caso, proyectos) se planifica en el tiempo promedio del denominado Plan de Seguridad que ordena y organiza las actuaciones encaminadas a llevar el estado de riesgo a un punto aceptable y aceptado por la Dirección". Este proceso se desarrolla por medio de las siguientes actividades y tareas:[67]

2.2.4.3.3.1.ACTIVIDAD A3.1: TOMA DE DECISIONES

En esta actividad se traducen las conclusiones técnicas del proceso P2 en decisiones de actuación.[68]

- Tarea T3.1.1: Calificación de los riesgos

2.2.4.3.3.2.ACTIVIDAD A3.2: PLAN DE SEGURIDAD

En esta actividad se traducen las decisiones de actuación en acciones concretas: proyectos de mejora de la seguridad planificados en el tiempo. [69]

- Tarea T3.2.1: Programas de seguridad
- Tarea T3.2.2: Plan de ejecución

[66] Véase la nota 28
[67] Véase la nota 28
[68] Véase la nota 28
[69] Véase la nota 28

2.2.4.3.3.3.ACTIVIDAD A3.3: EJECUCIÓN DEL PLAN

Esta actividad recoge la serie de proyectos que materializan el plan de seguridad y que se van realizando según dicho plan.[70]

- Tarea T3.3.: Ejecución de cada programa de seguridad

[70] Véase la nota 28

III. MATERIALES Y MÉTODOS

3.1. DISEÑO DE INVESTIGACIÓN

3.1.1. TIPO DE INVESTIGACIÓN

Esta tesis se basa en la Investigación Cualitativa, que según (LeCompte 1996, 11) busca extraer descripciones a partir de observaciones que adoptan la forma de entrevistas, narraciones, notas de campo, grabaciones, transcripciones de audio y vídeo.

Esta investigación es de TIPO: Descriptiva – Proyectiva

- **Descriptiva:** Mide o evalúa diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Desde el punto de vista científico, describir es medir. (Hernández, Fernández y Bautista 2003, 117)
- **Proyectiva:** Este tipo de investigación propone soluciones a una situación determinada a partir de un proceso de indagación. Implica explorar, describir, explicar y proponer alternativas de cambio, mas no necesariamente ejecutar la propuesta. Se trabajan relaciones de causa efecto, pues para diseñar una propuesta que permita modificar la situación es necesario primero explicar por qué y cómo ocurre tal situación; de otra manera la propuesta no resultaría efectiva.

Esta investigación tiene un DISEÑO: Experimental:

- **Experimental:** Predice lo que ocurrirá si se produce alguna modificación en la condición actual de un hecho, para lograr esto se aplica el razonamiento hipotético-deductivo y la metodología suele ser cuantitativa. Los experimentos pueden realizarse en el laboratorio o pueden ser de campo.

En Conclusión, se utilizará la INVESTIGACION (Cualitativa) TIPO (Descriptiva - Explicativo) y DISEÑO (Experimental)

3.1.2. HIPÓTESIS

Si se implementa un plan de seguridad acorde con MAGERIT la cual se basa en la ISO 31000 y 27001 que elevará los niveles de seguridad entonces se posibilitará la identificación, evaluación de riesgos y posibles vulnerabilidades de los activos de la información de la Unidad de Producción Hidráulica.

3.1.3. DISEÑO DE CONTRASTACIÓN DE HIPÓTESIS

El diseño de contrastación que se utilizó fue la siguiente:

Tabla 12. Diseño de contrastación de hipótesis

Variable independiente	Aplicación	Variable dependiente
O1: Plan de Seguridad	**X:** • Identificar y evaluar los activos de la organización además de sus amenazas que repercuten. • Establecer los mecanismos de protección apropiados para minimizar los riesgos críticos de la organización en estudio. • Proponer proyectos adecuados para tratar y minimizar los riesgos críticos encontrados.	**O2:** Identificación de los riesgos **O2:** Análisis y evaluación de los riesgos **O3:** Tratamiento de los riesgos de TI

3.1.4. VARIABLES

3.1.4.1. VARIABLE INDEPENDIENTE

- Plan de Seguridad

3.1.4.2. VARIABLE DEPENDIENTE

- Identificación de los riesgos
- Análisis y evaluación de los riesgos
- Tratamiento de los riesgos de TI

3.1.5. INDICADORES

Tabla 13: Indicadores

OBJETIVO ESPECIFICO	INDICADOR(ES)	DEFINICIÓN CONCEPTUAL	UNIDAD DE MEDIDA	INSTRUMENTO	DEFINICIÓN OPERACIONAL
Identificar y evaluar los activos de la organización además de sus amenazas que repercuten.	Número de Activos críticos Número de Amenazas	Identificación y evaluación de los activos y amenazas	Cuantitativo	Informe Modelo de Valor Informe de Amenazas	$\sum$ (Activos críticos encontrados) $\sum$ (Amenazas encontradas)
Establecer los mecanismos de protección apropiados para minimizar los riesgos críticos de la organización en estudio.	Número de salvaguardas	Identificación y evaluación de salvaguardas	Cuantitativo	Informe Evaluación de salvaguardas	$\sum$ (Salvaguardas propuestas)
Proponer proyectos adecuados para tratar y minimizar los riesgos críticos encontrados.	Número de proyectos propuestos	Identificar el tratamiento de los riesgos para poder proteger la información de la organización	Cuantitativo	Cartera de Proyectos	$\sum$ (Proyectos propuestos)

3.1.6. POBLACIÓN Y MUESTRA

3.1.6.1. POBLACIÓN

La población está dada por los 40 usuarios que pertenecen a la Central Hidroeléctrica, considerando que ellos son los principales afectados, debido a que están expuestos a riesgos y posibles vulnerabilidades en el acceso de información entre las áreas de la organización

3.1.6.2. MUESTRA

El tamaño de la muestra se obtiene aplicando la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

Donde:

- N= Universo
- e = 0.05 (Máximo de error permisible)
- Z = 1.96 (Valor tabla) (95%)
- P = 0.5 (Proporción de la población)
- Q = 0.5 (1-P)

Para el presente estudio se tiene:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

$$n = \frac{1.96^2 * 0.5 * 0.5 * 40}{(40-1) * 0.05^2 + (1.96^2 * 0.5 * 0.5)}$$

$$n = \frac{3.8416 * 0.5 * 0.5 * 40}{39 * 0.0025 + (3.84.16 * 0.5 * 0.5)}$$

$$n = \frac{38.416}{0.0975 + 0.9604}$$

$$n = \frac{38.416}{1.0579}$$

$$n = 36.31$$

La muestra a considerar para el estudio es: **36 usuarios**.

3.1.6.3. MUESTREO

Para el muestreo se toman los usuarios que forman parte de la muestra y que pertenezcan a las áreas donde se presente mayor problemática en la seguridad de acceso a la información.

3.1.7. MÉTODOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS

Tabla 14. Métodos y técnicas de recolección de datos.

MÉTODO	TÉCNICAS E INSTRUMENTOS	ELEMENTOS DE LA POBLACIÓN
Científico	**Observación**	Lista de Cotejos Fichas de Observación
	Documental	Libros, artículos, informes, tesis, sitios web, revistas, normativas.
	De campo	Entrevistas, encuestas y visitas a la institución

3.1.8. TÉCNICAS DE PROCESAMIENTO DE DATOS.

Entre las técnicas de procesamiento de datos se utilizará el Software: SPSS 19 y Microsoft Excel 2016.

3.2. METODOLOGÍA

Para el desarrollo de la investigación, se utilizará MAGERIT el cual propone e implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo (ISO 31000 y 27005) para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de información." (Ministerio de Hacienda y Administraciones Públicas, 2012:7). Asimismo, Se utilizará la herramienta EAR-PILAR, la cual ayuda a desarrollar esta metodología de manera más dinámica y flexible.

Esta metodología tiene como objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para manetener los riesgos bajo control.
- De manera indirecta, prepara a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Para esta metodología, hay dos grandes tareas a realizar.

- Análisis de Riesgos: Permite determinar que tiene la organización y estimar lo que podría pasar.

- Tratamiento de los Riesgos: Permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

Tabla 15: MAR - Método de Análisis de Riesgos

MAR – Método de Análisis de Riesgos
MAR. 1 – Caracterizaciónde los activos
MAR. 11 – Identificación de los activos
MAR. 12 – Dependencias entre activos
MAR. 13 – Valoración de los activos
MAR. 2 – Caracterización de las amenazas
MAR. 21 – Identificación de las amenazas
MAR. 22 – Valoración de las amenazas
MAR. 3 – Caracterización de las salvaguardas
MAR. 31 – Identificación de las salvaguardas pertinentes
MAR. 32 – Valoración de las salvaguardas
MAR. 4 – Estimación del estado de riesgo
MAR. 41 – Estimación del Impacto
MAR. 42 – Estimación del riesgo

- ***MAR.1: Caracterización de los activos***
  Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, de-terminando en qué dimensiones de seguridad son importantes y valorando esta importancia.
  El resultado de esta actividad es el informe denominado "modelo de valor".
  Sub-tareas:
    - **Tarea MAR.11:** Identificación de los activos
    - **Tarea MAR.12:** Dependencias entre activos
    - **Tarea MAR.13:** Valoración de los activos

- ***MAR.2: Caracterización de las amenazas***
  Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).
  El resultado de esta actividad es el informe denominado "mapa de riesgos". Subtareas:
    - **Tarea MAR.21:** Identificación de las amenazas
    - **Tarea MAR.22:** Valoración de las amenazas

- ***MAR.3: Caracterización de las salvaguardas***
  Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.
  El resultado de esta actividad se concreta en varios informes:
    - Declaración de aplicabilidad
    - Evaluación de salvaguardas
    - Insuficiencias (o vulnerabilidades del sistema de protección)

- ***MAR.4: Estimación del estado de riesgo***
  Esta actividad procesa todos los datos recopilados en las actividades anteriores para:
  - Realizar un informe del estado de riesgo: estimación de impacto y riesgo
  - Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

  Sub-tareas:
    - **Tarea MAR.41:** Estimación del impacto
    - **Tarea MAR.42:** Estimación del riesgo

  Es frecuente que las tareas relacionadas con los activos (MAR.1) se realicen concurrentemente con las tareas relacionadas con las amenazas sobre dichos activos (MAR.2) e identificación de las salvaguardas actuales (MAR.3), simplemente porque suelen coincidir las personas y es difícil que el interlocutor no tienda de forma natural a tratar cada activo "verticalmente", viendo todo lo que le afecta antes de pasar al siguiente.
  El tratamiento de riesgos se lleva a cabo por medio de las siguientes tareas:

Tabla 16: PAR - Proyecto de Análisis de Riesgos

PAR – Proyecto de Análisis de Riesgos
PAR. 1 – Actividades preliminares
PAR. 11 – Estudio de Oportunidad
PAR. 12 – Determinación del alcance del proyecto
PAR. 13 – Planificación del proyecto
PAR. 14 – Lanzamiento del proyecto
PAR. 2 – Elaboración del análisis de riesgos
PAR. 3 – Comunicación de resultados

- ***PAR.1: Actividades preliminares***
  Aquí se realizan las siguientes tareas que se deben de considerar antes de hacer un análisis de riesgos
    - **PAR. 11 –** Estudio de Oportunidad:
      Esta actividad se realiza para saber la factibilidad del proyecto dentro de la organización.
    - **PAR. 12 –** Determinación del alcance del proyecto
      Se plantean los objetivos finales del proyecto, su dominio y sus límites. El resultado de esta actividad, es mostrar el perfil del proyecto del análisis de riesgo y gestión de riesgos.
    - **PAR. 13 –** Planificación del proyecto
      En esta actividad se da por hecho que el proyecto de análisis de riesgos se va a ejecutar. Por tal motivo se debe recolectar la información por medio de entrevistas con las personas o grupos de personas que interactúan con los sistemas de información
    - **PAR. 14 –** Lanzamiento del proyecto
      En esta fase del proyecto se elaboran las preguntas para la obtención de información.
      El resultado de esta actividad está constituido por:
        - Los cuestionarios para las entrevistas
        - El catálogo de tipos de activos
        - La relación de dimensiones de seguridad

- Los criterios de valoración

- ***PAR.2: Elaboración del análisis de riesgo***

  La mayor parte de las tareas requerirán dos o tres entrevistas con los interlocutores apropiados:
  - Una primera entrevista para exponer las necesidades y recabar los datos
  - Una segunda entrevista para validar que los datos son completos y se han entendido correctamente
  - Según las circunstancias puede ser necesaria alguna entrevista adicional si la validación levanta muchas inexactitudes o dudas

  En Toda esta tarea debe procurarse manejar documentación escrita sometida a un proceso formal de gestión; es decir, aprobada y con unos procedimientos de revisión continua. La información de carácter verbal o informal debe limitarse a facilitar la comprensión, no a transmitir elementos sustanciales que no están documentados en parte alguna

- ***PAR.3: Comunicación de resultados***

  La salida de la fase de análisis es la entrada de la fase de tratamiento.
  Para tomar decisiones de tratamiento es necesario conocer tanto los indicadores residuales como los indicadores potenciales de impacto y riesgo. Y para cada escenario de riesgo es necesario disponer de información suficiente para poder entender en qué consiste el riesgo, así como su dinámica y los razonamientos o la base de las estimaciones empleadas para derivar resultados.

Tabla 17: PS - Plan de Seguridad

PS – Plan de Seguridad
PS. 1 – Identificación de proyectos de seguridad
PS. 2 – Plan de Ejecución
PS. 3 – Ejecución

- ***PS. 1: Identificación de proyectos de seguridad***

  Elaborar un conjunto armónico de programas de seguridad. En última instancia, se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales determinados por la dirección. En este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo

- ***PS. 2: Identificación de proyectos de seguridad***

  Ordenar temporalmente los programas de seguridad. Hay que ordenar en el tiempo los proyectos de seguridad teniendo en cuenta los siguientes factores:
  - La criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que se afronten situaciones críticas-
  - El coste del programa
  - La disponibilidad del personal propio para responsabilizarse de la dirección de las tareas programadas.
  - Otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, etc.

- ***PS. 3: Ejecución***

  Alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado

IV. RESULTADOS

IMPLEMENTACIÓN METODOLOGÍA MAGERIT

Los resultados que se muestran a continuación corresponden a la metodología MAGERIT V2, descrita en el marco teórico.

PROCESO P1: PLANIFICACIÓN

El primer paso de la presente metodología se debe definir lo que se debe cumplir:

1.1. ESTUDIO DE LA OPORTUNIDAD

1.1.1. DETERMINAR LA OPORTUNIDAD

Tabla 18: Estudio de la Oportunidad

P1: Planificación	
A1.1.: Estudio de Oportunidad	
Objetivos	Motivar, concienciar e involucrar a la Gerencia sobre seguridad de la información dentro de la Unidad de Producción Hidráulica.
Productos de salida	• Informe de Preliminar recomendando la elaboración del proyecto • Creación de comité de seguimiento.
Técnicas, prácticas y pautas	Entrevistas Encuestas (Anexos 1 y 2) Observación
Participantes	El promotor

Fuente: Modelo Estudio de la Oportunidad (Ministerio de Administración Públicas 2006)

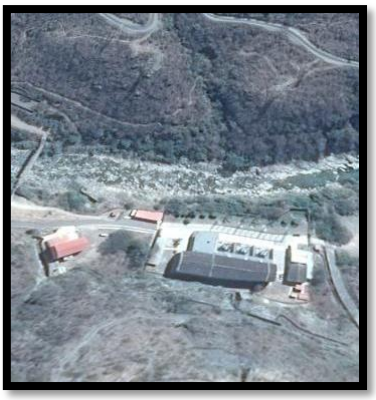
Productos de salida*: Creación de Comité de Seguimiento*

Está constituido por los responsables de las áreas afectadas por el proyecto; así como por los responsables de Informática de la Unidad de Producción Hidráulica, el cual lo conforma las siguientes personas:

- Jinko Chinen– Jefatura de Infraestructura y Operaciones TI
- Paul Salinas– Administrador de Servidores
- Enrique Barboza – Administrador de Base de Datos
- Carlos Saavedra – Administrador de Telecomunicaciones
- Leonardo Celis – Analista de Servicios y Soluciones de Negocio

Productos de salida: *Informe de Preliminar recomendando la elaboración del proyecto*

Tabla 19 Informe Preliminar del proyecto

Argumentos Básicos	La UNIDAD DE PRODUCCIÓN HIDRÁULICA, ubicada en la sierra norte del país, en el distrito de Llama, provincia de Chota, Departamento de Cajamarca, a 377 metros sobre el nivel del mar. *Figura 12: Vista aérea de la Unidad de Producción Hidráulica*  ***Fuente: Recuperado de* (Google 2015)** Es una empresa del tipo minería energética, el cual su producto es la generación de energía utilizando el agua del río Chancay como materia prima. Donde la principal problemática de la empresa son los intrusos que pretenden penetrar los niveles de seguridad de la red, creando el llamado "hueco de seguridad" que contribuye al desvío del flujo de información de un punto de transmisión a su debido destino, lo que genera la falta de seguridad y la poca previsión respecto a los riesgos que cuentan sus activos de información, que podrían llevarla a pérdidas económicas. Otra de las dificultades de la empresa son las insuficientes medidas y procedimientos recogidos en los planes de seguridad informática; que se rigen por los estándares internacionales que norman los sistemas de gestión de seguridad informática tanto en la prevención como recuperación ante desastres o ataques. El encargado del área de Tecnologías de Información menciona los siguientes problemas detallándose a continuación: • La ubicación de los servidores dentro de la organización no es la adecuada ya que se encuentran en una oficina que no corresponde al área de Tecnologías de la Información y está a la vista de todas las personas que puedan acceder a esta área, no tiene la temperatura adecuada (27º C) que por lo recomendable según juicios de expertos (Especialistas en el área de Telecomunicaciones de diferentes empresas debe estar en 19º C; el lugar no es cerrado, por lo que puede fallar cualquiera de los equipos del área según recomendación por la ISO/IEC 17999 el lugar del cuarto de servidores deberá de estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división en la unidad de informática, recubierta de material aislante o protegido contra el fuego. • Realizando una encuesta dirigida a los trabajadores que conforman la Unidad de Producción Hidráulica, el 40,63% de los usuarios dejan sus computadoras sin bloquearlas cuando van a trabajar al campo (Anexo 2 – Figura 65). Y el 56.25% de los trabajadores han brindado su contraseña a un compañero como se puede

<table>
<tr><td></td><td>observar (Aun sabiendo sobre temas de seguridad 46,88% y no teniendo algún conocimiento 9, 38% han brindado su contraseña aun compañero (Anexo 2 – Figura 70)). Esto potencia el riesgo como lo manifiesta (Universidad Miutar Nueva Granada 2013) de que se utilice los sistemas de la empresa sin privilegios otorgados y se haga uso inadecuado de la información y que terceros puedan utilizarla en contra de la empresa y del mismo trabajador. Esto traería como consecuencia suplantación de identidad, degradación, corrupción y divulgación de información, Acceso no autorizado, ingreso de falsa información y robo.

• Existen colaboradores que se conectan a la red corporativa por medio de cable Ethernet lo cual se encuentra prohibido por ética laboral, ya que el acceso a internet y a redes públicas exponen a los sistemas de la Unidad de Producción Hidráulica a estar propensos a software con código malicioso los cuales pueden comprometer a la red, ya que solo 53.13% de los usuarios utilizan a veces antivirus y 6. 25% nunca lo utilizan (Anexo 2 – Figura 66).</td></tr>
<tr><td>Finalidad</td><td>Mediante la implementación de una metodología de análisis y gestión de riesgos (MAGERIT) y ISO; concienciar a los trabajadores sobre la importancia de saber a qué riesgos están expuestos los sistemas de información de la empresa y como ayudarían ellos a gestionarlos, dando un tratamiento oportuno para mantenerlos bajo control. Ayudando a la reducción de costos operativos y financieros, y estableciendo una cultura de seguridad.</td></tr>
<tr><td>Principales Actividades</td><td>Figura 13: Procesos, Actividades y Tareas – MAGERIT
<table><tr><th>Procesos, actividades y tareas</th></tr><tr><td>Proceso P1: Planificación
Actividad A1.1: Estudio de oportunidad
Tarea T1.1.1: Determinar la oportunidad
Actividad A1.2: Determinación del alcance del proyecto
Tarea T1.2.1: Objetivos y restricciones generales
Tarea T1.2.2: Determinación del dominio y límites
Tarea T1.2.3: Identificación del entorno
Tarea T1.2.4: Estimación de dimensiones y coste
Actividad A1.3: Planificación del proyecto
Tarea T1.3.1: Evaluar cargas y planificar entrevistas
Tarea T1.3.2: Organizar a los participantes
Tarea T1.3.3: Planificar el trabajo
Actividad A1.4: Lanzamiento del proyecto
Tarea T1.4.1: Adaptar los cuestionarios
Tarea T1.4.2: Criterios de evaluación
Tarea T1.4.3: Recursos necesarios
Tarea T1.4.4: Sensibilización</td></tr><tr><td>Proceso P2: Análisis de riesgos
Actividad A2.1: Caracterización de los activos
Tarea T2.1.1: Identificación de los activos
Tarea T2.1.2: Dependencias entre activos
Tarea T2.1.3: Valoración de los activos
Actividad A2.2: Caracterización de las amenazas
Tarea T2.2.1: Identificación de las amenazas
Tarea T2.2.2: Valoración de las amenazas
Actividad A2.3: Caracterización de las salvaguardas
Tarea T2.3.1: Identificación de las salvaguardas existentes
Tarea T2.3.2: Valoración de las salvaguardas existentes
Actividad A2.4: Estimación del estado de riesgo
Tarea T2.4.1: Estimación del impacto
Tarea T2.4.2: Estimación del riesgo
Tarea T2.4.3: Interpretación de los resultados</td></tr></table>Fuente: (Ministerio de Administración Públicas 2006)</td></tr>
<tr><td>Duración</td><td>6 meses</td></tr>
</table>

1.2. DETERMINACIÓN DEL ALCANCE DE PROYECTO

1.2.1. OBJETIVOS Y RESTRICCIONES GENERALES

Tabla 20: Alcance de Proyecto – Objetivos y Restricciones Generales

P1: Planificación	
A1.2.: Determinar el Alcance del Proyecto	
A 1.2.1: Objetivos y Restricciones Generales	
Objetivos	Definir los objetivos y restricciones abarcar del proyecto.
Productos de Entrada	Compendio de documentación de la Unidad de producción hidráulica
Productos de salida	• Objetivos específicos del proyecto • Restricciones Generales del proyecto
Técnicas, prácticas y pautas	Entrevistas Encuestas (Anexos 1 y 2) Observación
Participantes	Comité de Seguimiento

Fuente: Modelo alcance de proyecto (Ministerio de Administración Públicas 2006)

Productos de salida*: Objetivos Específicos*

- Mejorar el nivel de conocimiento del personal sobre seguridad de la información
- Mejorar el nivel de criterio de evaluación para la implementación de controles para salvaguardar los riesgos de seguridad en la Entidad
- Incrementar el nivel de seguridad en los Activos de información de la empresa Unidad de Producción Hidráulica.

Productos de salida*: Restricciones Generales*

- Respetar restricciones de acuerdos de confidencialidad.

1.2.2. DETERMINACIÓN DEL DOMINIO Y LÍMITES

Tabla 21: Alcance de Proyecto - Determinación del dominio y límites

P1: Planificación	
A1.2.: Determinar el Alcance del Proyecto	
A 1.2.2: Determinación del dominio y límites	
Objetivos	Determinar el dominio y límites del Proyecto
Productos de Entrada	Compendio de documentación de la Unidad de Producción Hidráulica.
Productos de salida	• Descripción de la organización • Designación de Director de Proyecto • Lista de Responsabilidades de los miembros del comité de Seguimiento. • Relación de Áreas que se verán afectadas con la implementación del proyecto.
Técnicas, prácticas y pautas	Entrevistas Encuestas (Anexos 1 y 2) y Observación

Participantes	Comité de Seguimiento

Fuente: Modelo alcance de proyecto (Ministerio de Administración Públicas 2006)

Productos de salida*: Descripción de la Organización.*

Tabla 22: Descripción de la Unidad de Producción Hidráulica

Orazul ENERGY 	***CH. CARHUAQUERO***

- Ubicada en el distrito de Llama, provincia de Chota, en Cajamarca.
- Aprovecha las aguas del río Chancay- Lambayeque y suministra energía al SEIN.
- Inició operaciones en 1991 con 75 MW de capacidad; en 1998 amplía su capacidad a 95 MW y entre el 2007 y 2008, se unen Carhuaquero IV y Carhuaquero V proyectos certificados como proyectos MDL.
- Actualmente la C.H. Carhuaquero tiene 111 MW de capacidad con una producción de 620 GWh-año.

Fuente: (Duke Energy 2014)

Productos de salida*: Designación de Director de Proyecto*

El proyecto AGR[71] de los SI de la Unidad de Producción Hidráulica está constituido por los siguientes colaboradores:

- Equipo de estudio:
  - Director de Proyecto: Jinko Chinen
  - Promotor: Leonardo Celis

- Grupo de Usuarios:
  - Está formado por los utilizadores, actuales, del Sistema de Información (Colaboradores de la Central Hidroeléctrica)

Productos de salida*: Lista de Responsabilidades del comité de seguimiento*

[71] AGR: Análisis de Gestión de Riesgos

Tabla 23: Lista de Responsabilidades del Comité de seguimiento.

NOMBRE	ÀREA	RESPONSABILIDAD
Jinko Chinen	Infraestructura y Operaciones TI	Supervisar el área de tecnologías de Información
Paul Salinas	Administrador de Servidores	Se encarga de la gestión y administración de todos los servidores que se encuentran en cada una de las sedes que conforma la empresa
Enrique Barboza	Administrador de Base de Datos	Especialista en Base de Datos. Tiene la responsabilidad de mantener y administrar las bases de datos de cada uno de los ERP[72] de la empresa
Carlos Saavedra	Administrador de Telecomunicaciones	Se encarga de mantener y administrar la comunicación en cada una de las sedes que conforman la empresa
Leonardo Celis	Analista de Servicios y Soluciones de Negocio	Soporte a la Operación en Sede

Fuente: (Duke Energy 2014)

Productos de salida*: Relación de Áreas que se verían afectadas con la implementación del Proyecto.*

1.2.3. IDENTIFICACIÓN DEL ENTORNO

Tabla 24: Alcance de Proyecto - Identificación del Entorno

P1: Planificación	
A1.2.: Determinar el Alcance del Proyecto	
A 1.23: Identificación del Entorno	
Objetivos	Definir el entorno del dominio.
Productos de Entrada	Compendio de documentación de la Organización
Productos de salida	Lista de Responsabilidades de los miembros del comité de apoyo.
Técnicas, prácticas y pautas	Entrevistas, Encuestas (Anexos 1 y 2) y Observación
Participantes	Comité de Seguimiento

Fuente: Modelo alcance de proyecto (Ministerio de Administración Públicas 2006)

1.2.4. ESTIMACIÓN DE DIMENSIONES Y COSTE

Tabla 25: Alcance de Proyecto - Estimación de dimensiones y Coste

P1: Planificación	
A1.2.: Determinar el Alcance del Proyecto	
A 1.23: Identificación del Entorno	
Objetivos	Determinar las dimensiones y coste del proyecto.
Productos de Entrada	Resultados de Tabla 4 (Objetivos), Tabla 5 (Dominio y Limites) y Tabla 8 (Entorno)
Productos de salida	• Tamaño, complejidad y zonas del Incertidumbre. • Costes y beneficios del proyecto
Técnicas, prácticas y pautas	Entrevistas Encuestas (Anexos 1 y 2) Observación
Participantes	Comité de Seguimiento

Fuente: Modelo alcance de proyecto (Ministerio de Administración Públicas 2006)

[72] ERP: Enterprise Resource Planning: Sistemas de Planificación de recursos empresariales.

1.3. PLANIFICACIÓN DEL PROYECTO

1.3.1. EVALUAR CARGAS Y PLANIFICAR ENTREVISTAS.

En la Unidad de Producción Hidráulica, para la realización de las encuestas (revisar ANEXOS) se solicitarán una cita a cada entrevistado en un plazo no mayor 5 días laborales. Estas encuestas nos ayudarán a detener por ámbito a los usuarios afectados y a planificar la intervención de ellos en el proyecto.

1.3.2. ORGANIZAR A LOS PARTICIPANTES.

El proyecto AGR[73] de los SI de la Unidad de Producción Hidráulica está constituido por los siguientes colaboradores:

- Equipo de estudio:
  - Director de Proyecto: Jinko Chinen
  - Promotor: Leonardo Celis

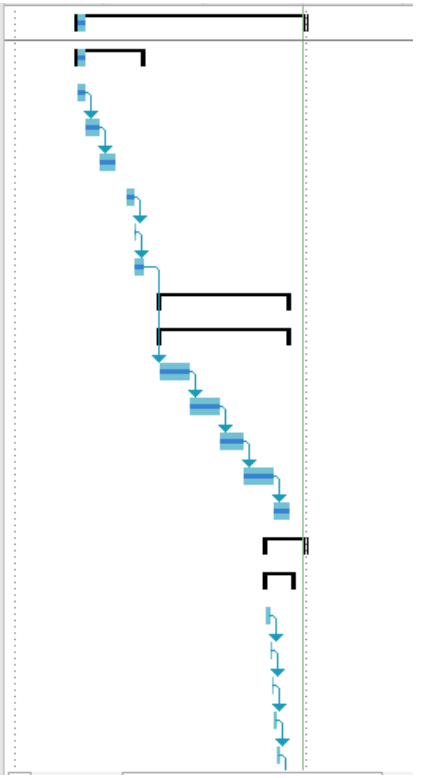
- Grupo de Usuarios:
  - Está formado por los utilizadores, actuales, del Sistema de Información (Colaboradores de la Central Hidroeléctrica)

[73] AGR: Análisis de Gestión de Riesgos

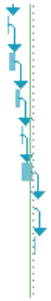
1.3.3. PLANIFICAR EL TRABAJO

Figura 14: Cronograma de Actividades

	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO	**301 días**	**mar 11/10/16**	**mar 5/12/17**
	PLAN DEL PROYECTO	**88 días**	**mar 11/10/16**	**jue 9/02/17**
	Selección y Delimitación del Tema	11 días	mar 11/10/16	mar 25/10/16
	Estudio de Oportunidad	20 días	mié 26/10/16	mar 22/11/16
	Determinar el alcance del proyecto	20 días	mié 23/11/16	mar 20/12/16
	Planificación del proyecto	10 días	mié 11/01/17	mar 24/01/17
	Adaptar los cuestionarios y entrevistas	2 días	mié 25/01/17	jue 26/01/17
	Lanzamiento del Proyecto	12 días	mié 25/01/17	jue 9/02/17
	DESARROLLO DEL PROYECTO	**170 días**	**lun 13/03/17**	**vie 3/11/17**
	Fases de la metodología a implementar	**170 días**	**lun 13/03/17**	**vie 3/11/17**
	Fase 01: Caracterización de los Activos	40 días	lun 13/03/17	vie 5/05/17
	Fase 02: Caracterización de las amenazas	40 días	sáb 6/05/17	vie 30/06/17
	Fase 03: Caracterización de las salvaguardas	30 días	sáb 1/07/17	vie 11/08/17
	Fase 04: Estimación del estado del riesgo	40 días	sáb 12/08/17	vie 6/10/17
	Fase 05: Gestión de Riesgos	20 días	sáb 7/10/17	vie 3/11/17
	REDACCIÓN DEL INFORME DEL PROYECTO	**54 días**	**jue 21/09/17**	**mar 5/12/17**
	Redacción del Informe	**38 días**	**jue 21/09/17**	**lun 13/11/17**
	Parte 01: Definir Materiales y Métodos	6 días	jue 21/09/17	jue 28/09/17
	Parte 02: Análisis e Interpretación de los Resultados (En base a la metodología propuesta)	3 días	vie 29/09/17	mar 3/10/17
	Exposición al 20% del Informe	1 día	mié 4/10/17	mié 4/10/17
	Parte 03: Definir Discusiones y Conclusiones	6 días	jue 5/10/17	jue 12/10/17
	Parte 04: Recomendaciones y Referencias Bibliográficas	4 días	vie 13/10/17	mié 18/10/17



	Exposición al 50% del Informe	1 día	jue 19/10/17	jue 19/10/17
	Parte 05: Anexos	8 días	vie 20/10/17	mar 31/10/17
	Parte 06: Introducción, Resume & Abstract	8 días	mié 1/11/17	vie 10/11/17
	Exposición al 80% del Informe	1 día	lun 13/11/17	lun 13/11/17
	Revisión del Informe	14 días	mar 14/11/17	vie 1/12/17
	Presentación del Informe	1 día	lun 4/12/17	lun 4/12/17
	Sustentación Final	1 día	mar 5/12/17	mar 5/12/17



1.4. LANZAMIENTO DEL PROYECTO

1.4.1. ADAPTAR LOS CUESTIONARIOS.

Las técnicas a emplear son las que se especifican y recomienda MAGERIT. La información relevante acerca del caso de estudio, se puede saber de las entrevistas y encuestas realizadas hacía la jefatura y usuarios colaboradores de la Central Hidroeléctrica.

1.4.2. CRITERIOS DE EVALUACIÓN.

Esta información fue estructurada por Leonardo Celis, autor de este proyecto y revisada por Jinko Chinen, Director del Proyecto.

Esta técnica mencionada y utilizada para la recojo de información se adaptan con el objeto de identificar correctamente los elementos de trabajo:

- Activos
- Amenazas
- Vulnerabilidades
- Impactos
- Salvaguardas Existentes
- Restricciones Generales

1.4.3. RECURSOS NECESARIOS

La Unidad de Producción Hidráulica dispone los recursos necesarios para el desarrollo del proyecto:

- ✓ Equipos
- ✓ Personal de TI (Tecnología de Información)
- ✓ Medios Económicos
- ✓ Manuales de Seguridad

1.4.4. SENSIBILIZACIÓN.

Se ha realizado la comunicación sobre el lanzamiento del proyecto al Jefe de Unidad de la Sede Carhuaquero Sr. Juan Ñeco, quien no supo informar su agrado y apoyo para la realización de este proyecto en mención. Se explicó los objetivos y la metodología a realizar.

2. PROCESO P2: ANÁLISIS DE RIESGOS

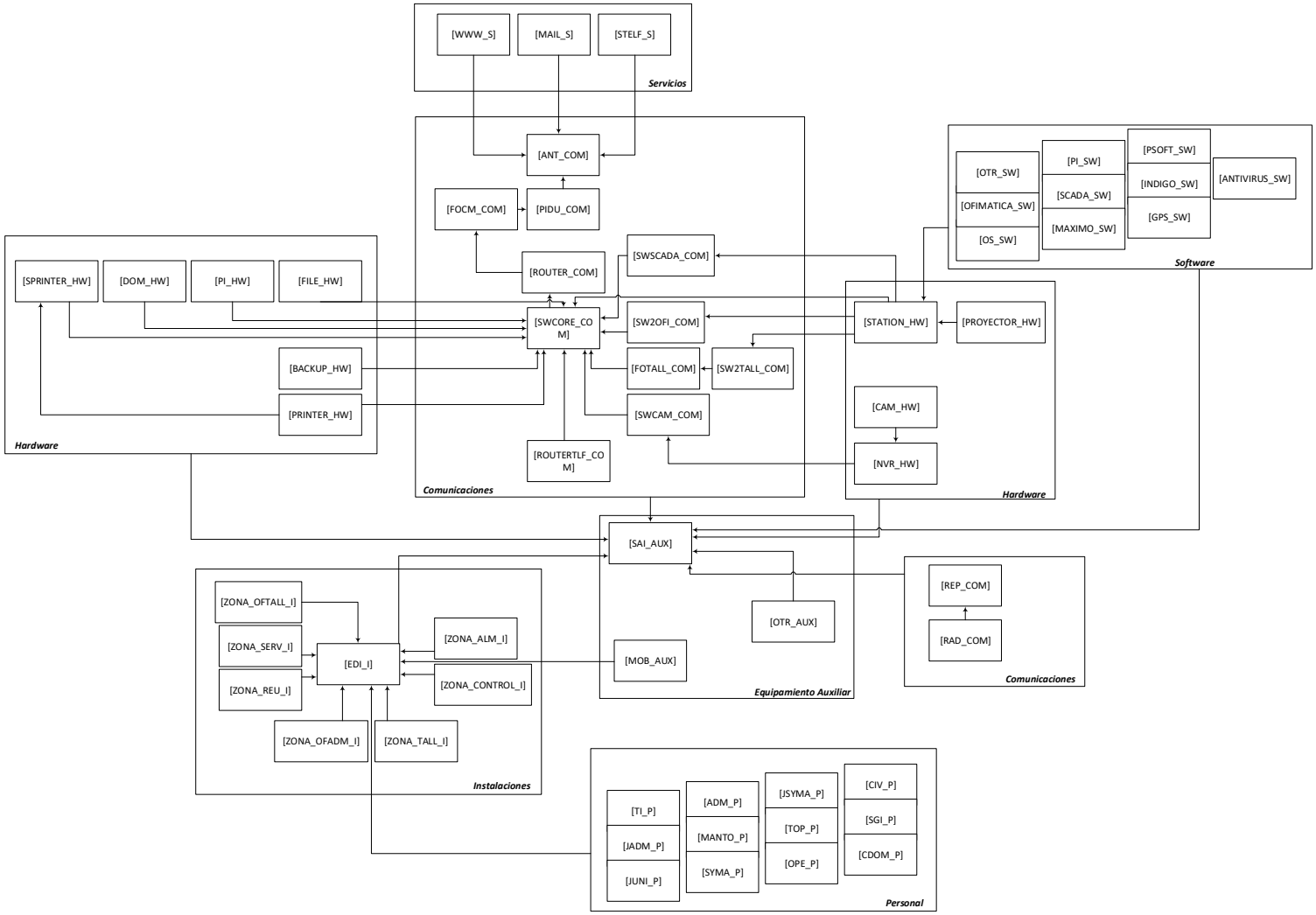
2.1. CARACTERIZACIÓN DE LOS ACTIVOS

2.1.1. IDENTIFICACIÓN DE ACTIVOS

Es importante ya que permite materializar con precisión el alcance del proyecto, permite valorar los activos con exactitud e identificando y valorando las amenazas a las que están expuestos dichos activos. (Lucero y Valverde 2012).
Para realizar este ítem en mención, se utilizó la herramienta EAR-PILAR (ANEXO N°4)

2.1.2. DEPENDENCIAS ENTRE ACTIVOS.

Figura 15: Dependencia de Activos



Leyenda:

1. Software:

[OS_SW] Sistema Operativo
[OFIMATICA_SW] Ofimática
[OTR_SW] Otros Software
[PI_SW] PI Process Book
[SCADA_SW] Sistema Tiempo Real
[MAXIMO_SW] Maximo
[PSOFT_SW] PeopleSoft
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras
[GPS_SW] Sistema de Frecuencia
[ANTIVIRUS_SW] Antivirus

2. Comunicaciones:

[ANT_COM] Antena (Enlace Microondas)
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso
[SWSCADA_COM] Switch SCADA
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso
[SWCAM_COM] Switch Cámaras de Video vigilancia
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa
[FOTALL_COM] Media Converter - Fibra óptica talleres
[PKSHA_COM] Packet Shaper 2500
[ROUTER_COM] Router Cisco
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)
[REP_COM] Repetidoras
[RAD_COM] Radios

3. Hardware:

[DOM_HW] Controlador de Dominio Windows 2012 Server
[FILE_HW] Servidor de Archivos
[PI_HW] Servidor PI
[BACKUP_HW] Servidor Copias de Seguridad
[SPRINTER_HW] Servidor de Impresión
[NVR_HW] Servidor de Grabación CCTV-NVR
[STATION_HW] Estaciones de Trabajo
[PRINTER_HW] Equipos de Impresión
[PROYECTOR_HW] Proyectores Salas de Reuniones
[CAM_HW] Cámaras de Video Vigilancia

4. Servicios:

[WWW_S] Internet
[MAIL_S] Correo Electrónico
[STELF_S] Telefonía IP (Servicio)

5. Equipamiento Auxiliar:

[MOB_AUX] Mobiliario
[SAI_AUX] Sistema de Alimentación Ininterrumpida
[OTR_AUX] Otros Equipos Auxiliares

6. Instalaciones:

[EDI_I] Edificio
[ZONA_SERV_I] Sala de Servidores
[ZONA_REU_I] Sala de Reuniones
[ZONA_ALM_I] Almacén
[ZONA_OFADM_I] Oficinas Casa de Máquinas
[ZONA_OFTALL_I] Oficinas Talleres
[ZONA_CONTROL_I] Sala Control
[ZONA_TALL_I] Talleres

7. Personal:

[TI_P] Coordinador TI
[ADM_P] Personal de administración y logístico
[JADM_P] Jefatura de administración
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico
[JUNI_P] Jefe de Unidad
[SYMA_P] Personal SyMA
[JSYMA_P] Jefatura SyMA
[TOP_P] Tópico
[OPE_P] Personal Operaciones
[JOPE_P] Jefatura de Operaciones
[CIV_P] Personal Ing. Civil
[SGI_P] Personal SGI
[CDOM_P] Coordinaciones O&M

2.1.3. VALORIZACIÓN DE LOS ACTIVOS

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el Informe de Identificación y evaluación de Activos (ANEXO N°4) en donde se explicará el desarrollo de esta fase

2.2. CARACTERIZACIÓN DE LAS AMENAZAS

2.2.1. IDENTIFICACIÓN DE AMENAZAS

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el Informe de Identificación y evaluación de amenazas (ANEXO N°5) en donde se explicará el desarrollo de esta fase

2.2.2. VALORIZACIÓN DE AMENAZAS

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el informe de Identificación y evaluación de amenazas (ANEXO N°5) en donde se explicará el desarrollo de esta fase

2.3. CARACTERIZACIÓN DE LAS SALVAGUARDAS

2.3.1. IDENTIFICACIÓN DE LAS SALVAGUARDAS

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el informe de identificación y evaluación de las salvaguardas (ANEXO N°6) en donde se explicará el desarrollo de esta fase

2.3.2. VALORIZACIÓN DE LAS SALVAGUARDAS

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el informe de identificación y evaluación de las salvaguardas (ANEXO N°6) en donde se explicará el desarrollo de esta fase

2.4. ESTIMACIÓN DEL ESTADO DE RIESGO

2.4.1. ESTIMACIÓN DEL IMPACTO

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el informe de Impacto acumulado (ANEXO N°8) en donde se explicará el desarrollo de esta fase

Impacto Potencial:

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema. Para poder ver estos resultados, pueden revisar el informe de Impacto Repercutido (Anexo N° 07) y el informe de Impacto Acumulado (Anexo N° 08) en donde se explicará el desarrollo de esta fase

Impacto residual acumulado:

El impacto acumulado se calcula con los datos de impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas sobre dicho activo. Para poder ver estos resultados, pueden revisar el informe de Impacto Repercutido (Anexo N° 07) y el informe de Impacto Acumulado (Anexo N° 08)

2.4.2. ESTIMACIÓN DEL RIESGO

A continuación, se mostrará la resolución del ítem en mención. Para esto se utilizó la herramienta EAR-PILAR y pueden revisar el informe Riesgo acumulado (ANEXO N°9), en donde se explicará el desarrollo de esta fase
Sus objetivos son:

RIESGO POTENCIAL

Se dice que riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. Para poder ver estos resultados, pueden revisar el informe Riesgo Acumulado (Anexo N°09) y el informe Riesgo Repercutido (Anexo N°10).
El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

RIESGO RESIDUAL

La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo. Para poder ver estos resultados, pueden revisar el informe Riesgo Acumulado (Anexo N°09) y el informe Riesgo Repercutido (Anexo N°10).

3. PROCESO P3: GESTIÓN DE RIESGOS

Después de haber realizado el proceso del análisis de riesgos, se puede visualizar los riesgos y el impacto que tienen en la organización.
Para esto se tomará la mejor decisión. En el caso que sea crítico (atención de prioridad), grave (requiere atención) o apreciable (objeto de estudio)

3.1.TOMA DE DECISIONES:

3.1.1. IDENTIFICACIÓN DE LOS RIESGOS CRÍTICOS:

En base al análisis realizado y conocido el riesgo a los que está expuesta la organización, se han seleccionado los activos que poseen un nivel de riesgo que necesitan una atención prioritaria y que requieren de atención.

Donde:

DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

PROBABILIDAD

- [MR] muy rara
- [PP] poco probable
- [P] posible
- [MA] muy alto
- [CS] casi seguro

Tabla 26: Riesgos críticos

Amenaza	***dimensión***	***impacto***	***probabilidad***	***riesgo***
[I.*] Desastres industriales	D	[10]	P	{6,8}
[A.15] Modificación de la información	I	[8]	MA	{6,6}
[A.11] Acceso no autorizado	I	[8]	MA	{6,6}

Fuente: EAR-PILAR

Tabla 27: Riesgos Críticos

Activo	***Amenaza***	***dimensión***	***impacto***	***probabilidad***	***riesgo***
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.STATION_HW] Estaciones de Trabajo	[A.6] Abuso de privilegios de acceso	D	[8]	MA	{6,5}
[HW.STATION_HW] Estaciones de Trabajo	[A.11] Acceso no autorizado	D	[8]	MA	{6,5}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[9]	P	{6,5}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[10]	P	{6,4}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.6] Corte del suministro eléctrico	D	[9]	P	{6,3}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.5] Avería de origen físico o lógico	D	[9]	P	{6,3}

Fuente: EAR-PILAR

Tabla 28: Riesgo Potencial

Activo	***Amenaza***	***dimensión***	***impacto***	***probabilidad***	***riesgo***
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	PP	{3,9}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[7]	PP	{3,8}
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[7]	PP	{3,8}
[COM.PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[I.8] Fallo de servicios de comunicaciones	D	[6]	PP	{3,8}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.2] Errores del administrador del sistema / de la seguridad	D	[6]	PP	{3,7}
[COM.ANT_COM] Antena (Enlace Microondas)	[I.8] Fallo de servicios de comunicaciones	D	[6]	PP	{3,7}
[COM.PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	PP	{3,7}

A continuación, se mostrará otra tabla con la recomendación que nos da PILAR aplicando más salvaguardas según su consideración. En donde el nivel de riesgo baja a un más, asimismo el nivel de impacto disminuye.

Tabla 29: Riesgo Residual

Activo	***Amenaza***	***dimensión***	***impacto***	***probabilidad***	***riesgo***
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[6]	MR	{2,9}
[HW.STATION_HW] Estaciones de Trabajo	[A.6] Abuso de privilegios de acceso	D	[4]	P	{2,9}
[HW.FILE_HW] Servidor de Archivos	[I.1] Fuego	D	[5]	PP	{2,8}
[HW.FILE_HW] Servidor de Archivos	[I.2] Daños por agua	D	[5]	PP	{2,8}
[HW.FILE_HW] Servidor de Archivos	[I.6] Corte del suministro eléctrico	D	[5]	PP	{2,8}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.5] Avería de origen físico o lógico	D	[5]	PP	{2,7}

Tanto en las dos tablas, el nivel de impacto y riesgo se convierten en residuales.

3.1.2. CALIFICACIÓN DEL RIESGO:

A continuación, se gestionan los activos con riesgos críticos.

Tabla 30: Tratamiento de riesgo

ACTIVOS:	**[HW. FILE_HW] Servidor de Archivos** **[HW. PI_HW] Servidor PI** **[HW. BACKUP_HW] Servidor Copias de Seguridad** **[HW.NVR_HW] Servidor de Grabación CCTV-NVR**
DESCRIPCIÓN:	Este activo pertenece a la capa de Equipamiento -> subcapa Hardware, una vez realizado el estudio de amenazas y haber escogido el control o salvaguarda adecuada se obtiene lo siguiente: La amenaza de mayor relevancia es el Fuego que puede afectar la disponibilidad (6,8). En el caso que llegue a materializarse esta amenaza, podrías tener pérdidas grandes en temas de equipos y más aún en la información que se encuentra alojada.

ACCIONES A TOMAR:	• Reforzar las charlas de seguridad de 5 minutos, cambiar las fechas de realización (de todos los lunes a lunes a viernes) • Cada proceso de trabajo conlleva a riesgos de Incendio o explosiones perfectamente identificados, por ello es necesario conocerlo y protegerlo, por ello la presencia de la brigada, la cual debe tener amplios conocimientos de la planta nos ayudarán a la prevención. • Concientizar a los empleados las medidas de prevención, las zonas de producción, zonas de almacenamiento. <u>Toda esta labor lo realiza el área de SyMA</u>
FOTOS:	 

Tabla 31: Tratamiento de riesgo

ACTIVOS:	**[HW.DOM_HW] Controlador de Dominio Windows 2012 Server**
DESCRIPCIÓN:	Este activo pertenece a la capa de Equipamiento -> subcapa Hardware, una vez realizado el estudio de amenazas y haber escogido el control o salvaguarda adecuada se obtiene lo siguiente: La mayor amenaza de mayor relevancia es el Desastres Naturales que afecta en la disponibilidad (6,4). En el caso que llegue a materializarse esta amenaza, podrías tener pérdidas grandes en temas de equipos y más aún en la información que se encuentra alojada.
ACCIONES A TOMAR:	• Reforzar las charlas de seguridad de 5 minutos, cambiar las fechas de realización (de todos los lunes a lunes a viernes) • Cada proceso de trabajo conlleva a riesgos de Incendio o explosiones perfectamente identificados, por ello es necesario conocerlo y protegerlo, por ello la presencia de la brigada, la cual debe tener amplios conocimientos de la planta nos ayudarán a la prevención. • Concientizar a los empleados las medidas de prevención, las zonas de producción, zonas de almacenamiento. Toda esta labor lo realiza el área de SyMA

Tabla 32: Tratamiento de riesgo

ACTIVOS:	**[HW.STATION_HW] Estaciones de Trabajo**
DESCRIPCIÓN:	Este activo pertenece a la capa de Equipamiento -> subcapa Hardware, una vez realizado el estudio de amenazas y haber escogido el control o salvaguarda adecuada se obtiene lo siguiente: Se encontraron 02 amenazas mayores: Abuso de privilegios de acceso y accesos no autorizados que afecta en la disponibilidad (6,5). En el caso que llegue a materializarse esta amenaza, podrías tener pérdidas grandes en temas de información. Asimismo, afecta a la integridad y confiabilidad de la misma. Un ejemplo claro de esto es que los usuarios ingresan a PC's que no se encuentran asignadas a sus personas y también tienen contraseñas de otros usuarios e ingresan a estas cuentas.
ACCIONES A TOMAR:	• Realizar una capacitación sobre temas de seguridad de la información y de lo que implica los accesos no autorizados. Esta capacitación estará dirigida para el personal (empleados y practicantes) que pertenecen a la empresa Orazul Energy del Perú S.A. Toda esta labor lo realiza el área de tecnologías de la información

3.1.3. PLAN DE SEGURIDAD

En esta fase del proyecto se trata de cómo llevar a cabo los planes de seguridad, llevando a cabo proyectos para poder poner en marcha las decisiones adoptadas en el tratamiento de riesgos.

- **Identificación de proyectos de Seguridad:**
  Para este punto se realizará 03 actividades:
  - Capacitación de Seguridad de la Información
  - Prevención ante desastres naturales
  - Mantenimiento de UPS y cableados de energía

3.1.3.1 CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Para esta actividad se realizará una capacitación en una fecha planificada con el Coordinador O&M (para ver la disponibilidad del personal de mantenimiento y

operaciones) y con cada una de las jefaturas de las áreas que restan (Logística, SyMA, Administración)
Cabe mencionar, que se encuentra dirigida solo al personal (empleados y practicante) de Orazul Energy del Perú S.A.
En esta capacitación se dará a conocer:

- Innovaciones en la seguridad de la información
- Documentación del uso correcto de los equipos informáticos
- Documentación del uso de los servicios de Internet
- Bloqueo de los puertos USB

3.1.3.2 PREVENCIÓN ANTE DESASTRES NATURALES

Para esta actividad, se debería de reforzar las charlas de seguridad de 5 minutos; cambiar las fechas de realización (de todos los lunes a lunes a viernes). Cada proceso de trabajo conlleva a riesgos de Incendio o explosiones perfectamente identificados, por ello es necesario conocerlo y protegerlo, por ello la presencia de la brigada, la cual debe tener amplios conocimientos de la planta nos ayudarán a la prevención. Concientizar a los empleados las medidas de prevención, las zonas de producción, zonas de almacenamiento.

Esta actividad se encuentra encargada el área de Seguridad y Medio Ambiental en coordinación con el área de TI para que pueda explicar las dificultades que se puedan presentar si se materializa la amenaza

3.1.3.3 MANTENIMIENTO DE UPS Y CABLEADOS DE ENERGÍA

Para esta actividad; se debe realizar la compra de un supresor industrial de energía para conectarlo con al UPS. Además de realizar el mantenimiento planificado tanto del UPS como el cableado de energía (UPS-Suministro eléctrico). Porque no solo beneficiará a un solo equipo, sino a varios. Asimismo, agregar en el mantenimiento, a todos los UPS y baterías que están en la Central
Con la aplicación de las salvaguardas correspondientes se llega a tener los siguientes resultados:
En donde se nota que el nivel de riesgo actual a un objetivo (el cual se presenta en la siguiente tabla) disminuye considerablemente.
Adicionar, que esto se da con las herramientas que se tienen actualmente en la organización.

V. DISCUSIÓN

En este capítulo se discuten los antecedentes y los principales hallazgos encontrados en la presente investigación.

Todos los trabajos consultados y tomados como antecedentes, así como la presente investigación comparten la importancia de mejorar la disponibilidad, confiabilidad e integridad de la información, con el fin de minimizar y tratar riesgos, además de las amenazas presentes en los activos de la organización.

Se puede decir que:

- Se rectifica lo mencionado por (Aurela Pereira 2013), el cual expresa que hoy en día el volumen y complejidad de la información así como la creciente dependencia de las organizaciones hacia procesos y sistemas informáticos han llevado a todos los profesionales de TI a enfrentar grandes retos y amenazas persistentes que no dan señales de desaceleración. Para esto, creo de manera práctica un plan de trabajo que permita implementar la ISO/IEC 27001:2005 estableciendo así el análisis de riesgos de una compañía.
  En la presente investigación, se desarrolló el análisis y gestión de riesgos basándose en una metodología: MAGERIT. Además, los mecanismos de protección, tratamiento de riesgos y proyectos para poder minimizar estos riesgos. Con MAGERIT, podemos realizar este análisis de riesgos de manera más dinámica y fiable. Esta metodología está basada en la ISO 27001 la cual le da más realce.
  Una de las diferencias resaltantes que podemos obtener, es que la empresa de estudio que expone (Aurela Pereira 2013) es ficticia. En la presente investigación, la empresa si existe.

- Aprobando lo mencionado por (Gaona Vasquez 2013), el cual expresa que al aplicar la metodología MAGERIT ayudará en la búsqueda y selección de salvaguardas que son parte del análisis y gestión de riesgos informáticos para el proyecto de investigación y además será una herramienta clave para mitigar los riesgos analizados.
  En la presente investigación, se ratifica lo que menciona (Gaona Vasquez 2013), MAGERIT ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Además, apoya la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación. Esta metodología, ofrece un método sistematizado para analizar los riesgos. Ayuda a identificar y planificar medidas necesarias para reducir los riesgos. Esto se demuestra con los resultados obtenidos al realizar el análisis y gestión de riesgos (ANEXO 04 al 11), además de la capacitación aplicada como post test en la Sede UPH. Carhuaquero (ANEXO N°03).

- Se rectifica lo mencionado por (Viteri Silva 2015), el cual expresa que la evaluación basada en riesgos permite a una institución u organización considerar que eventos u amenazas potenciales puedan influir en la realización de los objetivos estratégicos. No solo utilizando MAGERIT sino marcos de referencia como COBIT que pueden apoyarnos con esta evaluación. COBIT maneja principios, políticas y estrategias que nos permite llevar la gestión de riesgos aun

enfoque directivo, consistente y conectado con los objetivos corporativos de una organización. La gestión de riesgos no es una tarea paralela o una carga adicional, debe ser una práctica que impulse a la organización a cumplir sus objetivos no solo una barrera para neutralizar los problemas que existan. COBIT, tiene su propia metodología para la gestión de riesgos, el cual es parecido a un plan empresarial.

- Referente a lo que expone (Barrantes Porras y Hugo Herrera 2013) y (Ríos Villafuerte 2014), ellos se refieren más a un diseño de un SGSI (Sistema de Gestión de Seguridad de la información). Para esto, previamente se debió de realizar un plan de seguridad para poder armar un SGSI. En la presente tesis; proponemos, desarrollamos e implementamos un plan de seguridad para la organización en estudio. El siguiente paso sería realizar un SGSI.

- Se rectifica lo que expone (Huerta Aranda 2016) sobre los procedimientos para realizar una buena auditoría física, ya que parte de la metodología de MAGERIT es velar por la seguridad física de los activos y en especial de un Data Center donde se encuentran instalados los activos tecnológicos críticos. (Huerta Aranda 2016) dice que debemos basarnos en la norma ANSI (TIA942) la cual nos ayudará en el desarrollo de los mecanismos de protección o salvaguardas de seguridad física que proponemos y forman parte de los resultados de la presente tesis (VER ANEXO N° 06).

- ISO 27002 como tal, consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. Esto expresa (Santa María Becerra 2013) en el uso de buenas prácticas en el rubro hotelero. La metodología MAGERIT si bien es cierto se basa en la ISO 27001 y cubre la fase AGR (Análisis y Gestión de riesgos), no obstante, ISO 27001 necesita de las buenas prácticas y recomendaciones (ISO 27002) para que pueda ser desarrollada y lograr así la certificación como tal en una organización. Realizando una comparación entre ISO 27002 y MAGERIT, ISO 27002 tiene menos controles en cantidad y en método hay menos controles tecnológicos, adicionalmente se cuentan con políticas de control más claras y específicas para unas buenas prácticas para la gestión de seguridad de la información. Con respecto a MAGERIT, es un método que tiene el objetivo de identificar y mitigar los posibles riesgos que se pueden presentar.

- Se rectifica lo que expresan (Santa Cruz Quiroz 2016) y (Fernández Fernández 2015), ya que estas dos tesis tienen como núcleo a la ISO 27001 para el desarrollo de su investigación y MAGERIT se basa en la norma ISO 27001

VI. CONCLUSIONES

1. UPH. Carhuaquero no tiene un documento en donde se detalle el plan de seguridad de la información, el cual se debería utilizar ante una eventualidad de cualquiera índole. De esta forma, la presente tesis ayuda a revisar y comparar metodologías siendo elegida MAGERIT pues ella ayudará a realizar de manera dinámica el análisis y gestión de riesgos para la presente tesis.

De todos los activos que conforman UPH. Carhuaquero, se han establecido 25 activos de carácter "crítico" que representan el 40,98% de todos los activos encontrados. Por otro lado, entre las amenazas encontradas, se han establecido 15 de carácter "Muy Alto" que equivalen al 30% del total de ellas.

2. Según la evaluación realizada en conjunto con el cliente y de acuerdo a las amenazas críticas encontradas, se proponen 240 salvaguardas de las cuales 3 se deben de aplicar con prioridad. Para ello se utilizó la herramienta PILAR, para gestionar, tomar decisiones y minimizar el riesgo.

SALVAGUARDAS A APLICAR	
TIPO	**PROYECTOS**
Protección de las comunicaciones	Mantenimiento de ups y cableados de energía Capacitación en seguridad de la información
Identificación y autenticación	Capacitación en seguridad de la información
Control de Acceso lógico	Capacitación en seguridad de la información

3. Para esta propuesta, se proponen 02 proyectos de Seguridad.

- **CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN**
  Con respecto a este proyecto propuesto, se implementó y se ejecutó en un 100%. Esto ayudó a concienciar de forma detallada conceptos sobre Seguridad de la información, importancia de un plan de seguridad de la información, así como se da a conocer el caso de estudio realizado en la organización.
  Luego de ello se aplicó el post test a los usuarios de UPH. Carhuaquero, sus resultados arrojaron la conformidad por parte de los usuarios sobre la calidad de la capacitación brindada y el impactado al ver la realidad en varios ámbitos presentados.

- **MANTENIMIENTO DE UPS Y CABLEADOS DE ENERGÍA**
  Los equipos de comunicación que conforman el Enlace Microondas que brindan a UPH. Carhuaquero, la conectividad a la red corporativa de Orazul, se encuentra instalada en una caseta ubicada en el Cerro la Mesa y línea que brinda energía a esta zona se encuentra deteriorada razón por la que se desarrolla este proyecto.

  Los equipos que conforman el Enlace Microondas, se catalogaron como activo crítico pues actualmente, se encuentra conectado el enlace microondas a un sistema fotovoltaico el cual se cataloga como un riesgo mayor corriendo el riesgo de que se acabe la energía que contienen las baterías instaladas es por ello la importancia de este proyecto cuyos avances hasta el momento son:
  - Se tiene un proveedor para poder realizar el mantenimiento de las líneas de energía, en especial la línea 10KV que va desde Casa Fuerza al Cerro

la Mesa y mejorar el sistema de respaldo para la conectividad de red corporativa.

- Los términos de referencia y las licitaciones fueron elaboradas por el área de Operaciones.

VII. RECOMENDACIONES

1. Se sugiere realizar charlas, capacitaciones o talleres (virtuales o presenciales) en diferentes temas de Seguridad de la Información al personal de manera semestral ya que con esto se logrará que los usuarios tengan estos conceptos actualizados en estos temas de manera permanente.

2. Como segundo punto, la capacitación para el personal del área de Tecnologías de la información sobre las actualizaciones de estos estándares y mejores prácticas de Seguridad debe ser carácter prioritario y obligatorio ya que son la cara hacia al usuario ante cualquier solicitud de esta índole.

3. La creación del área de seguridad de la información que ayude a fomentar e implementar políticas para el cuidado y protección de los activos, así como generar proyectos de Seguridad de la información

4. La alineación de marcos de referencias, mejores prácticas y estándares complementan el desarrollo de un plan de seguridad, en temas de conceptos y la dinámica de cómo realizarlo. Es importante conocer estos temas para poder ampliar conocimientos, realizar comparaciones y así realizar una buena toma de decisiones. Entre los estándares que pueden complementar esta tesis es la ISO 27002 que establece un catálogo de buenas prácticas que determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27701 en relación con el tratamiento de riesgos. Cabe recalcar que MAGERIT se basa en la ISO 27001, 27005 y 31000. Como marco de referencia tenemos a COBIT que se centra en los procesos básicos de gobierno y gestión del riesgo, para optimizar el riesgo y en cómo identificar, analizar, responder y reportar sobre el riesgo a diario. Temas de gobierno es un valor adicional que le da este marco de referencia ya que asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones.

VIII. REFERENCIAS BIBLIOGRÁFICAS

1. ADEA. «Ingeniería documental.» *ADEA: Ingeniería documental*, 2017.
2. AENOR. «La norma ISO 27001 del Sistema de Gestión de la Seguridad de Información.» *AENOR*, 2012: 40 - 44.
3. Amutio, M., y J. Candau. *MAGERIT - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I.* Madrid: Ministerio de Haciendo y Administraciones Públicas, 2012.
4. Areitio Bertolin, Javier. *Seguridad de la Información. Redes, Informática y sistemas de información.* Madrid: Paraninfo, 2008.
5. Aurela Pereira, José. «L'Oberta en Obert.» *Plan de Implementación de la norma ISO/IEC 27001:2005.* Junio de 2013. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23704/7/jaurelaTFM0613memoria.pdf (último acceso: 10 de Setiembre de 2016).
6. Baldecchi , R. «Implementación efectiva de UN SGSI ISO 27001.» *ISACA.* 04 de Setiembre de 2014. http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf (último acceso: 03 de Enero de 2017).
7. Barrantes Porras, Carlos Eduardo, y Javier Roberto Hugo Herrera. «Repositorio académico Universidad de San Martín de Porres.» *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos.* 08 de Abril de 2013. http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf (último acceso: 14 de Setiembre de 2016).
8. Candau, Javier, y Miguel Angel Amutio Gómez. *MAGERIT-Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II.* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.
9. Córdova, Norma. *Plan de Seguridad Informática para Entidad Financiera.* Tesis, Lima: UNMSM, 2003.
10. Duke Energy. *Central Hidroeléctrica Carhuaquero.* Articulo, Lima: Duke Energy, 2014.
11. Fernández Fernández, Damaris. «Repositorio de Tesis USAT.» *Modelo de gestión de riesgos de TI de acuerdo con las exigencias de las SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, MAGERIT para la Caja de Ahorro y Créditos Sipán SA.* 19 de Noviembre de 2015. http://tesis.usat.edu.pe/bitstream/usat/540/1/TL_Fernandez_Fernandez_Damaris.pdf (último acceso: 20 de Setiembre de 2016).
12. Gaona Vasquez, Karina del Rocio. «Repositorio Digital-UPS.» *"Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial BRAVITO S.A. en la ciudad de Machala".* Octubre de 2013. https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf (último acceso: 15 de Setiembre de 2016).
13. García-Cervigon Hurtado, Alfonso, y María del Pilar Alegre Ramos. *Seguridad Inforática.* 1° Edición. Madrid: Paraninfo, 2011.
14. Giner de la Fuente, Fernando. *Los sistemas de información en la sociedad del conocimiento.* Madrid: ESIC Editorial, 2004.
15. González, J. *Elaboración de un Plan de implementación de la norma ISO/IEC 27001:2013* . Tesis, Barcelona: Universitat Oberta de Catalunya, 2015.

16. Google. *Google Earth.* 02 de 09 de 2015. https://www.google.es/intl/es/earth/index.html (último acceso: 02 de Septiembre de 2015).
17. Hernández, M. *Diseño de un Plan Estratégico de seguridad de Información en una empresa del sector comercial.* Tesis de Grado, Guayaquil: Escuela Superior Politecnica del Litorial, 2006.
18. Hernández, S., C. Fernández, y L. Bautista. *Metodología de la Investigación.* México: McGraw-Hill, 2003.
19. Huerta Aranda, Melissa. «Repositorio Institucional Digital-Universidad Nacional de San Cristobal de Huamanga.» *Procedimientos para la auditoría en Seguridad Física del Data Center de la municipalidad provincial de Huamanga.* 28 de Octubre de 2016. http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1064/Tesis%20Sis23_Hue.pdf?sequence=1&isAllowed=y (último acceso: 04 de Enero de 2017).
20. ISO/IEC 27001. *ISO/IEC 27001:2005.* 2005. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-1:v1:en (último acceso: 03 de Agosto de 2014).
21. ISO27000. *ISO27000.* 2012. http://www.iso27000.es/download/doc_sgsi_all.pdf (último acceso: 02 de Septiembre de 2015).
22. ISO27001security. *ISO27001security.* 03 de Enero de 2009. http://www.iso27001security.com/ (último acceso: 10 de Septiembre de 2014).
23. LeCompte. «Enfoques de una Investigación Cualitativa.» En *Metodología de la Investigación Cualitativa*, de G. Rodrígez, J. Gil y E. García, 1-35. Málaga, 1996.
24. Lucero, A., y J. Valverde. *Análisis y Gestión de Riesgos de los Sistemas Cooperativa de Ahorro y Crédito Jardín Azuayo.* Tesis, Cuenca: Universidad de Cuenca, 2012.
25. Ministerio de Administración Públicas. *MAGERIT - Versión 2.* Catñalogo General de Publicaciones Oficiales, Madrid: NIPO, 2006.
26. Ortiz Orellana, Avidán, y René Arturo Villegas Lara. «Seguridad de la Información.» *Revista de la segunda cohorte del doctorado en seguridad estratégica*, 2014: 373.
27. Pallas, G. *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Tesis de Maestría, Montevideo: Universidad de la República, 2009.
28. Ríos Villafuerte, Josefina. «Repositorio digital de tesis PUCP.» *Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos.* 15 de Agosto de 2014. http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5555/RIOS_JOSEFINA_SISTEMA_GESTION_SEGURIDAD_INFORMACION_CENTRAL_RIESGOS.pdf?sequence=1&isAllowed=y (último acceso: 15 de Setiembre de 2016).
29. Santa Cruz Quiroz, Hilda Milagros. «Repositorio de tesis Universidad Señor de Sipan.» *Implementación de gestión de riesgos de ti para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque.* 2016. http://alicia.concytec.gob.pe/vufind/Record/USSS_f50f47c48d47ecfccec1bc7ebebf2f4c/Description#tabnav (último acceso: 05 de Enero de 2017).
30. Santa María Becerra, Franck Jhonathan. «Repositorio de Tesis USAT.» *Buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo.* 01 de Marzo de 2013. http://tesis.usat.edu.pe/bitstream/usat/532/1/TL_SantaMaria_Becerra_Franck.pdf (último acceso: 25 de Setiembre de 2016).
31. Secretaria de gobierno digital. «Gobierno Digital.» Editado por Maurice Frayssinet Delgado. 22 de Mayo de 2014. http://www.gobiernodigital.gob.pe/docs/ISO_27001_v011.pdf (último acceso: 02 de Enero de 2017).

32. Universidad Miutar Nueva Granada. *Políticas de Seguridad de Activos de Información.* 25 de Julio de 2013. http://webcache.googleusercontent.com/search?q=cache:WtnpPrUu3m8J:www.umng.edu.co/documents/10162/75102/Resolucion%2B2097%2Bde%2B2013.pdf+&cd=2&hl=es&ct=clnk&gl=pe (último acceso: 01 de Noviembre de 2015).
33. Viteri Silva, Cristian Fabricio. «Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE.» *Evaluación de riesgos tecnológicos del centro de datos de la Universidad Nacional de Chimborazo usando los procesos de TI basados en Cobit y MAGERIT.* 15 de Mayo de 2015. http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/10826/T-ESPE-049506.pdf?sequence=4&isAllowed=y (último acceso: 05 de Setiembre de 2016).

ANEXOS

ANEXO N° 01: ENCUESTA DE SEGURIDAD INFORMATICA – ÁREA: TI
ENCUESTA: SEGURIDAD INFORMÁTICA

Dirigido al personal de sistemas de información de la Central Hidroeléctrica Carhuaquero.
Objetivos:

- Conocer que tan involucrados se encuentran los trabajadores en el resguardo de la Tecnología de Información.
- Saber si los trabajadores utilizan de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

Instrucciones:
Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

1. Sexo:
   - Masculino ()
   - Femenino ()

2. Cargo del Informante: ……

Pregunta	Sí	No
¿Se han establecido controles para mitigar los riesgos de los recursos de información más críticos?		
¿Se ha identificado los activos o servicios más críticos para el cumplimiento de los objetivos del área de tecnologías de información?		
¿Se han identificado los riesgos asociados a los recursos más críticos?		
¿Se informa periódicamente a la administración respecto a las amenazas y riesgos asociados a los recursos de TI y los requerimientos para mitigar esos riesgos?		
¿Se utilizan claves seguras de acceso?		
¿Se renuevan periódicamente los registros de acceso a los sistemas?		
¿Se eliminan los accesos a funcionarios inactivos o que han dejado de laborar para la Unidad?		
¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la Unidad o por motivo de reparación?		
¿Se tiene una clasificación de la información de la unidad por nivel de sensibilidad o privacidad?		
¿Se aplican mecanismos para garantizar la protección de los equipos informáticos?		
¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?		

ANEXO N° 02: ENCUESTA DE SEGURIDAD INFORMATICA – ÁREA: USUARIO
ENCUESTA: SEGURIDAD INFORMÁTICA

Dirigido a los trabajadores de la Central Hidroeléctrica Carhuaquero.
Objetivos:

- Conocer que tan involucrados se encuentran los trabajadores en el resguardo de la Tecnología de Información.
- Saber si los trabajadores utilizan de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

Instrucciones:
Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

a. Sexo:
   - Masculino ( )
   - Femenino ( )

b. Cargo del Informante: ……

c. A qué área pertenece: ……...

d. Usted apaga los equipos informáticos debidamente después de utilizarlos.
   SI ( ) NO ( )

   Si tu respuesta es Sí, Cómo apagas tu equipo después de trabajar
   a. Apagando directamente el estabilizador. ( )
   b. Desenchufando el cable de energía de la computadora. ( )
   c. Manteniendo presionando el botón de apagado del CPU. ( )
   d. Bajando la llave de energía. ( )
   e. Otros, Especifique: ( )
   f. Ninguno. ( )

e. Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro de la Organización frente a cualquier desastre natural o humano
   SI ( ) NO ( )

f. Ha observado algún extintor cerca de los equipos informáticos.
   SI ( ) NO ( )

g. Ha observado algún tipo de señalización de emergencia en los ambientes donde existen equipos informáticos.
   SI ( ) NO ( )

h. Sabe utilizar de forma adecuada un extintor.
   SI ( ) NO ( )

   Si la respuesta es Sí; Lo aprendió a utilizar a través de:
   a. Charlas y capacitaciones fuera de la Organización ( )
   b. Charlas y capacitaciones dentro de la Organización ( )
   c. Manuales de extintor ( )

d. Internet ( )

i. Ha participado de algún simulacro frente a cualquier desastre natural o humano, especialmente en áreas donde hay equipos informáticos.
SI ( ) NO ( )

j. Cuando tiene que realizar trabajos en campo, usted deja su computadora bloqueada.
SI ( ) NO ( )

k. Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar.
SI ( ) NO ( )

l. Si en el transcurso del uso de su equipo informático se detecta alguna actividad sospechosa como ingresando a lugares restringidos, usted sería capaz de afrontarla (por la responsabilidad que asume en ese determinado momento sobre el equipo asignado)

SI ( ) NO ( )

m. Hace usted uso de los antivirus en los equipos informáticos de la Central Hidroeléctrica cuando ingresa o saca información en algún dispositivo de almacenamiento
Si ( ) A veces ( ) Nunca ( )

n. Que hace cuando detecta un virus en su computadora
   a. Activa el antivirus ( )
   b. Activa el antivirus, detecta los virus y los eliminar ( )
   c. Borra el archivo ( )
   d. Formatea el dispositivo de almacenamiento ( )
   e. No hago nada (Por qué no sé) ( )
   f. Otros, Especificar ( )

o. Tu clave de acceso es la misma para todos los servicios que te brinda la Organización.

SI ( ) NO ( )

Normalmente tu clave hace referencia a:
   a. Su nombre y apellido ( )
   b. Su fecha de nacimiento ( )
   c. Teléfono (de casa o móvil) ( )
   d. Nombre de su esposo(a) o hijo(a) ( )
   e. No comparte con nadie su clave ( )

p. Y si nunca cambio su clave, cuál es y porque motivo no lo hizo

…….

q. La Clave con la cual a la Intranet de la empresa es conocida también por:
   a. Un compañero de trabajo ( )

b. Mi esposo(a) o hijo(a) ( )
c. Otros, Especifique: ( )

r. Utiliza el servicio de correo electrónico que se le asigna en la organización
SI ( ) NO ( )

Si su respuesta es Sí; Con qué frecuencia recibe correos no deseados o spam:
a. De 1 a 10 correos al día ( )
b. De 10 a 20 correos al día ( )
c. De 20 a más correos al día ( )

s. Usted recibió alguna capacitación acerca de Seguridad de la Información en la Central Hidroeléctrica
SI ( ) NO ( )

t. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información.
SI ( ) NO ( )

Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:
a. Folletos y boletines ( )
b. Charlas o conferencias ( )
c. Como parte de algún curso en tu carrera ( )
d. Otros, Especifique: ( )

u. Usted ha realizado alguna de las siguientes actividades en su PC:
a. Instalando algún software que necesitaba ( )
b. Haciendo limpieza de componente de su PC ( )
c. Desarmando el CPU por algún sonido o falla ( )
d. Otros, Especifique: ( )
e. Ninguna ( )

v. ¿Qué hace usted cuando uno de sus componentes o aplicativos no funcionan correctamente en su PC?
a. Intenta arreglarlo ( )
b. Lo arregla mi compañero de trabajo más cercano ( )
c. Llamo a un técnico de taller de computo ( )

w. Cree usted que su equipo se encuentra seguro frente a cualquier peligro como:
a. Acceso a sus cuentas personales ( )
b. Ingreso de Virus ( )
c. Existencia de un extinguidor cerca ( )
d. No lo sé ( )
e. Otros, Especifique: ( )

x. Cada vez que sufre algún inconveniente con la PC o aplicación la cual desea trabajar, porque medio informa o reporta el inconveniente:
a. Teléfono (anexo) ( )

b. Correo electrónico al área de cómputo ( )
c. Voy físicamente a buscar algún encargado de cómputo ( )
d. Espero que pasen por mi área de trabajo ( )
e. Otros, Especifique ( )
f. Ninguna ( )

ANEXO N° 03: RESULTADO DE ENCUESTAS

NIVELES DE INCERTIDUMBRE A TRAVES DE TABLAS DE CONTINGENCIA SOBRE EL CUMPLIMIENTO DE LAS NORMAS DE SEGURIDAD DE LA CENTRAL HIDROELÉCTRICA CARHUAQUERO (SITUACIÓN ACTUAL DE LA EMPRESA)

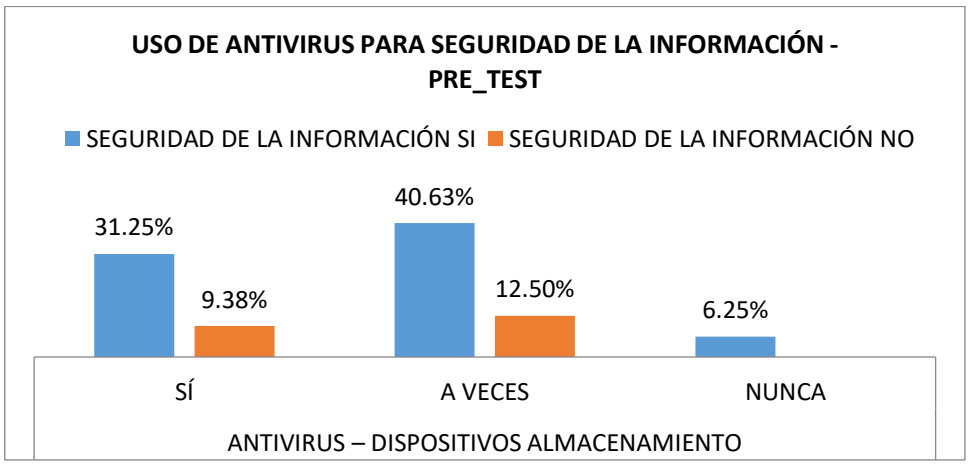
USO DE ANTIVIRUS PARA SEGURIDAD DE LA INFORMACIÓN

a. Pre-Test

Tabla 33: Uso de Antivirus para seguridad de la Información - Pre Test

		ANTIVIRUS – DISPOSITIVOS ALMACENAMIENTO			TOTAL
		SÍ	A VECES	NUNCA	
SEGURIDAD DE LA INFORMACIÓN	SI	31,25%	40,63%	6,25%	78,13%
	NO	9,38%	12,50%	0,00%	21,88%
TOTAL		40,63%	53,13%	6,25%	100%

Figura 16: Uso de Antivirus para seguridad de la Información - Pre Test

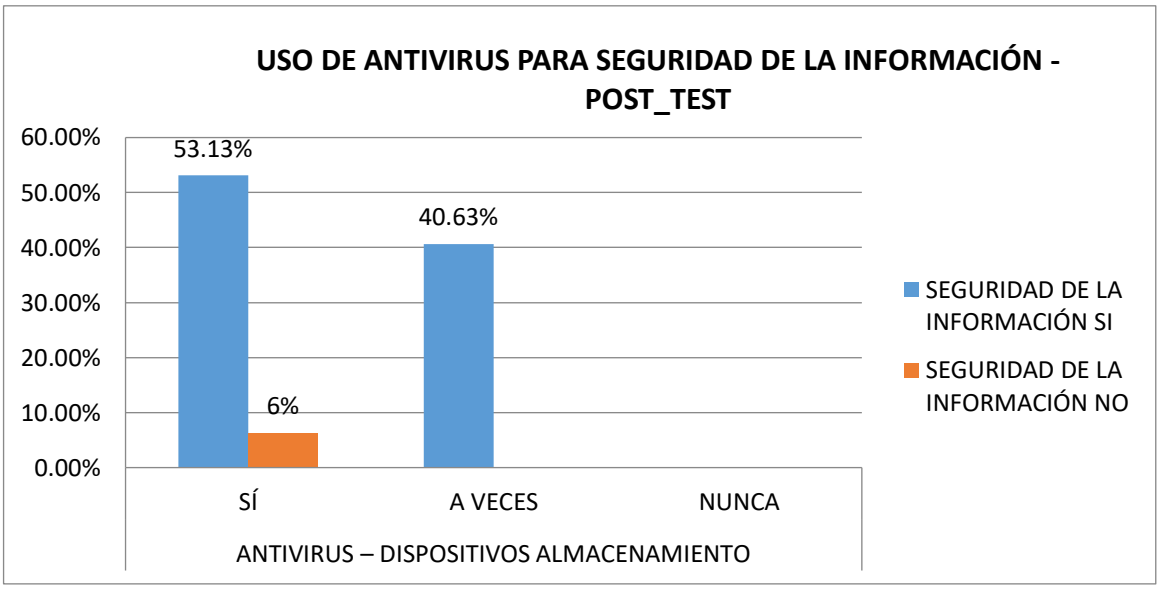


b. Post-Test

Tabla 34: Uso de Antivirus - Post Test

		ANTIVIRUS – DISPOSITIVOS ALMACENAMIENTO			TOTAL
		SÍ	A VECES	NUNCA	
SEGURIDAD DE LA INFORMACIÓN	SI	53,13%	40,63%	0%	93,75%
	NO	6%	0%	0%	6,25%
TOTAL		59,38%	40,63%	0%	100%

Figura 17: Uso de Antivirus - Post Test



Interpretación de Tablas y Gráficos: Uso de Antivirus para seguridad de la Información (Pre-test y Post-test)

Con lo referente a las tablas y gráficos del Uso de Antivirus según los conocimientos de Seguridad de la Información se tiene que el 31,25% utiliza el antivirus, 40,63% lo utiliza a veces y 6,25 % que nunca lo utiliza, teniendo en cuenta que él usuario conoce sobre seguridad de la información. A comparación de las personas que no conocen sobre seguridad de la información, lo cual los resultados serían los siguientes: 9,38% lo utiliza y 12,50% a veces. Esto demuestra, que el nivel de conocimiento sobre seguridad de la información para el tema de antivirus es muy bajo. Para estos casos, se refuerza con una capacitación en seguridad de la información, teniendo en cuenta el uso del antivirus y la importancia que tiene. Los resultados son positivos y se refleja en el nivel de porcentaje de utilización del antivirus el cual llega aún 53,13%.

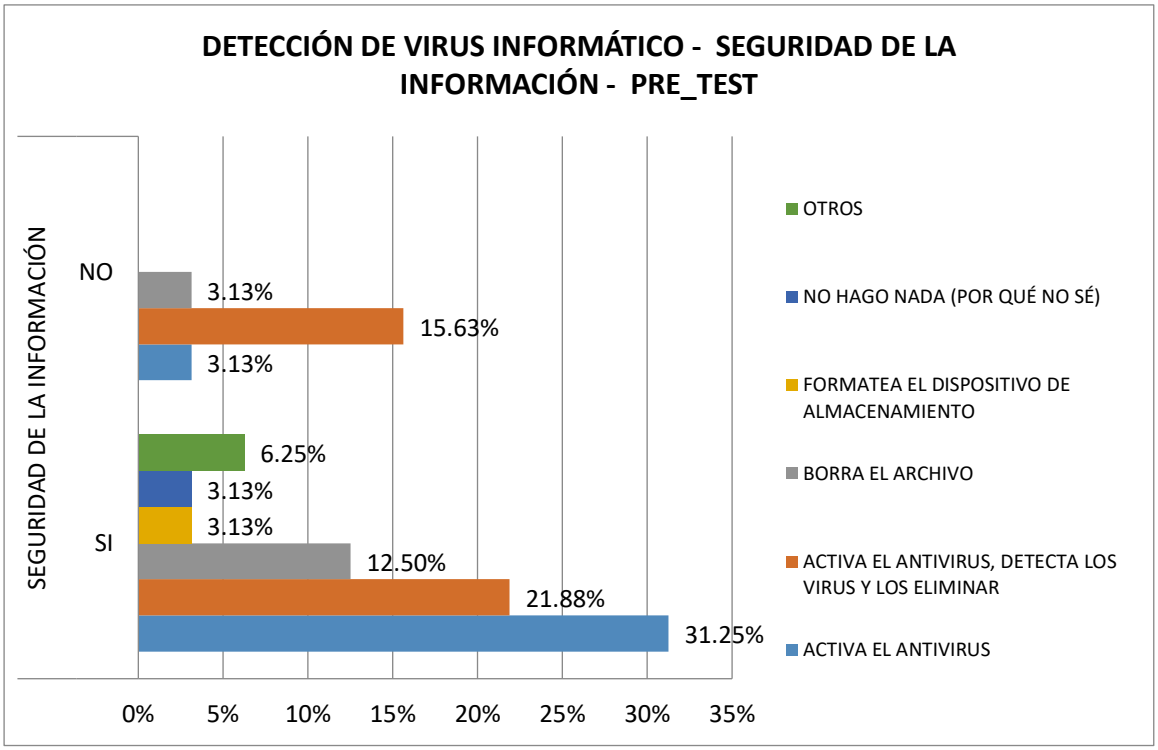
ACTUAR CUANDO DETECTA UN ANTIVIRUS

c. Pre-Test

Tabla 35: Detección de virus informático - Seguridad de la información - pre_test

		ACTUAR CUANDO DETECTA UN VIRUS INFORMÁTICO						
		ACTIVA EL ANTIVIRUS	ACTIVA EL ANTIVIRUS, DETECTA LOS VIRUS Y LOS ELIMINAR	BORRA EL ARCHIVO	FORMATEA EL DISPOSITIVO DE ALMACENAMIENTO	NO HAGO NADA (POR QUÉ NO SÉ)	OTROS	TOTAL
SEGURIDAD DE LA INFORMACIÓN	SI	31,25%	21,88%	12,50%	3,13%	3,13%	6,25%	78,13%
	NO	3,13%	15,63%	3,13%	0%	0%	0%	21,88%
TOTAL		34,38%	37,51%	15,63%	3,13%	3,13%	6,25%	100%

Figura 18: Detección de virus informático - Seguridad de la información - pre_test

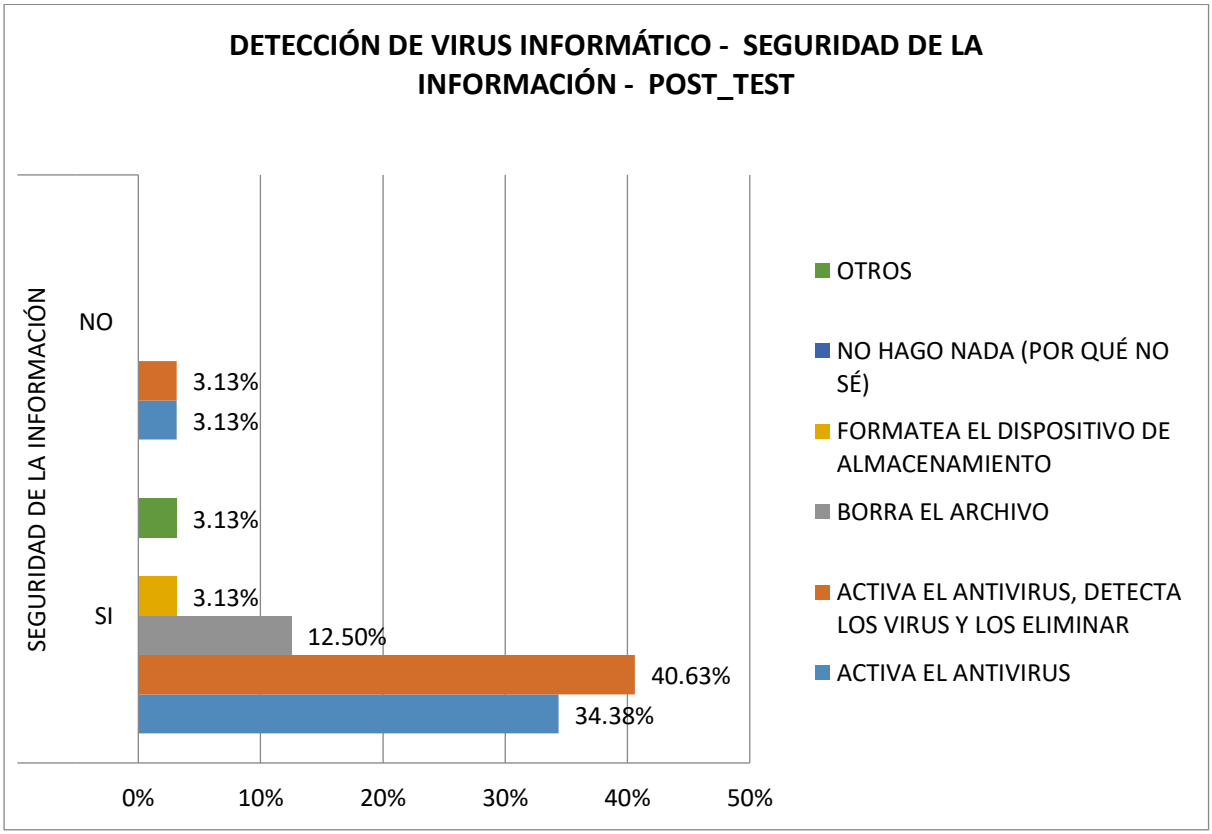


d. Post-Test

Tabla 36: Detección de virus informático - Seguridad de la información - post test

		ACTUAR CUANDO DETECTA UN VIRUS INFORMÁTICO						
		ACTIVA EL ANTIVIRUS	ACTIVA EL ANTIVIRUS, DETECTA LOS VIRUS Y LOS ELIMINAR	BORRA EL ARCHIVO	FORMATEA EL DISPOSITIVO DE ALMACENAMIENTO	NO HAGO NADA (POR QUÉ NO SÉ)	OTROS	TOTAL
SEGURIDAD DE LA INFORMACIÓN	SI	34,38%	40,63%	12,50%	3,13%	0%	3,13%	93,75%
	NO	3,13%	3,13%	0,00%	0%	0%	0%	6,25%
TOTAL		37,50%	43,75%	12,50%	3,13%	0%	3,13%	100%

Figura 19: Detección de virus informático - Seguridad de la información - post –test



<u>Interpretación de Tablas y Gráficos: Detección de virus informático - Seguridad de la información (Pre-test y Post-test)</u>

En estas tablas y gráficos, se refleja de como el usuario actúa a la hora que detecta un virus informático según su conocimiento en temas de seguridad de la información
En la primera encuesta realizada; teniendo en cuenta que, si tiene conocimientos en seguridad de la información, realiza lo siguiente: Activa el Antivirus (31,25%) y Activa el antivirus, detecta los virus y los elimina (21,88%) a comparación de los que no tienen conocimiento en seguridad de la información: Activa el antivirus (3,13%) y Activa el antivirus, detecta los virus y los elimina (15,63%). Esto demuestra que aún el nivel de conocimiento es muy bajo. Para esto se realiza una capacitación, obteniendo resultados positivos, demostrando que el nivel de conocimiento aumentó para poder actuar ante la detección de un virus informático: Activar el

antivirus (40,63%) y Activar el antivirus (34,38%), y adicionar el 3,13% que no sabía qué hacer ante este incidente, se redujo a 0%

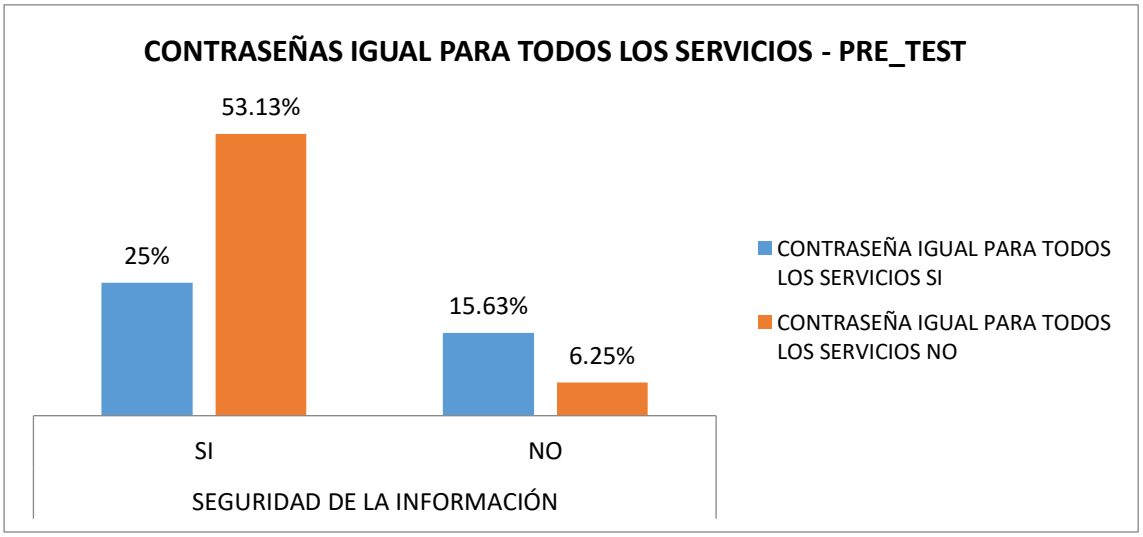
CONTRASEÑA IGUAL PARA TODOS LOS SERVICIOS

a. Pre-Test

Tabla 37: Contraseña igual para todos los servicios - pre test

		CONTRASEÑA IGUAL PARA TODOS LOS SERVICIOS		TOTAL
		SI	NO	
SEGURIDAD DE LA INFORMACIÓN	SI	25%	53,13%	78%
	NO	15,63%	6,25%	21,88%
TOTAL		41%	59,38%	100%

Figura 20: Contraseña igual para todos los servicios - pre test

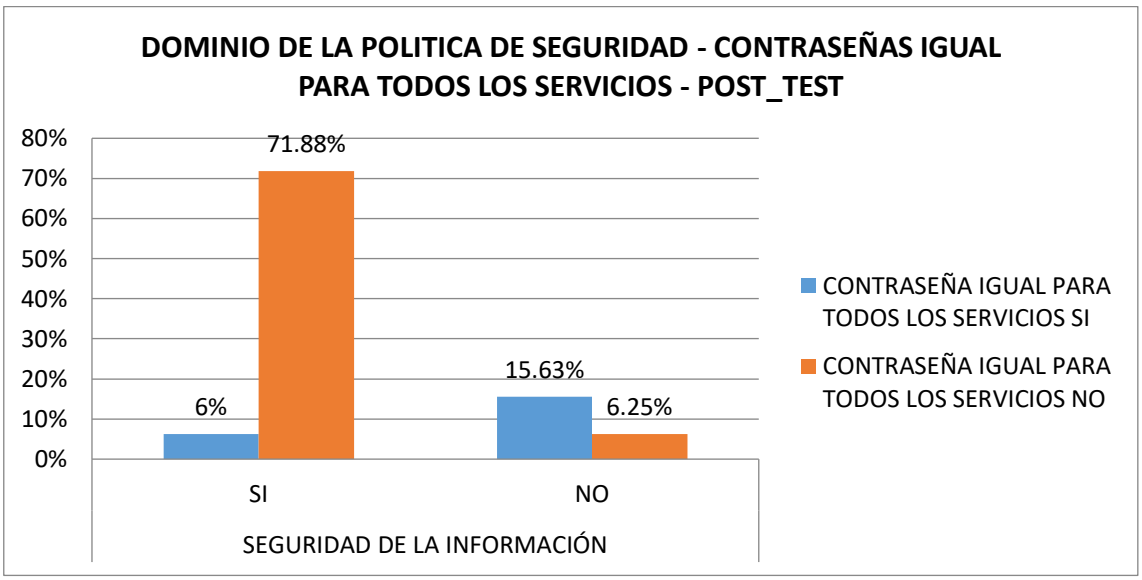


b. Post-Test

Tabla 38: Contraseña igual para todos los servicios - post test

		CONTRASEÑA IGUAL PARA TODOS LOS SERVICIOS		TOTAL
		SI	NO	
SEGURIDAD DE LA INFORMACIÓN	SI	6%	71,88%	78%
	NO	15,63%	6,25%	21,88%
TOTAL		22%	78.13%	100%

Figura 21: Contraseña igual para todos los servicios - post test



Interpretación de Tablas y Gráficos: Contraseña igual para todos los servicios (Pre-test y Post-test)

En estas tablas y gráficos reflejan que hay usuarios que utilizan la misma contraseña para ingresar a sus equipos en las aplicaciones u otros servicios. En donde se tiene que, el usuario tiene conocimiento en seguridad de la información, afirma el 25% del total de usuarios que, si tiene la contraseña igual para todas las aplicaciones y servicios; en tanto que, el 53,13% no tiene la misma contraseña para todas las aplicaciones y servicios. A comparación de las personas que no tienen conocimiento afirman que el 15,63% del total de usuario si mantienen la misma contraseña y 6,25% que no tiene la misma contraseña para todos las aplicaciones y servicios. Para esto se realiza una capacitación, obteniendo resultados positivos, en donde se obtiene que del 25% de usuarios que afirmaban tener la misma contraseña para todas sus aplicaciones que utilizaban, baja aún 6% y que las personas que no utilizaban la misma contraseña, aumenta aún 71,88%. A pesar, que hay algunos usuarios que afirman no tener conocimiento sobre seguridad de la información, se debido a que no participaron de la capacitación por diversos motivos.

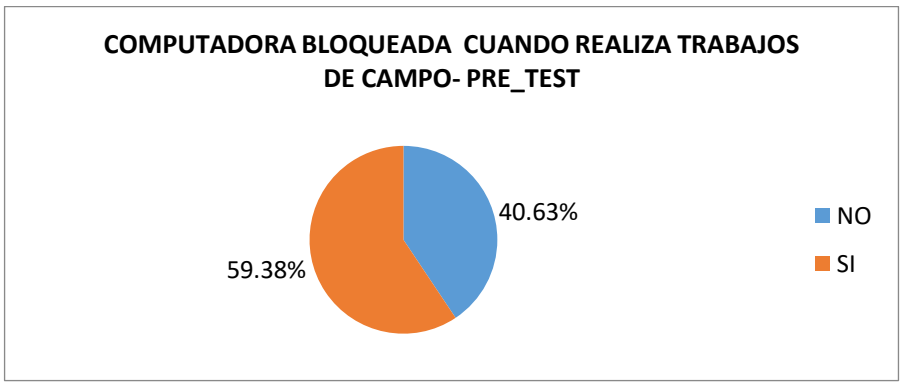
COMPUTADORA BLOQUEADA CUANDO REALIZA TRABAJOS DE CAMPO

a. Pre-Test

Tabla 39: Computadora bloqueada cuando realiza trabajos de campo - pre test

CUANDO TIENE QUE REALIZAR TRABAJOS EN CAMPO, USTED DEJA SU COMPUTADORA BLOQUEADA	**NO**	40,63%
	SI	59,38%

Figura 22: Computadora bloqueada cuando realiza trabajos de campos - pre test

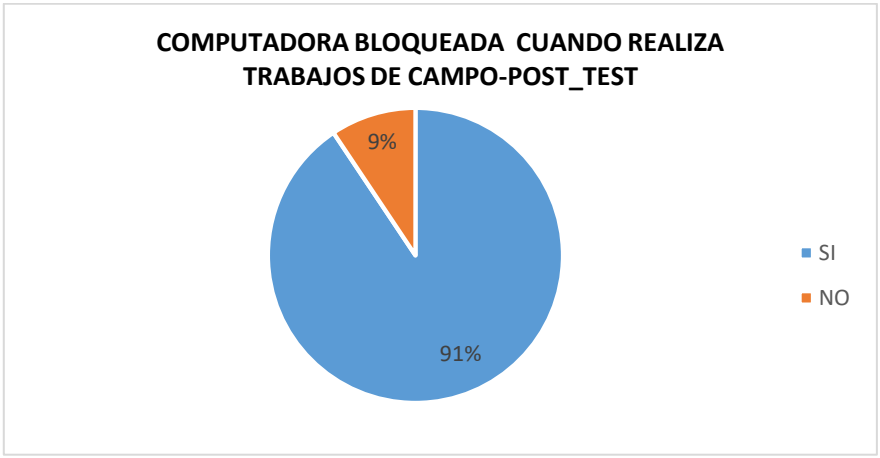


b. Post - Test

Tabla 40: Computadora bloqueada cuando realiza trabajos de campos - post test

CUANDO TIENE QUE REALIZAR TRABAJOS EN CAMPO, USTED DEJA SU COMPUTADORA BLOQUEADA	**NO**	9,38%
	SI	90,63%

Figura 23: Computadora bloqueada cuando realiza trabajos de campo - pos test



<u>Interpretación de Tablas y Gráficos: Computadora bloqueada cuando realiza trabajos de campos (Pre-test y Post-test)</u>

Para estas tablas y gráficos, se refleja si el usuario bloquea su computadora cuando sale a Campo (Fuera de oficina). Para esto, según la primera encuesta realizada se tiene los siguientes resultados, en donde el 59,38% afirma que si bloquea su equipo y el 40,63% afirma que no bloquea el equipo, el cual es un porcentaje demasiado elevado.

Para esto se realiza una capacitación, en donde los resultados obtenidos fueron positivos y se refleja que de los usuarios que no bloqueaban sus equipos (40,63% del total de usuario) aumenta aún 90,63%, el cual es un porcentaje considerable y bueno. Aún queda 9,38%, el cual puede reforzarse preguntándoles sus dudas uno por uno.

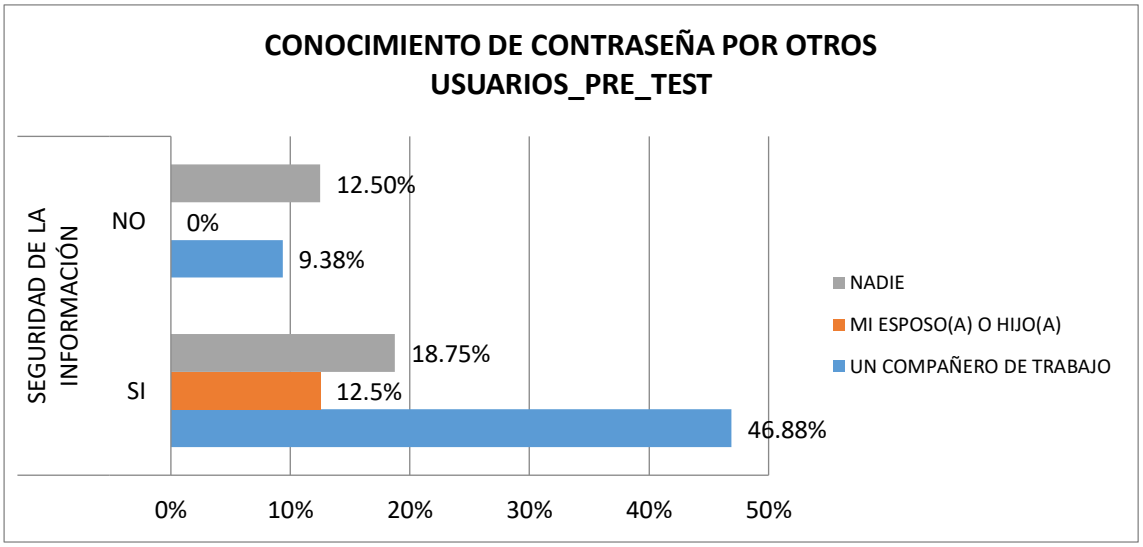
CONOCIMIENTO DE CONTRASEÑA POR OTROS USUARIOS

a. Pre-Test

Tabla 41: Conocimiento de contraseña por otros usuarios_pre_test

		CONOCIMIENTO DE CONTRASEÑA POR OTROS USUARIOS			TOTAL
		UN COMPAÑERO DE TRABAJO	MI ESPOSO(A) O HIJO(A)	NADIE	
SEGURIDAD DE LA INFORMACIÓN	SI	46,88%	12,5%	18,75%	78,13%
	NO	9,38%	0%	12,50%	21,88%
TOTAL		56,25%	12,5%	31,25%	100%

Figura 24: Conocimiento de contraseña por otros usuarios_pre_test

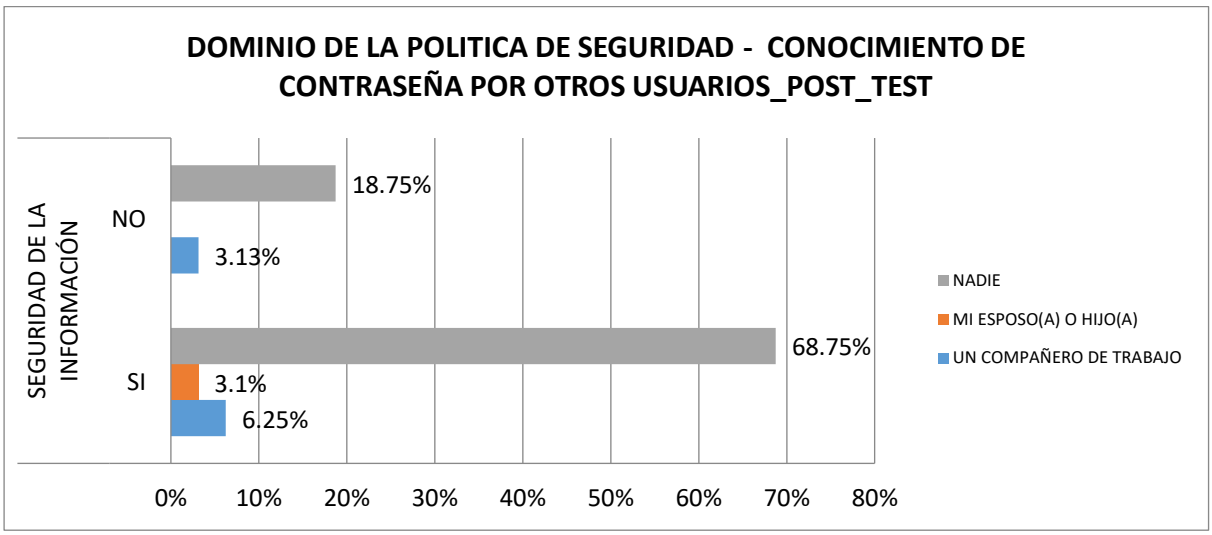


b. Post-Test

Tabla 42: Conocimiento de contraseña por otros usuarios _ post test

		CONOCIMIENTO DE CONTRASEÑA POR OTROS USUARIOS			TOTAL
		UN COMPAÑERO DE TRABAJO	MI ESPOSO(A) O HIJO(A)	NADIE	
SEGURIDAD DE LA INFORMACIÓN	SI	6,25%	3,1%	68,75%	78,13%
	NO	3,13%	0%	18,75%	21,88%
TOTAL		9,38%	3,1%	87,50%	100%

Figura 25: Conocimiento de contraseña por otros usuarios_post test



Interpretación de Tablas y Gráficos: Conocimiento de contraseña por otros usuarios (Pre-test y Post-test)

Para estas tablas y gráficos mostrados, se refleja en los usuarios que a pesar de que saben que no deben compartir la contraseña con otros usuarios, o compartirla con sus esposas e hijos, en una primera encuesta se refleja un porcentaje elevado del 46,88% lo comparten entre compañeros de trabajo y un 12,5% a sus esposas e hijos, en menor porcentaje (18,75%) no lo comparte con nadie. Esto es un tema crítico porque atenta contra la confiabilidad, integridad y llegar a la disponibilidad de la información.

Para esto, se realiza una Capacitación en seguridad de la información en donde los resultados son positivos y se refleja un cambio notable en los usuarios, dando así que el 68,75% nadie comparte su contraseña, quedando para poder reforzar un número menor de usuarios en estos temas, resolviendo sus dudas con cada uno.

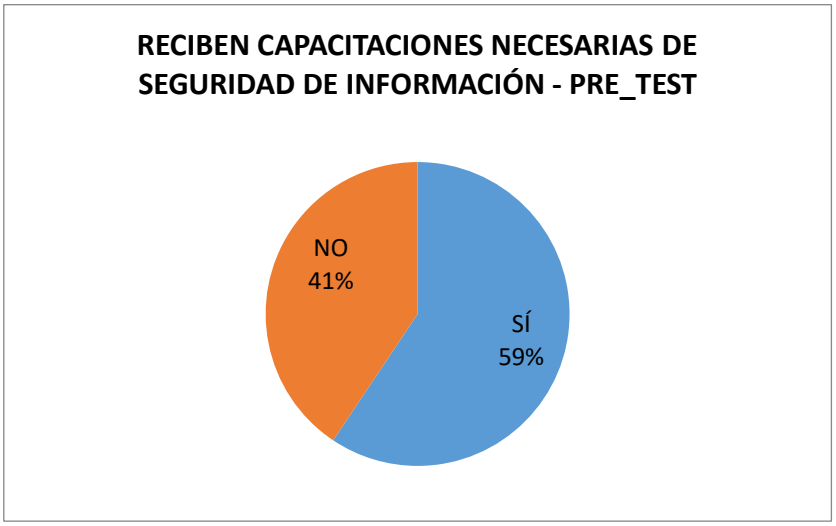
CAPACITACIONES DE USUARIOS

a. Pre-Test

Tabla 43: Reciben capacitaciones necesarias de seguridad de información - pre_test

RECIBEN CAPACITACIONES NECESARIAS DE SEGURIDAD DE INFORMACIÓN	**SÍ**	59,38%
	NO	41%

Figura 26: Reciben capacitaciones necesarias de seguridad de información - pre_test

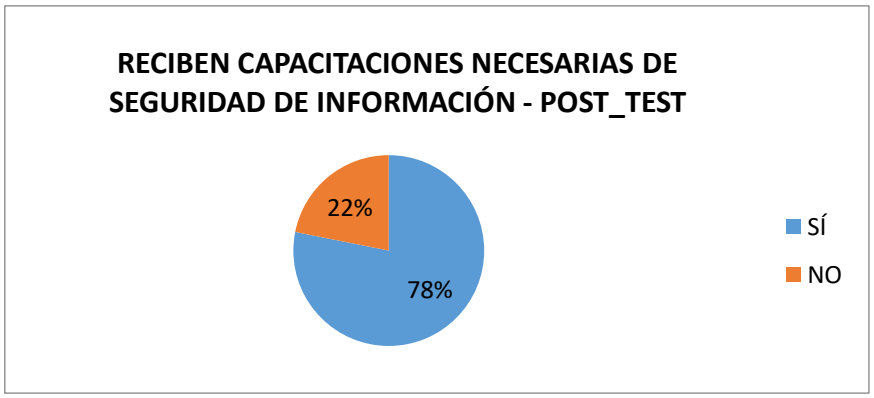


b. Post-Test

Tabla 44: Reciben capacitaciones necesarias de seguridad de información - post – test

RECIBEN CAPACITACIONES NECESARIAS DE SEGURIDAD DE INFORMACIÓN	**SÍ**	78,13%
	NO	22%

Figura 27: Reciben capacitaciones necesarias de seguridad de información - post_test



<u>Interpretación de Tablas y Gráficos: Conocimiento de contraseña por otros usuarios (Pre-test y Post-test)</u>

Con estas tablas y gráficos, se refleja que casi la mitad del total de usuarios (41%) no se encuentra capacitado en temas de seguridad de la información. Para esto, con una capacitación se refuerza estos temas y sus resultados son positivos, bajando el porcentaje de número de personas al 22%. Este 22%, queda pendiente debido a que todos los usuarios no asistieron a la capacitación por diversos motivos.

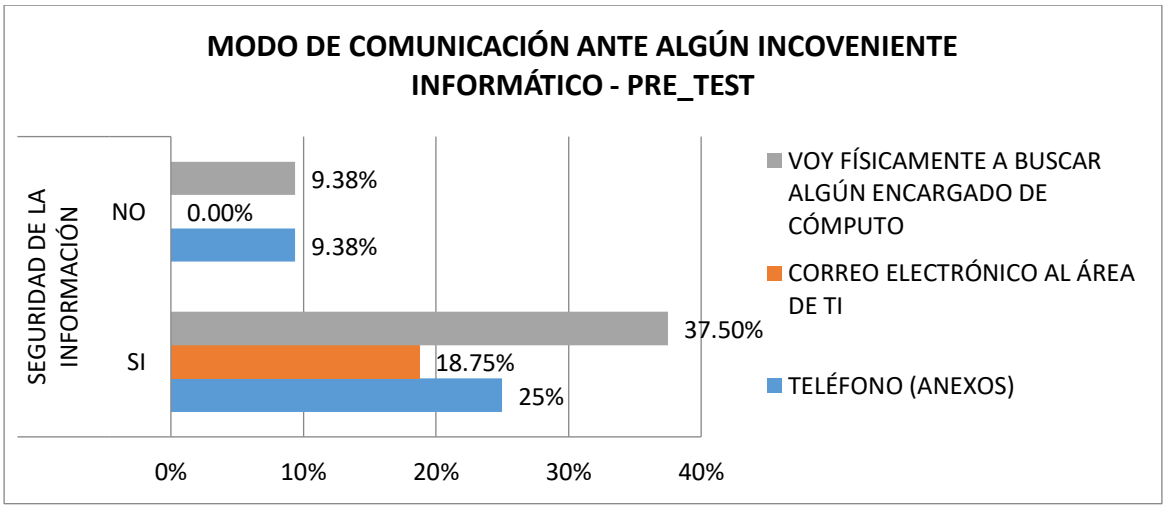
MODO DE COMUNICACIÓN ANTE ALGÚN INCONVENIENTE INFORMÁTICO.

a. Pre-Test

Tabla 45: Modo de comunicación ante algún inconveniente informático - pre_test

		MODO DE COMUNICACIÓN ANTE ALGÚN INCONVENIENTE INFORMÁTICO			TOTAL
		TELÉFONO (ANEXOS)	CORREO ELECTRÓNICO AL ÁREA DE TI	VOY FÍSICAMENTE A BUSCAR ALGÚN ENCARGADO DE CÓMPUTO	
SEGURIDAD DE LA INFORMACIÓN	SI	25%	18,75%	37,50%	81,25%
	NO	9,38%	3.13%	9,38%	18,75%
TOTAL		34,38%	18,75%	46,88%	100%

Figura 28: Modo de comunicación ante algún inconveniente informático - pre_test

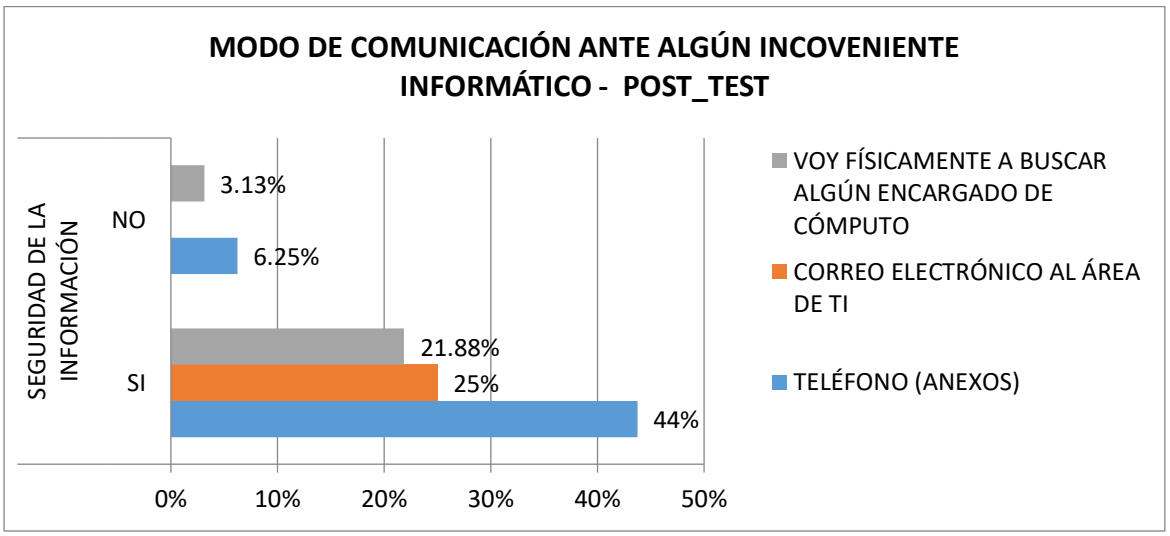


b. Post-Test

Tabla 46: Modo de comunicación ante algún inconveniente informático - post_test

		MODO DE COMUNICACIÓN ANTE ALGÚN INCONVENIENTE INFORMÁTICO			TOTAL
		TELÉFONO (ANEXOS)	CORREO ELECTRÓNICO AL ÁREA DE TI	VOY FÍSICAMENTE A BUSCAR ALGÚN ENCARGADO DE CÓMPUTO	
SEGURIDAD DE LA INFORMACIÓN	SI	44%	25%	21,88%	90,63%
	NO	6,25%	0%	3,13%	9,38%
TOTAL		50%	25,00%	25%	100%

Figura 29: Modo de comunicación ante algún inconveniente informático - post test



<u>Interpretación de Tablas y Gráficos: Conocimiento de contraseña por otros usuarios (Pre-test y Post-test)</u>

Con estas tablas y gráficos, se demuestra que hay usuarios que aún no reportan sus inconvenientes ante algún incidente de seguridad; en una primera encuesta, el 18,75% del total de usuarios no reportan estos tipos de inconvenientes. Para esto se realiza una capacitación en donde se refuerza el uso de las herramientas para poder reportar este tipo de inconvenientes (Anexo, Correo electrónico, Físicamente) obteniendo resultados positivos y disminuyendo a un 9,38% el cual es un resultado significativo y que se puede manejar.

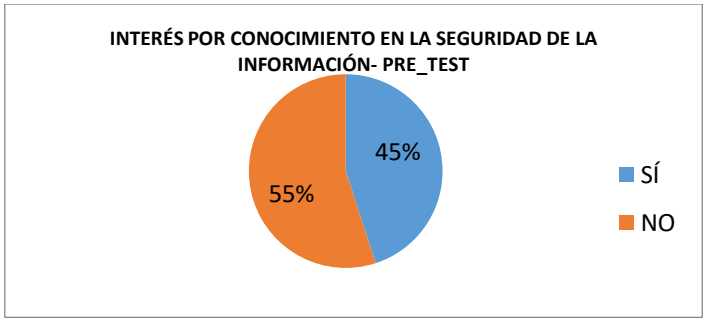
INTERÉS POR CONOCIMIENTO EN LA SEGURIDAD DE LA INFORMACIÓN

a. Pre-Test

Tabla 47: Interés por conocimiento en la seguridad de la información- pre_test

	INTERÉS POR CONOCIMIENTO EN LA SEGURIDAD DE LA INFORMACIÓN		TOTAL
	SÍ	NO	
TOTAL	45%	55%	100%

Figura 30: Interés por conocimiento en la seguridad de la información- pre_test

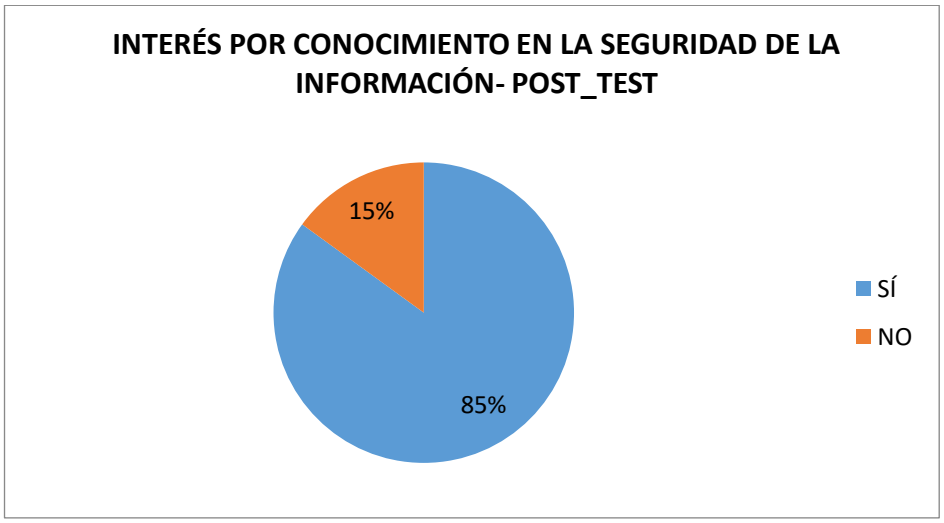


b. Post-Test

Tabla 48: Interés por conocimiento en la seguridad de la información- post_test

	INTERÉS POR CONOCIMIENTO EN LA SEGURIDAD DE LA INFORMACIÓN		TOTAL
	SÍ	NO	
TOTAL	85%	15%	100%

Figura 31: Interés por conocimiento en la seguridad de la información- post_test



Interpretación de Tablas y Gráficos: Interés por conocimiento en la Seguridad de la Información (Pre-test y Post-test)

Para estas tablas y gráficos en mención se refleja, en primer lugar, el no interés del personal de la organización (55%) en conocer sobre Seguridad de la Información. Reflejado este incidente, se lleva a cabo una Capacitación reforzando la importancia de la seguridad de la información en la organización y en la vida cotidiana. Esto dio resultados positivos, aumentando el porcentaje de interés en este tema llegando a un 85% del total de usuarios que conforman la organización.

ANEXO N° 04: IDENTIFICACIÓN Y EVALUACIÓN DE ACTIVOS

MODELO DE VALOR

PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO:

PROYECTO:	UPH. CARHUAQUERO
DESCRIPCIÓN:	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE:	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN:	ORAZUL ENERGY PERU S.A.
VERSIÓN:	1
FECHA:	1/11/2017
BIBLIOTECA:	[std] BIBLIOTECA INFOSEC (6.6.2016)

2. LICENCIA:

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. DIMENSIONES:

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

4. DOMINIOS DE SEGURIDAD:

- [base] Base

5. ACTIVOS

Dominio: [base] Base

a. CAPA: [B] ACTIVOS ESENCIALES

[INFO] Información del negocio

b. CAPA: [E] EQUIPAMIENTO

[SW] Software

[OS_SW] Sistema Operativo
[OFIMATICA_SW] Ofimática
[OTR_SW] Otros Software
[PI_SW] PI Process Book
[SCADA_SW] Sistema Tiempo Real
[MAXIMO_SW] Maximo
[PSOFT_SW] PeopleSoft
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras
[GPS_SW] Sistema de Frecuencia
[ANTIVIRUS_SW] Antivirus

[HW] Hardware
[DOM_HW] Controlador de Dominio Windows 2012 Server
[FILE_HW] Servidor de Archivos
[PI_HW] Servidor PI
[BACKUP_HW] Servidor Copias de Seguridad
[SPRINTER_HW] Servidor de Impresión
[NVR_HW] Servidor de Grabación CCTV-NVR
[STATION_HW] Estaciones de Trabajo
[PRINTER_HW] Equipos de Impresión
[PROYECTOR_HW] Proyectores Salas de Reuniones
[CAM_HW] Cámaras de Video Vigilancia
[COM] Comunicaciones
[ANT_COM] Antena (Enlace Microondas)
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso
[SWSCADA_COM] Switch SCADA
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso
[SWCAM_COM] Switch Cámaras de Video vigilancia
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa
[FOTALL_COM] Media Converter - Fibra óptica talleres
[PKSHA_COM] Packet Shaper 2500
[ROUTER_COM] Router Cisco
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)
[REP_COM] Repetidoras
[RAD_COM] Radios

c. CAPA: [S] SERVICIOS

[WWW_S] Internet
[MAIL_S] Correo Electrónico
[STELF_S] Telefonía IP (Servicio)

d. CAPA: [AUX] EQUIPAMIENTO AUXILIAR

[MOB_AUX] Mobiliario
[SAI_AUX] Sistema de Alimentación Ininterrumpida
[OTR_AUX] Otros Equipos Auxiliares

e. CAPA: [I] INSTALACIONES

[EDI_I] Edificio
[ZONA_SERV_I] Sala de Servidores
[ZONA_REU_I] Sala de Reuniones
[ZONA_ALM_I] Almacén
[ZONA_OFADM_I] Oficinas Casa de Máquinas
[ZONA_OFTALL_I] Oficinas Talleres
[ZONA_CONTROL_I] Sala Control
[ZONA_TALL_I] Talleres

f. CAPA: [P] PERSONAL

[TI_P] Coordinador TI
[ADM_P] Personal de administración y logístico
[JADM_P] Jefatura de administración
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico
[JUNI_P] Jefe de Unidad
[SYMA_P] Personal SyMA
[JSYMA_P] Jefatura SyMA
[TOP_P] Tópico
[OPE_P] Personal Operaciones
[JOPE_P] Jefatura de Operaciones
[CIV_P] Personal Ing. Civil
[SGI_P] Personal SGI

[CDOM_P] Coordinaciones O&M

6. VALORACIÓN DE LOS ACTIVOS

Dominio: [base] Base

CAPA: [B] ACTIVOS ESENCIALES

Activo	*[D]*	*[I]*	*[C]*	*[A]*	*[T]*	*[V]*
[INFO] Información del negocio	[7](1)	[9](2)	[3](3)	[2]	[2]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

(3) [si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

(4) [olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

(5) [adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(6) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

CAPA: [E] EQUIPAMIENTO

Activo	*[D]*	*[I]*	*[C]*	*[A]*	*[T]*	*[V]*
[OS_SW] Sistema Operativo	[7](1)	[0]	[2]	[6]	[0]	[6]
[OFIMATICA_SW] Ofimática	[1](2)	[4]	[0]	[4]	[0]	[4]
[OTR_SW] Otros Software	[2]	[0]	[2]	[2]	[0]	[2]
[PI_SW] PI Process Book	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[SCADA_SW] Sistema Tiempo Real	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[MAXIMO_SW] Maximo	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[PSOFT_SW] PeopleSoft	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[GPS_SW] Sistema de Frecuencia	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[ANTIVIRUS_SW] Antivirus	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[10]	[7]	[0]	[6]	[0]	[10]
[FILE_HW] Servidor de Archivos	[10]	[7]	[0]	[6]	[0]	[10]
[PI_HW] Servidor PI	[10]	[7]	[0]	[6]	[0]	[10]
[BACKUP_HW] Servidor Copias de Seguridad	[10]	[7]	[0]	[6]	[0]	[10]
[SPRINTER_HW] Servidor de Impresión	[8]	[7]	[0]	[4]	[0]	[8]
[NVR_HW] Servidor de Grabación CCTV-NVR	[10]	[7]	[0]	[6]	[0]	[10]
[STATION_HW] Estaciones de Trabajo	[8]	[4]	[0]	[6]	[0]	[8]
[PRINTER_HW] Equipos de Impresión	[8]	[4]	[0]	[6]	[0]	[8]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[4]	[0]	[0]	[0]	[0]	[4]
[CAM_HW] Cámaras de Video Vigilancia	[8]	[0]	[0]	[6]	[0]	[8]
[ANT_COM] Antena (Enlace Microondas)	[10]	[0]	[0]	[0]	[7]	[10]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[10]	[0]	[0]	[0]	[7]	[10]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2	[9]	[5]	[0]	[7]	[4]	[9]

Piso						
[SWSCADA_COM] Switch SCADA	[9]	[5]	[0]	[7]	[4]	[9]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[9]	[0]	[0]	[7]	[0]	[9]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[9]	[0]	[0]	[7]	[0]	[9]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[9]	[0]	[0]	[7]	[0]	[9]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[9]	[0]	[0]	[7]	[0]	[9]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[9]	[0]	[0]	[7]	[0]	[9]
[PKSHA_COM] Packet Shaper 2500	[9]	[0]	[0]	[7]	[0]	[9]
[ROUTER_COM] Router Cisco	[9]	[5]	[0]	[7]	[4]	[9]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[9]	[5]	[0]	[7]	[4]	[9]
[REP_COM] Repetidoras	[7]	[0]	[0]	[6]	[0]	[7]
[RAD_COM] Radios	[5]	[0]	[0]	[5]	[0]	[5]

(1) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(2) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(3) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(4) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(5) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

CAPA: [S] SERVICIOS

Activo	***[D]***	***[I]***	***[C]***	***[A]***	***[T]***	***[V]***
[WWW_S] Internet	[8]	[7]	[7]	[8]	[8]	[8]
[MAIL_S] Correo Electrónico	[8]	[7]	[7]	[8]	[8]	[8]
[STELF_S] Telefonía IP (Servicio)	[7]	[5]	[3]	[5]	[5]	[0]

CAPA: [AUX] EQUIPAMIENTO AUXILIAR

Activo	***[D]***	***[I]***	***[C]***	***[A]***	***[T]***	***[V]***
[MOB_AUX] Mobiliario	[5]	[0]	[0]	[2]	[0]	[5]
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[9]	[7]	[0]	[0]	[7]	[9]
[OTR_AUX] Otros Equipos Auxiliares	[5]	[0]	[0]	[2]	[0]	[5]

CAPA: [I] INSTALACIONES

Activo	*[D]*	*[I]*	*[C]*	*[A]*	*[T]*	*[V]*
[EDI_I] Edificio	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_SERV_I] Sala de Servidores	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_REU_I] Sala de Reuniones	[5]	[0]	[0]	[5]	[0]	[5]
[ZONA_ALM_I] Almacén	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_OFTALL_I] Oficinas Talleres	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_CONTROL_I] Sala Control	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_TALL_I] Talleres	[8]	[0]	[0]	[6](1)	[0]	[7]

(1) [ps] Seguridad de las personas

CAPA: [P] PERSONAL

Activo	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[V]**
[TI_P] Coordinador TI	[8]	[0]	[0]	[8]	[0]	[8]
[ADM_P] Personal de administración y logístico	[5]	[0]	[0]	[5]	[0]	[5]
[JADM_P] Jefatura de administración	[8]	[0]	[0]	[8]	[0]	[8]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[5]	[0]	[0]	[5]	[0]	[5]
[JUNI_P] Jefe de Unidad	[8]	[0]	[0]	[8]	[0]	[8]
[SYMA_P] Personal SyMA	[5]	[0]	[0]	[5]	[0]	[5]
[JSYMA_P] Jefatura SyMA	[8]	[0]	[0]	[8]	[0]	[8]
[TOP_P] Tópico	[5]	[0]	[0]	[5]	[0]	[5]
[OPE_P] Personal Operaciones	[5]	[0]	[0]	[5]	[0]	[5]
[JOPE_P] Jefatura de Operaciones	[8]	[0]	[0]	[8]	[0]	[8]
[CIV_P] Personal Ing. Civil	[5]	[0]	[0]	[5]	[0]	[5]
[SGI_P] Personal SGI	[5]	[0]	[0]	[5]	[0]	[5]
[CDOM_P] Coordinaciones O&M	[8]	[0]	[0]	[8]	[0]	[8]

7. VALORACIÓN DE LOS DOMINIOS

DOMINIO DE SEGURIDAD	*[D]*	*[I]*	*[C]*	*[A]*	*[T]*	*[V]*
[base] Base	[7]	[9]	[3]	[2]	[2]	[8]

ACTIVOS

[INFO] Información del negocio
[essential] Activos esenciales
[essential.info] información
[D.biz] datos de interés para el negocio
[D.per] datos de carácter personal
[D.per.M] nivel: medio
[D.classified] información clasificada
[D.classified.C] CONFIDENCIAL
[D.classified.R] DIFUSIÓN LIMITADA

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[7](1)	[7]
[I] Integridad de los datos	[9](2)	[9]
[C] Confidencialidad de los datos	[3](3)	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[2]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización
(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
(3) [lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
(4) [si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
(5) [olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
(6) [adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización
(7) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

[OS_SW] SISTEMA OPERATIVO

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[7](4)	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[2]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[6]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización
(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
(3) [lro] Obligaciones legales:

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

(4) [si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

(5) [olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

(6) [adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

[OFIMATICA_SW] OFIMÁTICA

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[1](5)	[7]
[I] Integridad de los datos	[4]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[4]	[4]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[4]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos

(3) [lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

(4) [si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

(5) [olm] Operaciones:

[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

(6) [adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas
[1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

[OTR_SW] OTROS SOFTWARE

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.std.other] otros ...
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[2]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[2]	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[2]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos

(3) [lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

(4) [si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

(5) [olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística

(6) [adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas
[1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

[OTR_SW] OTROS SOFTWARE

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](6)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:

[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[SCADA_SW] SISTEMA TIEMPO REAL

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.app] servidor de aplicaciones
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](6)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[MAXIMO_SW] MAXIMO

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](6)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[PSOFT_SW] PEOPLESOFT

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows

[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](6)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](8)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5

[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[GPS_SW] SISTEMA DE FRECUENCIA

[SW] Aplicaciones (Software)
[SW.prp] Desarrollo propio (In house)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](8)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ANTIVIRUS_SW] ANTIVIRUS

[SW] Aplicaciones (Software)
[SW.sub] Desarrollo a medida (Subcontratado)
[SW.std] Estándar (Off the shelf)
[SW.std.browser] Navegador web
[SW.std.email_client] Cliente de correo electrónico
[SW.std.email_server] Servidor de correo electrónico
[SW.std.file] Servidor de ficheros
[SW.std.dbms] Sistema de gestión de bases de datos
[SW.std.office] Ofimática
[SW.std.os] Sistema operativo
[SW.std.os.windows] Windows
[SW.std.hypervisor] Hypervisor (Gestor de la máquina virtual)
[SW.std.ts] Servidor de terminales
[SW.std.backup] Servicio de backup
[SW.sec] Herramientas de seguridad
[SW.sec.av] Antivirus
[SW.sec.ids] IDS / IPS (Detección / Prevención de intrusión)
[SW.sec.traf] Análisis de tráfico

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9](8)	[9]
[I] Integridad de los datos	[7](7)	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[DOM_HW] CONTROLADOR DE DOMINIO WINDOWS 2012 SERVER

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[FILE_HW] SERVIDOR DE ARCHIVOS

[D] Datos / Información
[D.files] Ficheros de datos
[D.backup] copias de respaldo
[SW] Aplicaciones (Software)
[SW.std] Estándar (Off the shelf)
[SW.std.file] Servidor de ficheros
[SW.std.backup] Servicio de backup
[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.vhost] Equipos virtuales (Máquinas virtuales)
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:

[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[PI_HW] SERVIDOR PI

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[BACKUP_HW] SERVIDOR COPIAS DE SEGURIDAD

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:

[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SPRINTER_HW] SERVIDOR DE IMPRESIÓN

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[4]	[4]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas
(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización
(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización
(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[NVR_HW] SERVIDOR DE GRABACIÓN CCTV-NVR

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[STATION_HW] ESTACIONES DE TRABAJO

[D] Datos / Información
[D.files] Ficheros de datos
[D.multimedia] Multimedia
[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red

[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[4]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[PRINTER_HW] EQUIPOS DE IMPRESIÓN

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[4]	[4]
[C] Confidencialidad de los datos	[0]	[0]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[0]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia

[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[PROYECTOR_HW] PROYECTORES SALAS DE REUNIONES

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[4]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[0]	[2]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[4]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[CAM_HW] CÁMARAS DE VIDEO VIGILANCIA

[HW] Equipamiento informático (Hardware)
[HW.host] Grandes equipos (Host)
[HW.mid] Equipos medios
[HW.pc] Informática personal
[HW.mobile] Informática móvil
[HW.backup] Equipamiento de respaldo
[HW.data] Almacenamiento de datos
[HW.peripheral] Periféricos
[HW.peripheral.print] Medios de impresión
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[HW.network.switch] Conmutador
[HW.network.wap] Punto de acceso wireless
[HW.ipphone] Teléfono IP
[HW.other] otros ...

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]

[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ANT_COM] ANTENA (ENLACE MICROONDAS)

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.other] Otros ...
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.MAN] Red metropolitana

[COM.WAN] red de área amplia
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[0]	[2]
[T] Trazabilidad del servicio y de los datos	[7]	[7]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada

[7.rto] RTO < 4 horas

[PIDU_COM] CONVERSOR COAXIAL-ETHERNET (ENLACE MICROONDAS)

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.bridge] puente
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet
[COM.vpn] canal cifrado (red privada virtual)

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[0]	[2]
[T] Trazabilidad del servicio y de los datos	[7]	[7]
[V] Valor	[10]	[10]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SWCORE_COM] SWITCH CORE CAPA3 OFICINAS ADMINISTRATIVAS 2 PISO

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[HW.network.router] encaminador
[COM] Redes de comunicaciones
[COM.PSTN] red telefónica
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet
[COM.backup] comunicaciones de respaldo

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[5]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):

[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SWSCADA_COM] SWITCH SCADA

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[HW.network.router] encaminador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[5]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia

[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SW2TALL_COM] SWITCH OFICINAS TALLERES 2 PISO

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[HW.network.bridge] puente
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SW2OF1_COM] SWITCH OFICINAS ADMINISTRATIVAS 1 PISO

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SWCAM_COM] SWITCH CÁMARAS DE VIDEO VIGILANCIA

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización
(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización
(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas
(5) [1.pi1] Pudiera causar molestias a un individuo

[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[FOCM_COM] MEDIA CONVERTER - FIBRA ÓPTICA CERRO LA MESA

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[FOTALL_COM] MEDIA CONVERTER - FIBRA ÓPTICA TALLERES

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.hub] Concentrador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[PKSHA_COM] PACKET SHAPER 2500

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.router] encaminador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.MAN] Red metropolitana
[COM.WAN] red de área amplia
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ROUTER_COM] ROUTER CISCO

[HW] Equipamiento informático (Hardware)
[HW. network] soporte de la red
[HW.network.router] encaminador
[COM] Redes de comunicaciones
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.VLAN] LAN virtual
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[5]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ROUTERTLF_COM] GATEWAY DE VOZ (TELEFONÍA IP)

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.switch] Conmutador
[COM] Redes de comunicaciones
[COM.PSTN] red telefónica
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[5]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[7]	[7]
[T] Trazabilidad del servicio y de los datos	[4]	[4]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo

[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[REP_COM] REPETIDORAS

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.other] Otros ...
[COM] Redes de comunicaciones
[COM.ISDN] RDSI (red digital)
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[7]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6]	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[7]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[RAD_COM] RADIOS

[HW] Equipamiento informático (Hardware)
[HW.network] Soporte de la red
[HW.network.other] Otros ...
[COM] Redes de comunicaciones
[COM.ISDN] RDSI (red digital)
[COM.pp] Punto a punto
[COM.radio] Red inalámbrica
[COM.wifi] WiFi
[COM.LAN] Red local
[COM.MAN] Red metropolitana
[COM.Internet] Internet

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[WWW_S] INTERNET

[S] Servicios
[S.prov] Proporcionado por nosotros
[S.prov.email] Correo electrónico
[S.prov.voip] Voz sobre IP
[S.3rd] Contratado a terceros
[S.3rd.ISP] Proveedor de acceso a Internet
[S.3rd.print] Impresión
[S.3rd.cloud] Servicios en la nube
[S.3rd.cloud.SaaS] Software como servicio
[S.3rd.cloud.PaaS] Plataforma como servicio
[S.3rd.cloud.IaaS] Infraestructura como servicio

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[8]	[8]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[MAIL_S] CORREO ELECTRÓNICO

[S] Servicios
[S.client] Somos clientes de ...
[S.client.email] Correo electrónico
[S.3rd] Contratado a terceros
[S.3rd.cloud] Servicios en la nube
[S.3rd.cloud.SaaS] Software como servicio
[S.3rd.cloud.PaaS] Plataforma como servicio
[S.3rd.cloud.IaaS] Infraestructura como servicio

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[7]	[9]
[C] Confidencialidad de los datos	[7]	[7]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[8]	[8]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[STELF_S] TELEFONÍA IP (SERVICIO)

[S] Servicios
[S.prov] Proporcionado por nosotros
[S.prov.voip] Voz sobre IP
[HW] Equipamiento informático (Hardware)
[HW.ipphone] Teléfono IP
[COM] Redes de comunicaciones
[COM.PSTN] red telefónica

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[7]	[7]
[I] Integridad de los datos	[5]	[9]
[C] Confidencialidad de los datos	[3]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[5]	[5]
[V] Valor	[0]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización

[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[MOB_AUX] MOBILIARIO

[AUX] Equipamiento auxiliar
[AUX.furniture] Mobiliario

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5

[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[SAI_AUX] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

[AUX] Equipamiento auxiliar
[AUX.ups] SAI- Sistemas de alimentación ininterrumpida

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[7]	[7]
[C] Confidencialidad de los datos	[0]	[0]
[A] Autenticidad de los usuarios y de la información	[0]	[0]
[T] Trazabilidad del servicio y de los datos	[7]	[7]
[V] Valor	[9]	[9]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización

[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[OTR_AUX] OTROS EQUIPOS AUXILIARES

[AUX] Equipamiento auxiliar
[AUX.power] Fuentes de alimentación
[AUX.gen] Generadores eléctricos
[AUX.ac] Equipos de climatización
[AUX.cabling] Cableado de datos
[AUX.cabling.wire] Cable eléctrico
[AUX.cabling.fiber] Fibra óptica
[AUX.supply] Suministros esenciales
[AUX.safe] Cajas fuertes
[AUX.other] Otros ...

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[EDI_I] EDIFICIO

[L] Instalaciones
[L.building] Edificio

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de

incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ZONA_SERV_I] SALA DE SERVIDORES

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ZONA_REU_I] SALA DE REUNIONES

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

[ZONA_ALM_I] ALMACÉN

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6](9)	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[7]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos

[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[ZONA_OFADM_I] OFICINAS CASA DE MÁQUINAS

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6](9)	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[7]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[ZONA_OFTALL_I] OFICINAS TALLERES

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6](9)	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[7]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:

[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[ZONA_CONTROL_I] SALA CONTROL

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

○ [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos

[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[ZONA_TALL_I] TALLERES

[L] Instalaciones
[L.local] Cuarto

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[6](9)	[6]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[7]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o

logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[TI_P] COORDINADOR TI

[P] Personal
[P.ui] Usuarios internos
[P.adm] Administradores de sistemas

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5

[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[ADM_P] PERSONAL DE ADMINISTRACIÓN Y LOGÍSTICO

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo

[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[JADM_P] JEFATURA DE ADMINISTRACIÓN

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo

[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[MANTO_P] PERSONAL MANTENIMIENTO MECÁNICO Y ELÉCTRICO

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:

[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[JUNI_P] JEFE DE UNIDAD

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:

[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[SYMA_P] PERSONAL SYMA

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación

[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[JSYMA_P] JEFATURA SYMA

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[TOP_P] TÓPICO

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[OPE_P] PERSONAL OPERACIONES

[P] Personal
[P.ui] Usuarios internos
[P.op] Operadores

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]

[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[JOPE_P] JEFATURA DE OPERACIONES

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[CIV_P] PERSONAL ING. CIVIL

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[SGI_P] PERSONAL SGI

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[5]	[7]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[5]	[5]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[5]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo

[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas

[CDOM_P] COORDINACIONES O&M

[P] Personal
[P.ui] Usuarios internos

DOMINIO DE SEGURIDAD

- [base] Base

VALOR

Dimensión	*Valor*	*Valores acumulados*
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[0]	[9]
[C] Confidencialidad de los datos	[0]	[3]
[A] Autenticidad de los usuarios y de la información	[8]	[8]
[T] Trazabilidad del servicio y de los datos	[0]	[2]
[V] Valor	[8]	[8]

(1) [6.pi1] Probablemente afecte gravemente a un grupo de individuos
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[5.cei.a] De interés significativo para la competencia
[7.adm] Probablemente impediría la operación efectiva de la organización

(2) [pi] Información personal:
[6.pi1] Probablemente afecte gravemente a un grupo de individuos
[lro] Obligaciones legales:
[7.lro] Probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(3) [lg] Pérdida de Confianza (Reputación):
[3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización

(4) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

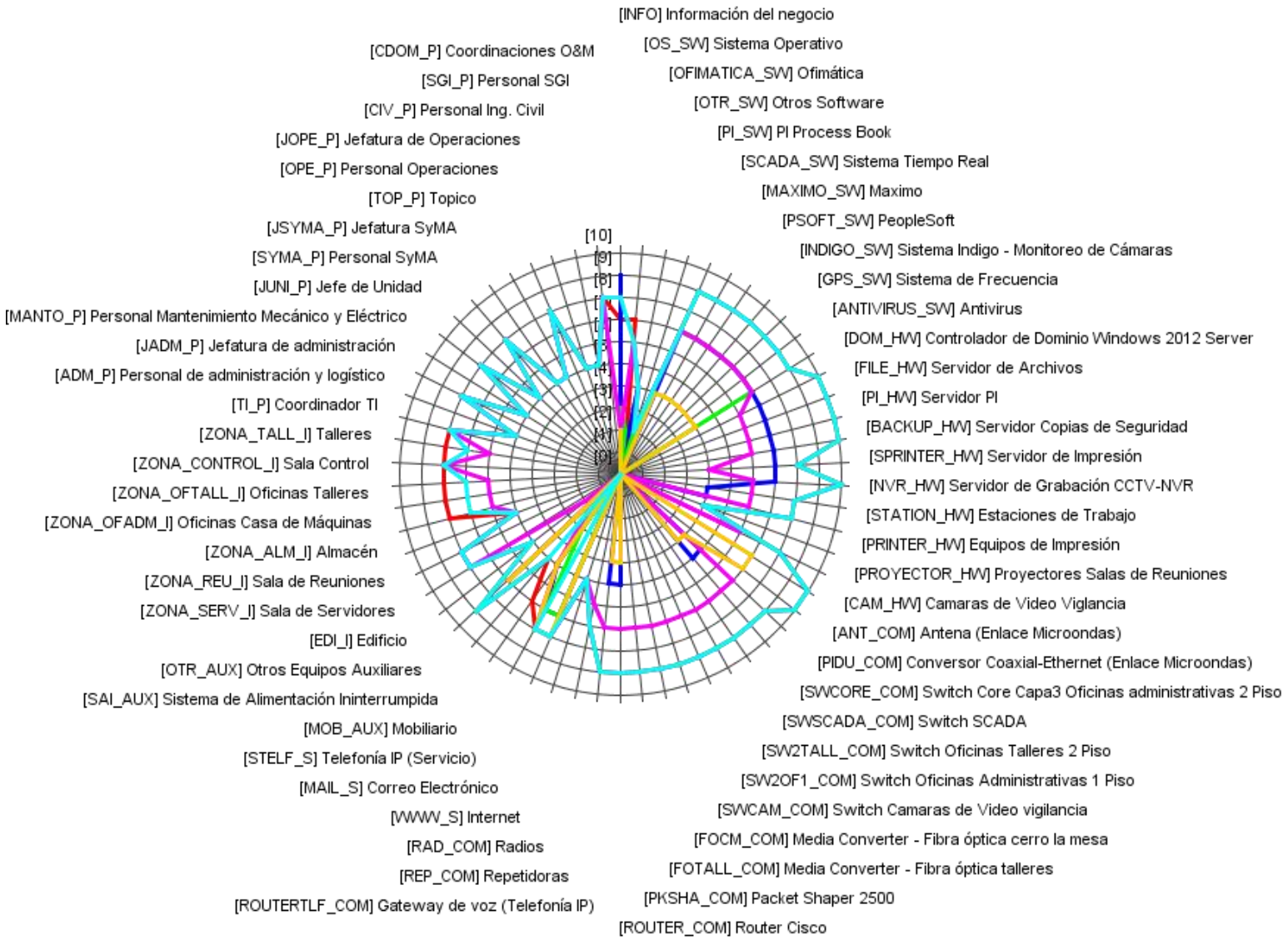
(5) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(6) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(7) [4.pi1] Probablemente afecte a un grupo de individuos
[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

(9) [ps] Seguridad de las personas


[INFO] Información del negocio
[OS_SW] Sistema Operativo
[OFIMATICA_SW] Ofimática
[OTR_SW] Otros Software
[PI_SW] PI Process Book
[SCADA_SW] Sistema Tiempo Real
[MAXIMO_SW] Maximo
[PSOFT_SW] PeopleSoft
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras
[GPS_SW] Sistema de Frecuencia
[ANTIVIRUS_SW] Antivirus
[DOM_HW] Controlador de Dominio Windows 2012 Server
[FILE_HW] Servidor de Archivos
[PI_HW] Servidor PI
[BACKUP_HW] Servidor Copias de Seguridad
[SPRINTER_HW] Servidor de Impresión
[NVR_HW] Servidor de Grabación CCTV-NVR
[STATION_HW] Estaciones de Trabajo
[PRINTER_HW] Equipos de Impresión
[PROYECTOR_HW] Proyectores Salas de Reuniones
[CAM_HW] Camaras de Video Viglancia
[ANT_COM] Antena (Enlace Microondas)
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso
[SWSCADA_COM] Switch SCADA
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso
[SWCAM_COM] Switch Camaras de Video vigilancia
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa
[FOTALL_COM] Media Converter - Fibra óptica talleres
[PKSHA_COM] Packet Shaper 2500
[ROUTER_COM] Router Cisco
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)
[REP_COM] Repetidoras
[RAD_COM] Radios
[WWW_S] Internet
[MAIL_S] Correo Electrónico
[STELF_S] Telefonía IP (Servicio)
[MOB_AUX] Mobiliario
[SAI_AUX] Sistema de Alimentación Ininterrumpida
[OTR_AUX] Otros Equipos Auxiliares
[EDI_I] Edificio
[ZONA_SERV_I] Sala de Servidores
[ZONA_REU_I] Sala de Reuniones
[ZONA_ALM_I] Almacén
[ZONA_OFADM_I] Oficinas Casa de Máquinas
[ZONA_OFTALL_I] Oficinas Talleres
[ZONA_CONTROL_I] Sala Control
[ZONA_TALL_I] Talleres
[TI_P] Coordinador TI
[ADM_P] Personal de administración y logístico
[JADM_P] Jefatura de administración
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico
[JUNI_P] Jefe de Unidad
[SYMA_P] Personal SyMA
[JSYMA_P] Jefatura SyMA
[TOP_P] Topico
[OPE_P] Personal Operaciones
[JOPE_P] Jefatura de Operaciones
[CIV_P] Personal Ing. Civil
[SGI_P] Personal SGI
[CDOM_P] Coordinaciones O&M
[10]
[9]
[8]
[4]
[3]
[2]

ANEXO N° 05: IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS

Informe de amenazas

PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO

PROYECTO:	UPH. Carhuaquero
DESCRIPCIÓN:	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE:	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN:	ORAZUL ENERGY PERU S.A.
VERSIÓN:	1
FECHA:	1/11/2017
BIBLIOTECA:	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

4. DOMINIOS DE SEGURIDAD

- [base] Base

5. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado
  - [105.a] Se permite el acceso a Internet
  - [105.b] Se permite la ejecución de programas sin autorización previa
  - [105.c] Se permite la instalación de programas sin autorización previa
  - [105.d] Se permite la conexión de dispositivos removibles
  - [111.b] Conectado a un conjunto reducido y controlado de redes
  - [111.d] Conectado a Internet
  - [112.b] En un área de acceso abierto

6. AMENAZAS / ACTIVO

[OS_SW] SISTEMA OPERATIVO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	MA	A	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[E.8] Difusión de software dañino
propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[OFIMATICA_SW] OFIMÁTICA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	P	A	-	-	-	-	-
[A.8] Difusión de software dañino	P	A	-	-	-	-	-
[A.22] Manipulación de programas	P	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[E.21] Errores de mantenimiento / actualización de programas (software)
Falta de mantenimiento en el Sistema, puede causar problemas tanto en los registros del sistema como en partes físicas como el disco duro. Esto vulnera al software base a fallar

[OTR_SW] OTROS SOFTWARE

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	MA	A	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[E.21] Errores de mantenimiento / actualización de programas (software)
Falta de mantenimiento en el Sistema, puede causar problemas tanto en los registros del sistema como en partes físicas como el disco duro. Esto vulnera al software base a fallar
[A.8] Difusión de software dañino
Instalación de programas no licencias y con crack, puede que ese archivo llamado "licencia o crack" pueda ser un software dañino para el sistema que puede llegar a corromper.

[PI_SW] PI PROCESS BOOK

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	MA	MA	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[SCADA_SW] SISTEMA TIEMPO REAL

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	MA	MA	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	A	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[MAXIMO_SW] MAXIMO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	MA	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[PSOFT_SW] PeopleSoft

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	MA	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	-	-	-	-	-

[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[INDIGO_SW] SISTEMA INDIGO - MONITOREO DE CÁMARAS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	MA	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	M	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
[A.8] Difusión de software dañino
Instalación de programas no licencias y con crack, puede que ese archivo llamado "licencia o crack" pueda ser un software dañino para el sistema que puede llegar a corromper.

[GPS_SW] SISTEMA DE FRECUENCIA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	M	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
[E.21] Errores de mantenimiento / actualización de programas (software)
defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[ANTIVIRUS_SW] ANTIVIRUS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[E.8] Difusión de software dañino	P	M	-	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	P	A	-	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	M	-	-	-	-	-
[A.8] Difusión de software dañino	MA	A	-	-	-	-	-
[A.22] Manipulación de programas	MA	A	-	-	-	-	-

[I.5] Avería de origen físico o lógico

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[E.21] Errores de mantenimiento / actualización de programas (software)

defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[DOM_HW] CONTROLADOR DE DOMINIO WINDOWS 2012 SERVER

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	A	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego

Incendio: posibilidad de que el fuego acabe con los recursos del sistema

Entorno (accidental)

Humano (accidental o deliberado)

[I.2] Daños por agua

Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Entorno (accidental)

Humano (accidental o deliberado)

[I.*] Desastres industriales

Derrumbes: Zona de la Sierra norte del Peru

Sobrecarga eléctrica: Empresa de Energía

[I.3] Contaminación medioambiental

Vibraciones, polvo, suciedad

Entorno (accidental)

Humano (accidental o deliberado)

[I.5] Avería de origen físico o lógico

Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] Corte del suministro eléctrico

Cese de la alimentación de potencia instalada

[I.7] Condiciones inadecuadas de temperatura o humedad

Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos:

excesivo calor.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso

[E.24] Caída del sistema por agotamiento de recursos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.6] Abuso de privilegios de acceso

Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto

Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.11] Acceso no autorizado

El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.23] Manipulación del hardware

Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo

Vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[FILE_HW] SERVIDOR DE ARCHIVOS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	-	-	-	-
[A.7] Uso no previsto	MA	M	M	-	-	-	-
[A.11] Acceso no autorizado	MA	M	M	-	-	-	-
[A.23] Manipulación del hardware	P	M	-	-	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego

Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)

[I.2] Daños por agua
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[I.3] Contaminación medioambiental
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)

[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] Corte del suministro eléctrico
Cese de la alimentación de potencia instalada

[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso

[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto
utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[PI_HW] SERVIDOR PI

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-

[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	A	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.*] Desastres naturales
Terremoto
[I.1] Fuego
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[I.2] Daños por agua
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)
[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[I.3] Contaminación medioambiental
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.6] Corte del suministro eléctrico
Cese de la alimentación de potencia instalada
[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso
[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.7] Uso no previsto
utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando

una persona autorizada lo utiliza.

[A.24] Denegación de servicio

la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[BACKUP_HW] SERVIDOR COPIAS DE SEGURIDAD

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	A	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego

Incendio: posibilidad de que el fuego acabe con los recursos del sistema

Entorno (accidental)

Humano (accidental o deliberado)

[I.2] Daños por agua

escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Entorno (accidental)

Humano (accidental o deliberado)

[I.*] Desastres industriales

Derrumbes: Zona de la Sierra norte del Peru

Sobrecarga eléctrica: Empresa de Energía

[I.3] Contaminación medioambiental

vibraciones, polvo, suciedad

Entorno (accidental)

Humano (accidental o deliberado)

[I.5] Avería de origen físico o lógico

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] Corte del suministro eléctrico

Cese de la alimentación de potencia instalada

[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.7] Uso no previsto
utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.24] Denegación de servicio
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.26] Ataque destructivo
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[SPRINTER_HW] SERVIDOR DE IMPRESIÓN

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	A	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.*] Desastres naturales
Terremoto

[I.1] Fuego
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[I.2] Daños por agua
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)
[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[I.3] Contaminación medioambiental
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.6] Corte del suministro eléctrico
Cese de la alimentación de potencia instalada
[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.7] Uso no previsto
utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.24] Denegación de servicio
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.26] Ataque destructivo
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[NVR_HW] SERVIDOR DE GRABACIÓN CCTV-NVR

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	MA	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-

[N.*] Desastres naturales	PP	MA	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	MA	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	M	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	A	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego

Incendio: posibilidad de que el fuego acabe con los recursos del sistema

Entorno (accidental)

Humano (accidental o deliberado)

[I.2] Daños por agua

escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Entorno (accidental)

Humano (accidental o deliberado)

[I.*] Desastres industriales

Derrumbes: Zona de la Sierra norte del Peru

Sobrecarga eléctrica: Empresa de Energía

[I.3] Contaminación medioambiental

vibraciones, polvo, suciedad

Entorno (accidental)

Humano (accidental o deliberado)

[I.5] Avería de origen físico o lógico

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] Corte del suministro eléctrico

Cese de la alimentación de potencia instalada

[I.7] Condiciones inadecuadas de temperatura o humedad

deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[E.24] Caída del sistema por agotamiento de recursos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.6] Abuso de privilegios de acceso

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos,

consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.11] Acceso no autorizado

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.23] Manipulación del hardware

alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio

la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[STATION_HW] ESTACIONES DE TRABAJO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	A	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	M	-	-	-	-	-
[I.*] Desastres industriales	P	M	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	A	-	-	-	-
[A.7] Uso no previsto	MA	M	M	-	-	-	-
[A.11] Acceso no autorizado	MA	M	A	-	-	-	-
[A.23] Manipulación del hardware	P	A	-	-	-	-	-
[A.24] Denegación de servicio	MA	A	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	A	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego

Incendio: posibilidad de que el fuego acabe con los recursos del sistema

Entorno (accidental)

Humano (accidental o deliberado)

[I.2] Daños por agua

Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Entorno (accidental)

Humano (accidental o deliberado)

[I.*] Desastres industriales

Derrumbes: Zona de la Sierra norte del Peru

Sobrecarga eléctrica: Empresa de Energía

[I.3] Contaminación medioambiental

vibraciones, polvo, suciedad

Entorno (accidental)

Humano (accidental o deliberado)

[I.5] Avería de origen físico o lógico

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] Corte del suministro eléctrico

Cese de la alimentación de potencia instalada

[I.7] Condiciones inadecuadas de temperatura o humedad

deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[E.24] Caída del sistema por agotamiento de recursos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[E.25] Pérdida de equipos

la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[A.6] Abuso de privilegios de acceso

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.11] Acceso no autorizado

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.23] Manipulación del hardware

alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio

la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[PRINTER_HW] EQUIPOS DE IMPRESIÓN

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	M	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	M	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	M	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	M	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	M	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	M	-	-	-

[A.6] Abuso de privilegios de acceso	MA	M	M	M	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	M	M	-	-	-
[A.23] Manipulación del hardware	P	M	-	A	-	-	-
[A.24] Denegación de servicio	MA	M	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	M	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[N.1] Fuego
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.*] Desastres naturales
Terremoto
[I.1] Fuego
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[I.2] Daños por agua
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)
[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[I.3] Contaminación medioambiental
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.6] Corte del suministro eléctrico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.7] Uso no previsto
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.24] Denegación de servicio
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.26] Ataque destructivo
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por

personas contratadas de forma temporal.

[PROYECTOR_HW] PROYECTORES SALAS DE REUNIONES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	B	-	-	-	-	-
[N.2] Daños por agua	PP	B	-	-	-	-	-
[N.*] Desastres naturales	PP	B	-	-	-	-	-
[I.1] Fuego	P	B	-	-	-	-	-
[I.2] Daños por agua	P	B	-	-	-	-	-
[I.*] Desastres industriales	P	B	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	B	-	-	-	-	-
[I.4] Contaminación electromagnética	P	B	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	B	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	M	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	B	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	B	-	-	-
[A.6] Abuso de privilegios de acceso	MA	B	B	B	-	-	-
[A.7] Uso no previsto	MA	B	M	B	-	-	-
[A.11] Acceso no autorizado	MA	M	B	B	-	-	-
[A.23] Manipulación del hardware	P	B	-	B	-	-	-
[A.24] Denegación de servicio	MA	B	-	-	-	-	-
[A.25] Robo de equipos	MA	B	-	B	-	-	-
[A.26] Ataque destructivo	P	B	-	-	-	-	-

[N.1] Fuego
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.*] Desastres naturales
Terremoto
[I.1] Fuego
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[I.2] Daños por agua
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)
[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[I.3] Contaminación medioambiental
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.6] Corte del suministro eléctrico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[E.24] Caída del sistema por agotamiento de recursos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[E.25] Pérdida de equipos

la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[A.6] Abuso de privilegios de acceso

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.11] Acceso no autorizado

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.23] Manipulación del hardware

alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio

la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.26] Ataque destructivo

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[CAM_HW] CÁMARAS DE VIDEO VIGILANCIA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	A	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	A	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[I.4] Contaminación electromagnética	P	B	-	-	-	-	-
[I.5] Avería de origen físico o lógico	P	A	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	A	-	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-	-
[I.11] Emanaciones electromagnéticas	P	-	-	B	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[E.25] Pérdida de equipos	P	M	-	A	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	A	A	-	-	-
[A.7] Uso no previsto	MA	M	M	M	-	-	-
[A.11] Acceso no autorizado	MA	M	A	A	-	-	-
[A.23] Manipulación del hardware	P	A	-	A	-	-	-
[A.24] Denegación de servicio	MA	A	-	-	-	-	-
[A.25] Robo de equipos	MA	M	-	A	-	-	-
[A.26] Ataque destructivo	P	A	-	-	-	-	-

[N.1] Fuego

Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.*] Desastres naturales

Terremoto

[I.1] Fuego
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[I.2] Daños por agua
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)
[I.*] Desastres industriales
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[I.3] Contaminación medioambiental
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[I.5] Avería de origen físico o lógico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.6] Corte del suministro eléctrico
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
[I.7] Condiciones inadecuadas de temperatura o humedad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[E.24] Caída del sistema por agotamiento de recursos
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.6] Abuso de privilegios de acceso
cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.7] Uso no previsto
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.11] Acceso no autorizado
el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
[A.23] Manipulación del hardware
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.24] Denegación de servicio
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.26] Ataque destructivo
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[ANT_COM] ANTENA (ENLACE MICROONDAS)

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-

[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[PIDU_COM] CONVERSOR COAXIAL-ETHERNET (ENLACE MICROONDAS)

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[SWCORE_COM] SWITCH CORE CAPA3 OFICINAS ADMINISTRATIVAS 2 PISO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[SWSCADA_COM] SWITCH SCADA

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	P	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[SW2TALL_COM] SWITCH OFICINAS TALLERES 2 PISO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[SW2OF1_COM] SWITCH OFICINAS ADMINISTRATIVAS 1 PISO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-

[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[SWCAM_COM] SWITCH CÁMARAS DE VIDEO VIGILANCIA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[FOCM_COM] MEDIA CONVERTER - FIBRA ÓPTICA CERRO LA MESA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[FOTALL_COM] MEDIA CONVERTER - FIBRA ÓPTICA TALLERES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-

[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[PKSHA_COM] PACKET SHAPER 2500

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[ROUTER_COM] ROUTER CISCO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[ROUTERTLF_COM] GATEWAY DE VOZ (TELEFONÍA IP)

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]

[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[REP_COM] REPETIDORAS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[RAD_COM] RADIOS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.9] Errores de [re-]encaminamiento	P	-	-	-	-	-	-
[E.10] Errores de secuencia	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	P	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.9] [Re-]encaminamiento de mensajes	P	-	-	-	-	-	-
[A.10] Alteración de secuencia	P	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.12] Análisis de tráfico	P	-	-	-	-	-	-
[A.14] Interceptación de información (escucha)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	PP	-	-	-	-	-	-

[WWW_S] INTERNET

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.8] Fallo de servicios de comunicaciones	P	MA	-	-	-	-	-
[E.1] Errores de los usuarios	P	M	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	M	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.18] Destrucción de la información	P	M	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-	-
[A.5] Suplantación de la identidad	P	-	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	B	-	-	-	-	-
[A.7] Uso no previsto	MA	B	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.13] Repudio (negación de actuaciones)	P	-	-	-	-	-	-
[A.15] Modificación de la información	MA	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	A	-	-	-	-	-
[A.19] Revelación de información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	MA	A	-	-	-	-	-

[MAIL_S] CORREO ELECTRÓNICO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[I.9] Interrupción de otros servicios o suministros esenciales	P	A	-	-	-	-	-
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	M	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[A.5] Suplantación de la identidad	P	-	A	A	A	-	-
[A.13] Repudio (negación de actuaciones)	P	-	-	-	-	A	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	A	-	-	-	-	-
[A.19] Revelación de información	MA	-	-	A	-	-	-
[A.24] Denegación de servicio	MA	A	-	-	-	-	-

[STELF_S] TELEFONÍA IP (SERVICIO)

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.1] Errores de los usuarios	P	-	-	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	P	-	-	-	-	-	-
[E.15] Alteración de la información	P	-	-	-	-	-	-
[E.18] Destrucción de la información	P	-	-	-	-	-	-
[E.19] Fugas de información	P	-	-	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	MA	-	-	-	-	-	-
[A.5] Suplantación de la identidad	MA	-	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	-	-	-	-	-	-
[A.7] Uso no previsto	MA	-	-	-	-	-	-
[A.11] Acceso no autorizado	MA	-	-	-	-	-	-
[A.13] Repudio (negación de actuaciones)	MA	-	-	-	-	-	-
[A.15] Modificación de la información	CS	-	-	-	-	-	-
[A.18] Destrucción de la información	MA	-	-	-	-	-	-
[A.24] Denegación de servicio	CS	-	-	-	-	-	-

[MOB_AUX] MOBILIARIO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	M	-	-	-	-	-
[N.2] Daños por agua	PP	M	-	-	-	-	-
[N.*] Desastres naturales	PP	M	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	M	-	-	-	-	-

[I.*] Desastres industriales	P	M	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	M	-	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	B	B	-	-	-
[A.23] Manipulación del hardware	P	M	-	M	-	-	-
[A.25] Robo de equipos	P	M	-	M	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[SAI_AUX] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	A	-	-	-	-	-
[N.2] Daños por agua	PP	A	-	-	-	-	-
[N.*] Desastres naturales	PP	A	-	-	-	-	-
[I.1] Fuego	P	A	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	A	-	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	A	-	-	-	-	-
[A.7] Uso no previsto	MA	A	-	-	-	-	-
[A.23] Manipulación del hardware	P	A	-	-	-	-	-
[A.25] Robo de equipos	P	A	-	-	-	-	-
[A.26] Ataque destructivo	P	A	-	-	-	-	-

[OTR_AUX] OTROS EQUIPOS AUXILIARES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	PP	M	-	-	-	-	-
[N.2] Daños por agua	PP	M	-	-	-	-	-
[N.*] Desastres naturales	PP	M	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	M	-	-	-	-	-
[I.*] Desastres industriales	P	M	-	-	-	-	-
[I.3] Contaminación medioambiental	PP	M	-	-	-	-	-
[I.6] Corte del suministro eléctrico	P	M	-	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	P	M	-	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.23] Manipulación del hardware	P	M	-	-	-	-	-
[A.25] Robo de equipos	P	M	-	A	-	-	-
[A.26] Ataque destructivo	P	M	-	-	-	-	-

[EDI_I] EDIFICIO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-

[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_SERV_I] SALA DE SERVIDORES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_REU_I] SALA DE REUNIONES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_ALM_I] ALMACÉN

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_OFADM_I] OFICINAS CASA DE MÁQUINAS

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-

[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_OFTALL_I] OFICINAS TALLERES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_CONTROL_I] SALA CONTROL

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[ZONA_TALL_I] TALLERES

amenaza	***probabilidad***	[D]	[I]	[C]	[A]	[T]	[V]
[N.1] Fuego	P	M	-	-	-	-	-
[N.2] Daños por agua	P	A	-	-	-	-	-
[N.*] Desastres naturales	P	A	-	-	-	-	-
[I.1] Fuego	P	M	-	-	-	-	-
[I.2] Daños por agua	P	A	-	-	-	-	-
[I.*] Desastres industriales	P	A	-	-	-	-	-
[I.3] Contaminación medioambiental	P	M	-	-	-	-	-
[I.4] Contaminación electromagnética	PP	M	-	-	-	-	-
[A.6] Abuso de privilegios de acceso	MA	M	-	-	-	-	-
[A.7] Uso no previsto	MA	M	-	-	-	-	-
[A.26] Ataque destructivo	PP	M	-	-	-	-	-
[A.27] Ocupación enemiga	P	M	-	-	-	-	-

[TI_P] COORDINADOR TI

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[ADM_P] PERSONAL DE ADMINISTRACIÓN Y LOGÍSTICO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	A	-	-	-	-
[E.18] Destrucción de la información	P	A	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	M	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[JADM_P] JEFATURA DE ADMINISTRACIÓN

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	M	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	B	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	PP	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	A	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[MANTO_P] PERSONAL MANTENIMIENTO MECÁNICO Y ELÉCTRICO

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	A	-	-	-	-
[E.18] Destrucción de la información	P	A	-	-	-	-	-
[E.19] Fugas de información	P	-	-	A	-	-	-
[E.28] Indisponibilidad del personal	P	B	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	A	-	-	-	-	-
[A.19] Revelación de información	PP	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	MR	B	-	-	-	-	-
[A.29] Extorsión	P	M	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[JUNI_P] JEFE DE UNIDAD

Amenaza	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-

[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[SYMA_P] PERSONAL SYMA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[JSYMA_P] JEFATURA SYMA

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	A	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	B	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[TOP_P] TÓPICO

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	MA	-	-	-	-
[E.18] Destrucción de la información	P	M	-	-	-	-	-
[E.19] Fugas de información	P	-	-	A	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[OPE_P] PERSONAL OPERACIONES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	MA	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-

[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[JOPE_P] JEFATURA DE OPERACIONES

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[CIV_P] PERSONAL ING. CIVIL

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[SGI_P] PERSONAL SGI

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-
[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

[CDOM_P] COORDINACIONES O&M

Amenaza	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[E.15] Alteración de la información	P	-	M	-	-	-	-
[E.18] Destrucción de la información	P	B	-	-	-	-	-
[E.19] Fugas de información	P	-	-	M	-	-	-
[E.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.15] Modificación de la información	MA	-	A	-	-	-	-

[A.18] Destrucción de la información	MA	M	-	-	-	-	-
[A.19] Revelación de información	MR	-	-	M	-	-	-
[A.28] Indisponibilidad del personal	P	M	-	-	-	-	-
[A.29] Extorsión	P	A	M	M	-	-	-
[A.30] Ingeniería social (picaresca)	P	A	A	A	-	-	-

7. ACTIVOS / AMENAZA

[N.1] FUEGO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	PP	MA	-	-	-	-	-
[FILE_HW] Servidor de Archivos	PP	MA	-	-	-	-	-
[PI_HW] Servidor PI	PP	MA	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	PP	MA	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	PP	MA	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	PP	MA	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	PP	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	PP	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	PP	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	PP	A	-	-	-	-	-
[MOB_AUX] Mobiliario	PP	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	PP	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	PP	M	-	-	-	-	-
[EDI_I] Edificio	P	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[FILE_HW] Servidor de Archivos
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[PI_HW] Servidor PI
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[BACKUP_HW] Servidor Copias de Seguridad
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[SPRINTER_HW] Servidor de Impresión
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[NVR_HW] Servidor de Grabación CCTV-NVR
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[STATION_HW] Estaciones de Trabajo
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[PRINTER_HW] Equipos de Impresión
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[PROYECTOR_HW] Proyectores Salas de Reuniones
Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[CAM_HW] Cámaras de Video Vigilancia
Incendios: posibilidad de que el fuego acabe con recursos del sistema.

[N.2] DAÑOS POR AGUA

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	PP	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	PP	A	-	-	-	-	-
[PI_HW] Servidor PI	PP	A	-	-	-	-	-

[BACKUP_HW] Servidor Copias de Seguridad	PP	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	PP	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	PP	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	PP	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	PP	A	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	PP	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	PP	A	-	-	-	-	-
[MOB_AUX] Mobiliario	PP	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	PP	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	PP	M	-	-	-	-	-
[EDI_I] Edificio	P	A	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	A	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	A	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	A	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	A	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	A	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	A	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	A	-	-	-	-	-

[N.*] DESASTRES NATURALES

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	PP	MA	-	-	-	-	-
[FILE_HW] Servidor de Archivos	PP	MA	-	-	-	-	-
[PI_HW] Servidor PI	PP	MA	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	PP	MA	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	PP	MA	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	PP	MA	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	PP	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	PP	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	PP	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	PP	A	-	-	-	-	-
[MOB_AUX] Mobiliario	PP	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	PP	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	PP	M	-	-	-	-	-
[EDI_I] Edificio	P	A	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	A	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	A	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	A	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	A	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	A	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	A	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	A	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
Terremoto
[FILE_HW] Servidor de Archivos
Terremoto
[PI_HW] Servidor PI
Terremoto
[BACKUP_HW] Servidor Copias de Seguridad
Terremoto
[SPRINTER_HW] Servidor de Impresión
Terremoto
[NVR_HW] Servidor de Grabación CCTV-NVR
Terremoto
[STATION_HW] Estaciones de Trabajo
Terremoto
[PRINTER_HW] Equipos de Impresión

Terremoto
[PROYECTOR_HW] Proyectores Salas de Reuniones
Terremoto
[CAM_HW] Cámaras de Video Vigilancia
Terremoto

[I.1] FUEGO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	A	-	-	-	-	-
[PI_HW] Servidor PI	P	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-
[MOB_AUX] Mobiliario	P	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-
[EDI_I] Edificio	P	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[FILE_HW] Servidor de Archivos
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[PI_HW] Servidor PI
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[BACKUP_HW] Servidor Copias de Seguridad
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[SPRINTER_HW] Servidor de Impresión
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[NVR_HW] Servidor de Grabación CCTV-NVR
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[STATION_HW] Estaciones de Trabajo
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)
[PRINTER_HW] Equipos de Impresión

Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)

[PROYECTOR_HW] Proyectores Salas de Reuniones
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)

[CAM_HW] Cámaras de Video Vigilancia
Incendio: posibilidad de que el fuego acabe con los recursos del sistema
Entorno (accidental)
Humano (accidental o deliberado)

[I.2] DAÑOS POR AGUA

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	A	-	-	-	-	-
[PI_HW] Servidor PI	P	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	A	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-
[MOB_AUX] Mobiliario	P	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-
[EDI_I] Edificio	P	A	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	A	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	A	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	A	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	A	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	A	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	A	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	A	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[FILE_HW] Servidor de Archivos
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[PI_HW] Servidor PI
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[BACKUP_HW] Servidor Copias de Seguridad
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[SPRINTER_HW] Servidor de Impresión
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[NVR_HW] Servidor de Grabación CCTV-NVR
escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Entorno (accidental)
Humano (accidental o deliberado)

[STATION_HW] Estaciones de Trabajo
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[PRINTER_HW] Equipos de Impresión
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[PROYECTOR_HW] Proyectores Salas de Reuniones
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[CAM_HW] Cámaras de Video Vigilancia
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
Entorno (accidental)
Humano (accidental o deliberado)

[I.*] DESASTRES INDUSTRIALES

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	MA	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	MA	-	-	-	-	-
[PI_HW] Servidor PI	P	MA	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	MA	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	MA	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	MA	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-
[MOB_AUX] Mobiliario	P	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-
[EDI_I] Edificio	P	A	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	A	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	A	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	A	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	A	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	A	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	A	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	A	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[FILE_HW] Servidor de Archivos
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[PI_HW] Servidor PI
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[BACKUP_HW] Servidor Copias de Seguridad
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[SPRINTER_HW] Servidor de Impresión
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[NVR_HW] Servidor de Grabación CCTV-NVR

Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[STATION_HW] Estaciones de Trabajo
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[PRINTER_HW] Equipos de Impresión
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[PROYECTOR_HW] Proyectores Salas de Reuniones
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía
[CAM_HW] Cámaras de Video Vigilancia
Derrumbes: Zona de la Sierra norte del Peru
Sobrecarga eléctrica: Empresa de Energía

[I.3] CONTAMINACIÓN MEDIOAMBIENTAL

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	PP	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	PP	A	-	-	-	-	-
[PI_HW] Servidor PI	PP	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	PP	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	PP	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	PP	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	PP	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	PP	A	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	PP	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	PP	A	-	-	-	-	-
[MOB_AUX] Mobiliario	PP	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	PP	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	PP	M	-	-	-	-	-
[EDI_I] Edificio	P	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[FILE_HW] Servidor de Archivos
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[PI_HW] Servidor PI
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[BACKUP_HW] Servidor Copias de Seguridad
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[SPRINTER_HW] Servidor de Impresión
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)

[NVR_HW] Servidor de Grabación CCTV-NVR
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[STATION_HW] Estaciones de Trabajo
vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[PRINTER_HW] Equipos de Impresión
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[PROYECTOR_HW] Proyectores Salas de Reuniones
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)
[CAM_HW] Cámaras de Video Vigilancia
Vibraciones, polvo, suciedad
Entorno (accidental)
Humano (accidental o deliberado)

[I.4] CONTAMINACIÓN ELECTROMAGNÉTICA

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	M	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	M	-	-	-	-	-
[PI_HW] Servidor PI	P	M	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	M	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	M	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	M	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	B	-	-	-	-	-
[EDI_I] Edificio	PP	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	PP	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	PP	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	PP	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	PP	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	PP	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	PP	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	PP	M	-	-	-	-	-

[I.5] AVERÍA DE ORIGEN FÍSICO O LÓGICO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	MA	A	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	A	-	-	-	-	-
[OTR_SW] Otros Software	MA	A	-	-	-	-	-
[PI_SW] PI Process Book	MA	MA	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	MA	MA	-	-	-	-	-
[MAXIMO_SW] Maximo	P	MA	-	-	-	-	-
[PSOFT_SW] PeopleSoft	P	MA	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	P	MA	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	P	A	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	P	A	-	-	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	A	-	-	-	-	-
[PI_HW] Servidor PI	P	A	-	-	-	-	-

[BACKUP_HW] Servidor Copias de Seguridad	P	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	A	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-

[OS_SW] Sistema Operativo

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[OFIMATICA_SW] Ofimática

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[OTR_SW] Otros Software

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[PI_SW] PI Process Book

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[SCADA_SW] Sistema Tiempo Real

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[MAXIMO_SW] Maximo

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[PSOFT_SW] PeopleSoft

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[GPS_SW] Sistema de Frecuencia

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[ANTIVIRUS_SW] Antivirus

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[DOM_HW] Controlador de Dominio Windows 2012 Server

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[FILE_HW] Servidor de Archivos

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[PI_HW] Servidor PI

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[BACKUP_HW] Servidor Copias de Seguridad

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[SPRINTER_HW] Servidor de Impresión

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[NVR_HW] Servidor de Grabación CCTV-NVR

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[STATION_HW] Estaciones de Trabajo

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[PRINTER_HW] Equipos de Impresión

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[PROYECTOR_HW] Proyectores Salas de Reuniones

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[CAM_HW] Cámaras de Video Vigilancia

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.6] CORTE DEL SUMINISTRO ELÉCTRICO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	A	-	-	-	-	-
[PI_HW] Servidor PI	P	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	M	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

Cese de la alimentación de potencia instalada

[FILE_HW] Servidor de Archivos

Cese de la alimentación de potencia instalada

[PI_HW] Servidor PI

Cese de la alimentación de potencia instalada

[BACKUP_HW] Servidor Copias de Seguridad

Cese de la alimentación de potencia instalada

[SPRINTER_HW] Servidor de Impresión

Cese de la alimentación de potencia instalada

[NVR_HW] Servidor de Grabación CCTV-NVR

Cese de la alimentación de potencia instalada

[STATION_HW] Estaciones de Trabajo

Cese de la alimentación de potencia instalada

[PRINTER_HW] Equipos de Impresión

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[PROYECTOR_HW] Proyectores Salas de Reuniones

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[CAM_HW] Cámaras de Video Vigilancia

fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	A	-	-	-	-	-
[PI_HW] Servidor PI	P	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	A	-	-	-	-	-

[STATION_HW] Estaciones de Trabajo	P	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	M	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[FILE_HW] Servidor de Archivos
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[PI_HW] Servidor PI
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[BACKUP_HW] Servidor Copias de Seguridad
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[SPRINTER_HW] Servidor de Impresión
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[NVR_HW] Servidor de Grabación CCTV-NVR
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[STATION_HW] Estaciones de Trabajo
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[PRINTER_HW] Equipos de Impresión
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[PROYECTOR_HW] Proyectores Salas de Reuniones
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.
[CAM_HW] Cámaras de Video Vigilancia
deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor.

[I.8] FALLO DE SERVICIOS DE COMUNICACIONES

activo	***probabilidad***	[D]	[I]	[C]	[A]	[T]	[V]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-
[WWW_S] Internet	P	MA	-	-	-	-	-

[I.9] INTERRUPCIÓN DE OTROS SERVICIOS O SUMINISTROS ESENCIALES

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[MAIL_S] Correo Electrónico	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-

[I.11] EMANACIONES ELECTROMAGNÉTICAS

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	-	-	B	-	-	-
[FILE_HW] Servidor de Archivos	P	-	-	-	-	-	-
[PI_HW] Servidor PI	P	-	-	B	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	-	-	B	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	-	-	B	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	-	-	B	-	-	-
[STATION_HW] Estaciones de Trabajo	P	-	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	-	-	B	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	-	-	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	-	-	B	-	-	-

[E.1] ERRORES DE LOS USUARIOS

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	P	M	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	P	-	-	-	-	-	-

[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-
[WWW_S] Internet	P	M	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	P	-	-	-	-	-	-

[E.8] DIFUSIÓN DE SOFTWARE DAÑINO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	P	M	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	M	-	-	-	-	-
[OTR_SW] Otros Software	P	M	-	-	-	-	-
[PI_SW] PI Process Book	P	M	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	P	M	-	-	-	-	-
[MAXIMO_SW] Maximo	P	M	-	-	-	-	-
[PSOFT_SW] PeopleSoft	P	M	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	P	M	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	P	M	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	P	M	-	-	-	-	-

[OS_SW] Sistema Operativo

propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[E.9] ERRORES DE [RE-]ENCAMINAMIENTO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-

[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-

[E.10] ERRORES DE SECUENCIA

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-

[E.15] ALTERACIÓN DE LA INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-
[WWW_S] Internet	P	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	P	-	M	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	P	-	-	-	-	-	-
[TI_P] Coordinador TI	P	-	M	-	-	-	-
[ADM_P] Personal de administración y logístico	P	-	A	-	-	-	-
[JADM_P] Jefatura de administración	P	-	M	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y	P	-	A	-	-	-	-

Eléctrico							
[JUNI_P] Jefe de Unidad	P	-	M	-	-	-	-
[SYMA_P] Personal SyMA	P	-	M	-	-	-	-
[JSYMA_P] Jefatura SyMA	P	-	M	-	-	-	-
[TOP_P] Tópico	P	-	MA	-	-	-	-
[OPE_P] Personal Operaciones	P	-	MA	-	-	-	-
[JOPE_P] Jefatura de Operaciones	P	-	M	-	-	-	-
[CIV_P] Personal Ing. Civil	P	-	M	-	-	-	-
[SGI_P] Personal SGI	P	-	M	-	-	-	-
[CDOM_P] Coordinaciones O&M	P	-	M	-	-	-	-

[E.18] DESTRUCCIÓN DE LA INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	P	M	-	-	-	-	-
[MAIL_S] Correo Electrónico	P	M	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	P	-	-	-	-	-	-
[TI_P] Coordinador TI	P	B	-	-	-	-	-
[ADM_P] Personal de administración y logístico	P	A	-	-	-	-	-
[JADM_P] Jefatura de administración	P	M	-	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	P	A	-	-	-	-	-
[JUNI_P] Jefe de Unidad	P	B	-	-	-	-	-
[SYMA_P] Personal SyMA	P	B	-	-	-	-	-
[JSYMA_P] Jefatura SyMA	P	A	-	-	-	-	-
[TOP_P] Tópico	P	M	-	-	-	-	-
[OPE_P] Personal Operaciones	P	B	-	-	-	-	-
[JOPE_P] Jefatura de Operaciones	P	B	-	-	-	-	-
[CIV_P] Personal Ing. Civil	P	B	-	-	-	-	-
[SGI_P] Personal SGI	P	B	-	-	-	-	-
[CDOM_P] Coordinaciones O&M	P	B	-	-	-	-	-

[E.19] FUGAS DE INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-
[WWW_S] Internet	P	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	P	-	-	M	-	-	-
[STELF_S] Telefonía IP (Servicio)	P	-	-	-	-	-	-
[TI_P] Coordinador TI	P	-	-	M	-	-	-
[ADM_P] Personal de administración y logístico	P	-	-	M	-	-	-
[JADM_P] Jefatura de administración	P	-	-	M	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	P	-	-	A	-	-	-
[JUNI_P] Jefe de Unidad	P	-	-	M	-	-	-
[SYMA_P] Personal SyMA	P	-	-	M	-	-	-

[JSYMA_P] Jefatura SyMA	P	-	-	M	-	-	-
[TOP_P] Tópico	P	-	-	A	-	-	-
[OPE_P] Personal Operaciones	P	-	-	M	-	-	-
[JOPE_P] Jefatura de Operaciones	P	-	-	M	-	-	-
[CIV_P] Personal Ing. Civil	P	-	-	M	-	-	-
[SGI_P] Personal SGI	P	-	-	M	-	-	-
[CDOM_P] Coordinaciones O&M	P	-	-	M	-	-	-

[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	P	A	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	A	-	-	-	-	-
[OTR_SW] Otros Software	P	A	-	-	-	-	-
[PI_SW] PI Process Book	P	A	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	P	A	-	-	-	-	-
[MAXIMO_SW] Maximo	P	A	-	-	-	-	-
[PSOFT_SW] PeopleSoft	P	A	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	P	A	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	P	A	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	P	A	-	-	-	-	-

[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	MA	A	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	A	-	-	-	-	-
[OTR_SW] Otros Software	P	M	-	-	-	-	-
[PI_SW] PI Process Book	MA	A	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	MA	A	-	-	-	-	-
[MAXIMO_SW] Maximo	P	M	-	-	-	-	-
[PSOFT_SW] PeopleSoft	P	M	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	MA	M	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	MA	M	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	MA	M	-	-	-	-	-

[OS_SW] Sistema Operativo
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[OFIMATICA_SW] Ofimática
: Falta de mantenimiento en el Sistema, puede causar problemas tanto en los registros del sistema como en partes físicas como el disco duro. Esto vulnera al software base a fallar

[OTR_SW] Otros Software
: Falta de mantenimiento en el Sistema, puede causar problemas tanto en los registros del sistema como en partes físicas como el disco duro. Esto vulnera al software base a fallar

[PI_SW] PI Process Book
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[SCADA_SW] Sistema Tiempo Real
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[MAXIMO_SW] Maximo
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[PSOFT_SW] PeopleSoft
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras
: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[GPS_SW] Sistema de Frecuencia

defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[ANTIVIRUS_SW] Antivirus

defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	-	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	M	-	-	-	-	-
[PI_HW] Servidor PI	P	M	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	M	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	M	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	M	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	M	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	M	-	-	-	-	-
[MOB_AUX] Mobiliario	P	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso

[FILE_HW] Servidor de Archivos

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso

[PI_HW] Servidor PI

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso

[BACKUP_HW] Servidor Copias de Seguridad

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[SPRINTER_HW] Servidor de Impresión

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[NVR_HW] Servidor de Grabación CCTV-NVR

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[STATION_HW] Estaciones de Trabajo

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[PRINTER_HW] Equipos de Impresión

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[PROYECTOR_HW] Proyectores Salas de Reuniones

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[CAM_HW] Cámaras de Video Vigilancia

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	A	-	-	-	-	-
[FILE_HW] Servidor de Archivos	MA	A	-	-	-	-	-

[PI_HW] Servidor PI	MA	A	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	A	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	A	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	A	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	A	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	MA	A	-	-	-	-	-
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-
[WWW_S] Internet	MA	A	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[FILE_HW] Servidor de Archivos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[PI_HW] Servidor PI

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[BACKUP_HW] Servidor Copias de Seguridad

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[SPRINTER_HW] Servidor de Impresión

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[NVR_HW] Servidor de Grabación CCTV-NVR

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[STATION_HW] Estaciones de Trabajo

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[PRINTER_HW] Equipos de Impresión

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[PROYECTOR_HW] Proyectores Salas de Reuniones

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[CAM_HW] Cámaras de Video Vigilancia

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[E.25] PÉRDIDA DE EQUIPOS

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	M	-	M	-	-	-

[FILE_HW] Servidor de Archivos	P	M	-	-	-	-	-
[PI_HW] Servidor PI	P	M	-	M	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	M	-	M	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	M	-	M	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	M	-	M	-	-	-
[STATION_HW] Estaciones de Trabajo	P	M	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	M	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	M	-	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	M	-	A	-	-	-

[STATION_HW] Estaciones de Trabajo

la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[PROYECTOR_HW] Proyectores Salas de Reuniones

la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[E.28] INDISPONIBILIDAD DEL PERSONAL

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	P	M	-	-	-	-	-
[ADM_P] Personal de administración y logístico	P	M	-	-	-	-	-
[JADM_P] Jefatura de administración	P	B	-	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	P	B	-	-	-	-	-
[JUNI_P] Jefe de Unidad	P	M	-	-	-	-	-
[SYMA_P] Personal SyMA	P	M	-	-	-	-	-
[JSYMA_P] Jefatura SyMA	P	B	-	-	-	-	-
[TOP_P] Tópico	P	M	-	-	-	-	-
[OPE_P] Personal Operaciones	P	M	-	-	-	-	-
[JOPE_P] Jefatura de Operaciones	P	M	-	-	-	-	-
[CIV_P] Personal Ing. Civil	P	M	-	-	-	-	-
[SGI_P] Personal SGI	P	M	-	-	-	-	-
[CDOM_P] Coordinaciones O&M	P	M	-	-	-	-	-

[A.5] SUPLANTACIÓN DE LA IDENTIDAD

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	MA	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-

[RAD_COM] Radios	MA	-	-	-	-	-	-
[WWW_S] Internet	P	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	P	-	A	A	A	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-

[A.6] ABUSO DE PRIVILEGIOS DE ACCESO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	M	M	A	-	-	-
[FILE_HW] Servidor de Archivos	MA	M	M	-	-	-	-
[PI_HW] Servidor PI	MA	M	M	A	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	M	M	A	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	M	M	A	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	M	M	A	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	M	A	-	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	M	M	M	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	B	B	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	MA	M	A	A	-	-	-
[WWW_S] Internet	MA	B	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-
[EDI_I] Edificio	MA	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	MA	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	MA	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	MA	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	MA	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	MA	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	MA	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	MA	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[FILE_HW] Servidor de Archivos

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[PI_HW] Servidor PI

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[BACKUP_HW] Servidor Copias de Seguridad

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[SPRINTER_HW] Servidor de Impresión

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[NVR_HW] Servidor de Grabación CCTV-NVR

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[STATION_HW] Estaciones de Trabajo

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[PRINTER_HW] Equipos de Impresión

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[PROYECTOR_HW] Proyectores Salas de Reuniones

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[CAM_HW] Cámaras de Video Vigilancia

cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] USO NO PREVISTO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	M	M	M	-	-	-
[FILE_HW] Servidor de Archivos	MA	M	M	-	-	-	-
[PI_HW] Servidor PI	MA	M	M	M	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	M	M	M	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	M	M	M	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	M	M	M	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	M	M	-	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	M	M	M	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	B	M	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	MA	M	M	M	-	-	-
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	MA	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-
[RAD_COM] Radios	MA	-	-	-	-	-	-
[WWW_S] Internet	MA	B	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-
[MOB_AUX] Mobiliario	MA	M	B	B	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	MA	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	MA	M	-	-	-	-	-
[EDI_I] Edificio	MA	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	MA	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	MA	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	MA	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	MA	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	MA	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	MA	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	MA	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[FILE_HW] Servidor de Archivos

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[PI_HW] Servidor PI

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[BACKUP_HW] Servidor Copias de Seguridad

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[SPRINTER_HW] Servidor de Impresión

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos,

consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[NVR_HW] Servidor de Grabación CCTV-NVR

utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[STATION_HW] Estaciones de Trabajo

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[PRINTER_HW] Equipos de Impresión

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[PROYECTOR_HW] Proyectores Salas de Reuniones

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[CAM_HW] Cámaras de Video Vigilancia

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.8] DIFUSIÓN DE SOFTWARE DAÑINO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	MA	A	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	A	-	-	-	-	-
[OTR_SW] Otros Software	MA	A	-	-	-	-	-
[PI_SW] PI Process Book	MA	A	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	MA	A	-	-	-	-	-
[MAXIMO_SW] Maximo	MA	A	-	-	-	-	-
[PSOFT_SW] PeopleSoft	MA	A	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	MA	A	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	MA	A	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	MA	A	-	-	-	-	-

[OTR_SW] Otros Software

Instalación de programas no licencias y con crack, puede que ese archivo llamado "licencia o crack" pueda ser un software dañino para el sistema que puede llegar a corromper.

[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras

Instalación de programas no licencias y con crack, puede que ese archivo llamado "licencia o crack" pueda ser un software dañino para el sistema que puede llegar a corromper.

[A.9] [RE-]ENCAMINAMIENTO DE MENSAJES

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-

[RAD_COM] Radios	P	-	-	-	-	-	-

[A.10] ALTERACIÓN DE SECUENCIA

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-

[A.11] ACCESO NO AUTORIZADO

Activo	*Probabilidad*	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	M	M	A	-	-	-
[FILE_HW] Servidor de Archivos	MA	M	M	-	-	-	-
[PI_HW] Servidor PI	MA	M	M	A	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	M	M	A	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	M	M	A	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	M	M	A	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	M	A	-	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	M	M	M	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	M	B	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	MA	M	A	A	-	-	-
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-
[RAD_COM] Radios	MA	-	-	-	-	-	-
[WWW_S] Internet	MA	-	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[FILE_HW] Servidor de Archivos

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[PI_HW] Servidor PI

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[BACKUP_HW] Servidor Copias de Seguridad

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[SPRINTER_HW] Servidor de Impresión

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[NVR_HW] Servidor de Grabación CCTV-NVR

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[STATION_HW] Estaciones de Trabajo

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[PRINTER_HW] Equipos de Impresión

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[PROYECTOR_HW] Proyectores Salas de Reuniones

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[CAM_HW] Cámaras de Video Vigilancia

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.12] ANÁLISIS DE TRÁFICO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	P	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	P	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	P	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	P	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	P	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	P	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	P	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	P	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	P	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	P	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	P	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	P	-	-	-	-	-	-
[REP_COM] Repetidoras	P	-	-	-	-	-	-
[RAD_COM] Radios	P	-	-	-	-	-	-

[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	P	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	P	-	-	-	-	A	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-

[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	MA	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-

[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-
[RAD_COM] Radios	MA	-	-	-	-	-	-

[A.15] MODIFICACIÓN DE LA INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	MA	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-
[RAD_COM] Radios	MA	-	-	-	-	-	-
[WWW_S] Internet	MA	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	MA	-	A	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	CS	-	-	-	-	-	-
[TI_P] Coordinador TI	MA	-	A	-	-	-	-
[ADM_P] Personal de administración y logístico	MA	-	A	-	-	-	-
[JADM_P] Jefatura de administración	MA	-	A	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	MA	-	A	-	-	-	-
[JUNI_P] Jefe de Unidad	MA	-	A	-	-	-	-
[SYMA_P] Personal SyMA	MA	-	A	-	-	-	-
[JSYMA_P] Jefatura SyMA	MA	-	A	-	-	-	-
[TOP_P] Tópico	MA	-	A	-	-	-	-
[OPE_P] Personal Operaciones	MA	-	A	-	-	-	-
[JOPE_P] Jefatura de Operaciones	MA	-	A	-	-	-	-
[CIV_P] Personal Ing. Civil	MA	-	A	-	-	-	-
[SGI_P] Personal SGI	MA	-	A	-	-	-	-
[CDOM_P] Coordinaciones O&M	MA	-	A	-	-	-	-

[A.18] DESTRUCCIÓN DE LA INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[ANT_COM] Antena (Enlace Microondas)	MA	-	-	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	MA	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	MA	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	MA	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	MA	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	MA	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	MA	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	MA	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	MA	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	MA	-	-	-	-	-	-

[ROUTER_COM] Router Cisco	MA	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	MA	-	-	-	-	-	-
[REP_COM] Repetidoras	MA	-	-	-	-	-	-
[RAD_COM] Radios	MA	-	-	-	-	-	-
[WWW_S] Internet	MA	A	-	-	-	-	-
[MAIL_S] Correo Electrónico	MA	A	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	MA	-	-	-	-	-	-
[TI_P] Coordinador TI	MA	M	-	-	-	-	-
[ADM_P] Personal de administración y logístico	MA	M	-	-	-	-	-
[JADM_P] Jefatura de administración	PP	M	-	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	MA	A	-	-	-	-	-
[JUNI_P] Jefe de Unidad	MA	M	-	-	-	-	-
[SYMA_P] Personal SyMA	MA	M	-	-	-	-	-
[JSYMA_P] Jefatura SyMA	MA	M	-	-	-	-	-
[TOP_P] Tópico	MA	M	-	-	-	-	-
[OPE_P] Personal Operaciones	MA	M	-	-	-	-	-
[JOPE_P] Jefatura de Operaciones	MA	M	-	-	-	-	-
[CIV_P] Personal Ing. Civil	MA	M	-	-	-	-	-
[SGI_P] Personal SGI	MA	M	-	-	-	-	-
[CDOM_P] Coordinaciones O&M	MA	M	-	-	-	-	-

[A.19] REVELACIÓN DE INFORMACIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	MA	-	-	-	-	-	-
[MAIL_S] Correo Electrónico	MA	-	-	A	-	-	-
[TI_P] Coordinador TI	MR	-	-	M	-	-	-
[ADM_P] Personal de administración y logístico	MR	-	-	M	-	-	-
[JADM_P] Jefatura de administración	MR	-	-	M	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	PP	-	-	M	-	-	-
[JUNI_P] Jefe de Unidad	MR	-	-	M	-	-	-
[SYMA_P] Personal SyMA	MR	-	-	M	-	-	-
[JSYMA_P] Jefatura SyMA	MR	-	-	M	-	-	-
[TOP_P] Tópico	MR	-	-	M	-	-	-
[OPE_P] Personal Operaciones	MR	-	-	M	-	-	-
[JOPE_P] Jefatura de Operaciones	MR	-	-	M	-	-	-
[CIV_P] Personal Ing. Civil	MR	-	-	M	-	-	-
[SGI_P] Personal SGI	MR	-	-	M	-	-	-
[CDOM_P] Coordinaciones O&M	MR	-	-	M	-	-	-

[A.22] MANIPULACIÓN DE PROGRAMAS

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	MA	A	-	-	-	-	-
[OFIMATICA_SW] Ofimática	P	A	-	-	-	-	-
[OTR_SW] Otros Software	MA	A	-	-	-	-	-
[PI_SW] PI Process Book	MA	A	-	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	MA	A	-	-	-	-	-
[MAXIMO_SW] Maximo	MA	A	-	-	-	-	-
[PSOFT_SW] PeopleSoft	MA	A	-	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	MA	A	-	-	-	-	-
[GPS_SW] Sistema de Frecuencia	MA	A	-	-	-	-	-
[ANTIVIRUS_SW] Antivirus	MA	A	-	-	-	-	-

[A.23] MANIPULACIÓN DEL HARDWARE

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	M	-	A	-	-	-
[FILE_HW] Servidor de Archivos	P	M	-	-	-	-	-
[PI_HW] Servidor PI	P	M	-	A	-	-	-

[BACKUP_HW] Servidor Copias de Seguridad	P	M	-	A	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	M	-	A	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	M	-	A	-	-	-
[STATION_HW] Estaciones de Trabajo	P	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	A	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	B	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	A	-	-	-
[MOB_AUX] Mobiliario	P	M	-	M	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[FILE_HW] Servidor de Archivos
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[PI_HW] Servidor PI
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[BACKUP_HW] Servidor Copias de Seguridad
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[SPRINTER_HW] Servidor de Impresión
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[NVR_HW] Servidor de Grabación CCTV-NVR
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[STATION_HW] Estaciones de Trabajo
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[PRINTER_HW] Equipos de Impresión
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[PROYECTOR_HW] Proyectores Salas de Reuniones
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[CAM_HW] Cámaras de Video Vigilancia
alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] DENEGACIÓN DE SERVICIO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	M	-	-	-	-	-
[FILE_HW] Servidor de Archivos	MA	M	-	-	-	-	-
[PI_HW] Servidor PI	MA	M	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	M	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	M	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	M	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	MA	A	-	-	-	-	-
[ANT_COM] Antena (Enlace Microondas)	PP	-	-	-	-	-	-

[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	PP	-	-	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	PP	-	-	-	-	-	-
[SWSCADA_COM] Switch SCADA	PP	-	-	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	PP	-	-	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	PP	-	-	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	PP	-	-	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	PP	-	-	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	PP	-	-	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	PP	-	-	-	-	-	-
[ROUTER_COM] Router Cisco	PP	-	-	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	PP	-	-	-	-	-	-
[REP_COM] Repetidoras	PP	-	-	-	-	-	-
[RAD_COM] Radios	PP	-	-	-	-	-	-
[WWW_S] Internet	MA	A	-	-	-	-	-
[MAIL_S] Correo Electrónico	MA	A	-	-	-	-	-
[STELF_S] Telefonía IP (Servicio)	CS	-	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[FILE_HW] Servidor de Archivos
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[PI_HW] Servidor PI
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[BACKUP_HW] Servidor Copias de Seguridad
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[SPRINTER_HW] Servidor de Impresión
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[NVR_HW] Servidor de Grabación CCTV-NVR
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[STATION_HW] Estaciones de Trabajo
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[PRINTER_HW] Equipos de Impresión
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[PROYECTOR_HW] Proyectores Salas de Reuniones
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[CAM_HW] Cámaras de Video Vigilancia
la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.25] ROBO DE EQUIPOS

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	MA	M	-	A	-	-	-
[FILE_HW] Servidor de Archivos	MA	M	-	A	-	-	-
[PI_HW] Servidor PI	MA	M	-	A	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	MA	M	-	A	-	-	-
[SPRINTER_HW] Servidor de Impresión	MA	M	-	A	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	MA	M	-	A	-	-	-
[STATION_HW] Estaciones de Trabajo	MA	M	-	A	-	-	-
[PRINTER_HW] Equipos de Impresión	MA	M	-	M	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	MA	B	-	B	-	-	-

[CAM_HW] Cámaras de Video Vigilancia	MA	M	-	A	-	-	-
[MOB_AUX] Mobiliario	P	M	-	M	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	A	-	-	-

[A.26] ATAQUE DESTRUCTIVO

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[DOM_HW] Controlador de Dominio Windows 2012 Server	P	M	-	-	-	-	-
[FILE_HW] Servidor de Archivos	P	M	-	-	-	-	-
[PI_HW] Servidor PI	P	M	-	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	P	M	-	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	P	M	-	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	P	M	-	-	-	-	-
[STATION_HW] Estaciones de Trabajo	P	A	-	-	-	-	-
[PRINTER_HW] Equipos de Impresión	P	M	-	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	P	B	-	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	P	A	-	-	-	-	-
[MOB_AUX] Mobiliario	P	M	-	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	P	A	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	P	M	-	-	-	-	-
[EDI_I] Edificio	PP	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	PP	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	PP	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	PP	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	PP	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	PP	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	PP	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	PP	M	-	-	-	-	-

[DOM_HW] Controlador de Dominio Windows 2012 Server

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[FILE_HW] Servidor de Archivos

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[PI_HW] Servidor PI

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[BACKUP_HW] Servidor Copias de Seguridad

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[SPRINTER_HW] Servidor de Impresión

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[NVR_HW] Servidor de Grabación CCTV-NVR

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[STATION_HW] Estaciones de Trabajo

vandalismo, terrorismo, acción militar, ...

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[PRINTER_HW] Equipos de Impresión

vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[PROYECTOR_HW] Proyectores Salas de Reuniones
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[CAM_HW] Cámaras de Video Vigilancia
vandalismo, terrorismo, acción militar, ...
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[A.27] OCUPACIÓN ENEMIGA

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	P	M	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	P	M	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	P	M	-	-	-	-	-
[ZONA_ALM_I] Almacén	P	M	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	P	M	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	P	M	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	P	M	-	-	-	-	-
[ZONA_TALL_I] Talleres	P	M	-	-	-	-	-

[A.28] INDISPONIBILIDAD DEL PERSONAL

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	P	M	-	-	-	-	-
[ADM_P] Personal de administración y logístico	P	M	-	-	-	-	-
[JADM_P] Jefatura de administración	P	M	-	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	MR	B	-	-	-	-	-
[JUNI_P] Jefe de Unidad	P	M	-	-	-	-	-
[SYMA_P] Personal SyMA	P	M	-	-	-	-	-
[JSYMA_P] Jefatura SyMA	P	M	-	-	-	-	-
[TOP_P] Tópico	P	M	-	-	-	-	-
[OPE_P] Personal Operaciones	P	M	-	-	-	-	-
[JOPE_P] Jefatura de Operaciones	P	M	-	-	-	-	-
[CIV_P] Personal Ing. Civil	P	M	-	-	-	-	-
[SGI_P] Personal SGI	P	M	-	-	-	-	-
[CDOM_P] Coordinaciones O&M	P	M	-	-	-	-	-

[A.29] EXTORSIÓN

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	P	A	M	M	-	-	-
[ADM_P] Personal de administración y logístico	P	M	M	M	-	-	-
[JADM_P] Jefatura de administración	P	A	A	M	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	P	M	M	M	-	-	-
[JUNI_P] Jefe de Unidad	P	A	M	M	-	-	-
[SYMA_P] Personal SyMA	P	A	M	M	-	-	-
[JSYMA_P] Jefatura SyMA	P	A	M	M	-	-	-
[TOP_P] Tópico	P	A	M	M	-	-	-
[OPE_P] Personal Operaciones	P	A	M	M	-	-	-
[JOPE_P] Jefatura de Operaciones	P	A	M	M	-	-	-
[CIV_P] Personal Ing. Civil	P	A	M	M	-	-	-
[SGI_P] Personal SGI	P	A	M	M	-	-	-

[CDOM_P] Coordinaciones O&M	P	A	M	M	-	-	-

[A.30] INGENIERÍA SOCIAL (PICARESCA)

Activo	***Probabilidad***	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	P	A	A	A	-	-	-
[ADM_P] Personal de administración y logístico	P	A	A	A	-	-	-
[JADM_P] Jefatura de administración	P	A	A	A	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	P	A	A	A	-	-	-
[JUNI_P] Jefe de Unidad	P	A	A	A	-	-	-
[SYMA_P] Personal SyMA	P	A	A	A	-	-	-
[JSYMA_P] Jefatura SyMA	P	A	A	A	-	-	-
[TOP_P] Tópico	P	A	A	A	-	-	-
[OPE_P] Personal Operaciones	P	A	A	A	-	-	-
[JOPE_P] Jefatura de Operaciones	P	A	A	A	-	-	-
[CIV_P] Personal Ing. Civil	P	A	A	A	-	-	-
[SGI_P] Personal SGI	P	A	A	A	-	-	-
[CDOM_P] Coordinaciones O&M	P	A	A	A	-	-	-

ANEXO N° 06: IDENTIFICACIÓN Y EVALUACIÓN DE LAS SALVAGUARDAS

Evaluación de las Salvaguardas

Proyecto: [01] UPH. Carhuaquero

1. DATOS DEL PROYECTO

PROYECTO	UPH. Carhuaquero
DESCRIPCIÓN	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN	ORAZUL ENERGY PERU S.A.
VERSIÓN	1
FECHA	1/11/2017
BIBLIOTECA	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. NIVELES DE MADUREZ

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 – optimizado

4. DOMINIOS DE SEGURIDAD

- [base] Base

5. FASES DEL PROYECTO

- [Current] situación actual
- [Target] situación objetivo
- [PILAR] recomendación

6. DOMINIO DE SEGURIDAD: [BASE] BASE

[IA] IDENTIFICACIÓN Y AUTENTICACIÓN

Salvaguarda	R	[current]	[target]	[pilar]
[IA] Identificación y autenticación	8	L2	L3	L2-L5
[IA.1] Se dispone de normativa de identificación y autenticación	3	L2	L3	L3
[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación	3	L2	L3	L3
[IA.3] Identificación de los usuarios	5	L2	L3	L3
[IA.4] Gestión de la identificación y autenticación de usuario	5	L2	L3	L2-L3
[IA.4.1] Se mantiene un registro de todos los usuarios con su identificador	2	L2	L3	L2
[IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario	5	L2	L3	L2-L3
[IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticado	4	L2	L3	L3
[IA.4.4] Se limita el número de autenticadores necesarios por usuario	3	L2	L3	L3

[IA.4.5] Los autenticadores se distribuyen de forma segura	3	L2	L3	L3
[IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticado	2	L2	L3	L2
[IA.4.7] El usuario confirma la recepción del autenticado	2	L2	L3	L2
[IA.4.8] El usuario se hace cargo personalmente del control del autenticado	2	L2	L3	L2
[IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)	2	L2	L3	L2
[IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello	5	L2	L3	L3
[IA.5] Cuentas especiales (administración)	5	L2	L3	L2-L3
[IA.6] Canal seguro de autenticación	6	L2	L3	L4
[IA.7] {xor} Factores de autenticación que se requieren:	8	L2	L3	L3-L5
[IA.7.1] Algo que se tiene - token físico (ej. tarjeta)	6 (u)	L2	L3	L3-L4
[IA.7.2] Algo que se conoce (ej. contraseña)	7 (u)			L3-L4
[IA.7.3] Certificados software (criptografía de clave pública)	8			L3-L5
[IA.7.4] Algo que se es - biometría (ej. huella dactilar)	8			L3-L5
[IA.7.5] 2 factores: token + contraseña	8			L3-L5
[IA.7.6] 2 factores: token + certificados	8			L3-L5
[IA.7.7] 2 factores: contraseña de un solo uso (OTP) con token	8			L3-L5
[IA.7.8] 2 factores: contraseña de un solo uso (OTP) por canal separado	8			L4-L5
[IA.7.9] 2 factores: biometría + contraseña	8			L3-L5
[IA.7.a] 3 factores: biometría + token + contraseña	8 (o)			L3-L5

[AC] CONTROL DE ACCESO LÓGICO

Salvaguarda	R	[current]	[target]	[pilar]
[AC] Control de acceso lógico	7	L2	L2-L3	L2-L4
[AC.1] Gestión de privilegios	5	L2	L2	L2-L3
[AC.2] Imposición del control de acceso	5	L2	L2	L2-L3
[AC.2.1] Restricción de acceso a la información	4	L2	L2	L3
[AC.2.2] Se restringe el uso de las utilidades del sistema	3	L2	L2	L2-L3
[AC.2.5] Se controla el trabajo fuera del horario normal	4	L2	L2	L2-L3
[AC.2.6] {xor} Modelo de control de acceso	5	L2	L2	L3
[AC.2.7] Conexión en terminales (logon)	5	L2	L2	L2-L3
[AC.2.8] Se limita el tiempo de conexión	3	L2	L2	L3
[AC.2.9] Se limita el número de sesiones concurrentes de un usuario	4	L2	L2	L3
[AC.2.a] Equipo informático de usuario desatendido	5	L2	L2	L3
[AC.2.b] Los terminales se desconectan automáticamente	5	L2	L2	L3
[H.ST] Segregación de tareas	7	L2	L3	L2-L4
[H.ST.1] Se separan las responsabilidades de administración y operación	7	L2	L3	L4
[H.ST.2] Todos los procesos críticos requieren al menos 2 personas	5	L2	L3	L3
[H.ST.3] Se definen roles con autorización exclusiva para realizar tareas	4	L2	L3	L2-L3
[H.ST.4] Se controla la efectividad de la estructura de segregación	4	L2	L3	L2-L3

[D] PROTECCIÓN DE LA INFORMACIÓN

Salvaguarda	R	[current]	[target]	[pilar]
[D] Protección de la Información	6	_-L2	_-L3	L2-L4
[D.1] Se dispone de un inventario de activos de información	4	L2	L3	L3
[D.2] Normativa	3	_-L2	_-L3	L2-L3
[D.2.1] Se clasifica la información	3	L2	L2	L2-L3
[D.2.2] Atributos de seguridad	3			L3
[D.2.3] Los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales	2			L2
[D.2.4] IPR: Se protegen los derechos de propiedad intelectual de la información	2			L2
[D.2.5] Se dispone de normativa de retención de datos	3	L1	L3	L3
[D.I] Protección de la integridad	5			L3

[D.4] Protección de la confidencialidad	4	_-L2	_-L2	L2-L3
[D.C] Cifrado de la información	3	L1-L2	L2	L2-L3
[D.C.1] Se dispone de normativa relativa al uso de cifra	2	L2	L2	L2
[D.C.2] Se dispone de procedimientos relativos al cifrado de información	2	L2	L2	L2
[D.C.3] Se han designado responsables	2	L1	L2	L2
[D.C.4] Mecanismo de cifrado	3	L2	L2	L3
[D.4.2] Limpieza de documentos publicados	4			L3
[D.4.3] Marcado de la información	3 (o)			L3
[D.backup] Copias de seguridad (backups)	4	L1-L2	L2-L3	L3
[D.backup.1] Protección de la información	4	L1	L2	L3
[D.backup.1.1] Las copias de seguridad se protegen de acuerdo a la información que contienen	4	L1	L2	L3
[D.backup.1.2] Se cifran las copias de seguridad	3	L1	L2	L3
[D.backup.1.3] El acceso a las copias de seguridad requiere autorización previa	3	L1	L2	L3
[D.backup.2] Protección de la disponibilidad de la información		L2	L2-L3	
[D.backup.2.1] Se dispone de normativa relativa a copias de seguridad (backup)		L2	L3	
[D.backup.2.2] Se dispone de procedimientos para las tareas de realización de copias de seguridad (backup), su protección y su conservación		L2	L2	
[D.backup.2.3] Gestión de las copias de seguridad de los datos (backup)		L2	L2	
[D.backup.2.3.1] Se hacen copias de la información en consonancia con sus requisitos de disponibilidad		L2	L2	
[D.backup.2.3.2] Se hacen copias de las claves para descifrar		L2	L2	
[D.backup.2.3.3] Se hacen copias de la información de verificación de firmas		L2	L2	
[D.backup.2.3.4] Las copias de seguridad, y los procedimientos, se almacenan en lugares diferentes de tal forma que los datos originales y las copias no se vean afectados simultáneamente por un incidente		L2	L2	
[D.backup.2.3.5] Periódicamente, se verifican las copias de seguridad		L2	L2	
[D.backup.2.3.6] Periódicamente, se prueban los procedimientos de restauración		L2	L2	
[D.backup.2.4] {xor} Mecanismo de backup		L2	L3	
[D.DS] Uso de firmas electrónicas	6			L2-L4
[D.DS.1] Se dispone de normativa sobre firma electrónica	2			L2
[D.DS.2] Se dispone de procedimientos para las tareas relacionadas con el empleo de firmas electrónicas	2			L2
[D.DS.3] Se han designado responsables	2			L2
[D.DS.4] Se garantiza la eficacia probatoria de la firma	3			L3
[D.DS.5] {xor} Certificados electrónicos	5			L3
[D.DS.6] {xor} Implantación de los algoritmos	5			L3
[D.DS.7] {xor} Mecanismo de firma electrónica	6			L4
[D.DS.8] Se revisan regularmente las vulnerabilidades de los algoritmos	3			L3
[D.DS.9] Se emplean algoritmos certificados / acreditados	4			L3
[D.DS.a] Se emplean productos o servicios certificados o acreditados	5			L3

[K] PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Salvaguarda	R	[current]	[target]	[pilar]
[K] Protección de claves criptográficas		L2	L3	
[K.comms] Protección de claves de comunicaciones		L2	L3	
[K.comms.1] Se dispone de normativa de gestión de claves		L2	L3	
[K.comms.2] Se dispone de procedimientos de gestión de claves		L2	L3	
[K.comms.3] Se identifican las personas responsables de cada clave		L2	L3	
[K.comms.4] Operación		L2	L3	
[K.comms.5] Las claves se generan en un entorno separado del de explotación		L2	L3	
[K.comms.6] {xor} Generación de claves		L2	L3	
[K.comms.7] {xor} Distribución de claves		L2	L3	
[K.comms.8] {xor} Almacenamiento de las claves		L2	L3	

[K.comms.9] Las claves se destruyen de forma segura		L2	L3	
[K.comms.a] Se retienen copias de las claves		L2	L3	

[S] PROTECCIÓN DE LOS SERVICIOS

Salvaguarda	R	[current]	[target]	[pilar]
[S] Protección de los Servicios	6	_-L3	_-L3	L2-L4
[S.1] Prestación de los servicios	6	_-L2	_-L3	L2-L4
[S.1.1] Se dispone de normativa relativa al uso de los servicios	2			L2
[S.1.2] Se dispone de un inventario de servicios	2			L2
[S.cont] Aseguramiento de la disponibilidad	5			L2-L3
[S.cont.1] Protección frente a ataques de denegación de servicio (DoS)	5			L2-L3
[S.cont.2] Gestión de recursos	5			L3
[S.SC] Se aplican perfiles de seguridad	6	L2	L3	L3-L4
[S.op] Explotación	5			L3
[S.op.1] Se realizan análisis periódicos de vulnerabilidades	4			L3
[S.op.2] Se detectan casos de intrusión en el servicio	4			L3
[S.op.3] Prevención del repudio	5			L3
[S.op.4] El personal recibe formación específica en configuración de servicios	3			L3
[S.CM] Gestión de cambios (mejoras y sustituciones)	3	L2	L3	L2-L3
[S.CM.1] Se dispone de normativa de control de cambios	2	L2	L3	L2
[S.CM.2] Se designan responsables	2	L2	L3	L2
[S.CM.3] Se dispone de procedimientos para ejecutar cambios	2	L2	L3	L2
[S.CM.4] Se hace un seguimiento permanente (servicios externos)	3	L2	L3	L3
[S.CM.5] Evaluación del impacto potencial del cambio	3	L2	L3	L2-L3
[S.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	3	L2	L3	L3
[S.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	3	L2	L3	L3
[S.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	3	L2	L3	L3
[S.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	2	L2	L3	L2
[S.CM.a] Se realiza por personal debidamente autorizado	3	L2	L3	L3
[S.CM.b] Se realizan pruebas de regresión	2	L2	L3	L2
[S.CM.c] Se registran las actualizaciones de servicios	2	L2	L3	L2
[S.CM.d] Documentación	2	L2	L3	L2
[S.CM.e] Se actualizan todos los procedimientos de producción afectados	2	L2	L3	L2
[S.CM.f] Se actualizan todos los procedimientos de recuperación afectados	2	L2	L3	L2
[S.end] Desmantelamiento	4			L2-L3
[S.email] Protección del correo electrónico	5			L2-L3
[S.email.1] Se establece el responsable de la administración del servicio	2			L2
[S.email.2] Se registra el uso del servicio	3			L3
[S.email.3] Protección de la configuración	3			L3
[S.email.4] Medidas anti-spam	3			L3
[S.email.5] Medidas frente a código dañino en el servidor	3			L3
[S.email.6] Servicios de no repudio	5			L3
[S.email.7] {xor} Se asegura la disponibilidad del servicio según política	4			L3
[S.1.a] Seguridad del comercio electrónico	4			L2-L3
[S.1.a.1] Se tienen en cuenta los requisitos	2			L2
[S.1.a.2] Redacción y aprobación de un documento que consigne los términos acordados entre las partes	2			L2
[S.1.a.3] Controles sobre el desarrollo del proceso (fijación de precios, contratación, etc.)	3			L3
[S.1.a.4] Implantación de mecanismos de autenticación de las partes	4			L3
[S.1.a.5] Establecimiento de mecanismos de autorización del proceso	3			L3
[S.1.a.6] Se dispone de un registro de actividades	3			L3
[S.voip] Voz sobre IP	4			L2-L3
[S.voip.1] Se requiere autorización previa para el uso de VoIP	2			L2
[S.voip.2] Se monitoriza el uso de VoIP	2			L2
[S.voip.3] Se separan redes LAN para voz y datos (VLAN)	3			L3

[S.voip.4] Autenticación entre dispositivos	4			L3
[S.voip.5] Protección criptográfica	4			L2-L3
[S.voip.5.1] Se dispone de normativa relativa al uso de los controles criptográficos	2			L2
[S.voip.5.2] Se han designado responsables	2			L2
[S.voip.5.3] {xor} Mecanismo de cifrado	4			L3
[S.voip.5.4] Se revisan regularmente las vulnerabilidades de los algoritmos	2			L2
[S.voip.5.5] Se emplean algoritmos certificados / acreditados	3			L3
[S.2] Servicios subcontratados	6	_-L3	_-L3	L2-L4
[S.2.1] Aspectos generales	2			L2
[S.2.1.1] Se dispone de un registro de servicios subcontratados	2			L2
[S.2.1.2] Se requiere aprobación previa para el uso de servicios externos	2			L2
[S.2.1.3] Se identifican las aplicaciones sensibles o críticas que debe retener la Organización	2			L2
[S.2.1.4] Se identifican los riesgos derivados de depender de un proveedor externo	2			L2
[S.2.2] Contratos de prestación de servicios	3			L2-L3
[S.2.2.1] Se define la política aplicable sobre seguridad de la información	2			L2
[S.2.2.2] Constan las obligaciones de todas las partes	2			L2
[S.2.2.3] Se incluyen los requisitos de seguridad	3			L2-L3
[S.2.2.4] Se define, y se incorpora al contrato el procedimiento para medir el cumplimiento de las medidas de seguridad	2			L2
[S.2.2.5] IPR: Se contemplan los temas relativos a propiedad intelectual	2			L2
[S.2.2.6] Se contempla la protección de la información de carácter personal	2			L2
[S.2.2.7] Se establecen los términos para la implicación de terceros (subcontratistas)	2			L2
[S.2.2.8] Se describen los servicios disponibles	2			L2
[S.2.2.9] Se definen las responsabilidades sobre instalación y mantenimiento de HW y SW	2			L2
[S.2.2.a] Se definen las responsabilidades en la supervisión del cumplimiento del contrato	3			L3
[S.2.3] Operación	6			L2-L4
[S.2.4] Gestión de cambios	2			L2
[S.2.5] Autenticación del servidor	4			L2-L3
[S.2.5.1] Se autentica el servidor antes de transferir información alguna	4			L3
[S.2.5.2] {xor} Mecanismo de autenticación	3			L3
[S.2.5.2.1] Secreto compartido	3			L3
[S.2.5.2.2] Criptografía: firma digital	3			L3
[S.2.5.3] Protección de datos y software de autenticación	3			L2-L3
[S.2.5.3.1] {xor} Implementación del mecanismo	3			L3
[S.2.5.3.1.1] por programa (SW)	3			L3
[S.2.5.3.1.2] En dispositivo físico (token HW)	3			L2-L3
[S.2.5.3.2] Se protege el uso por medio de contraseña	1			L2
[S.2.5.3.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	3			L3
[S.2.5.3.4] Se usa un producto certificado o acreditado	3			L3
[S.2.5.4] Se toman medidas para impedir el secuestro de sesiones establecidas	3			L3
[S.2.6] Continuidad de operaciones	5	L3	L3	L3
[S.2.7] Desmantelamiento	4			L2-L3
[S.2.7.1] Se requiere autorización previa	2			L2
[S.2.7.2] Se estudia el impacto en el negocio	2			L2
[S.2.7.3] Se planifica de forma que minimice la interrupción del servicio	2			L2
[S.2.7.4] Destrucción de la información en el proveedor	4			L3
[S.2.7.5] Desactivación del servicio por personal autorizado	3			L3
[S.2.7.6] Se actualizan todos los procedimientos de producción afectados	2			L2
[S.2.7.7] Se actualizan todos los procedimientos de recuperación afectados	2			L2
[S.3] Los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales	3	L2	L3	L3

[SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS (SW)

Salvaguarda	R	[current]	[target]	[pilar]
[SW] Protección de las Aplicaciones Informáticas (SW)	7	L2	L3	L2-L4
[SW.1] Se dispone de un inventario de aplicaciones (SW)	3	L2	L3	L3
[SW.2] Se dispone de normativa relativa a las aplicaciones (SW)	2	L2	L3	L2
[SW.3] Se dispone de procedimientos de uso de las aplicaciones	2	L2	L3	L2
[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)	3	L2	L3	L2-L3
[SW.backup] Copias de seguridad (backup) (SW)	5	L2	L3	L2-L3
[SW.start] Puesta en producción	5	L2	L3	L2-L3
[SW.SC] Se aplican perfiles de seguridad	7	L2	L3	L3-L4
[SW.op] Explotación / Producción	5	L2	L3	L2-L3
[SW.op.1] Se dispone de normativa relativa al software en producción	2	L2	L3	L2
[SW.op.2] Los sistemas de producción no contienen herramientas de desarrollo	4	L2	L3	L3
[SW.op.3] {xor} Se controla la integridad del código ejecutable	4	L2	L3	L3
[SW.op.4] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	5	L2	L3	L3
[SW.op.5] Aislamiento de sistemas que manejen asuntos delicados	3	L2	L3	L2-L3
[SW.op.6] Seguridad de las aplicaciones	3	L2	L3	L2-L3
[SW.op.7] Seguridad de los ficheros de datos de la aplicación	5	L2	L3	L3
[SW.op.8] Se protegen los ficheros de configuración	5	L2	L3	L3
[SW.op.9] Se protegen los ficheros del sistema	5	L2	L3	L3
[SW.op.a] Se controla la ejecución de código móvil (ej. 'applets')	3	L2	L3	L2-L3
[SW.op.b] Ejecución de programas colaborativos (ej. teleconferencia)	3	L2	L3	L3
[SW.op.c] Seguridad de los mecanismos de comunicación entre procesos	5	L2	L3	L3
[SW.op.d] Regularmente se realiza un análisis de vulnerabilidades, y se actúa en consecuencia	3	L2	L3	L3
[SW.op.e] Formación del personal en configuración de aplicaciones	2	L2	L3	L2
[SW.CM] Cambios (actualizaciones y mantenimiento)	4	L2	L3	L2-L3
[SW.CM.1] Se dispone de una política	2	L2	L3	L2
[SW.CM.2] Se dispone de procedimientos para ejecutar cambios	2	L2	L3	L2
[SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches	3	L2	L3	L3
[SW.CM.4] Evaluación del impacto y riesgo residual tras el cambio	3	L2	L3	L2-L3
[SW.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	4	L2	L3	L3
[SW.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	3	L2	L3	L3
[SW.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	3	L2	L3	L3
[SW.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	3	L2	L3	L3
[SW.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	2	L2	L3	L2
[SW.CM.a] Control de versiones de toda actualización del software	3	L2	L3	L3
[SW.CM.b] Realización por personal debidamente autorizado	3	L2	L3	L3
[SW.CM.c] Se retienen copias de las versiones anteriores de software como medida de precaución para contingencias	4	L2	L3	L3
[SW.CM.d] Se retienen copias de las versiones anteriores de configuración	3	L2	L3	L3
[SW.CM.e] Se prueba previamente en un equipo que no esté en producción	3	L2	L3	L3
[SW.CM.f] Pruebas de regresión	3	L2	L3	L3
[SW.CM.g] Se registra toda actualización de SW	2	L2	L3	L2
[SW.CM.h] Documentación	2	L2	L3	L2
[SW.CM.i] Se actualizan todos los procedimientos de producción afectados	3	L2	L3	L3
[SW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	2	L2	L3	L2
[SW.end] Desmantelamiento	3	L2	L3	L3

[HW] Protección de los Equipos Informáticos (HW)

Salvaguarda	R	[current]	[target]	[pilar]
[HW] Protección de los Equipos Informáticos (HW)	7	L2	L3	L2-L4
[HW.1] Se dispone de un inventario de equipos (HW)	2	L2	L3	L2
[HW.2] Se dispone de normativa sobre el uso correcto de los equipos	2	L2	L3	L2
[HW.3] Se dispone de procedimientos de uso del equipamiento	2	L2	L3	L2
[HW.start] Puesta en producción	4	L2	L3	L2-L3
[HW.SC] Se aplican perfiles de seguridad	7	L2	L3	L3-L4
[HW.cont] Aseguramiento de la disponibilidad	6	L2	L3	L2-L4
[HW.cont.1] Se dimensiona holgadamente y se planifica la adquisición de repuestos	6	L2	L3	L4
[HW.cont.2] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	4	L2	L3	L3
[HW.cont.3] El mantenimiento lo realiza personal debidamente autorizado	4	L2	L3	L3
[HW.cont.4] Se ejecutan regularmente las rutinas de diagnóstico	3	L2	L3	L3
[HW.cont.5] Se monitorizan fallos e incidentes	3	L2	L3	L3
[HW.cont.6] Se registran los fallos, reales o sospechados y de mantenimiento preventivo y correctivo	3	L2	L3	L3
[HW.cont.7] Se hacen copias de seguridad de la configuración	5	L2	L3	L3
[HW.cont.8] Se hacen copias de seguridad de las claves de descifrado	3	L2	L3	L3
[HW.cont.9] {xor} Opciones sustitutorias	3	L2	L3	L3
[HW.cont.9.1] Equipo alternativo	3	L2	L3	L3
[HW.cont.9.2] Equipo alternativo preconfigurado con replicación de discos síncrona o asíncrona	3			L3
[HW.cont.9.3] Sistema redundante propio en centro alternativo	3			L3
[HW.cont.9.4] Contrato de prestación de servicio con el proveedor del sistema, de acuerdo a los requisitos del negocio	3			L3
[HW.cont.a] {xor} Alta disponibilidad	5	L2	L3	L3
[HW.cont.b] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento	2	L2	L3	L2
[HW.7] Los medios alternativos están sujetos a las mismas garantías de protección que los habituales	3	L2	L3	L3
[HW.8] Contenedores criptográficos (HW, HW virtual)	6	L2	L3	L3-L4
[HW.9] {xor} Prevención de emanaciones electromagnéticas (TEMPEST equipment)	4	L2	L3	L3
[HW.a] Instalación	3	L2	L3	L3
[HW.op] Operación	5	L2	L3	L2-L3
[HW.op.1] Proceso de autorización de recursos para el tratamiento de la información	2	L2	L3	L2
[HW.op.2] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	5	L2	L3	L3
[HW.op.3] Protección física de los equipos	5	L2	L3	L3
[HW.op.4] Seguridad del equipamiento de oficina	3	L2	L3	L2-L3
[HW.op.5] Seguridad de los equipos fuera de las instalaciones	4	L2	L3	L2-L3
[HW.op.6] Protección de los dispositivos de red	5	L2	L3	L2-L3
[HW.op.8] Formación del personal en configuración de equipos	2	L2	L3	L2
[HW.CM] Cambios (actualizaciones y mantenimiento)	4	L2	L3	L2-L3
[HW.CM.1] Se dispone de una política	2	L2	L3	L2
[HW.CM.2] Se dispone de procedimientos para ejecutar cambios	2	L2	L3	L2
[HW.CM.3] Se siguen las recomendaciones del fabricante o proveedor	3	L2	L3	L3
[HW.CM.4] Se hace un seguimiento permanente de actualizaciones	3	L2	L3	L3
[HW.CM.5] Evaluación del impacto potencial del cambio	2	L2	L3	L2
[HW.CM.6] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	4	L2	L3	L3
[HW.CM.7] Se mantiene en todo momento la regla de 'funcionalidad mínima'	3	L2	L3	L3
[HW.CM.8] Se mantiene en todo momento la regla de 'seguridad por defecto'	3	L2	L3	L3
[HW.CM.9] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	3	L2	L3	L3
[HW.CM.a] Se planifica el cambio de forma que minimice la interrupción del servicio	2	L2	L3	L2
[HW.CM.b] Realización por personal debidamente autorizado	3	L2	L3	L3
[HW.CM.c] Se retienen copias de las versiones anteriores de configuración	3	L2	L3	L3
[HW.CM.d] Se prueba previamente en un entorno que no esté en producción	3	L2	L3	L3

[HW.CM.e] Pruebas de regresión	3	L2	L3	L3
[HW.CM.f] Todos los cambios quedan registrados	2	L2	L3	L2
[HW.CM.g] Documentación	2	L2	L3	L2
[HW.CM.h] Control de versiones de todo cambio de hw	2	L2	L3	L2
[HW.CM.i] Se actualizan todos los procedimientos de producción afectados	3	L2	L3	L3
[HW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	2	L2	L3	L2
[HW.end] Desmantelamiento	2	L2	L3	L2
[HW.PCD] Informática móvil	5	L2	L3	L2-L3
[HW.PCD.1] Se mantiene un inventario de equipos móviles con identificación del responsable de cada uno	2	L2	L3	L2
[HW.PCD.2] Se requiere autorización previa antes de poder usarlos	2	L2	L3	L2
[HW.PCD.3] Cada equipo se marca con el nivel máximo de información que puede almacenar o procesar	2	L2	L3	L2
[HW.PCD.4] Se han identificado los riesgos correspondientes	2	L2	L3	L2
[HW.PCD.5] Se han determinado las medidas y precauciones a tomar	3	L2	L3	L2-L3
[HW.PCD.6] Se sigue un plan de concienciación sobre los riesgos y las medidas pertinentes	2	L2	L3	L2
[HW.PCD.7] Se sigue un plan de formación sobre las medidas pertinentes	2	L2	L3	L2
[HW.PCD.8] Controles aplicables	5	L2	L3	L3
[HW.PCD.8.1] Se han determinado las medidas para la protección física del dispositivo	3	L2	L3	L3
[HW.PCD.8.2] Se instalan detectores de violación	3	L2	L3	L3
[HW.PCD.8.3] Se han establecido los requisitos sobre control de acceso	4	L2	L3	L3
[HW.PCD.8.4] Se utiliza un sistema de defensa perimetral (cortafuegos)	3	L2	L3	L3
[HW.PCD.8.5] Se han establecido los requisitos de cifrado	4	L2	L3	L3
[HW.PCD.8.6] Se han establecido los requisitos sobre copias de seguridad (backups)	5	L2	L3	L3
[HW.PCD.8.7] Se instala software antivirus y se mantiene actualizado	3	L2	L3	L3
[HW.PCD.9] Guías para los usuarios	2	L2	L3	L2
[HW.PCD.a] Gestión de incidentes en informática móvil	3	L2	L3	L2-L3
[HW.f] Máquinas virtuales	5	L2	L3	L2-L3
[HW.f.1] Creación de nuevas máquinas virtuales	2	L2	L3	L2
[HW.f.1.1] se requiere autorización previa	2	L2	L3	L2
[HW.f.1.2] se requiere un privilegio específico	2	L2	L3	L2
[HW.f.2] El equipo base de virtualización tiene como clasificación la más exigente de las clasificaciones de las máquinas virtuales que soporta	2	L2	L3	L2
[HW.f.3] Las máquinas virtuales se gestionan como si fueran máquinas reales	2	L2	L3	L2
[HW.f.3.1] Se mantiene la separación de funciones entre usuarios y administradores	2	L2	L3	L2
[HW.f.3.2] Configuración de seguridad	2	L2	L3	L2
[HW.f.3.3] Herramientas de seguridad	2	L2	L3	L2
[HW.f.3.4] Parches de seguridad	2	L2	L3	L2
[HW.f.3.5] Mantenimiento de los programas	2	L2	L3	L2
[HW.f.4] Las redes virtuales software entre máquinas virtuales se gestionan como si fueran redes reales	2	L2	L3	L2
[HW.f.4.1] Se requiere un privilegio específico para poder establecerlas	2	L2	L3	L2
[HW.f.4.2] Configuración de seguridad	2	L2	L3	L2
[HW.f.4.3] Herramientas de seguridad	2	L2	L3	L2
[HW.f.5] Se tiene en cuenta el impacto potencial de ataques de denegación de servicio a equipos virtualizados sobre la disponibilidad del sistema en su conjunto	5	L2	L3	L3
[HW.f.6] Se tiene en cuenta el impacto potencial de ataques a equipos virtuales sobre la resiliencia del sistema en su conjunto	5	L2	L3	L3
[HW.f.7] Se controla el hypervisor	3	L2	L3	L2-L3
[HW.f.7.1] Se controla el acceso al hypervisor	2	L2	L3	L2
[HW.f.7.2] Se controla el acceso a recursos compartidos	3	L2	L3	L3
[HW.f.8] Se controla el acceso a las imágenes de las máquinas virtuales	3	L2	L3	L3
[HW.f.9] Se protegen las copias de seguridad de las imágenes de las máquinas virtuales	3	L2	L3	L3
[HW.f.a] No se instalan sobre el mismo equipo anfitrión servidores y clientes virtuales	3	L2	L3	L3
[HW.f.b] No se instalan sobre el mismo equipo anfitrión servidores que requieren	3	L2	L3	L3

diferentes niveles de seguridad				
[HW.f.c] No se comparten placas físicas de red entre máquinas virtuales que requieren diferentes niveles de seguridad	3	L2	L3	L3
[HW.f.d] La red local (SAN) usada como soporte de virtualización, está aislada y sólo es accesible por la máquina anfitrión	3	L2	L3	L3
[HW.f.e] No se instalan sobre el mismo equipo anfitrión equipos de frontera y equipos internos (ej. cortafuegos, pasarelas, etc.)	4	L2	L3	L3
[HW.f.f] Retirada de servicio	3	L2	L3	L2-L3
[HW.f.f.1] Se registra la retirada del servicio	2	L2	L3	L2
[HW.f.f.2] {xor} Se aplican al soporte de la imagen virtual los mecanismos previstos para soportes de información	3	L2	L3	L3
[HW.print] Reproducción de documentos	3	L2	L3	L2-L3
[HW.print.1] Control de los dispositivos de reproducción (fotocopiadoras, fax, etc.)	3	L2	L3	L3
[HW.print.2] Asignación de cuentas de usuario	3	L2	L3	L3
[HW.print.3] Destrucción o borrado seguro de las partes de los dispositivos de reproducción que puedan contener información previamente a su sustitución	3	L2	L3	L3
[HW.print.4] Se requiere autorización previa para realizar copias, y numeración de las mismas	2	L2	L3	L2
[HW.print.5] Se registra y se revisa la actividad de los dispositivos de reproducción (número de copias, usuarios que las han realizado, etc.)	3	L2	L3	L3
[HW.i] Voz, facsímil y video	3	L2	L3	L2-L3
[HW.i.1] Está prohibido establecer de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección	3	L2	L3	L3
[HW.i.2] Está prohibido dejar mensajes confidenciales en contestadores automáticos	3	L2	L3	L3
[HW.i.3] Los usuarios están concienciados y reciben formación sobre el uso seguro de los sistemas y recursos disponibles	2	L2	L3	L2
[HW.i.4] Se controla el acceso a la memoria interna del equipo de fax	3	L2	L3	L3
[HW.i.5] Se prohíbe la programación no autorizada del equipo de fax	3	L2	L3	L3
[HW.i.6] Se previene el envío de documentos a números equivocados	3	L2	L3	L3

[COM] PROTECCIÓN DE LAS COMUNICACIONES

Salvaguarda	R	[current]	[target]	[pilar]
[COM] Protección de las Comunicaciones	9	L0-L3	L0-L3	L2-L5
[COM.1] Se dispone de un inventario de servicios de comunicación	2	L2	L2	L2
[COM.2] Se dispone de normativa sobre el uso correcto de las comunicaciones	3	L2	L2	L3
[COM.3] Se dispone de procedimientos de uso de las comunicaciones	3	L0	L0	L3
[COM.start] Entrada en servicio	5	L2	L3	L2-L3
[COM.SC] Se aplican perfiles de seguridad	9	L2	L2-L3	L3-L5
[COM.cont] Aseguramiento de la disponibilidad	6	L1-L3	L2-L3	L2-L4
[COM.cont.1] Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	6	L2	L3	L4
[COM.cont.2] Se dimensiona holgadamente y se planifica la adquisición de repuestos	5	L2	L3	L3
[COM.cont.3] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	5	L2	L2	L3
[COM.cont.4] Se monitorizan enlaces y dispositivos de red	5	L3	L3	L3
[COM.cont.5] Se registran los fallos detectados, sean reales o sospechados	3	L2	L3	L3
[COM.cont.6] Se registran las actuaciones de mantenimiento preventivo y correctivo	3	L2	L3	L3
[COM.cont.7] Se realizan copias de seguridad de la configuración (backup)	4	L2	L3	L3
[COM.cont.8] Se hacen copias de seguridad de las claves de autenticación	4	L2	L3	L3
[COM.cont.9] Se hacen copias de seguridad de las claves de descifrado	4	L2	L3	L3
[COM.cont.a] {xor} Redundancia	4	L1	L3	L3
[COM.cont.b] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento	2	L2	L3	L2
[COM.7] Los medios alternativos están sujetos a las mismas garantías de protección que los habituales	3	L2	L3	L3
[COM.aut] Autenticación del canal	5	L2	L2	L2-L3

[COM.aut.1] Se requiere autorización previa	2	L2	L2	L2
[COM.aut.2] Se verifica la identidad del usuario antes de entregarle el mecanismo de autenticación	3	L2	L2	L3
[COM.aut.3] Se autentica el origen de la conexión	3	L2	L2	L3
[COM.aut.4] Se autentica el destino de la conexión	3	L2	L2	L3
[COM.aut.5] {xor} Mecanismo de autenticación	5	L2	L2	L3
[COM.aut.5.1] Algo que se conoce (ej. contraseña)	5	L2	L2	L3
[COM.aut.5.2] Certificados software (criptografía de clave pública)	5			L3
[COM.aut.5.3] 2 factores: token + contraseña	5			L2-L3
[COM.aut.5.4] 2 factores: token + certificados	5			L3
[COM.aut.5.5] 2 factores: contraseña de un solo uso (OTP) con token	5			L3
[COM.aut.5.6] 2 factores: contraseña de un solo uso (OTP) por canal separado	5			L3
[COM.aut.6] Canal de autenticación	4	L2	L2	L3
[COM.aut.7] Se toman medidas para impedir el secuestro de sesiones establecidas	3	L2	L2	L3
[COM.I] {xor} Protección de la integridad de los datos intercambiados	6	L2	L3	L4
[COM.a] Se toman medidas frente a la inyección de información espuria	6	L2	L2	L4
[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados	5	L2	L3	L3
[COM.C.1] Se dispone de normativa relativa al uso de controles criptográficos	4	L2	L3	L3
[COM.C.2] Se han designado responsables	4	L2	L3	L3
[COM.C.3] {xor} Implantación de los algoritmos	4	L2	L3	L3
[COM.C.4] {xor} Mecanismo de cifrado (secreto compartido o cifra simétrica)	4	L2	L3	L3
[COM.C.5] Se revisan regularmente las vulnerabilidades de los algoritmos	5	L2	L3	L3
[COM.C.6] Se emplean algoritmos certificados / acreditados	5	L2	L3	L3
[COM.C.7] Se emplean productos o servicios certificados o acreditados	5	L2	L3	L3
[COM.op] Operación	5	L2	L2	L2-L3
[COM.op.1] Control de acceso a la red	5	L2	L2	L2-L3
[COM.op.1.1] Se dispone de normativa de uso de los servicios de red	2	L2	L2	L2
[COM.op.1.2] Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios	2	L2	L2	L2
[COM.op.1.3] Acceso remoto	4	L2	L2	L2-L3
[COM.op.1.4] {xor} Protección de los puertos de diagnóstico remoto	5	L2	L2	L2-L3
[COM.op.1.5] Autenticación de nodos de la red	5	L2	L2	L3
[COM.op.1.6] Control del encaminamiento	3	L2	L2	L3
[COM.op.2] Seguridad de los servicios de red	4	L2	L2	L3
[COM.op.2.1] Se monitorizan los servicios de red	3	L2	L2	L3
[COM.op.2.2] Revisiones periódicas de la seguridad	4	L2	L2	L3
[COM.op.3] Se prevé protección frente a análisis del tráfico	3	L2	L2	L3
[COM.op.4] Formación del personal en configuración de las comunicaciones	3	L2	L2	L3
[COM.CM] Cambios (actualizaciones y mantenimiento)	5	L2-L3	L3	L2-L3
[COM.CM.1] Se dispone de una política	2	L3	L3	L2
[COM.CM.2] Se dispone de procedimientos para ejecutar cambios	2	L2	L3	L2
[COM.CM.3] Se hace un seguimiento permanente de actualizaciones	3	L2	L3	L3
[COM.CM.4] Evaluación del impacto y riesgo residual tras el cambio	3	L2	L3	L2-L3
[COM.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	5	L2	L3	L3
[COM.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	3	L2	L3	L3
[COM.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	3	L2	L3	L3
[COM.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	3	L3	L3	L3
[COM.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	3	L2	L3	L3
[COM.CM.a] Realización por personal debidamente autorizado	4	L2	L3	L3
[COM.CM.b] Se retienen copias de las versiones anteriores de configuración	3	L2	L3	L3
[COM.CM.c] Se prueba previamente en un entorno que no esté en producción	4	L2	L3	L3
[COM.CM.d] Pruebas de regresión	4	L2	L3	L3
[COM.CM.e] Todas las actuaciones quedan registradas	3	L2	L3	L3
[COM.CM.f] Documentación	2	L2	L3	L2
[COM.CM.g] Se actualizan todos los procedimientos de producción afectados	3	L2	L3	L3
[COM.CM.h] Se actualizan todos los procedimientos de recuperación afectados	3	L2	L3	L3

[COM.end] Desmantelamiento	3	L2	L2	L3
[COM.wifi] Seguridad Wireless (WiFi)	7	L2	L2	L3-L4
[COM.wifi.1] Se requiere autorización previa para desplegar puntos de acceso (AP)	3	L2	L2	L3
[COM.wifi.2] Al instalar un punto de acceso (AP) se tiene en cuenta el alcance de la señal para evitar una exposición gratuíta a ataques	3	L2	L2	L3
[COM.wifi.3] Se requiere autorización previa para la conexión de clientes	3	L2	L2	L3
[COM.wifi.4] Se eliminan las claves por defecto en tarjetas y puntos de accesos antes de su despliegue	7	L2	L2	L4
[COM.wifi.5] Se desactivan los puertos y servicios no usados	4	L2	L2	L3
[COM.wifi.6] Se deshabilitan los protocolos de gestión no esenciales	7	L2	L2	L4
[COM.wifi.7] Se aplican restricciones al protocolo SNMP en redes wireless	4	L2	L2	L3
[COM.wifi.8] Se comprueban periódicamente los puntos de acceso (mediante broadcast o herramientas)	4	L2	L2	L3
[COM.wifi.9] Se desactiva el modo de conexión ad-hoc en los dispositivos de usuario	4	L2	L2	L3
[COM.wifi.a] Se autentican los dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)	5	L2	L2	L3
[COM.wifi.b] Se controlan las direcciones IP	4	L2	L2	L3
[COM.DS] Segregación de las redes en dominios	6	L2	L2	L3-L4
[COM.i] Redes privadas virtuales	6	L2	L2	L3-L4
[COM.i.1] Configuración segura	4	L2	L2	L3
[COM.i.1.1] se eliminan los servicios que no se utilizan	4	L2	L2	L3
[COM.i.1.2] se eliminan las cuentas por defecto	4	L2	L2	L3
[COM.i.1.3] se elimina el software que no se utiliza	4	L2	L2	L3
[COM.i.1.4] se configuran parámetros aprobados	4	L2	L2	L3
[COM.i.1.5] se activa el registro de la actividad	4	L2	L2	L3
[COM.i.1.6] la configuración se revisa regularmente y cuando hay cambios (nuevas versiones y parches de seguridad)	4	L2	L2	L3
[COM.i.2] Autenticación del canal	4	L2	L2	L3
[COM.i.2.1] no se incluyen contraseñas en ningún procedimiento automático de establecimiento de acceso	4	L2	L2	L3
[COM.i.2.2] los sistemas interconectados (sean fijos o móviles) se autentican mutuamente	4	L2	L2	L3
[COM.i.2.3] la red local se autentica usando un certificado software	4	L2	L2	L3
[COM.i.2.4] la autenticación utiliza mecanismos criptográficos y parámetros aprobados	4	L2	L2	L3
[COM.i.3] Cifrado del canal – Protección de la confidencialidad	4	L2	L2	L3
[COM.i.3.1] se emplean algoritmos criptográficos y parámetros aprobados	4	L2	L2	L3
[COM.i.3.2] las LAN fijas usan dispositivos hardware de cifra	4	L2	L2	L3
[COM.i.4] Protección de la integridad de los datos	6	L2	L2	L4
[COM.i.5] Cuando se cierra la sesión a través del canal virtual, también se cierra la sesión de usuario en el lado servidor	5	L2	L2	L3

[IP] SISTEMA DE PROTECCIÓN DE FRONTERA LÓGICA

Salvaguarda	R	[current]	[target]	[pilar]
[IP] Sistema de protección de frontera lógica		L2	L3	
[IP.BS] Protección de los equipos de frontera		L2	L3	
[IP.BS.2] Se aplican perfiles de seguridad		L2	L3	

[AUX] ELEMENTOS AUXILIARES

Salvaguarda	R	[current]	[target]	[pilar]
[AUX] Elementos Auxiliares	6	_-L3	_-L3	L2-L4
[AUX.1] Se dispone de un inventario de equipamiento auxiliar	3			L3
[AUX.cont] Aseguramiento de la disponibilidad	5			L3
[AUX.cont.1] Se siguen las recomendaciones del fabricante o proveedor	5			L3
[AUX.cont.2] Continuidad de operaciones	5			L3
[AUX.start] Instalación	5			L3
[AUX.power] Suministro eléctrico	5	L2	L2	L2-L3

[AUX.power.1] Se dimensiona el sistema considerando necesidades futuras	3	L2	L2	L3
[AUX.power.2] Instalación de acuerdo a la normativa vigente	2	L2	L2	L2
[AUX.power.3] Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas	4	L2	L2	L3
[AUX.power.4] Interruptor general de la alimentación del sistema situado en la entrada de cada área	3	L2	L2	L3
[AUX.power.5] Interruptores etiquetados y protegidos frente a activaciones accidentales	3	L2	L2	L3
[AUX.power.6] Alimentación de respaldo	5	L2	L2	L2-L3
[AUX.AC] Climatización	5	L0-L3	L2-L3	L3
[AUX.wires] Protección del cableado	6	L2	L3	L3-L4
[AUX.7] Se disponen medidas frente a posibles robos	5			L3
[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos	5			L3

[L] PROTECCIÓN DE LAS INSTALACIONES

Salvaguarda	R	[current]	[target]	[pilar]
[L] Protección de las Instalaciones	7	_-L4	_-L4	L2-L4
[L.1] Se dispone de normativa de seguridad	2	L2	L3	L2
[L.2] Se dispone de un inventario de instalaciones	4			L2-L3
[L.3] Entrada en servicio	4			L2-L3
[L.3.1] Se dispone de normativa de entrada en servicio	2			L2
[L.3.2] Se requiere autorización previa	2			L2
[L.3.3] Se han determinado las acreditaciones o certificaciones pertinentes	4			L3
[L.3.4] Se requiere haber pasado las inspecciones o acreditaciones establecidas	3			L3
[L.3.5] Plan de Protección	4			L2-L3
[L.3.5.1] Se dispone de un Plan de Acondicionamiento	3			L3
[L.3.5.2] Se dispone de un Plan de Seguridad	3			L3
[L.3.5.3] Plan de Emergencia	4			L2-L3
[L.3.5.3.1] Plan de Evacuación	3			L2-L3
[L.3.5.3.2] Plan de Comunicación	3			L3
[L.3.5.3.3] Acceso físico a las instalaciones en caso de emergencia	4			L2-L3
[L.3.5.3.4] Existe un plan de emergencia para hacer frente a la violencia	3			L3
[L.design] Diseño	5	L0-L2	L2-L3	L3
[L.design.1] El diseño atiende a las reglas y normas relevantes sobre salud y sanidad	3	L2	L3	L3
[L.design.3] Se encuentran separadas las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.)	5	L2	L2	L3
[L.design.4] Almacenes	3	L2	L3	L3
[L.design.4.1] los almacenes siempre están vigilados mientras permanecen abiertos	3	L2	L3	L3
[L.design.5] ventilación	3	L0	L2	L3
[L.design.5.1] Hay filtros en los conductos HVAC	3	L0	L2	L3
[L.design.5.2] Hay detectores y filtros de ántrax	3	L0	L2	L3
[L.design.5.3] Hay detectores de sustancias químicas peligrosas	3	L0	L2	L3
[L.6] Protección frente a desastres	7	_-L4	_-L4	L2-L4
[L.6.1] La iluminación de emergencia cubre todas las áreas necesarias para garantizar la continuidad de las misiones críticas	5			L3
[L.6.2] Protección frente a Incendios	6			L2-L4
[L.6.3] Protección frente a inundaciones	7	_-L4	_-L4	L3-L4
[L.6.4] Protección frente a accidentes naturales e industriales	6			L3-L4
[L.6.5] Protección frente a contaminación medioambiental	5			L3
[L.6.6] Se ha previsto protección frente a contaminación electromagnética	5			L3
[L.6.7] Protección frente a explosivos	5			L3
[L.6.8] Eliminación residuos	4			L3
[L.6.8.1] el sitio cuenta con un programa de recuperación y reciclaje de residuos	4			L3
[L.6.8.2] Se puede cerrar los contenedores de basura por la noche	4			L3
[L.6.9] Seguros	4			L3
[L.cont] Continuidad de operaciones	5	L2-L3	L3	L3
[L.cont.1] Se analizan las implicaciones para la continuidad del negocio	4	L2	L3	L3

[L.cont.2] Se establece un protocolo de actuación en caso de contingencia	4	L3	L3	L3
[L.cont.3] Se dispone de instalaciones alternativas	5	L2	L3	L3
[L.cont.4] Las instalaciones alternativas están sujetas a las mismas garantías de protección que las habituales	4	L2	L3	L3
[L.cont.5] El sitio cuenta con un plan para hacer frente a cualquier ataque repentino o sin previo aviso	5	L2	L3	L3

[PS] GESTIÓN DEL PERSONAL

Salvaguarda	R	[current]	[target]	[pilar]
[PS] Gestión del Personal	6	_-L4	_-L4	L2-L4
[PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)	3	L2	L3	L3
[PS.2] Se dispone de procedimientos para la gestión de personal (en materia de seguridad)	3	L2	L3	L3
[PS.3] Relación de personal	3			L3
[PS.4] Puestos de trabajo	3	_-L2	_-L3	L2-L3
[PS.4.1] Se dispone de un inventario de puestos de trabajo	2			L2
[PS.4.2] Se especifican las funciones de los puestos de trabajo	2			L2
[PS.4.3] Se han determinado las responsabilidades en materia de seguridad de los puestos de trabajo	3			L3
[PS.4.4] Se tienen en cuenta los requisitos de seguridad de los puestos de trabajo	3			L3
[PS.4.5] Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo	3	L2	L3	L2-L3
[PS.4.6] Se mide el desempeño efectivo, en materia de seguridad, del personal asignado al puesto	3			L3
[PS.4.7] Se revisa periódicamente la especificación del puesto	2			L2
[PS.5] Contratación	6	_-L1	_-L1	L2-L4
[PS.5.1] Se dispone de normativa para la contratación de personal	3			L3
[PS.5.2] Se dispone de procedimientos para la contratación de personal	3			L3
[PS.5.3] Selección de personal	5			L3
[PS.5.4] Términos y condiciones de la relación laboral	3	_-L1	_-L1	L2-L3
[PS.5.4.1] Inclusión del ámbito, el alcance y el periodo de las responsabilidades en materia de seguridad	2	L1	L1	L2
[PS.5.4.2] Inclusión de obligaciones y derechos legales de ambas partes	2			L2
[PS.5.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente	2			L2
[PS.5.4.4] Acuerdos de confidencialidad	3			L2-L3
[PS.5.4.5] Procedimiento disciplinario	3			L2-L3
[PS.5.5] Finalización de la relación laboral	6			L2-L4
[PS.6] Cambio de puesto de trabajo	3			L3
[PS.AT] Formación y concienciación	3	L1	L1	L2-L3
[PS.8] Procedimientos de prevención y reacción	6	L2-L4	L3-L4	L4
[PS.8.2] frente a Phishing	6	L2	L3	L4
[PS.8.3] frente a extorsión	6	L4	L4	L4
[PS.8.4] frente a ataques de ingeniería social	6	L3	L3	L4
[PS.9] Protección del usuario frente a coacciones	5			L3
[S.cont] Aseguramiento de la disponibilidad	4	L1-L2	L3	L2-L3
[PS.cont.1] Se prevé suficiente holgura en el dimensionamiento de los equipos de trabajo	3	L2	L3	L3
[PS.cont.2] Se monitorizan continuamente los incidentes de disponibilidad de personal	3	L1	L3	L3
[PS.cont.3] Redundancia	4	L2	L3	L3
[PS.cont.4] El personal alternativo está sujeto a las mismas garantías de seguridad que el habitual	2	L2	L3	L2

[PDS] SERVICIOS POTENCIALMENTE PELIGROSOS

Salvaguarda	R	[current]	[target]	[pilar]
[PDS] Servicios potencialmente peligrosos	4	L2	L2	L2-L3
[PDS.email] Uso del correo electrónico (e-mail)	4	L2	L2	L2-L3
[PDS.email.1] Se dispone de normativa de uso	3	L2	L2	L2-L3
[PDS.email.2] Se detectan casos de uso inaceptable	4	L2	L2	L3
[PDS.email.3] Se verifica regularmente que se cumple la política	4	L2	L2	L3
[PDS.email.4] Se forma a los usuarios en el uso de los servicios	3	L2	L2	L3
[PDS.email.5] Se dispone de un procedimiento de actuación en caso de incumplimiento	3	L2	L2	L3
[PDS.email.6] Se aplican medidas disciplinarias en caso de incumplimiento	3	L2	L2	L3
[PDS.email.7] Protección de la información	4	L2	L2	L3
[PDS.email.8] Medidas frente a la recepción de spam	4	L2	L2	L3
[PDS.email.9] Medidas frente a código dañino en los clientes de correo	4	L2	L2	L3
[PDS.email.a] Software de prestación del servicio	4	L2	L2	L3

[IR] GESTIÓN DE INCIDENTES

Salvaguarda	R	[current]	[target]	[pilar]
[IR] Gestión de incidentes	6	L2	L3	L2-L4
[IR.1] Se dispone de normativa de actuación para la gestión de incidentes	2	L2	L3	L2
[IR.2] Se dispone de procedimientos para la gestión de incidentes	5	L2	L3	L2-L3
[IR.2.1] Actuación frente a código dañino	3	L2	L3	L2-L3
[IR.2.2] Actuación frente a ataques de denegación de servicio (DoS)	5	L2	L3	L3
[IR.2.3] Actuación ante fallos del sistema e interrupciones del servicio	5	L2	L3	L3
[IR.2.4] Actuación ante errores que resulten de datos del negocio inexactos o incompletos	4	L2	L3	L3
[IR.2.5] Actuación frente a violaciones de la confidencialidad	3	L2	L3	L3
[IR.2.6] Actuación frente a alarmas de los sistemas de detección de intrusión	3	L2	L3	L3
[IR.2.7] Actuación frente a alarmas de los sistemas de prevención de intrusión	3	L2	L3	L3
[IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros	3	L2	L3	L3
[IR.2.9] Actuación frente a alarmas de uso no autorizado del sistema	3	L2	L3	L3
[IR.2.a] Actuación frente a fallos del software	5	L2	L3	L3
[IR.2.b] Actuación frente a estaciones base wifi no autorizadas	3	L2	L3	L3
[IR.2.c] Detección y reacción frente a actividades de espionaje industrial	3	L2	L3	L3
[IR.2.d] Detección y reacción frente a actividades de robo de datos de carácter personal	3	L2	L3	L3
[IR.2.e] Actuación frente a otros incidentes	3	L2	L3	L3
[IR.2.f] Coordinación con otros sistemas de información afectados	3	L2	L3	L3
[IR.3] Contención del incidente	6	L2	L3	L3-L4
[IR.3.1] El personal designado cubre las 24h los 7 días de la semana	3	L2	L3	L3
[IR.3.2] El fallo del sistema deja a este en un estado controlado	3	L2	L3	L3
[IR.3.3] Se suspenden cautelarmente los trabajos en el sistema afectado	6	L2	L3	L4
[IR.3.4] Se aísla cautelarmente el sistema afectado	6	L2	L3	L4
[IR.4] Gestión del incidente	4	L2	L3	L2-L3
[IR.4.1] Se identifica y analiza la causa	2	L2	L3	L2
[IR.4.2] Se analiza el impacto del incidente	3	L2	L3	L2-L3
[IR.4.3] Se planifica la implantación de medidas correctoras	2	L2	L3	L2
[IR.4.4] Hay comunicación con los afectados por el incidente	4	L2	L3	L3
[IR.4.5] Hay comunicación con los implicados en la recuperación del incidente	3	L2	L3	L3
[IR.4.6] Se informa de las acciones a la autoridad respectiva de la organización	2	L2	L3	L2
[IR.4.7] Evidencias	3	L2	L3	L3
[IR.5] Cooperación con otras organizaciones	5	L2	L3	L3
[IR.6] Comunicación de los incidentes de seguridad	3	L2	L3	L3
[IR.7] Comunicación de las deficiencias de seguridad	2	L2	L3	L2
[IR.8] Comunicación de los fallos del software	3	L2	L3	L3
[IR.9] Se dispone de un registro de incidentes	3	L2	L3	L3
[IR.a] Los fallos y las medidas correctoras se registran y se revisan	3	L2	L3	L2-L3
[IR.b] Control formal del proceso de recuperación ante el incidente	3	L2	L3	L2-L3
[IR.c] Formación y concienciación	3	L2	L3	L2-L3

[IR.c.1] Concienciación en la detección y reporte de incidentes	2	L2	L3	L2
[IR.c.2] Formación del personal en detección y gestión de incidentes	2	L2	L3	L2
[IR.c.3] Se tiene en cuenta la singularidad del sistema	3	L2	L3	L2-L3
[IR.c.3.1] Requisitos de seguridad	2	L2	L3	L2
[IR.c.3.2] Responsabilidades legales y contractuales	2	L2	L3	L2
[IR.c.3.3] Amenazas potenciales	2	L2	L3	L2
[IR.c.3.4] Vulnerabilidades identificadas	2	L2	L3	L2
[IR.c.3.5] Incidentes ocurridos	3	L2	L3	L3
[IR.c.4] Se prueban regularmente los procedimientos de gestión de incidentes	2	L2	L3	L2
[IR.d] Se aprende de los incidentes	3	L2	L3	L2-L3
[IR.e] Se toman medidas para prevenir la repetición	4	L2	L3	L3

[TOOLS] HERRAMIENTAS DE SEGURIDAD

Salvaguarda	R	[current]	[target]	[pilar]
[tools] Herramientas de seguridad	8	L2-L3	L2-L3	L2-L5
[tools.AV] Herramienta contra código dañino	8	L3	L3	L3-L5
[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión	6	L3	L3	L3-L4
[tools.traffic] Herramienta de monitorización de tráfico	5	L2	L2	L2-L3
[tools.DLP] DLP: Herramienta de monitorización de contenidos	5	L2	L2	L2-L3
[tools.SFV] Verificación de las funciones de seguridad	6	L2	L2	L3-L4

[V] GESTIÓN DE VULNERABILIDADES

Salvaguarda	R	[current]	[target]	[pilar]
[V] Gestión de vulnerabilidades	6	L0-L2	L0-L2	L2-L4
[V.1] Se dispone de personas dedicadas a la gestión de vulnerabilidades	3	L0	L1	L3
[V.2] Se han previsto mecanismos para estar informados de vulnerabilidades ...	4	L1	L1	L3
[tools.V] Herramienta de análisis de vulnerabilidades	6	L0	L0	L3-L4
[V.4] Se analiza el impacto potencial (estimación de riesgos)	3	L2	L2	L2-L3
[V.5] Pruebas de penetración	4	L2	L2	L3
[V.6] Se dispone de procedimientos de reacción	3	L2	L2	L2-L3
[V.7] Reparación de las vulnerabilidades detectadas	5	L2	L2	L3

[A] REGISTRO Y AUDITORÍA

Salvaguarda	R	[current]	[target]	[pilar]
[A] Registro y auditoría	5	L2	L2	L2-L3
[A.1] Administración	4	L2	L2	L3
[A.2] Herramientas	5	L2	L2	L2-L3
[A.3] Información	5	L2	L2	L2-L3
[A.4] Actividades	4	L2	L2	L3

[BC] CONTINUIDAD DEL NEGOCIO

Salvaguarda	R	[current]	[target]	[pilar]
[BC] Continuidad del negocio	5	_-L3	_-L3	L2-L3
[BC.1] Gestión de la continuidad	3	_-L3	_-L3	L2-L3
[BC.1.1] Se dispone de normativa relativa a la continuidad del negocio	3			L2-L3
[BC.1.2] Se tienen en cuenta los requisitos de seguridad de la información	3	_-L1	_-L2	L3
[BC.1.2.1] Los requisitos de seguridad de la información se trasladan a los elementos dispuestos para garantizar la continuidad	3			L3
[BC.1.2.2] Se verifica regularmente que los elementos dispuestos para garantizar la continuidad satisfacen los requisitos de seguridad de la información	3	L1	L2	L3
[BC.1.2.3] Los incidentes detectados durante pruebas, ejercicios o activaciones de los procesos de continuidad se analizan como si se hubieran producido sobre el sistema base	3	L1	L2	L3
[BC.1.3] El inventario se actualiza regularmente	3	L1-L3	L3	L2-L3
[BC.BIA] Se ha realizado un análisis de impacto (BIA)	2			L2
[BC.3] Actividades preparatorias	3	L1	L2	L3
[BC.4] Reacción (gestión de crisis)	3	L1	L2	L2-L3

[BC.DRP] Plan de Recuperación de Desastres (DRP)	5	L1	L2	L2-L3
[BC.DRP.1] Se han designado responsables	2	L1	L2	L2
[BC.DRP.2] Todas las áreas de la organización están coordinadas	4	L1	L2	L3
[BC.DRP.3] Documentación	2	L1	L2	L2
[BC.DRP.4] Notificación y activación	2	L1	L2	L2
[BC.DRP.5] Se dispone de un plan de recuperación	5	L1	L2	L2-L3
[BC.DRP.5.1] Están detalladas las actividades de recuperación	2	L1	L2	L2
[BC.DRP.5.2] Están detallados los procedimientos de recuperación	2	L1	L2	L2
[BC.DRP.5.3] Se han previsto los recursos necesarios	3	L1	L2	L3
[BC.DRP.5.4] Están previstas instalaciones alternativas	5	L1	L2	L3
[BC.DRP.5.5] Las copias de seguridad (backup) se realizan con la frecuencia acordada	5	L1	L2	L3
[BC.DRP.5.6] Están previstos los medios alternativos de almacenamiento de la información	5	L1	L2	L3
[BC.DRP.5.7] Están previstos los medios alternativos de procesamiento de la información	5	L1	L2	L3
[BC.DRP.5.8] Están previstos medios alternativos de comunicación	5	L1	L2	L3
[BC.DRP.5.9] Está previsto personal alternativo	5	L1	L2	L3
[BC.DRP.5.a] Están previstos los lugares alternativos de trabajo	5	L1	L2	L3
[BC.DRP.6] Se ejecuta un plan de formación	2	L1	L2	L2
[BC.DRP.7] Los planes se prueban regularmente	4	L1	L2	L3
[BC.6] Restitución (retorno a condiciones normales de trabajo)	2			L2

[G] ORGANIZACIÓN

Salvaguarda	**R**	**[current]**	**[target]**	**[pilar]**
[G] Organización	5	_-L2	_-L3	L2-L3
[G.1] Organización interna	3			L2-L3
[G.1.1] Comité de seguridad de la información	2			L2
[G.1.2] Coordinación interna	2			L2
[G.1.3] Roles identificados	3			L2-L3
[G.1.4] Asignación de responsabilidades para la seguridad de la información	2			L2
[G.1.5] Se dispone de asesoramiento especializado en seguridad	2			L2
[G.2] Documentación técnica (componentes)	3	_-L0	_-L1	L2-L3
[G.2.1] Documentación de los componentes del sistema	2			L2
[G.2.1.1] Documentación de las instalaciones	2			L2
[G.2.1.2] Documentación de las comunicaciones	2			L2
[G.2.1.3] Puntos de interconexión (entre zonas de confianza)	2			L2
[G.2.1.4] Documentación de los puntos de acceso lógico al sistema	2			L2
[G.2.1.5] Documentación del control de acceso	2			L2
[G.2.2] Criterios de aceptación para versiones o sistemas nuevos	2			L2
[G.2.3] Seguridad de la documentación del sistema	3	_-L0	_-L1	L2-L3
[G.3] Documentación organizativa (normas y procedimientos)	3			L2-L3
[G.3.1] Marco de referencia	2			L2
[G.3.2] Política de Seguridad de la Organización	3			L2-L3
[G.3.3] Normas de seguridad	2			L2
[G.3.4] Procedimientos operativos de seguridad (POS)	2			L2
[G.3.5] Se revisa periódicamente el cumplimiento por parte del personal	2			L2
[G.4] Protección de datos de carácter personal (Documento de seguridad - LOPD)	3			L3
[RM] Gestión de riesgos	3			L2-L3
[RM.1] Se dispone de normativa en materia de gestión de riesgos	3			L2-L3
[RM.2] Se han designado responsables	3			L3
[RM.3] Se dispone de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos	3			L3
[RM.4] Activos	3			L3
[RM.5] Amenazas	3			L3
[RM.6] Salvaguardas	3			L3
[RM.7] Evaluación de riesgos	3			L3
[RM.8] Se revisa periódicamente	3			L3

[G.plan] Planificación de la seguridad	3	L2	L2	L2-L3
[G.plan.1] Se dispone de normativa de planificación (de seguridad)	2	L2	L2	L2
[G.plan.2] Procedimientos de planificación (de seguridad)	2	L2	L2	L2
[G.plan.3] Planificación de capacidades	3	L2	L2	L2-L3
[G.plan.4] Componentes críticos: carentes de suministradores alternativos	2	L2	L2	L2
[G.plan.5] Planificación de actividades de seguridad	3	L2	L2	L2-L3
[G.exam] Inspecciones de seguridad	5	L2	L3	L2-L3

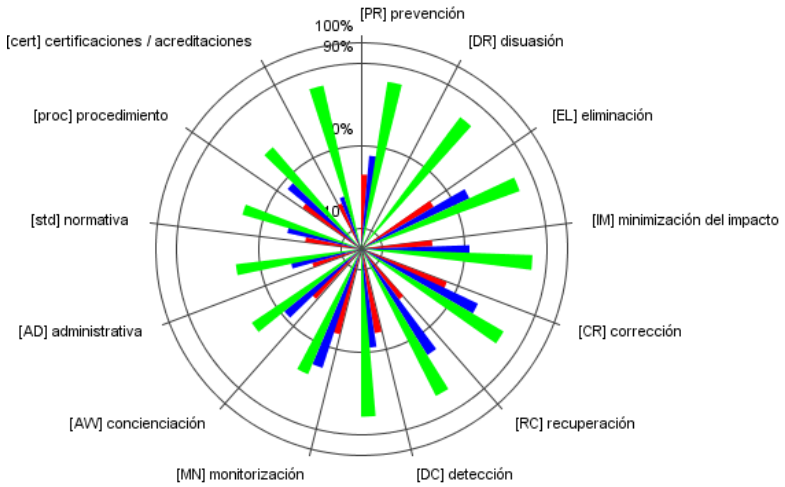
[E] RELACIONES EXTERNAS

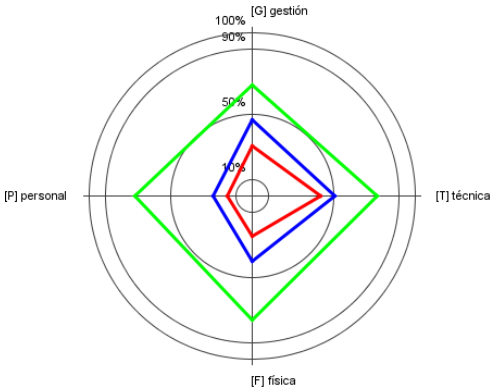
Salvaguarda	R	[current]	[target]	[pilar]
[E] Relaciones Externas	6	L2	L3	L2-L4
[E.1] Acuerdos para intercambio de información y software	6	L2	L3	L3-L4
[E.2] Acceso externo	5	L2	L3	L2-L3

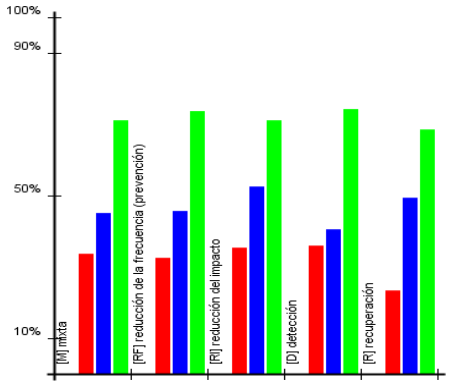
[NEW] ADQUISICIÓN / DESARROLLO

Salvaguarda	R	[current]	[target]	[pilar]
[NEW] Adquisición / desarrollo	5	_-L3	_-L3	L2-L3
[NEW.1] Gestión de proyectos	2			L2
[NEW.1.1] La seguridad se integra en el método de gestión de proyectos de la organización para asegurar que los riesgos se identifican y gestionan como parte integral de todos los proyectos	2			L2
[NEW.1.2] Los objetivos de seguridad de la información se incluyen en los objetivos del proyecto	2			L2
[NEW.1.3] Una evaluación del riesgo seguridad de la información se lleva a cabo en una etapa temprana del proyecto para identificar los controles necesarios	2			L2
[NEW.1.4] La seguridad de información es parte de todas las fases de la metodología de gestión de proyectos	2			L2
[NEW.1.5] Las implicaciones para la seguridad de la información se abordan y revisan regularmente en todos los proyectos	2			L2
[NEW.1.6] Las responsabilidades de seguridad de la información se definen y se asignan a roles específicos definidos en los métodos de gestión de proyectos	2			L2
[NEW.S] Servicios: Adquisición o desarrollo	4			L2-L3
[NEW.S.1] Se asignan recursos suficientes	1			L2
[NEW.S.2] Se establecen previamente los requisitos funcionales	2			L2
[NEW.S.3] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	2			L2
[NEW.S.4] Se identifican los requisitos técnicos de seguridad	3			L2-L3
[S.start] Aceptación y puesta en operación	4			L2-L3
[NEW.SW] Aplicaciones: Adquisición o desarrollo	5	_-L3	_-L3	L2-L3
[NEW.SW.1] Se establecen previamente los requisitos funcionales	2			L2
[NEW.SW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	2			L2
[NEW.SW.3] Se identifican los requisitos técnicos de seguridad	3			L2-L3
[NEW.SW.4] Los operadores y usuarios son consultados en el proceso de desarrollo	2			L2
[NEW.SW.5] Adquisición de aplicaciones (SW)	3			L2-L3
[NEW.SW.6] Desarrollo	5	_-L3	_-L3	L2-L3
[NEW.SW.7] Aceptación y puesta en operación	4			L2-L3
[NEW.SW.8] Se prefieren aplicaciones que funcionan sobre varios sistemas operativos	3			L3
[NEW.HW] Equipos: Adquisición o desarrollo	4			L2-L3
[NEW.HW.1] Se establecen previamente los requisitos funcionales	2			L2
[NEW.HW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	2			L2
[NEW.HW.3] Se identifican los requisitos técnicos de seguridad	3			L2-L3
[NEW.HW.4] Adquisición de HW	3			L2-L3
[NEW.HW.5] Desarrollo de HW	4			L2-L3

[NEW.HW.6] Se tienen en cuenta las necesidades de formación	2			L2
[NEW.HW.7] Se tienen en cuenta las necesidades de repuestos	2			L2
[NEW.HW.8] Documentación del HW	2			L2
[NEW.HW.9] Se disponen derechos de acceso para auditar la calidad y exactitud del trabajo realizado	2			L2
[NEW.HW.a] La calidad y exactitud del trabajo realizado se certifica según los estándares requeridos	2			L2
[NEW.HW.b] Entorno de pruebas	4			L3
[NEW.COM] Comunicaciones: Adquisición o contratación	3			L2-L3
[NEW.C] Productos certificados o acreditados	5			L3







ANEXO N° 07: IMPACTO REPERCUTIDO

Análisis de impacto en el negocio

proyecto: [01] UPH. Carhuaquero

1. DATOS DEL PROYECTO

PROYECTO:	UPH. Carhuaquero
DESCRIPCIÓN:	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE:	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN:	ORAZUL ENERGY PERU S.A.
VERSIÓN:	1
FECHA:	1/11/2017
BIBLIOTECA:	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

4. DOMINIOS DE SEGURIDAD

- [base] Base

5. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado
  - [105.a] Se permite el acceso a Internet
  - [105.b] Se permite la ejecución de programas sin autorización previa
  - [105.c] Se permite la instalación de programas sin autorización previa
  - [105.d] Se permite la conexión de dispositivos removibles
  - [111.b] Conectado a un conjunto reducido y controlado de redes
  - [111.d] Conectado a Internet
  - [112.b] En un área de acceso abierto

6. FASES DEL PROYECTO

- [Current] situación actual
- [Target] situación objetivo
- [PILAR] recomendación

7. IMPACTO REPERCUTIDO

7.1. FASE: [CURRENT] SITUACIÓN ACTUAL

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[5]	[3]	[3]			
[OS_SW] Sistema Operativo	[3]	[0]	[0]			
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]			
[OTR_SW] Otros Software	[0]	[0]	[0]			
[PI_SW] PI Process Book	[5]	[3]	[3]			
[SCADA_SW] Sistema Tiempo Real	[5]	[3]	[3]			
[MAXIMO_SW] Maximo	[5]	[3]	[3]			
[PSOFT_SW] PeopleSoft	[5]	[3]	[3]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[5]	[3]	[3]			
[GPS_SW] Sistema de Frecuencia	[5]	[3]	[3]			
[ANTIVIRUS_SW] Antivirus	[5]	[3]	[3]			
[HW] Hardware	[8]	[2]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[8]	[2]	[0]			
[FILE_HW] Servidor de Archivos	[8]	[2]	[0]			
[PI_HW] Servidor PI	[8]	[2]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[8]	[2]	[0]			
[SPRINTER_HW] Servidor de Impresión	[6]	[2]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[8]	[2]	[0]			
[STATION_HW] Estaciones de Trabajo	[5]	[1]	[0]			
[PRINTER_HW] Equipos de Impresión	[5]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[5]	[0]	[0]			
[COM] Comunicaciones	[7]	[2]	[0]	[4]		
[ANT_COM] Antena (Enlace Microondas)	[7]	[0]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[7]	[0]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[6]	[2]	[0]	[4]		
[SWSCADA_COM] Switch SCADA	[6]	[2]	[0]	[4]		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[6]	[0]	[0]	[4]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[6]	[0]	[0]	[4]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[6]	[0]	[0]	[4]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[6]	[0]	[0]	[4]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[6]	[0]	[0]	[4]		
[PKSHA_COM] Packet Shaper 2500	[6]	[0]	[0]	[4]		
[ROUTER_COM] Router Cisco	[7]	[2]	[0]	[4]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[6]	[2]	[0]	[4]		
[REP_COM] Repetidoras	[4]	[0]	[0]	[3]		
[RAD_COM] Radios	[2]	[0]	[0]	[2]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[6]	[4]	[4]	[5]	[5]	
[MAIL_S] Correo Electrónico	[5]	[4]	[4]	[5]	[5]	
[STELF_S] Telefonía IP (Servicio)	[5]	[2]	[0]	[2]	[2]	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[0]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[6]					
[OTR_AUX] Otros Equipos Auxiliares	[0]		[0]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[5]					
[ZONA_SERV_I] Sala de Servidores	[5]					
[ZONA_REU_I] Sala de Reuniones	[2]					
[ZONA_ALM_I] Almacén	[5]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[5]					
[ZONA_OFTALL_I] Oficinas Talleres	[5]					
[ZONA_CONTROL_I] Sala Control	[5]					
[ZONA_TALL_I] Talleres	[5]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[5]	[0]	[0]			
[ADM_P] Personal de administración y logístico	[2]	[0]	[0]			
[JADM_P] Jefatura de administración	[5]	[0]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[2]	[0]	[0]			
[JUNI_P] Jefe de Unidad	[5]	[0]	[0]			
[SYMA_P] Personal SyMA	[2]	[0]	[0]			
[JSYMA_P] Jefatura SyMA	[5]	[0]	[0]			
[TOP_P] Tópico	[2]	[0]	[0]			
[OPE_P] Personal Operaciones	[2]	[0]	[0]			
[JOPE_P] Jefatura de Operaciones	[5]	[0]	[0]			
[CIV_P] Personal Ing. Civil	[2]	[0]	[0]			
[SGI_P] Personal SGI	[2]	[0]	[0]			
[CDOM_P] Coordinaciones O&M	[5]	[0]	[0]			

7.2. FASE: [Target] SITUACIÓN OBJETIVO

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[4]	[3]	[3]			
[OS_SW] Sistema Operativo	[2]	[0]	[0]			
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]			
[OTR_SW] Otros Software	[0]	[0]	[0]			
[PI_SW] PI Process Book	[4]	[3]	[3]			
[SCADA_SW] Sistema Tiempo Real	[4]	[3]	[3]			
[MAXIMO_SW] Maximo	[4]	[3]	[3]			
[PSOFT_SW] PeopleSoft	[4]	[3]	[3]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[4]	[3]	[3]			
[GPS_SW] Sistema de Frecuencia	[4]	[3]	[3]			
[ANTIVIRUS_SW] Antivirus	[4]	[3]	[3]			
[HW] Hardware	[7]	[1]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[7]	[1]	[0]			
[FILE_HW] Servidor de Archivos	[7]	[1]	[0]			
[PI_HW] Servidor PI	[7]	[1]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[7]	[1]	[0]			
[SPRINTER_HW] Servidor de Impresión	[5]	[1]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[7]	[1]	[0]			
[STATION_HW] Estaciones de Trabajo	[4]	[0]	[0]			
[PRINTER_HW] Equipos de Impresión	[4]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[4]	[0]	[0]			
[COM] Comunicaciones	[6]	[1]	[0]	[3]		
[ANT_COM] Antena (Enlace Microondas)	[6]	[0]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[6]	[0]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[5]	[1]	[0]	[3]		
[SWSCADA_COM] Switch SCADA	[5]	[1]	[0]	[3]		

[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[5]	[0]	[0]	[3]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[5]	[0]	[0]	[3]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[5]	[0]	[0]	[3]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[5]	[0]	[0]	[3]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[5]	[0]	[0]	[3]		
[PKSHA_COM] Packet Shaper 2500	[5]	[0]	[0]	[3]		
[ROUTER_COM] Router Cisco	[6]	[1]	[0]	[3]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[5]	[1]	[0]	[3]		
[REP_COM] Repetidoras	[3]	[0]	[0]	[2]		
[RAD_COM] Radios	[1]	[0]	[0]	[1]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[5]	[3]	[3]	[4]	[4]	
[MAIL_S] Correo Electrónico	[4]	[3]	[3]	[4]	[4]	
[STELF_S] Telefonía IP (Servicio)	[4]	[1]	[0]	[1]	[1]	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[0]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[5]					
[OTR_AUX] Otros Equipos Auxiliares	[0]		[0]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[4]					
[ZONA_SERV_I] Sala de Servidores	[4]					
[ZONA_REU_I] Sala de Reuniones	[1]					
[ZONA_ALM_I] Almacén	[4]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[4]					
[ZONA_OFTALL_I] Oficinas Talleres	[4]					
[ZONA_CONTROL_I] Sala Control	[4]					
[ZONA_TALL_I] Talleres	[4]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[4]	[0]	[0]			
[ADM_P] Personal de administración y logístico	[2]	[0]	[0]			
[JADM_P] Jefatura de administración	[4]	[0]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[2]	[0]	[0]			
[JUNI_P] Jefe de Unidad	[4]	[0]	[0]			
[SYMA_P] Personal SyMA	[1]	[0]	[0]			
[JSYMA_P] Jefatura SyMA	[5]	[0]	[0]			
[TOP_P] Tópico	[1]	[0]	[0]			
[OPE_P] Personal Operaciones	[1]	[0]	[0]			
[JOPE_P] Jefatura de Operaciones	[4]	[0]	[0]			
[CIV_P] Personal Ing. Civil	[1]	[0]	[0]			
[SGI_P] Personal SGI	[1]	[0]	[0]			
[CDOM_P] Coordinaciones O&M	[4]	[0]	[0]			

7.3. FASE: [PILAR] RECOMENDACIÓN

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[4]	[2]	[2]			
[OS_SW] Sistema Operativo	[2]	[0]	[0]			
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]			
[OTR_SW] Otros Software	[0]	[0]	[0]			

[PI_SW] PI Process Book	[4]	[2]	[2]			
[SCADA_SW] Sistema Tiempo Real	[4]	[2]	[2]			
[MAXIMO_SW] Maximo	[4]	[2]	[2]			
[PSOFT_SW] PeopleSoft	[4]	[2]	[2]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[4]	[2]	[2]			
[GPS_SW] Sistema de Frecuencia	[4]	[2]	[2]			
[ANTIVIRUS_SW] Antivirus	[4]	[2]	[2]			
[HW] Hardware	[6]	[0]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[6]	[0]	[0]			
[FILE_HW] Servidor de Archivos	[6]	[0]	[0]			
[PI_HW] Servidor PI	[6]	[0]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[6]	[0]	[0]			
[SPRINTER_HW] Servidor de Impresión	[4]	[0]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[6]	[0]	[0]			
[STATION_HW] Estaciones de Trabajo	[3]	[0]	[0]			
[PRINTER_HW] Equipos de Impresión	[3]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[3]	[0]	[0]			
[COM] Comunicaciones	[5]	[0]	[0]	[2]		
[ANT_COM] Antena (Enlace Microondas)	[5]	[0]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[5]	[0]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[4]	[0]	[0]	[2]		
[SWSCADA_COM] Switch SCADA	[4]	[0]	[0]	[2]		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[4]	[0]	[0]	[2]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[4]	[0]	[0]	[2]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[4]	[0]	[0]	[2]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[4]	[0]	[0]	[2]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[4]	[0]	[0]	[2]		
[PKSHA_COM] Packet Shaper 2500	[4]	[0]	[0]	[2]		
[ROUTER_COM] Router Cisco	[5]	[0]	[0]	[2]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[4]	[0]	[0]	[2]		
[REP_COM] Repetidoras	[2]	[0]	[0]	[1]		
[RAD_COM] Radios	[0]	[0]	[0]	[0]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[4]	[1]	[1]	[2]	[3]	
[MAIL_S] Correo Electrónico	[3]	[2]	[2]	[3]	[3]	
[STELF_S] Telefonía IP (Servicio)	[3]	[0]	[0]	[0]	[0]	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[0]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[4]					
[OTR_AUX] Otros Equipos Auxiliares	[0]		[0]			

[I] INSTALACIONES

activo	***[D]***	***[I]***	***[C]***	***[A]***	***[T]***	***[V]***
[EDI_I] Edificio	[3]					
[ZONA_SERV_I] Sala de Servidores	[3]					
[ZONA_REU_I] Sala de Reuniones	[0]					
[ZONA_ALM_I] Almacén	[3]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[3]					
[ZONA_OFTALL_I] Oficinas Talleres	[3]					
[ZONA_CONTROL_I] Sala Control	[3]					
[ZONA_TALL_I] Talleres	[3]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[3]	[0]	[0]			
[ADM_P] Personal de administración y logístico	[0]	[0]	[0]			
[JADM_P] Jefatura de administración	[3]	[0]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[0]	[0]	[0]			
[JUNI_P] Jefe de Unidad	[3]	[0]	[0]			
[SYMA_P] Personal SyMA	[0]	[0]	[0]			
[JSYMA_P] Jefatura SyMA	[3]	[0]	[0]			
[TOP_P] Tópico	[0]	[0]	[0]			
[OPE_P] Personal Operaciones	[0]	[0]	[0]			
[JOPE_P] Jefatura de Operaciones	[3]	[0]	[0]			
[CIV_P] Personal Ing. Civil	[0]	[0]	[0]			
[SGI_P] Personal SGI	[0]	[0]	[0]			
[CDOM_P] Coordinaciones O&M	[3]	[0]	[0]			

7.4. [D] Disponibilidad

[E] EQUIPAMIENTO

Activo	[current]	[target]	[pilar]
[SW] Software	[5]	[4]	[4]
[OS_SW] Sistema Operativo	[3]	[2]	[2]
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]
[OTR_SW] Otros Software	[0]	[0]	[0]
[PI_SW] PI Process Book	[5]	[4]	[4]
[SCADA_SW] Sistema Tiempo Real	[5]	[4]	[4]
[MAXIMO_SW] Maximo	[5]	[4]	[4]
[PSOFT_SW] PeopleSoft	[5]	[4]	[4]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[5]	[4]	[4]
[GPS_SW] Sistema de Frecuencia	[5]	[4]	[4]
[ANTIVIRUS_SW] Antivirus	[5]	[4]	[4]
[HW] Hardware	[8]	[7]	[6]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[8]	[7]	[6]
[FILE_HW] Servidor de Archivos	[8]	[7]	[6]
[PI_HW] Servidor PI	[8]	[7]	[6]
[BACKUP_HW] Servidor Copias de Seguridad	[8]	[7]	[6]
[SPRINTER_HW] Servidor de Impresión	[6]	[5]	[4]
[NVR_HW] Servidor de Grabación CCTV-NVR	[8]	[7]	[6]
[STATION_HW] Estaciones de Trabajo	[5]	[4]	[3]
[PRINTER_HW] Equipos de Impresión	[5]	[4]	[3]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]
[CAM_HW] Cámaras de Video Vigilancia	[5]	[4]	[3]
[COM] Comunicaciones	[7]	[6]	[5]
[ANT_COM] Antena (Enlace Microondas)	[7]	[6]	[5]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[7]	[6]	[5]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[6]	[5]	[4]
[SWSCADA_COM] Switch SCADA	[6]	[5]	[4]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[6]	[5]	[4]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[6]	[5]	[4]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[6]	[5]	[4]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[6]	[5]	[4]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[6]	[5]	[4]
[PKSHA_COM] Packet Shaper 2500	[6]	[5]	[4]
[ROUTER_COM] Router Cisco	[7]	[6]	[5]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[6]	[5]	[4]
[REP_COM] Repetidoras	[4]	[3]	[2]
[RAD_COM] Radios	[2]	[1]	[0]

[S] SERVICIOS

Activo	[current]	[target]	[pilar]
[WWW_S] Internet	[6]	[5]	[4]
[MAIL_S] Correo Electrónico	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[5]	[4]	[3]

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	[0]	[0]	[0]
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[6]	[5]	[4]
[OTR_AUX] Otros Equipos Auxiliares	[0]	[0]	[0]

[I] INSTALACIONES

Activo	[current]	[target]	[pilar]
[EDI_I] Edificio	[5]	[4]	[3]
[ZONA_SERV_I] Sala de Servidores	[5]	[4]	[3]
[ZONA_REU_I] Sala de Reuniones	[2]	[1]	[0]
[ZONA_ALM_I] Almacén	[5]	[4]	[3]
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[5]	[4]	[3]
[ZONA_OFTALL_I] Oficinas Talleres	[5]	[4]	[3]
[ZONA_CONTROL_I] Sala Control	[5]	[4]	[3]
[ZONA_TALL_I] Talleres	[5]	[4]	[3]

[P] PERSONAL

Activo	[current]	[target]	[pilar]
[TI_P] Coordinador TI	[5]	[4]	[3]
[ADM_P] Personal de administración y logístico	[2]	[2]	[0]
[JADM_P] Jefatura de administración	[5]	[4]	[3]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[2]	[2]	[0]
[JUNI_P] Jefe de Unidad	[5]	[4]	[3]
[SYMA_P] Personal SyMA	[2]	[1]	[0]
[JSYMA_P] Jefatura SyMA	[5]	[5]	[3]
[TOP_P] Tópico	[2]	[1]	[0]
[OPE_P] Personal Operaciones	[2]	[1]	[0]
[JOPE_P] Jefatura de Operaciones	[5]	[4]	[3]
[CIV_P] Personal Ing. Civil	[2]	[1]	[0]
[SGI_P] Personal SGI	[2]	[1]	[0]
[CDOM_P] Coordinaciones O&M	[5]	[4]	[3]

7.5. [I] Integridad de los datos

[E] EQUIPAMIENTO

Activo	[current]	[target]	[pilar]
[SW] Software	[3]	[3]	[2]
[OS_SW] Sistema Operativo	[0]	[0]	[0]
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]
[OTR_SW] Otros Software	[0]	[0]	[0]
[PI_SW] PI Process Book	[3]	[3]	[2]
[SCADA_SW] Sistema Tiempo Real	[3]	[3]	[2]
[MAXIMO_SW] Maximo	[3]	[3]	[2]
[PSOFT_SW] PeopleSoft	[3]	[3]	[2]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[3]	[3]	[2]
[GPS_SW] Sistema de Frecuencia	[3]	[3]	[2]
[ANTIVIRUS_SW] Antivirus	[3]	[3]	[2]
[HW] Hardware	[2]	[1]	[0]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[2]	[1]	[0]
[FILE_HW] Servidor de Archivos	[2]	[1]	[0]
[PI_HW] Servidor PI	[2]	[1]	[0]

[BACKUP_HW] Servidor Copias de Seguridad	[2]	[1]	[0]
[SPRINTER_HW] Servidor de Impresión	[2]	[1]	[0]
[NVR_HW] Servidor de Grabación CCTV-NVR	[2]	[1]	[0]
[STATION_HW] Estaciones de Trabajo	[1]	[0]	[0]
[PRINTER_HW] Equipos de Impresión	[0]	[0]	[0]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]
[CAM_HW] Cámaras de Video Vigilancia	[0]	[0]	[0]
[COM] Comunicaciones	[2]	[1]	[0]
[ANT_COM] Antena (Enlace Microondas)	[0]	[0]	[0]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[0]	[0]	[0]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[2]	[1]	[0]
[SWSCADA_COM] Switch SCADA	[2]	[1]	[0]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[0]	[0]	[0]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[0]	[0]	[0]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[0]	[0]	[0]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[0]	[0]	[0]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[0]	[0]	[0]
[PKSHA_COM] Packet Shaper 2500	[0]	[0]	[0]
[ROUTER_COM] Router Cisco	[2]	[1]	[0]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[2]	[1]	[0]
[REP_COM] Repetidoras	[0]	[0]	[0]
[RAD_COM] Radios	[0]	[0]	[0]

[S] SERVICIOS

Activo	[current]	[target]	[pilar]
[WWW_S] Internet	[4]	[3]	[1]
[MAIL_S] Correo Electrónico	[4]	[3]	[2]
[STELF_S] Telefonía IP (Servicio)	[2]	[1]	[0]

7.6. [C] Confidencialidad de los datos

[E] EQUIPAMIENTO

Activo	[current]	[target]	[pilar]
[SW] Software	[3]	[3]	[2]
[OS_SW] Sistema Operativo	[0]	[0]	[0]
[OFIMATICA_SW] Ofimática	[0]	[0]	[0]
[OTR_SW] Otros Software	[0]	[0]	[0]
[PI_SW] PI Process Book	[3]	[3]	[2]
[SCADA_SW] Sistema Tiempo Real	[3]	[3]	[2]
[MAXIMO_SW] Maximo	[3]	[3]	[2]
[PSOFT_SW] PeopleSoft	[3]	[3]	[2]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[3]	[3]	[2]
[GPS_SW] Sistema de Frecuencia	[3]	[3]	[2]
[ANTIVIRUS_SW] Antivirus	[3]	[3]	[2]
[HW] Hardware	[0]	[0]	[0]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[0]	[0]	[0]
[FILE_HW] Servidor de Archivos	[0]	[0]	[0]
[PI_HW] Servidor PI	[0]	[0]	[0]
[BACKUP_HW] Servidor Copias de Seguridad	[0]	[0]	[0]
[SPRINTER_HW] Servidor de Impresión	[0]	[0]	[0]
[NVR_HW] Servidor de Grabación CCTV-NVR	[0]	[0]	[0]
[STATION_HW] Estaciones de Trabajo	[0]	[0]	[0]
[PRINTER_HW] Equipos de Impresión	[0]	[0]	[0]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[0]	[0]	[0]
[CAM_HW] Cámaras de Video Vigilancia	[0]	[0]	[0]
[COM] Comunicaciones	[0]	[0]	[0]
[ANT_COM] Antena (Enlace Microondas)	[0]	[0]	[0]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[0]	[0]	[0]

[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[0]	[0]	[0]
[SWSCADA_COM] Switch SCADA	[0]	[0]	[0]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[0]	[0]	[0]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[0]	[0]	[0]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[0]	[0]	[0]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[0]	[0]	[0]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[0]	[0]	[0]
[PKSHA_COM] Packet Shaper 2500	[0]	[0]	[0]
[ROUTER_COM] Router Cisco	[0]	[0]	[0]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[0]	[0]	[0]
[REP_COM] Repetidoras	[0]	[0]	[0]
[RAD_COM] Radios	[0]	[0]	[0]

[S] SERVICIOS

Activo	[current]	[target]	[pilar]
[WWW_S] Internet	[4]	[3]	[1]
[MAIL_S] Correo Electrónico	[4]	[3]	[2]
[STELF_S] Telefonía IP (Servicio)	[0]	[0]	[0]

7.7. [A] Autenticidad de los usuarios y de la información

[E] EQUIPAMIENTO

Activo	[current]	[target]	[pilar]
[SW] Software			
[OS_SW] Sistema Operativo			
[OFIMATICA_SW] Ofimática			
[OTR_SW] Otros Software			
[PI_SW] PI Process Book			
[SCADA_SW] Sistema Tiempo Real			
[MAXIMO_SW] Maximo			
[PSOFT_SW] PeopleSoft			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras			
[GPS_SW] Sistema de Frecuencia			
[ANTIVIRUS_SW] Antivirus			
[HW] Hardware			
[DOM_HW] Controlador de Dominio Windows 2012 Server			
[FILE_HW] Servidor de Archivos			
[PI_HW] Servidor PI			
[BACKUP_HW] Servidor Copias de Seguridad			
[SPRINTER_HW] Servidor de Impresión			
[NVR_HW] Servidor de Grabación CCTV-NVR			
[STATION_HW] Estaciones de Trabajo			
[PRINTER_HW] Equipos de Impresión			
[PROYECTOR_HW] Proyectores Salas de Reuniones			
[CAM_HW] Cámaras de Video Vigilancia			
[COM] Comunicaciones	[4]	[3]	[2]
[ANT_COM] Antena (Enlace Microondas)	[0]	[0]	[0]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[0]	[0]	[0]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[4]	[3]	[2]
[SWSCADA_COM] Switch SCADA	[4]	[3]	[2]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[4]	[3]	[2]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[4]	[3]	[2]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[4]	[3]	[2]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[4]	[3]	[2]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[4]	[3]	[2]
[PKSHA_COM] Packet Shaper 2500	[4]	[3]	[2]
[ROUTER_COM] Router Cisco	[4]	[3]	[2]

[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[4]	[3]	[2]
[REP_COM] Repetidoras	[3]	[2]	[1]
[RAD_COM] Radios	[2]	[1]	[0]

[S] SERVICIOS

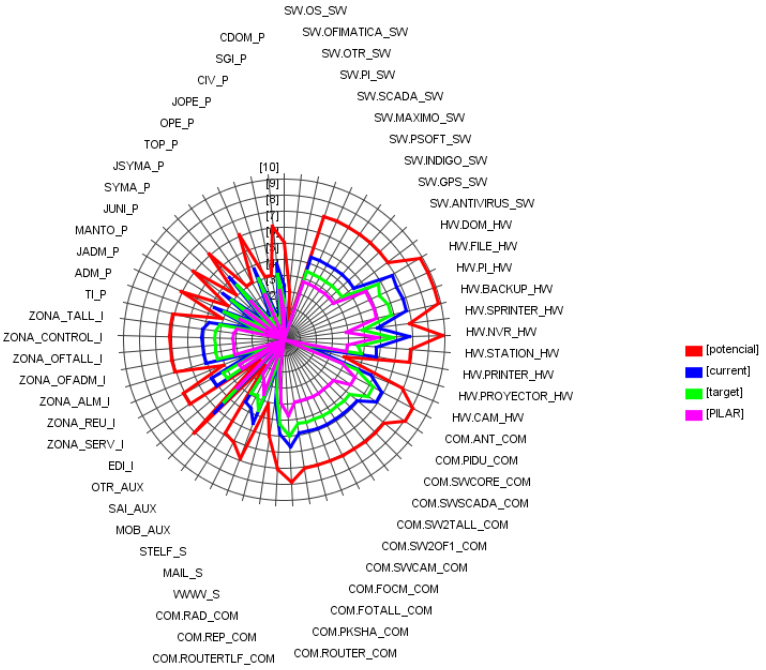
Activo	[current]	[target]	[pilar]
[WWW_S] Internet	[5]	[4]	[2]
[MAIL_S] Correo Electrónico	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[2]	[1]	[0]

7.8. [T] Trazabilidad del servicio y de los datos

[S] SERVICIOS

Activo	[current]	[target]	[pilar]
[WWW_S] Internet	[5]	[4]	[3]
[MAIL_S] Correo Electrónico	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[2]	[1]	[0]

7.9. [V] Valor



ANEXO N° 08: IMPACTO ACUMULADO

ANÁLISIS DE IMPACTO EN EL NEGOCIO
PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO

PROYECTO	UPH. Carhuaquero
DESCRIPCIÓN	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN	ORAZUL ENERGY PERU S.A.
VERSIÓN	1
FECHA	1/11/2017
BIBLIOTECA	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

4. DOMINIOS DE SEGURIDAD

- [base] Base

5. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado
  - [105.a] Se permite el acceso a Internet
  - [105.b] Se permite la ejecución de programas sin autorización previa
  - [105.c] Se permite la instalación de programas sin autorización previa
  - [105.d] Se permite la conexión de dispositivos removibles
  - [111.b] Conectado a un conjunto reducido y controlado de redes
  - [111.d] Conectado a Internet
  - [112.b] En un área de acceso abierto

6. FASES DEL PROYECTO

- [Potencial]
- [Current] situación actual
- [Target] situación objetivo
- [PILAR] recomendación

7. IMPACTO ACUMULADO

7.1. Fase: [Potencial]

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[8]	[8]	[6]			
[OS_SW] Sistema Operativo	[6]	[8]	[2]			
[OFIMATICA_SW] Ofimática	[6]	[8]	[2]			
[OTR_SW] Otros Software	[6]	[8]	[2]			
[PI_SW] PI Process Book	[8]	[8]	[6]			
[SCADA_SW] Sistema Tiempo Real	[8]	[8]	[6]			
[MAXIMO_SW] Maximo	[8]	[8]	[6]			
[PSOFT_SW] PeopleSoft	[8]	[8]	[6]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[8]	[8]	[6]			
[GPS_SW] Sistema de Frecuencia	[8]	[8]	[6]			
[ANTIVIRUS_SW] Antivirus	[8]	[8]	[6]			
[HW] Hardware	[10]	[8]	[2]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[10]	[8]	[2]			
[FILE_HW] Servidor de Archivos	[10]	[8]	[2]			
[PI_HW] Servidor PI	[10]	[8]	[2]			
[BACKUP_HW] Servidor Copias de Seguridad	[10]	[8]	[2]			
[SPRINTER_HW] Servidor de Impresión	[8]	[8]	[2]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[10]	[8]	[2]			
[STATION_HW] Estaciones de Trabajo	[8]	[8]	[2]			
[PRINTER_HW] Equipos de Impresión	[8]	[3]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[7]	[8]	[2]			
[CAM_HW] Cámaras de Video Vigilancia	[8]	[8]	[2]			
[COM] Comunicaciones	[9]	[8]	[2]	[6]		
[ANT_COM] Antena (Enlace Microondas)	[9]	[8]	[2]	[1]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[9]	[8]	[2]	[1]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[8]	[8]	[2]	[6]		
[SWSCADA_COM] Switch SCADA	[8]	[8]	[2]	[6]		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[8]	[8]	[2]	[6]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[8]	[8]	[2]	[6]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[8]	[8]	[2]	[6]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[8]	[8]	[2]	[6]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[8]	[8]	[2]	[6]		
[PKSHA_COM] Packet Shaper 2500	[8]	[8]	[2]	[6]		
[ROUTER_COM] Router Cisco	[9]	[8]	[2]	[6]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[8]	[8]	[2]	[6]		
[REP_COM] Repetidoras	[6]	[8]	[2]	[5]		
[RAD_COM] Radios	[6]	[8]	[2]	[4]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[8]	[8]	[6]	[7]	[7]	
[MAIL_S] Correo Electrónico	[7]	[8]	[6]	[7]	[7]	
[STELF_S] Telefonía IP (Servicio)	[7]	[8]	[2]	[4]	[4]	

[AUX] EQUIPAMIENTO AUXILIAR

activo	[D]	[I]	[C]	[A]	[T]	[V]
[MOB_AUX] Mobiliario	[4]	[3]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[8]					
[OTR_AUX] Otros Equipos Auxiliares	[4]		[2]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[7]					
[ZONA_SERV_I] Sala de Servidores	[7]					
[ZONA_REU_I] Sala de Reuniones	[6]					
[ZONA_ALM_I] Almacén	[7]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[7]					
[ZONA_OFTALL_I] Oficinas Talleres	[7]					
[ZONA_CONTROL_I] Sala Control	[7]					
[ZONA_TALL_I] Talleres	[7]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[7]	[8]	[2]			
[ADM_P] Personal de administración y logístico	[6]	[8]	[2]			
[JADM_P] Jefatura de administración	[7]	[8]	[2]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[6]	[8]	[2]			
[JUNI_P] Jefe de Unidad	[7]	[8]	[2]			
[SYMA_P] Personal SyMA	[6]	[8]	[2]			
[JSYMA_P] Jefatura SyMA	[7]	[8]	[2]			
[TOP_P] Tópico	[6]	[9]	[2]			
[OPE_P] Personal Operaciones	[6]	[9]	[2]			
[JOPE_P] Jefatura de Operaciones	[7]	[8]	[2]			
[CIV_P] Personal Ing. Civil	[6]	[8]	[2]			
[SGI_P] Personal SGI	[6]	[8]	[2]			
[CDOM_P] Coordinaciones O&M	[7]	[8]	[2]			

4.1. FASE: [CURRENT] SITUACIÓN ACTUAL

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[5]	[5]	[3]			
[OS_SW] Sistema Operativo	[3]	[5]	[0]			
[OFIMATICA_SW] Ofimática	[3]	[5]	[0]			
[OTR_SW] Otros Software	[3]	[5]	[0]			
[PI_SW] PI Process Book	[5]	[5]	[3]			
[SCADA_SW] Sistema Tiempo Real	[5]	[5]	[3]			
[MAXIMO_SW] Maximo	[5]	[5]	[3]			
[PSOFT_SW] PeopleSoft	[5]	[5]	[3]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[5]	[5]	[3]			
[GPS_SW] Sistema de Frecuencia	[5]	[5]	[3]			
[ANTIVIRUS_SW] Antivirus	[5]	[5]	[3]			
[HW] Hardware	[8]	[6]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[8]	[5]	[0]			
[FILE_HW] Servidor de Archivos	[8]	[6]	[0]			
[PI_HW] Servidor PI	[8]	[5]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[8]	[5]	[0]			
[SPRINTER_HW] Servidor de Impresión	[6]	[5]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[8]	[5]	[0]			
[STATION_HW] Estaciones de Trabajo	[6]	[6]	[0]			
[PRINTER_HW] Equipos de Impresión	[6]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[5]	[5]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[6]	[5]	[0]			
[COM] Comunicaciones	[7]	[6]	[0]	[4]		
[ANT_COM] Antena (Enlace Microondas)	[7]	[6]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[7]	[6]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[6]	[6]	[0]	[4]		
[SWSCADA_COM] Switch SCADA	[6]	[6]	[0]	[4]		

[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[6]	[6]	[0]	[4]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[6]	[6]	[0]	[4]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[6]	[6]	[0]	[4]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[6]	[6]	[0]	[4]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[6]	[6]	[0]	[4]		
[PKSHA_COM] Packet Shaper 2500	[6]	[6]	[0]	[4]		
[ROUTER_COM] Router Cisco	[7]	[6]	[0]	[4]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[6]	[6]	[0]	[4]		
[REP_COM] Repetidoras	[4]	[6]	[0]	[3]		
[RAD_COM] Radios	[4]	[6]	[0]	[2]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[www_s] internet	[6]	[6]	[4]	[5]	[5]	
[mail_s] correo electrónico	[5]	[6]	[4]	[5]	[5]	
[stelf_s] telefonía ip (servicio)	[5]	[6]	[0]	[2]	[2]	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[2]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[6]					
[OTR_AUX] Otros Equipos Auxiliares	[2]		[0]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[5]					
[ZONA_SERV_I] Sala de Servidores	[5]					
[ZONA_REU_I] Sala de Reuniones	[4]					
[ZONA_ALM_I] Almacén	[5]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[5]					
[ZONA_OFTALL_I] Oficinas Talleres	[5]					
[ZONA_CONTROL_I] Sala Control	[5]					
[ZONA_TALL_I] Talleres	[5]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[5]	[6]	[0]			
[ADM_P] Personal de administración y logístico	[4]	[6]	[0]			
[JADM_P] Jefatura de administración	[5]	[6]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[4]	[6]	[0]			
[JUNI_P] Jefe de Unidad	[5]	[6]	[0]			
[SYMA_P] Personal SyMA	[4]	[6]	[0]			
[JSYMA_P] Jefatura SyMA	[5]	[6]	[0]			
[TOP_P] Tópico	[4]	[7]	[0]			
[OPE_P] Personal Operaciones	[4]	[7]	[0]			
[JOPE_P] Jefatura de Operaciones	[5]	[6]	[0]			
[CIV_P] Personal Ing. Civil	[4]	[6]	[0]			
[SGI_P] Personal SGI	[4]	[6]	[0]			
[CDOM_P] Coordinaciones O&M	[5]	[6]	[0]			

4.2. FASE: [Target] SITUACIÓN OBJETIVO

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[4]	[5]	[3]			
[OS_SW] Sistema Operativo	[2]	[5]	[0]			
[OFIMATICA_SW] Ofimática	[2]	[5]	[0]			
[OTR_SW] Otros Software	[2]	[5]	[0]			

[PI_SW] PI Process Book	[4]	[5]	[3]			
[SCADA_SW] Sistema Tiempo Real	[4]	[5]	[3]			
[MAXIMO_SW] Maximo	[4]	[5]	[3]			
[PSOFT_SW] PeopleSoft	[4]	[5]	[3]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[4]	[5]	[3]			
[GPS_SW] Sistema de Frecuencia	[4]	[5]	[3]			
[ANTIVIRUS_SW] Antivirus	[4]	[5]	[3]			
[HW] Hardware	[7]	[5]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[7]	[5]	[0]			
[FILE_HW] Servidor de Archivos	[7]	[5]	[0]			
[PI_HW] Servidor PI	[7]	[5]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[7]	[5]	[0]			
[SPRINTER_HW] Servidor de Impresión	[5]	[5]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[7]	[5]	[0]			
[STATION_HW] Estaciones de Trabajo	[5]	[5]	[0]			
[PRINTER_HW] Equipos de Impresión	[5]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[4]	[5]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[5]	[5]	[0]			
[COM] Comunicaciones	[6]	[5]	[0]	[3]		
[ANT_COM] Antena (Enlace Microondas)	[6]	[5]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[6]	[5]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[5]	[5]	[0]	[3]		
[SWSCADA_COM] Switch SCADA	[5]	[5]	[0]	[3]		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[5]	[5]	[0]	[3]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[5]	[5]	[0]	[3]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[5]	[5]	[0]	[3]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[5]	[5]	[0]	[3]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[5]	[5]	[0]	[3]		
[PKSHA_COM] Packet Shaper 2500	[5]	[5]	[0]	[3]		
[ROUTER_COM] Router Cisco	[6]	[5]	[0]	[3]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[5]	[5]	[0]	[3]		
[REP_COM] Repetidoras	[3]	[5]	[0]	[2]		
[RAD_COM] Radios	[3]	[5]	[0]	[1]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[5]	[5]	[3]	[4]	[4]	
[MAIL_S] Correo Electrónico	[4]	[5]	[3]	[4]	[4]	
[STELF_S] Telefonía IP (Servicio)	[4]	[5]	[0]	[1]	[1]	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[1]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[5]					
[OTR_AUX] Otros Equipos Auxiliares	[1]		[0]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[4]					
[ZONA_SERV_I] Sala de Servidores	[4]					
[ZONA_REU_I] Sala de Reuniones	[3]					
[ZONA_ALM_I] Almacén	[4]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[4]					
[ZONA_OFTALL_I] Oficinas Talleres	[4]					
[ZONA_CONTROL_I] Sala Control	[4]					
[ZONA_TALL_I] Talleres	[4]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[4]	[6]	[0]			
[ADM_P] Personal de administración y logístico	[4]	[6]	[0]			
[JADM_P] Jefatura de administración	[4]	[6]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[4]	[6]	[0]			
[JUNI_P] Jefe de Unidad	[4]	[6]	[0]			
[SYMA_P] Personal SyMA	[3]	[6]	[0]			
[JSYMA_P] Jefatura SyMA	[5]	[6]	[0]			
[TOP_P] Tópico	[3]	[6]	[0]			
[OPE_P] Personal Operaciones	[3]	[6]	[0]			
[JOPE_P] Jefatura de Operaciones	[4]	[6]	[0]			
[CIV_P] Personal Ing. Civil	[3]	[6]	[0]			
[SGI_P] Personal SGI	[3]	[6]	[0]			
[CDOM_P] Coordinaciones O&M	[4]	[6]	[0]			

4.3. FASE: [PILAR] RECOMENDACIÓN

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	[4]	[4]	[2]			
[OS_SW] Sistema Operativo	[2]	[4]	[0]			
[OFIMATICA_SW] Ofimática	[2]	[4]	[0]			
[OTR_SW] Otros Software	[2]	[4]	[0]			
[PI_SW] PI Process Book	[4]	[4]	[2]			
[SCADA_SW] Sistema Tiempo Real	[4]	[4]	[2]			
[MAXIMO_SW] Maximo	[4]	[4]	[2]			
[PSOFT_SW] PeopleSoft	[4]	[4]	[2]			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[4]	[4]	[2]			
[GPS_SW] Sistema de Frecuencia	[4]	[4]	[2]			
[ANTIVIRUS_SW] Antivirus	[4]	[4]	[2]			
[HW] Hardware	[6]	[4]	[0]			
[DOM_HW] Controlador de Dominio Windows 2012 Server	[6]	[4]	[0]			
[FILE_HW] Servidor de Archivos	[6]	[4]	[0]			
[PI_HW] Servidor PI	[6]	[4]	[0]			
[BACKUP_HW] Servidor Copias de Seguridad	[6]	[4]	[0]			
[SPRINTER_HW] Servidor de Impresión	[4]	[4]	[0]			
[NVR_HW] Servidor de Grabación CCTV-NVR	[6]	[4]	[0]			
[STATION_HW] Estaciones de Trabajo	[4]	[4]	[0]			
[PRINTER_HW] Equipos de Impresión	[4]	[0]	[0]			
[PROYECTOR_HW] Proyectores Salas de Reuniones	[3]	[4]	[0]			
[CAM_HW] Cámaras de Video Vigilancia	[4]	[4]	[0]			
[COM] Comunicaciones	[5]	[4]	[0]	[2]		
[ANT_COM] Antena (Enlace Microondas)	[5]	[4]	[0]	[0]		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[5]	[4]	[0]	[0]		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[4]	[4]	[0]	[2]		
[SWSCADA_COM] Switch SCADA	[4]	[4]	[0]	[2]		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[4]	[4]	[0]	[2]		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[4]	[4]	[0]	[2]		
[SWCAM_COM] Switch Cámaras de Video vigilancia	[4]	[4]	[0]	[2]		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[4]	[4]	[0]	[2]		
[FOTALL_COM] Media Converter - Fibra óptica talleres	[4]	[4]	[0]	[2]		
[PKSHA_COM] Packet Shaper 2500	[4]	[4]	[0]	[2]		
[ROUTER_COM] Router Cisco	[5]	[4]	[0]	[2]		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[4]	[4]	[0]	[2]		
[REP_COM] Repetidoras	[2]	[4]	[0]	[1]		
[RAD_COM] Radios	[2]	[4]	[0]	[0]		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[www_s] internet	[4]	[3]	[1]	[2]	[3]	
[mail_s] correo electrónico	[3]	[4]	[2]	[3]	[3]	
[stelf_s] telefonía ip (servicio)	[3]	[4]	[0]	[0]	[0]	

[AUX] Equipamiento Auxiliar

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[0]	[0]	[0]			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[4]					
[OTR_AUX] Otros Equipos Auxiliares	[0]		[0]			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[3]					
[ZONA_SERV_I] Sala de Servidores	[3]					
[ZONA_REU_I] Sala de Reuniones	[2]					
[ZONA_ALM_I] Almacén	[3]					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[3]					
[ZONA_OFTALL_I] Oficinas Talleres	[3]					
[ZONA_CONTROL_I] Sala Control	[3]					
[ZONA_TALL_I] Talleres	[3]					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[3]	[4]	[0]			
[ADM_P] Personal de administración y logístico	[2]	[4]	[0]			
[JADM_P] Jefatura de administración	[3]	[4]	[0]			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[2]	[4]	[0]			
[JUNI_P] Jefe de Unidad	[3]	[4]	[0]			
[SYMA_P] Personal SyMA	[2]	[4]	[0]			
[JSYMA_P] Jefatura SyMA	[3]	[4]	[0]			
[TOP_P] Tópico	[2]	[5]	[0]			
[OPE_P] Personal Operaciones	[2]	[5]	[0]			
[JOPE_P] Jefatura de Operaciones	[3]	[4]	[0]			
[CIV_P] Personal Ing. Civil	[2]	[4]	[0]			
[SGI_P] Personal SGI	[2]	[4]	[0]			
[CDOM_P] Coordinaciones O&M	[3]	[4]	[0]			

4.4. [D] Disponibilidad

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	[8]	[5]	[4]	[4]
[OS_SW] Sistema Operativo	[6]	[3]	[2]	[2]
[OFIMATICA_SW] Ofimática	[6]	[3]	[2]	[2]
[OTR_SW] Otros Software	[6]	[3]	[2]	[2]
[PI_SW] PI Process Book	[8]	[5]	[4]	[4]
[SCADA_SW] Sistema Tiempo Real	[8]	[5]	[4]	[4]
[MAXIMO_SW] Maximo	[8]	[5]	[4]	[4]
[PSOFT_SW] PeopleSoft	[8]	[5]	[4]	[4]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[8]	[5]	[4]	[4]
[GPS_SW] Sistema de Frecuencia	[8]	[5]	[4]	[4]
[ANTIVIRUS_SW] Antivirus	[8]	[5]	[4]	[4]
[HW] Hardware	[10]	[8]	[7]	[6]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[10]	[8]	[7]	[6]
[FILE_HW] Servidor de Archivos	[10]	[8]	[7]	[6]
[PI_HW] Servidor PI	[10]	[8]	[7]	[6]

[BACKUP_HW] Servidor Copias de Seguridad	[10]	[8]	[7]	[6]
[SPRINTER_HW] Servidor de Impresión	[8]	[6]	[5]	[4]
[NVR_HW] Servidor de Grabación CCTV-NVR	[10]	[8]	[7]	[6]
[STATION_HW] Estaciones de Trabajo	[8]	[6]	[5]	[4]
[PRINTER_HW] Equipos de Impresión	[8]	[6]	[5]	[4]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[7]	[5]	[4]	[3]
[CAM_HW] Cámaras de Video Vigilancia	[8]	[6]	[5]	[4]
[COM] Comunicaciones	[9]	[7]	[6]	[5]
[ANT_COM] Antena (Enlace Microondas)	[9]	[7]	[6]	[5]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[9]	[7]	[6]	[5]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[8]	[6]	[5]	[4]
[SWSCADA_COM] Switch SCADA	[8]	[6]	[5]	[4]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[8]	[6]	[5]	[4]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[8]	[6]	[5]	[4]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[8]	[6]	[5]	[4]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[8]	[6]	[5]	[4]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[8]	[6]	[5]	[4]
[PKSHA_COM] Packet Shaper 2500	[8]	[6]	[5]	[4]
[ROUTER_COM] Router Cisco	[9]	[7]	[6]	[5]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[8]	[6]	[5]	[4]
[REP_COM] Repetidoras	[6]	[4]	[3]	[2]
[RAD_COM] Radios	[6]	[4]	[3]	[2]

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	[8]	[6]	[5]	[4]
[MAIL_S] Correo Electrónico	[7]	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[7]	[5]	[4]	[3]

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	[4]	[2]	[1]	[0]
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[8]	[6]	[5]	[4]
[OTR_AUX] Otros Equipos Auxiliares	[4]	[2]	[1]	[0]

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	[7]	[5]	[4]	[3]
[ZONA_SERV_I] Sala de Servidores	[7]	[5]	[4]	[3]
[ZONA_REU_I] Sala de Reuniones	[6]	[4]	[3]	[2]
[ZONA_ALM_I] Almacén	[7]	[5]	[4]	[3]
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[7]	[5]	[4]	[3]
[ZONA_OFTALL_I] Oficinas Talleres	[7]	[5]	[4]	[3]
[ZONA_CONTROL_I] Sala Control	[7]	[5]	[4]	[3]
[ZONA_TALL_I] Talleres	[7]	[5]	[4]	[3]

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	[7]	[5]	[4]	[3]
[ADM_P] Personal de administración y logístico	[6]	[4]	[4]	[2]
[JADM_P] Jefatura de administración	[7]	[5]	[4]	[3]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[6]	[4]	[4]	[2]
[JUNI_P] Jefe de Unidad	[7]	[5]	[4]	[3]
[SYMA_P] Personal SyMA	[6]	[4]	[3]	[2]
[JSYMA_P] Jefatura SyMA	[7]	[5]	[5]	[3]
[TOP_P] Tópico	[6]	[4]	[3]	[2]
[OPE_P] Personal Operaciones	[6]	[4]	[3]	[2]
[JOPE_P] Jefatura de Operaciones	[7]	[5]	[4]	[3]

[CIV_P] Personal Ing. Civil	[6]	[4]	[3]	[2]
[SGI_P] Personal SGI	[6]	[4]	[3]	[2]
[CDOM_P] Coordinaciones O&M	[7]	[5]	[4]	[3]

4.5. [I] Integridad de los datos

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	[8]	[5]	[5]	[4]
[OS_SW] Sistema Operativo	[8]	[5]	[5]	[4]
[OFIMATICA_SW] Ofimática	[8]	[5]	[5]	[4]
[OTR_SW] Otros Software	[8]	[5]	[5]	[4]
[PI_SW] PI Process Book	[8]	[5]	[5]	[4]
[SCADA_SW] Sistema Tiempo Real	[8]	[5]	[5]	[4]
[MAXIMO_SW] Maximo	[8]	[5]	[5]	[4]
[PSOFT_SW] PeopleSoft	[8]	[5]	[5]	[4]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[8]	[5]	[5]	[4]
[GPS_SW] Sistema de Frecuencia	[8]	[5]	[5]	[4]
[ANTIVIRUS_SW] Antivirus	[8]	[5]	[5]	[4]
[HW] Hardware	[8]	[6]	[5]	[4]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[8]	[5]	[5]	[4]
[FILE_HW] Servidor de Archivos	[8]	[6]	[5]	[4]
[PI_HW] Servidor PI	[8]	[5]	[5]	[4]
[BACKUP_HW] Servidor Copias de Seguridad	[8]	[5]	[5]	[4]
[SPRINTER_HW] Servidor de Impresión	[8]	[5]	[5]	[4]
[NVR_HW] Servidor de Grabación CCTV-NVR	[8]	[5]	[5]	[4]
[STATION_HW] Estaciones de Trabajo	[8]	[6]	[5]	[4]
[PRINTER_HW] Equipos de Impresión	[3]	[0]	[0]	[0]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[8]	[5]	[5]	[4]
[CAM_HW] Cámaras de Video Vigilancia	[8]	[5]	[5]	[4]
[COM] Comunicaciones	[8]	[6]	[5]	[4]
[ANT_COM] Antena (Enlace Microondas)	[8]	[6]	[5]	[4]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[8]	[6]	[5]	[4]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[8]	[6]	[5]	[4]
[SWSCADA_COM] Switch SCADA	[8]	[6]	[5]	[4]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[8]	[6]	[5]	[4]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[8]	[6]	[5]	[4]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[8]	[6]	[5]	[4]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[8]	[6]	[5]	[4]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[8]	[6]	[5]	[4]
[PKSHA_COM] Packet Shaper 2500	[8]	[6]	[5]	[4]
[ROUTER_COM] Router Cisco	[8]	[6]	[5]	[4]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[8]	[6]	[5]	[4]
[REP_COM] Repetidoras	[8]	[6]	[5]	[4]
[RAD_COM] Radios	[8]	[6]	[5]	[4]

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	[8]	[6]	[5]	[3]
[MAIL_S] Correo Electrónico	[8]	[6]	[5]	[4]
[STELF_S] Telefonía IP (Servicio)	[8]	[6]	[5]	[4]

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	[3]	[0]	[0]	[0]
[SAI_AUX] Sistema de Alimentación Ininterrumpida				
[OTR_AUX] Otros Equipos Auxiliares				

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	[8]	[6]	[6]	[4]
[ADM_P] Personal de administración y logístico	[8]	[6]	[6]	[4]
[JADM_P] Jefatura de administración	[8]	[6]	[6]	[4]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[8]	[6]	[6]	[4]
[JUNI_P] Jefe de Unidad	[8]	[6]	[6]	[4]
[SYMA_P] Personal SyMA	[8]	[6]	[6]	[4]
[JSYMA_P] Jefatura SyMA	[8]	[6]	[6]	[4]
[TOP_P] Tópico	[9]	[7]	[6]	[5]
[OPE_P] Personal Operaciones	[9]	[7]	[6]	[5]
[JOPE_P] Jefatura de Operaciones	[8]	[6]	[6]	[4]
[CIV_P] Personal Ing. Civil	[8]	[6]	[6]	[4]
[SGI_P] Personal SGI	[8]	[6]	[6]	[4]
[CDOM_P] Coordinaciones O&M	[8]	[6]	[6]	[4]

4.6. [C] Confidencialidad de los datos

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	[6]	[3]	[3]	[2]
[OS_SW] Sistema Operativo	[2]	[0]	[0]	[0]
[OFIMATICA_SW] Ofimática	[2]	[0]	[0]	[0]
[OTR_SW] Otros Software	[2]	[0]	[0]	[0]
[PI_SW] PI Process Book	[6]	[3]	[3]	[2]
[SCADA_SW] Sistema Tiempo Real	[6]	[3]	[3]	[2]
[MAXIMO_SW] Maximo	[6]	[3]	[3]	[2]
[PSOFT_SW] PeopleSoft	[6]	[3]	[3]	[2]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[6]	[3]	[3]	[2]
[GPS_SW] Sistema de Frecuencia	[6]	[3]	[3]	[2]
[ANTIVIRUS_SW] Antivirus	[6]	[3]	[3]	[2]
[HW] Hardware	[2]	[0]	[0]	[0]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[2]	[0]	[0]	[0]
[FILE_HW] Servidor de Archivos	[2]	[0]	[0]	[0]
[PI_HW] Servidor PI	[2]	[0]	[0]	[0]
[BACKUP_HW] Servidor Copias de Seguridad	[2]	[0]	[0]	[0]
[SPRINTER_HW] Servidor de Impresión	[2]	[0]	[0]	[0]
[NVR_HW] Servidor de Grabación CCTV-NVR	[2]	[0]	[0]	[0]
[STATION_HW] Estaciones de Trabajo	[2]	[0]	[0]	[0]
[PRINTER_HW] Equipos de Impresión	[0]	[0]	[0]	[0]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[2]	[0]	[0]	[0]
[CAM_HW] Cámaras de Video Vigilancia	[2]	[0]	[0]	[0]
[COM] Comunicaciones	[2]	[0]	[0]	[0]
[ANT_COM] Antena (Enlace Microondas)	[2]	[0]	[0]	[0]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[2]	[0]	[0]	[0]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[2]	[0]	[0]	[0]
[SWSCADA_COM] Switch SCADA	[2]	[0]	[0]	[0]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[2]	[0]	[0]	[0]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[2]	[0]	[0]	[0]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[2]	[0]	[0]	[0]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[2]	[0]	[0]	[0]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[2]	[0]	[0]	[0]
[PKSHA_COM] Packet Shaper 2500	[2]	[0]	[0]	[0]
[ROUTER_COM] Router Cisco	[2]	[0]	[0]	[0]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[2]	[0]	[0]	[0]
[REP_COM] Repetidoras	[2]	[0]	[0]	[0]
[RAD_COM] Radios	[2]	[0]	[0]	[0]

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	[6]	[4]	[3]	[1]
[MAIL_S] Correo Electrónico	[6]	[4]	[3]	[2]
[STELF_S] Telefonía IP (Servicio)	[2]	[0]	[0]	[0]

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	[0]	[0]	[0]	[0]
[SAI_AUX] Sistema de Alimentación Ininterrumpida				
[OTR_AUX] Otros Equipos Auxiliares	[2]	[0]	[0]	[0]

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	[2]	[0]	[0]	[0]
[ADM_P] Personal de administración y logístico	[2]	[0]	[0]	[0]
[JADM_P] Jefatura de administración	[2]	[0]	[0]	[0]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[2]	[0]	[0]	[0]
[JUNI_P] Jefe de Unidad	[2]	[0]	[0]	[0]
[SYMA_P] Personal SyMA	[2]	[0]	[0]	[0]
[JSYMA_P] Jefatura SyMA	[2]	[0]	[0]	[0]
[TOP_P] Tópico	[2]	[0]	[0]	[0]
[OPE_P] Personal Operaciones	[2]	[0]	[0]	[0]
[JOPE_P] Jefatura de Operaciones	[2]	[0]	[0]	[0]
[CIV_P] Personal Ing. Civil	[2]	[0]	[0]	[0]
[SGI_P] Personal SGI	[2]	[0]	[0]	[0]
[CDOM_P] Coordinaciones O&M	[2]	[0]	[0]	[0]

4.7. [A] Autenticidad de los usuarios y de la información

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software				
[OS_SW] Sistema Operativo				
[OFIMATICA_SW] Ofimática				
[OTR_SW] Otros Software				
[PI_SW] PI Process Book				
[SCADA_SW] Sistema Tiempo Real				
[MAXIMO_SW] Maximo				
[PSOFT_SW] PeopleSoft				
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras				
[GPS_SW] Sistema de Frecuencia				
[ANTIVIRUS_SW] Antivirus				
[HW] Hardware				
[DOM_HW] Controlador de Dominio Windows 2012 Server				
[FILE_HW] Servidor de Archivos				
[PI_HW] Servidor PI				
[BACKUP_HW] Servidor Copias de Seguridad				
[SPRINTER_HW] Servidor de Impresión				
[NVR_HW] Servidor de Grabación CCTV-NVR				
[STATION_HW] Estaciones de Trabajo				
[PRINTER_HW] Equipos de Impresión				
[PROYECTOR_HW] Proyectores Salas de Reuniones				
[CAM_HW] Cámaras de Video Vigilancia				
[COM] Comunicaciones	[6]	[4]	[3]	[2]
[ANT_COM] Antena (Enlace Microondas)	[1]	[0]	[0]	[0]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[1]	[0]	[0]	[0]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2	[6]	[4]	[3]	[2]

Piso				
[SWSCADA_COM] Switch SCADA	[6]	[4]	[3]	[2]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[6]	[4]	[3]	[2]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[6]	[4]	[3]	[2]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[6]	[4]	[3]	[2]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[6]	[4]	[3]	[2]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[6]	[4]	[3]	[2]
[PKSHA_COM] Packet Shaper 2500	[6]	[4]	[3]	[2]
[ROUTER_COM] Router Cisco	[6]	[4]	[3]	[2]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[6]	[4]	[3]	[2]
[REP_COM] Repetidoras	[5]	[3]	[2]	[1]
[RAD_COM] Radios	[4]	[2]	[1]	[0]

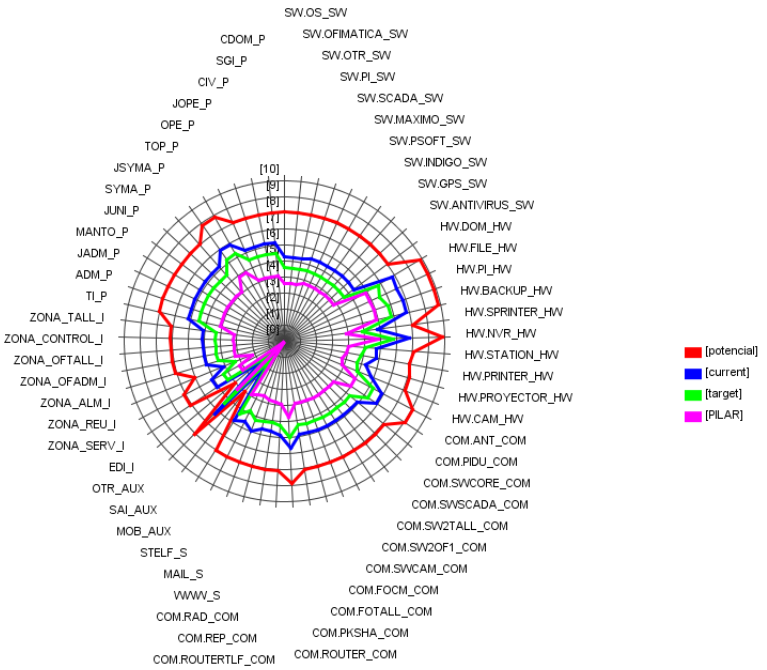
[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	[7]	[5]	[4]	[2]
[MAIL_S] Correo Electrónico	[7]	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[4]	[2]	[1]	[0]

4.8. [T] Trazabilidad del servicio y de los datos

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	[7]	[5]	[4]	[3]
[MAIL_S] Correo Electrónico	[7]	[5]	[4]	[3]
[STELF_S] Telefonía IP (Servicio)	[4]	[2]	[1]	[0]



ANEXO N° 09: RIESGO ACUMULADO

ANÁLISIS DE RIESGOS

PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO

PROYECTO:	UPH. Carhuaquero
DESCRIPCIÓN:	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE:	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN:	ORAZUL ENERGY PERU S.A.
VERSIÓN:	1
FECHA:	1/11/2017
BIBLIOTECA:	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. NIVELES DE CRITICIDAD

- {0}: = despreciable
- {1}: = bajo
- {2}: = medio
- {3}: = alto
- {4}: = muy alto
- {5}: = crítico
- {6}: = muy crítico
- {7}: = extremadamente crítico
- {8}: = desastre
- {9}: = catástrofe

4. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

5. DOMINIOS DE SEGURIDAD

- [base] Base

6. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado
  - [105.a] Se permite el acceso a Internet

- [105.b] Se permite la ejecución de programas sin autorización previa
- [105.c] Se permite la instalación de programas sin autorización previa
- [105.d] Se permite la conexión de dispositivos removibles
- [111.b] Conectado a un conjunto reducido y controlado de redes
- [111.d] Conectado a Internet
- [112.b] En un área de acceso abierto

7. FASES DEL PROYECTO

- [Potencial]
- [Current] situación actual
- [Target] situación objetivo
- [PILAR] recomendación

8. RIESGO ACUMULADO

8.1. FASE: [Potencial]

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{5,7}	{5,9}	{4,5}	-	-	-
[OS_SW] Sistema Operativo	{4,5}	{5,7}	{2,2}	-	-	-
[OFIMATICA_SW] Ofimática	{4,5}	{5,9}	{2,4}	-	-	-
[OTR_SW] Otros Software	{4,5}	{5,7}	{2,2}	-	-	-
[PI_SW] PI Process Book	{5,7}	{5,7}	{4,5}	-	-	-
[SCADA_SW] Sistema Tiempo Real	{5,7}	{5,7}	{4,5}	-	-	-
[MAXIMO_SW] Maximo	{5,7}	{5,7}	{4,5}	-	-	-
[PSOFT_SW] PeopleSoft	{5,7}	{5,7}	{4,5}	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{5,7}	{5,7}	{4,5}	-	-	-
[GPS_SW] Sistema de Frecuencia	{5,7}	{5,7}	{4,5}	-	-	-
[ANTIVIRUS_SW] Antivirus	{5,7}	{5,7}	{4,5}	-	-	-
[HW] Hardware	{6,8}	{6,6}	{3,1}	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	{6,4}	{4,8}	{2,2}	-	-	-
[FILE_HW] Servidor de Archivos	{6,8}	{4,8}	{2,2}	-	-	-
[PI_HW] Servidor PI	{6,8}	{4,8}	{2,2}	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	{6,8}	{4,8}	{2,2}	-	-	-
[SPRINTER_HW] Servidor de Impresión	{5,6}	{5,7}	{2,2}	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	{6,8}	{4,8}	{2,2}	-	-	-
[STATION_HW] Estaciones de Trabajo	{6,5}	{6,6}	{3,1}	-	-	-
[PRINTER_HW] Equipos de Impresión	{6,0}	{3,7}	{1,3}	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	{5,0}	{4,5}	{2,2}	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	{5,6}	{5,7}	{2,2}	-	-	-
[COM] Comunicaciones	{6,5}	{5,7}	{2,2}	{4,5}	-	-
[ANT_COM] Antena (Enlace Microondas)	{6,5}	{5,7}	{2,2}	{1,6}	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{6,3}	{5,7}	{2,2}	{1,6}	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[SWSCADA_COM] Switch SCADA	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[PKSHA_COM] Packet Shaper 2500	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[ROUTER_COM] Router Cisco	{6,2}	{5,7}	{2,2}	{4,5}	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{5,7}	{5,7}	{2,2}	{4,5}	-	-
[REP_COM] Repetidoras	{4,5}	{5,7}	{2,2}	{3,9}	-	-
[RAD_COM] Radios	{4,5}	{5,7}	{2,2}	{3,4}	-	-

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{6,2}	{6,2}	{5,0}	{5,6}	{5,3}	-
[MAIL_S] Correo Electrónico	{5,6}	{6,2}	{5,0}	{5,0}	{5,3}	-
[STELF_S] Telefonía IP (Servicio)	{5,9}	{6,5}	{3,0}	{4,1}	{4,8}	-

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{3,8}	{3,2}	{1,1}	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{6,2}	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	{3,8}	-	{2,3}	-	-	-

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{5,1}	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	{5,1}	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	{4,5}	-	-	-	-	-
[ZONA_ALM_I] Almacén	{5,1}	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{5,1}	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	{5,1}	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	{5,1}	-	-	-	-	-
[ZONA_TALL_I] Talleres	{5,1}	-	-	-	-	-

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{5,5}	{6,2}	{2,3}	-	-	-
[ADM_P] Personal de administración y logístico	{4,5}	{6,6}	{2,2}	-	-	-
[JADM_P] Jefatura de administración	{5,1}	{6,6}	{2,2}	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{5,4}	{6,6}	{2,2}	-	-	-
[JUNI_P] Jefe de Unidad	{5,1}	{6,6}	{2,2}	-	-	-
[SYMA_P] Personal SyMA	{4,5}	{6,6}	{2,2}	-	-	-
[JSYMA_P] Jefatura SyMA	{5,1}	{6,6}	{2,2}	-	-	-
[TOP_P] Tópico	{4,5}	{6,6}	{2,2}	-	-	-
[OPE_P] Personal Operaciones	{4,5}	{6,6}	{2,2}	-	-	-
[JOPE_P] Jefatura de Operaciones	{5,1}	{6,6}	{2,2}	-	-	-
[CIV_P] Personal Ing. Civil	{4,5}	{6,6}	{2,2}	-	-	-
[SGI_P] Personal SGI	{4,5}	{6,6}	{2,2}	-	-	-
[CDOM_P] Coordinaciones O&M	{5,1}	{6,6}	{2,2}	-	-	-

3.1. FASE: [CURRENT] SITUACIÓN ACTUAL

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{3,4}	{3,2}	{2,1}	-	-	-
[OS_SW] Sistema Operativo	{2,2}	{3,2}	{0,74}	-	-	-
[OFIMATICA_SW] Ofimática	{2,2}	{3,2}	{0,74}	-	-	-
[OTR_SW] Otros Software	{2,2}	{3,2}	{0,74}	-	-	-
[PI_SW] PI Process Book	{3,4}	{3,2}	{2,1}	-	-	-
[SCADA_SW] Sistema Tiempo Real	{3,4}	{3,2}	{2,1}	-	-	-
[MAXIMO_SW] Maximo	{3,4}	{3,2}	{2,1}	-	-	-
[PSOFT_SW] PeopleSoft	{3,4}	{3,2}	{2,1}	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{3,4}	{3,2}	{2,1}	-	-	-
[GPS_SW] Sistema de Frecuencia	{3,4}	{3,2}	{2,1}	-	-	-
[ANTIVIRUS_SW] Antivirus	{3,4}	{3,2}	{2,1}	-	-	-
[HW] Hardware	{4,9}	{4,6}	{1,3}	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	{4,6}	{2,5}	{0,82}	-	-	-
[FILE_HW] Servidor de Archivos	{4,8}	{2,8}	{0,88}	-	-	-
[PI_HW] Servidor PI	{4,9}	{2,5}	{0,82}	-	-	-

[BACKUP_HW] Servidor Copias de Seguridad	{4,9}	{2,5}	{0,82}	-	-	-
[SPRINTER_HW] Servidor de Impresión	{3,8}	{3,4}	{0,82}	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	{4,9}	{2,5}	{0,82}	-	-	-
[STATION_HW] Estaciones de Trabajo	{4,3}	{4,6}	{1,3}	-	-	-
[PRINTER_HW] Equipos de Impresión	{3,8}	{1,3}	{0,58}	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	{3,2}	{2,4}	{0,82}	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	{3,8}	{3,4}	{0,82}	-	-	-
[COM] Comunicaciones	{4,4}	{3,6}	{0,80}	{2,3}	-	-
[ANT_COM] Antena (Enlace Microondas)	{4,4}	{3,5}	{0,80}	{0,67}	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{4,4}	{3,6}	{0,80}	{0,67}	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[SWSCADA_COM] Switch SCADA	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[PKSHA_COM] Packet Shaper 2500	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[ROUTER_COM] Router Cisco	{4,2}	{3,6}	{0,80}	{2,3}	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{3,8}	{3,6}	{0,80}	{2,3}	-	-
[REP_COM] Repetidoras	{2,6}	{3,6}	{0,80}	{1,7}	-	-
[RAD_COM] Radios	{2,4}	{3,6}	{0,80}	{1,1}	-	-

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{3,9}	{3,8}	{2,6}	{3,2}	{3,0}	-
[MAIL_S] Correo Electrónico	{3,2}	{3,9}	{2,8}	{2,8}	{3,0}	-
[STELF_S] Telefonía IP (Servicio)	{3,8}	{4,4}	{0,98}	{2,1}	{2,7}	-

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{1,8}	{0,98}	{0,64}	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{4,2}	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	{1,7}	-	{0,86}	-	-	-

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{3,4}	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	{3,4}	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	{2,8}	-	-	-	-	-
[ZONA_ALM_I] Almacén	{3,4}	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{3,4}	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	{3,4}	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	{3,4}	-	-	-	-	-
[ZONA_TALL_I] Talleres	{3,4}	-	-	-	-	-

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{3,5}	{4,5}	{0,86}	-	-	-
[ADM_P] Personal de administración y logístico	{2,8}	{4,9}	{0,84}	-	-	-
[JADM_P] Jefatura de administración	{3,2}	{4,9}	{0,84}	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{3,7}	{4,9}	{0,89}	-	-	-
[JUNI_P] Jefe de Unidad	{3,2}	{4,9}	{0,84}	-	-	-
[SYMA_P] Personal SyMA	{2,6}	{4,9}	{0,84}	-	-	-
[JSYMA_P] Jefatura SyMA	{3,4}	{4,9}	{0,84}	-	-	-
[TOP_P] Tópico	{2,6}	{4,9}	{0,89}	-	-	-
[OPE_P] Personal Operaciones	{2,6}	{4,9}	{0,84}	-	-	-
[JOPE_P] Jefatura de Operaciones	{3,2}	{4,9}	{0,84}	-	-	-

[CIV_P] Personal Ing. Civil	{2,6}	{4,9}	{0,84}	-	-	-
[SGI_P] Personal SGI	{2,6}	{4,9}	{0,84}	-	-	-
[CDOM_P] Coordinaciones O&M	{3,2}	{4,9}	{0,84}	-	-	-

3.2. FASE: [Target] SITUACIÓN OBJETIVO

[E] EQUIPAMIENTO

activo	[D]	[I]	[C]	[A]	[T]	[V]
[SW] Software	{2,6}	{2,5}	{1,4}	-	-	-
[OS_SW] Sistema Operativo	{1,4}	{2,5}	{0,60}	-	-	-
[OFIMATICA_SW] Ofimática	{1,4}	{2,5}	{0,60}	-	-	-
[OTR_SW] Otros Software	{1,4}	{2,5}	{0,60}	-	-	-
[PI_SW] PI Process Book	{2,6}	{2,5}	{1,4}	-	-	-
[SCADA_SW] Sistema Tiempo Real	{2,6}	{2,5}	{1,4}	-	-	-
[MAXIMO_SW] Maximo	{2,6}	{2,5}	{1,4}	-	-	-
[PSOFT_SW] PeopleSoft	{2,6}	{2,5}	{1,4}	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{2,6}	{2,5}	{1,4}	-	-	-
[GPS_SW] Sistema de Frecuencia	{2,6}	{2,5}	{1,4}	-	-	-
[ANTIVIRUS_SW] Antivirus	{2,6}	{2,5}	{1,4}	-	-	-
[HW] Hardware	{4,1}	{4,1}	{0,94}	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	{3,8}	{1,9}	{0,66}	-	-	-
[FILE_HW] Servidor de Archivos	{3,8}	{2,2}	{0,75}	-	-	-
[PI_HW] Servidor PI	{4,1}	{1,9}	{0,66}	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	{4,1}	{1,9}	{0,66}	-	-	-
[SPRINTER_HW] Servidor de Impresión	{2,9}	{2,8}	{0,66}	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	{4,1}	{1,9}	{0,66}	-	-	-
[STATION_HW] Estaciones de Trabajo	{3,4}	{4,1}	{0,94}	-	-	-
[PRINTER_HW] Equipos de Impresión	{3,1}	{0,93}	{0,47}	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	{2,3}	{1,6}	{0,66}	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	{2,9}	{2,8}	{0,66}	-	-	-
[COM] Comunicaciones	{3,9}	{3,1}	{0,71}	{1,8}	-	-
[ANT_COM] Antena (Enlace Microondas)	{3,9}	{3,0}	{0,70}	{0,57}	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{3,8}	{3,1}	{0,71}	{0,57}	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[SWSCADA_COM] Switch SCADA	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[PKSHA_COM] Packet Shaper 2500	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[ROUTER_COM] Router Cisco	{3,6}	{3,1}	{0,71}	{1,8}	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{3,2}	{3,1}	{0,71}	{1,8}	-	-
[REP_COM] Repetidoras	{2,0}	{3,1}	{0,71}	{1,2}	-	-
[RAD_COM] Radios	{1,9}	{3,1}	{0,71}	{0,92}	-	-

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{3,2}	{3,2}	{2,1}	{2,6}	{2,3}	-
[MAIL_S] Correo Electrónico	{2,6}	{3,3}	{2,2}	{2,2}	{2,3}	-
[STELF_S] Telefonía IP (Servicio)	{3,2}	{3,9}	{0,88}	{1,6}	{2,2}	-

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{1,1}	{0,89}	{0,52}	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{3,5}	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	{0,98}	-	{0,74}	-	-	-

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{2,7}	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	{2,7}	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	{2,1}	-	-	-	-	-
[ZONA_ALM_I] Almacén	{2,7}	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{2,7}	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	{2,7}	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	{2,7}	-	-	-	-	-
[ZONA_TALL_I] Talleres	{2,7}	-	-	-	-	-

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{3,0}	{4,0}	{0,75}	-	-	-
[ADM_P] Personal de administración y logístico	{2,3}	{4,3}	{0,73}	-	-	-
[JADM_P] Jefatura de administración	{2,7}	{4,3}	{0,73}	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{3,2}	{4,3}	{0,78}	-	-	-
[JUNI_P] Jefe de Unidad	{2,7}	{4,3}	{0,73}	-	-	-
[SYMA_P] Personal SyMA	{2,1}	{4,3}	{0,73}	-	-	-
[JSYMA_P] Jefatura SyMA	{2,9}	{4,3}	{0,73}	-	-	-
[TOP_P] Tópico	{2,1}	{4,3}	{0,78}	-	-	-
[OPE_P] Personal Operaciones	{2,1}	{4,3}	{0,73}	-	-	-
[JOPE_P] Jefatura de Operaciones	{2,7}	{4,3}	{0,73}	-	-	-
[CIV_P] Personal Ing. Civil	{2,1}	{4,3}	{0,73}	-	-	-
[SGI_P] Personal SGI	{2,1}	{4,3}	{0,73}	-	-	-
[CDOM_P] Coordinaciones O&M	{2,7}	{4,3}	{0,73}	-	-	-

3.3. FASE: [PILAR] RECOMENDACIÓN

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{1,9}	{1,8}	{0,91}	-	-	-
[OS_SW] Sistema Operativo	{0,94}	{1,8}	{0,44}	-	-	-
[OFIMATICA_SW] Ofimática	{0,94}	{1,8}	{0,44}	-	-	-
[OTR_SW] Otros Software	{0,94}	{1,8}	{0,44}	-	-	-
[PI_SW] PI Process Book	{1,9}	{1,8}	{0,91}	-	-	-
[SCADA_SW] Sistema Tiempo Real	{1,9}	{1,8}	{0,91}	-	-	-
[MAXIMO_SW] Maximo	{1,9}	{1,8}	{0,91}	-	-	-
[PSOFT_SW] PeopleSoft	{1,9}	{1,8}	{0,91}	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{1,9}	{1,8}	{0,91}	-	-	-
[GPS_SW] Sistema de Frecuencia	{1,9}	{1,8}	{0,91}	-	-	-
[ANTIVIRUS_SW] Antivirus	{1,9}	{1,8}	{0,91}	-	-	-
[HW] Hardware	{3,2}	{2,9}	{0,66}	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	{2,9}	{0,99}	{0,51}	-	-	-
[FILE_HW] Servidor de Archivos	{3,2}	{0,98}	{0,49}	-	-	-
[PI_HW] Servidor PI	{3,2}	{0,99}	{0,51}	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	{3,2}	{0,99}	{0,51}	-	-	-
[SPRINTER_HW] Servidor de Impresión	{2,0}	{1,9}	{0,51}	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	{3,2}	{0,99}	{0,51}	-	-	-
[STATION_HW] Estaciones de Trabajo	{2,9}	{2,9}	{0,66}	-	-	-
[PRINTER_HW] Equipos de Impresión	{2,2}	{0,76}	{0,30}	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	{1,4}	{0,97}	{0,51}	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	{2,0}	{1,9}	{0,51}	-	-	-
[COM] Comunicaciones	{2,7}	{1,9}	{0,47}	{0,93}	-	-
[ANT_COM] Antena (Enlace Microondas)	{2,7}	{1,8}	{0,46}	{0,34}	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{2,6}	{1,9}	{0,47}	{0,34}	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[SWSCADA_COM] Switch SCADA	{2,0}	{1,9}	{0,46}	{0,93}	-	-

[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[PKSHA_COM] Packet Shaper 2500	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[ROUTER_COM] Router Cisco	{2,5}	{1,9}	{0,46}	{0,93}	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{2,0}	{1,9}	{0,46}	{0,93}	-	-
[REP_COM] Repetidoras	{0,96}	{1,9}	{0,46}	{0,81}	-	-
[RAD_COM] Radios	{0,95}	{1,9}	{0,46}	{0,69}	-	-

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{2,4}	{2,1}	{0,98}	{1,5}	{1,4}	-
[MAIL_S] Correo Electrónico	{1,8}	{2,4}	{1,2}	{1,2}	{1,4}	-
[STELF_S] Telefonía IP (Servicio)	{2,2}	{2,7}	{0,63}	{0,86}	{0,97}	-

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{0,82}	{0,70}	{0,31}	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{2,5}	-	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	{0,82}	-	{0,54}	-	-	-

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{1,7}	-	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	{1,6}	-	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	{1,0}	-	-	-	-	-
[ZONA_ALM_I] Almacén	{1,6}	-	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{1,6}	-	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	{1,6}	-	-	-	-	-
[ZONA_CONTROL_I] Sala Control	{1,6}	-	-	-	-	-
[ZONA_TALL_I] Talleres	{1,6}	-	-	-	-	-

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{1,9}	{2,7}	{0,54}	-	-	-
[ADM_P] Personal de administración y logístico	{1,1}	{3,1}	{0,52}	-	-	-
[JADM_P] Jefatura de administración	{1,6}	{3,1}	{0,52}	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{1,9}	{3,1}	{0,53}	-	-	-
[JUNI_P] Jefe de Unidad	{1,6}	{3,1}	{0,52}	-	-	-
[SYMA_P] Personal SyMA	{1,0}	{3,1}	{0,52}	-	-	-
[JSYMA_P] Jefatura SyMA	{1,6}	{3,1}	{0,52}	-	-	-
[TOP_P] Tópico	{1,0}	{3,1}	{0,53}	-	-	-
[OPE_P] Personal Operaciones	{1,0}	{3,1}	{0,52}	-	-	-
[JOPE_P] Jefatura de Operaciones	{1,6}	{3,1}	{0,52}	-	-	-
[CIV_P] Personal Ing. Civil	{1,0}	{3,1}	{0,52}	-	-	-
[SGI_P] Personal SGI	{1,0}	{3,1}	{0,52}	-	-	-
[CDOM_P] Coordinaciones O&M	{1,6}	{3,1}	{0,52}	-	-	-

3.4. [D] DISPONIBILIDAD

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{5,7}	{3,4}	{2,6}	{1,9}
[OS_SW] Sistema Operativo	{4,5}	{2,2}	{1,4}	{0,94}
[OFIMATICA_SW] Ofimática	{4,5}	{2,2}	{1,4}	{0,94}
[OTR_SW] Otros Software	{4,5}	{2,2}	{1,4}	{0,94}

[PI_SW] PI Process Book	{5,7}	{3,4}	{2,6}	{1,9}
[SCADA_SW] Sistema Tiempo Real	{5,7}	{3,4}	{2,6}	{1,9}
[MAXIMO_SW] Maximo	{5,7}	{3,4}	{2,6}	{1,9}
[PSOFT_SW] PeopleSoft	{5,7}	{3,4}	{2,6}	{1,9}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{5,7}	{3,4}	{2,6}	{1,9}
[GPS_SW] Sistema de Frecuencia	{5,7}	{3,4}	{2,6}	{1,9}
[ANTIVIRUS_SW] Antivirus	{5,7}	{3,4}	{2,6}	{1,9}
[HW] Hardware	{6,8}	{4,9}	{4,1}	{3,2}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{6,4}	{4,6}	{3,8}	{2,9}
[FILE_HW] Servidor de Archivos	{6,8}	{4,8}	{3,8}	{3,2}
[PI_HW] Servidor PI	{6,8}	{4,9}	{4,1}	{3,2}
[BACKUP_HW] Servidor Copias de Seguridad	{6,8}	{4,9}	{4,1}	{3,2}
[SPRINTER_HW] Servidor de Impresión	{5,6}	{3,8}	{2,9}	{2,0}
[NVR_HW] Servidor de Grabación CCTV-NVR	{6,8}	{4,9}	{4,1}	{3,2}
[STATION_HW] Estaciones de Trabajo	{6,5}	{4,3}	{3,4}	{2,9}
[PRINTER_HW] Equipos de Impresión	{6,0}	{3,8}	{3,1}	{2,2}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{5,0}	{3,2}	{2,3}	{1,4}
[CAM_HW] Cámaras de Video Vigilancia	{5,6}	{3,8}	{2,9}	{2,0}
[COM] Comunicaciones	{6,5}	{4,4}	{3,9}	{2,7}
[ANT_COM] Antena (Enlace Microondas)	{6,5}	{4,4}	{3,9}	{2,7}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{6,3}	{4,4}	{3,8}	{2,6}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SWSCADA_COM] Switch SCADA	{5,7}	{3,8}	{3,2}	{2,0}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{5,7}	{3,8}	{3,2}	{2,0}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{5,7}	{3,8}	{3,2}	{2,0}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{5,7}	{3,8}	{3,2}	{2,0}
[PKSHA_COM] Packet Shaper 2500	{5,7}	{3,8}	{3,2}	{2,0}
[ROUTER_COM] Router Cisco	{6,2}	{4,2}	{3,6}	{2,5}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{5,7}	{3,8}	{3,2}	{2,0}
[REP_COM] Repetidoras	{4,5}	{2,6}	{2,0}	{0,96}
[RAD_COM] Radios	{4,5}	{2,4}	{1,9}	{0,95}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{6,2}	{3,9}	{3,2}	{2,4}
[MAIL_S] Correo Electrónico	{5,6}	{3,2}	{2,6}	{1,8}
[STELF_S] Telefonía IP (Servicio)	{5,9}	{3,8}	{3,2}	{2,2}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{3,8}	{1,8}	{1,1}	{0,82}
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{6,2}	{4,2}	{3,5}	{2,5}
[OTR_AUX] Otros Equipos Auxiliares	{3,8}	{1,7}	{0,98}	{0,82}

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	{5,1}	{3,4}	{2,7}	{1,7}
[ZONA_SERV_I] Sala de Servidores	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_REU_I] Sala de Reuniones	{4,5}	{2,8}	{2,1}	{1,0}
[ZONA_ALM_I] Almacén	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_OFTALL_I] Oficinas Talleres	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_CONTROL_I] Sala Control	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_TALL_I] Talleres	{5,1}	{3,4}	{2,7}	{1,6}

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{5,5}	{3,5}	{3,0}	{1,9}
[ADM_P] Personal de administración y logístico	{4,5}	{2,8}	{2,3}	{1,1}
[JADM_P] Jefatura de administración	{5,1}	{3,2}	{2,7}	{1,6}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{5,4}	{3,7}	{3,2}	{1,9}
[JUNI_P] Jefe de Unidad	{5,1}	{3,2}	{2,7}	{1,6}
[SYMA_P] Personal SyMA	{4,5}	{2,6}	{2,1}	{1,0}
[JSYMA_P] Jefatura SyMA	{5,1}	{3,4}	{2,9}	{1,6}
[TOP_P] Tópico	{4,5}	{2,6}	{2,1}	{1,0}
[OPE_P] Personal Operaciones	{4,5}	{2,6}	{2,1}	{1,0}
[JOPE_P] Jefatura de Operaciones	{5,1}	{3,2}	{2,7}	{1,6}
[CIV_P] Personal Ing. Civil	{4,5}	{2,6}	{2,1}	{1,0}
[SGI_P] Personal SGI	{4,5}	{2,6}	{2,1}	{1,0}
[CDOM_P] Coordinaciones O&M	{5,1}	{3,2}	{2,7}	{1,6}

3.5. [I] INTEGRIDAD DE LOS DATOS

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{5,9}	{3,2}	{2,5}	{1,8}
[OS_SW] Sistema Operativo	{5,7}	{3,2}	{2,5}	{1,8}
[OFIMATICA_SW] Ofimática	{5,9}	{3,2}	{2,5}	{1,8}
[OTR_SW] Otros Software	{5,7}	{3,2}	{2,5}	{1,8}
[PI_SW] PI Process Book	{5,7}	{3,2}	{2,5}	{1,8}
[SCADA_SW] Sistema Tiempo Real	{5,7}	{3,2}	{2,5}	{1,8}
[MAXIMO_SW] Maximo	{5,7}	{3,2}	{2,5}	{1,8}
[PSOFT_SW] PeopleSoft	{5,7}	{3,2}	{2,5}	{1,8}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{5,7}	{3,2}	{2,5}	{1,8}
[GPS_SW] Sistema de Frecuencia	{5,7}	{3,2}	{2,5}	{1,8}
[ANTIVIRUS_SW] Antivirus	{5,7}	{3,2}	{2,5}	{1,8}
[HW] Hardware	{6,6}	{4,6}	{4,1}	{2,9}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{4,8}	{2,5}	{1,9}	{0,99}
[FILE_HW] Servidor de Archivos	{4,8}	{2,8}	{2,2}	{0,98}
[PI_HW] Servidor PI	{4,8}	{2,5}	{1,9}	{0,99}
[BACKUP_HW] Servidor Copias de Seguridad	{4,8}	{2,5}	{1,9}	{0,99}
[SPRINTER_HW] Servidor de Impresión	{5,7}	{3,4}	{2,8}	{1,9}
[NVR_HW] Servidor de Grabación CCTV-NVR	{4,8}	{2,5}	{1,9}	{0,99}
[STATION_HW] Estaciones de Trabajo	{6,6}	{4,6}	{4,1}	{2,9}
[PRINTER_HW] Equipos de Impresión	{3,7}	{1,3}	{0,93}	{0,76}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{4,5}	{2,4}	{1,6}	{0,97}
[CAM_HW] Cámaras de Video Vigilancia	{5,7}	{3,4}	{2,8}	{1,9}
[COM] Comunicaciones	{5,7}	{3,6}	{3,1}	{1,9}
[ANT_COM] Antena (Enlace Microondas)	{5,7}	{3,5}	{3,0}	{1,8}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{5,7}	{3,6}	{3,1}	{1,9}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{5,7}	{3,6}	{3,1}	{1,9}
[SWSCADA_COM] Switch SCADA	{5,7}	{3,6}	{3,1}	{1,9}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{5,7}	{3,6}	{3,1}	{1,9}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{5,7}	{3,6}	{3,1}	{1,9}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{5,7}	{3,6}	{3,1}	{1,9}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{5,7}	{3,6}	{3,1}	{1,9}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{5,7}	{3,6}	{3,1}	{1,9}
[PKSHA_COM] Packet Shaper 2500	{5,7}	{3,6}	{3,1}	{1,9}
[ROUTER_COM] Router Cisco	{5,7}	{3,6}	{3,1}	{1,9}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{5,7}	{3,6}	{3,1}	{1,9}
[REP_COM] Repetidoras	{5,7}	{3,6}	{3,1}	{1,9}
[RAD_COM] Radios	{5,7}	{3,6}	{3,1}	{1,9}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{6,2}	{3,8}	{3,2}	{2,1}
[MAIL_S] Correo Electrónico	{6,2}	{3,9}	{3,3}	{2,4}
[STELF_S] Telefonía IP (Servicio)	{6,5}	{4,4}	{3,9}	{2,7}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{3,2}	{0,98}	{0,89}	{0,70}
[SAI_AUX] Sistema de Alimentación Ininterrumpida	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	-	-	-	-

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	-	-	-	-
[ZONA_ALM_I] Almacén	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	-	-	-	-
[ZONA_CONTROL_I] Sala Control	-	-	-	-
[ZONA_TALL_I] Talleres	-	-	-	-

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{6,2}	{4,5}	{4,0}	{2,7}
[ADM_P] Personal de administración y logístico	{6,6}	{4,9}	{4,3}	{3,1}
[JADM_P] Jefatura de administración	{6,6}	{4,9}	{4,3}	{3,1}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{6,6}	{4,9}	{4,3}	{3,1}
[JUNI_P] Jefe de Unidad	{6,6}	{4,9}	{4,3}	{3,1}
[SYMA_P] Personal SyMA	{6,6}	{4,9}	{4,3}	{3,1}
[JSYMA_P] Jefatura SyMA	{6,6}	{4,9}	{4,3}	{3,1}
[TOP_P] Tópico	{6,6}	{4,9}	{4,3}	{3,1}
[OPE_P] Personal Operaciones	{6,6}	{4,9}	{4,3}	{3,1}
[JOPE_P] Jefatura de Operaciones	{6,6}	{4,9}	{4,3}	{3,1}
[CIV_P] Personal Ing. Civil	{6,6}	{4,9}	{4,3}	{3,1}
[SGI_P] Personal SGI	{6,6}	{4,9}	{4,3}	{3,1}
[CDOM_P] Coordinaciones O&M	{6,6}	{4,9}	{4,3}	{3,1}

3.6. [C] CONFIDENCIALIDAD DE LOS DATOS

[E] Equipamiento

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{4,5}	{2,1}	{1,4}	{0,91}
[OS_SW] Sistema Operativo	{2,2}	{0,74}	{0,60}	{0,44}
[OFIMATICA_SW] Ofimática	{2,4}	{0,74}	{0,60}	{0,44}
[OTR_SW] Otros Software	{2,2}	{0,74}	{0,60}	{0,44}
[PI_SW] PI Process Book	{4,5}	{2,1}	{1,4}	{0,91}
[SCADA_SW] Sistema Tiempo Real	{4,5}	{2,1}	{1,4}	{0,91}
[MAXIMO_SW] Maximo	{4,5}	{2,1}	{1,4}	{0,91}
[PSOFT_SW] PeopleSoft	{4,5}	{2,1}	{1,4}	{0,91}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{4,5}	{2,1}	{1,4}	{0,91}
[GPS_SW] Sistema de Frecuencia	{4,5}	{2,1}	{1,4}	{0,91}
[ANTIVIRUS_SW] Antivirus	{4,5}	{2,1}	{1,4}	{0,91}
[HW] Hardware	{3,1}	{1,3}	{0,94}	{0,66}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{2,2}	{0,82}	{0,66}	{0,51}
[FILE_HW] Servidor de Archivos	{2,2}	{0,88}	{0,75}	{0,49}
[PI_HW] Servidor PI	{2,2}	{0,82}	{0,66}	{0,51}

[BACKUP_HW] Servidor Copias de Seguridad	{2,2}	{0,82}	{0,66}	{0,51}
[SPRINTER_HW] Servidor de Impresión	{2,2}	{0,82}	{0,66}	{0,51}
[NVR_HW] Servidor de Grabación CCTV-NVR	{2,2}	{0,82}	{0,66}	{0,51}
[STATION_HW] Estaciones de Trabajo	{3,1}	{1,3}	{0,94}	{0,66}
[PRINTER_HW] Equipos de Impresión	{1,3}	{0,58}	{0,47}	{0,30}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{2,2}	{0,82}	{0,66}	{0,51}
[CAM_HW] Cámaras de Video Vigilancia	{2,2}	{0,82}	{0,66}	{0,51}
[COM] Comunicaciones	{2,2}	{0,80}	{0,71}	{0,47}
[ANT_COM] Antena (Enlace Microondas)	{2,2}	{0,80}	{0,70}	{0,46}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{2,2}	{0,80}	{0,71}	{0,47}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{2,2}	{0,80}	{0,71}	{0,46}
[SWSCADA_COM] Switch SCADA	{2,2}	{0,80}	{0,71}	{0,46}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{2,2}	{0,80}	{0,71}	{0,46}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{2,2}	{0,80}	{0,71}	{0,46}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{2,2}	{0,80}	{0,71}	{0,46}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{2,2}	{0,80}	{0,71}	{0,46}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{2,2}	{0,80}	{0,71}	{0,46}
[PKSHA_COM] Packet Shaper 2500	{2,2}	{0,80}	{0,71}	{0,46}
[ROUTER_COM] Router Cisco	{2,2}	{0,80}	{0,71}	{0,46}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{2,2}	{0,80}	{0,71}	{0,46}
[REP_COM] Repetidoras	{2,2}	{0,80}	{0,71}	{0,46}
[RAD_COM] Radios	{2,2}	{0,80}	{0,71}	{0,46}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,0}	{2,6}	{2,1}	{0,98}
[MAIL_S] Correo Electrónico	{5,0}	{2,8}	{2,2}	{1,2}
[STELF_S] Telefonía IP (Servicio)	{3,0}	{0,98}	{0,88}	{0,63}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{1,1}	{0,64}	{0,52}	{0,31}
[SAI_AUX] Sistema de Alimentación Ininterrumpida	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	{2,3}	{0,86}	{0,74}	{0,54}

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	-	-	-	-
[ZONA_ALM_I] Almacén	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	-	-	-	-
[ZONA_CONTROL_I] Sala Control	-	-	-	-
[ZONA_TALL_I] Talleres	-	-	-	-

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{2,3}	{0,86}	{0,75}	{0,54}
[ADM_P] Personal de administración y logístico	{2,2}	{0,84}	{0,73}	{0,52}
[JADM_P] Jefatura de administración	{2,2}	{0,84}	{0,73}	{0,52}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{2,2}	{0,89}	{0,78}	{0,53}
[JUNI_P] Jefe de Unidad	{2,2}	{0,84}	{0,73}	{0,52}
[SYMA_P] Personal SyMA	{2,2}	{0,84}	{0,73}	{0,52}
[JSYMA_P] Jefatura SyMA	{2,2}	{0,84}	{0,73}	{0,52}
[TOP_P] Tópico	{2,2}	{0,89}	{0,78}	{0,53}

[OPE_P] Personal Operaciones	{2,2}	{0,84}	{0,73}	{0,52}
[JOPE_P] Jefatura de Operaciones	{2,2}	{0,84}	{0,73}	{0,52}
[CIV_P] Personal Ing. Civil	{2,2}	{0,84}	{0,73}	{0,52}
[SGI_P] Personal SGI	{2,2}	{0,84}	{0,73}	{0,52}
[CDOM_P] Coordinaciones O&M	{2,2}	{0,84}	{0,73}	{0,52}

3.7. [A] AUTENTICIDAD DE LOS USUARIOS Y DE LA INFORMACIÓN

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	-	-	-	-
[OS_SW] Sistema Operativo	-	-	-	-
[OFIMATICA_SW] Ofimática	-	-	-	-
[OTR_SW] Otros Software	-	-	-	-
[PI_SW] PI Process Book	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	-	-	-	-
[MAXIMO_SW] Maximo	-	-	-	-
[PSOFT_SW] PeopleSoft	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	-	-	-	-
[GPS_SW] Sistema de Frecuencia	-	-	-	-
[ANTIVIRUS_SW] Antivirus	-	-	-	-
[HW] Hardware	-	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	-	-	-	-
[FILE_HW] Servidor de Archivos	-	-	-	-
[PI_HW] Servidor PI	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	-	-	-	-
[STATION_HW] Estaciones de Trabajo	-	-	-	-
[PRINTER_HW] Equipos de Impresión	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	-	-	-	-
[COM] Comunicaciones	{4,5}	{2,3}	{1,8}	{0,93}
[ANT_COM] Antena (Enlace Microondas)	{1,6}	{0,67}	{0,57}	{0,34}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{1,6}	{0,67}	{0,57}	{0,34}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SWSCADA_COM] Switch SCADA	{4,5}	{2,3}	{1,8}	{0,93}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{4,5}	{2,3}	{1,8}	{0,93}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{4,5}	{2,3}	{1,8}	{0,93}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{4,5}	{2,3}	{1,8}	{0,93}
[PKSHA_COM] Packet Shaper 2500	{4,5}	{2,3}	{1,8}	{0,93}
[ROUTER_COM] Router Cisco	{4,5}	{2,3}	{1,8}	{0,93}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{4,5}	{2,3}	{1,8}	{0,93}
[REP_COM] Repetidoras	{3,9}	{1,7}	{1,2}	{0,81}
[RAD_COM] Radios	{3,4}	{1,1}	{0,92}	{0,69}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,6}	{3,2}	{2,6}	{1,5}
[MAIL_S] Correo Electrónico	{5,0}	{2,8}	{2,2}	{1,2}
[STELF_S] Telefonía IP (Servicio)	{4,1}	{2,1}	{1,6}	{0,86}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	-	-	-	-

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	-	-	-	-
[ZONA_ALM_I] Almacén	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	-	-	-	-
[ZONA_CONTROL_I] Sala Control	-	-	-	-
[ZONA_TALL_I] Talleres	-	-	-	-

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	-	-	-	-
[ADM_P] Personal de administración y logístico	-	-	-	-
[JADM_P] Jefatura de administración	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	-	-	-	-
[JUNI_P] Jefe de Unidad	-	-	-	-
[SYMA_P] Personal SyMA	-	-	-	-
[JSYMA_P] Jefatura SyMA	-	-	-	-
[TOP_P] Tópico	-	-	-	-
[OPE_P] Personal Operaciones	-	-	-	-
[JOPE_P] Jefatura de Operaciones	-	-	-	-
[CIV_P] Personal Ing. Civil	-	-	-	-
[SGI_P] Personal SGI	-	-	-	-
[CDOM_P] Coordinaciones O&M	-	-	-	-

3.8. [T] Trazabilidad del servicio y de los datos

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	-	-	-	-
[OS_SW] Sistema Operativo	-	-	-	-
[OFIMATICA_SW] Ofimática	-	-	-	-
[OTR_SW] Otros Software	-	-	-	-
[PI_SW] PI Process Book	-	-	-	-
[SCADA_SW] Sistema Tiempo Real	-	-	-	-
[MAXIMO_SW] Maximo	-	-	-	-
[PSOFT_SW] PeopleSoft	-	-	-	-
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	-	-	-	-
[GPS_SW] Sistema de Frecuencia	-	-	-	-
[ANTIVIRUS_SW] Antivirus	-	-	-	-
[HW] Hardware	-	-	-	-
[DOM_HW] Controlador de Dominio Windows 2012 Server	-	-	-	-
[FILE_HW] Servidor de Archivos	-	-	-	-
[PI_HW] Servidor PI	-	-	-	-
[BACKUP_HW] Servidor Copias de Seguridad	-	-	-	-
[SPRINTER_HW] Servidor de Impresión	-	-	-	-
[NVR_HW] Servidor de Grabación CCTV-NVR	-	-	-	-
[STATION_HW] Estaciones de Trabajo	-	-	-	-
[PRINTER_HW] Equipos de Impresión	-	-	-	-
[PROYECTOR_HW] Proyectores Salas de Reuniones	-	-	-	-
[CAM_HW] Cámaras de Video Vigilancia	-	-	-	-

[COM] Comunicaciones	-	-	-	-
[ANT_COM] Antena (Enlace Microondas)	-	-	-	-
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	-	-	-	-
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	-	-	-	-
[SWSCADA_COM] Switch SCADA	-	-	-	-
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	-	-	-	-
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	-	-	-	-
[SWCAM_COM] Switch Cámaras de Video vigilancia	-	-	-	-
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	-	-	-	-
[FOTALL_COM] Media Converter - Fibra óptica talleres	-	-	-	-
[PKSHA_COM] Packet Shaper 2500	-	-	-	-
[ROUTER_COM] Router Cisco	-	-	-	-
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	-	-	-	-
[REP_COM] Repetidoras	-	-	-	-
[RAD_COM] Radios	-	-	-	-

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,3}	{3,0}	{2,3}	{1,4}
[MAIL_S] Correo Electrónico	{5,3}	{3,0}	{2,3}	{1,4}
[STELF_S] Telefonía IP (Servicio)	{4,8}	{2,7}	{2,2}	{0,97}

[AUX] EQUIPAMIENTO AUXILIAR

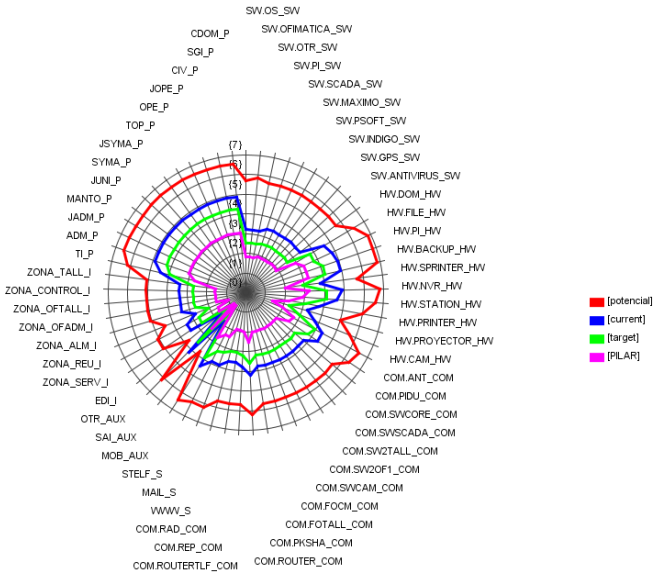
Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	-	-	-	-
[SAI_AUX] Sistema de Alimentación Ininterrumpida	-	-	-	-
[OTR_AUX] Otros Equipos Auxiliares	-	-	-	-

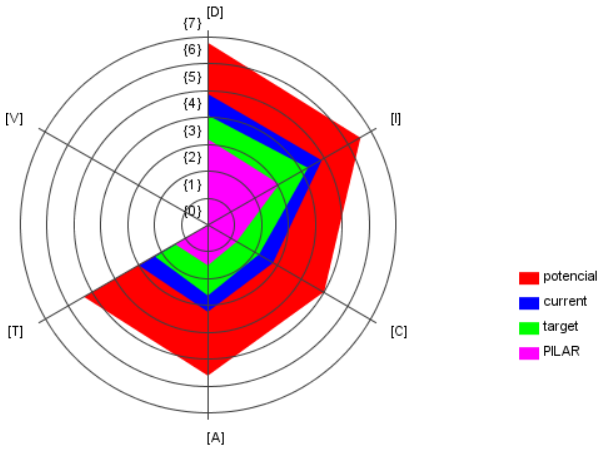
[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	-	-	-	-
[ZONA_SERV_I] Sala de Servidores	-	-	-	-
[ZONA_REU_I] Sala de Reuniones	-	-	-	-
[ZONA_ALM_I] Almacén	-	-	-	-
[ZONA_OFADM_I] Oficinas Casa de Máquinas	-	-	-	-
[ZONA_OFTALL_I] Oficinas Talleres	-	-	-	-
[ZONA_CONTROL_I] Sala Control	-	-	-	-
[ZONA_TALL_I] Talleres	-	-	-	-

[P] Personal

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	-	-	-	-
[ADM_P] Personal de administración y logístico	-	-	-	-
[JADM_P] Jefatura de administración	-	-	-	-
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	-	-	-	-
[JUNI_P] Jefe de Unidad	-	-	-	-
[SYMA_P] Personal SyMA	-	-	-	-
[JSYMA_P] Jefatura SyMA	-	-	-	-
[TOP_P] Tópico	-	-	-	-
[OPE_P] Personal Operaciones	-	-	-	-
[JOPE_P] Jefatura de Operaciones	-	-	-	-
[CIV_P] Personal Ing. Civil	-	-	-	-
[SGI_P] Personal SGI	-	-	-	-
[CDOM_P] Coordinaciones O&M	-	-	-	-


SW.OS_SW
SW.OFIMATICA_SW
SW.OTR_SW
SW.PI_SW
SW.SCADA_SW
SW.MAXIMO_SW
SW.PSOFT_SW
SW.INDIGO_SW
SW.GPS_SW
SW.ANTIVIRUS_SW
HW.DOM_HW
HW.FILE_HW
HW.PI_HW
HW.BACKUP_HW
HW.SPRINTER_HW
HW.NVR_HW
HW.STATION_HW
HW.PRINTER_HW
HW.PROYECTOR_HW
HW.CAM_HW
COM.ANT_COM
COM.PIDU_COM
COM.SWCORE_COM
COM.SWSCADA_COM
COM.SW2TALL_COM
COM.SW2OF1_COM
COM.SWCAM_COM
COM.FOCM_COM
COM.FOTALL_COM
COM.PKSHA_COM
COM.ROUTER_COM
COM.ROUTERTLF_COM
COM.REP_COM
COM.RAD_COM
WWW_S
MAIL_S
STELF_S
MOB_AUX
SAI_AUX
OTR_AUX
EDI_I
ZONA_SERV_I
ZONA_REU_I
ZONA_ALM_I
ZONA_OFADM_I
ZONA_OFTALL_I
ZONA_CONTROL_I
ZONA_TALL_I
TI_P
ADM_P
JADM_P
MANTO_P
JUNI_P
SYMA_P
JSYMA_P
TOP_P
OPE_P
JOPE_P
CIV_P
SGI_P
CDOM_P
{7}
{6}
{5}
{4}
{3}
{2}
{1}
{0}
[potencial]
[current]
[target]
[PILAR]


[D]
[I]
[C]
[A]
[T]
[V]
{7}
{6}
{5}
{4}
{3}
{2}
{1}
{0}
potencial
current
target
PILAR

ANEXO N° 10: RIESGO REPERCUTIDO

ANÁLISIS DE RIESGOS

PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO

PROYECTO	UPH. Carhuaquero
DESCRIPCIÓN	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN	ORAZUL ENERGY PERU S.A.
VERSIÓN	1
FECHA	1/11/2017
BIBLIOTECA	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. NIVELES DE CRITICIDAD

- {0}: = despreciable
- {1}: = bajo
- {2}: = medio
- {3}: = alto
- {4}: = muy alto
- {5}: = crítico
- {6}: = muy crítico
- {7}: = extremadamente crítico
- {8}: = desastre
- {9}: = catástrofe

4. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

5. DOMINIOS DE SEGURIDAD

- [base] Base

6. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado

- [105.a] Se permite el acceso a Internet
- [105.b] Se permite la ejecución de programas sin autorización previa
- [105.c] Se permite la instalación de programas sin autorización previa
- [105.d] Se permite la conexión de dispositivos removibles
- [111.b] Conectado a un conjunto reducido y controlado de redes
- [111.d] Conectado a Internet
- [112.b] En un área de acceso abierto

7. FASES DEL PROYECTO

- [Potencial]
- [Current] situación actual
- [Target] situación objetivo
- [PILAR] recomendación

8. RIESGO REPERCUTIDO

8.1. FASE: [Potencial]

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{5,7}	{4,5}	{4,5}			
[OS_SW] Sistema Operativo	{4,5}	{0,88}	{1,6}			
[OFIMATICA_SW] Ofimática	{1,0}	{3,0}	{0,92}			
[OTR_SW] Otros Software	{1,6}	{0,88}	{1,6}			
[PI_SW] PI Process Book	{5,7}	{4,5}	{4,5}			
[SCADA_SW] Sistema Tiempo Real	{5,7}	{4,5}	{4,5}			
[MAXIMO_SW] Maximo	{5,7}	{4,5}	{4,5}			
[PSOFT_SW] PeopleSoft	{5,7}	{4,5}	{4,5}			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{5,7}	{4,5}	{4,5}			
[GPS_SW] Sistema de Frecuencia	{5,7}	{4,5}	{4,5}			
[ANTIVIRUS_SW] Antivirus	{5,7}	{4,5}	{4,5}			
[HW] Hardware	{6,8}	{4,5}	{1,3}			
[DOM_HW] Controlador de Dominio Windows 2012 Server	{6,4}	{3,7}	{0,88}			
[FILE_HW] Servidor de Archivos	{6,8}	{3,7}	{0,88}			
[PI_HW] Servidor PI	{6,8}	{3,7}	{0,88}			
[BACKUP_HW] Servidor Copias de Seguridad	{6,8}	{3,7}	{0,88}			
[SPRINTER_HW] Servidor de Impresión	{5,6}	{4,5}	{0,88}			
[NVR_HW] Servidor de Grabación CCTV-NVR	{6,8}	{3,7}	{0,88}			
[STATION_HW] Estaciones de Trabajo	{6,5}	{3,7}	{1,3}			
[PRINTER_HW] Equipos de Impresión	{6,0}	{3,7}	{1,3}			
[PROYECTOR_HW] Proyectores Salas de Reuniones	{3,2}	{0,63}	{0,88}			
[CAM_HW] Cámaras de Video Vigilancia	{5,6}	{0,88}	{0,88}			
[COM] Comunicaciones	{6,5}	{3,4}	{0,88}	{4,5}		
[ANT_COM] Antena (Enlace Microondas)	{6,5}	{0,87}	{0,88}	{0,88}		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{6,3}	{0,88}	{0,88}	{0,88}		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{5,7}	{3,4}	{0,88}	{4,5}		
[SWSCADA_COM] Switch SCADA	{5,7}	{3,4}	{0,88}	{4,5}		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{5,7}	{0,88}	{0,88}	{4,5}		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{5,7}	{0,88}	{0,88}	{4,5}		
[SWCAM_COM] Switch Cámaras de Video vigilancia	{5,7}	{0,88}	{0,88}	{4,5}		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{5,7}	{0,88}	{0,88}	{4,5}		
[FOTALL_COM] Media Converter - Fibra óptica talleres	{5,7}	{0,88}	{0,88}	{4,5}		
[PKSHA_COM] Packet Shaper 2500	{5,7}	{0,88}	{0,88}	{4,5}		
[ROUTER_COM] Router Cisco	{6,2}	{3,4}	{0,88}	{4,5}		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{5,7}	{3,4}	{0,88}	{4,5}		
[REP_COM] Repetidoras	{4,5}	{0,88}	{0,88}	{3,9}		
[RAD_COM] Radios	{3,4}	{0,88}	{0,88}	{3,4}		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{6,2}	{5,0}	{5,0}	{5,6}	{5,3}	
[MAIL_S] Correo Electrónico	{5,6}	{5,0}	{5,0}	{5,0}	{5,3}	
[STELF_S] Telefonía IP (Servicio)	{5,9}	{4,1}	{3,0}	{4,1}	{4,8}	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{2,6}	{0,37}	{0,66}			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{6,2}					
[OTR_AUX] Otros Equipos Auxiliares	{2,6}		{0,89}			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{5,1}					
[ZONA_SERV_I] Sala de Servidores	{5,1}					
[ZONA_REU_I] Sala de Reuniones	{3,3}					
[ZONA_ALM_I] Almacén	{5,1}					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{5,1}					
[ZONA_OFTALL_I] Oficinas Talleres	{5,1}					
[ZONA_CONTROL_I] Sala Control	{5,1}					
[ZONA_TALL_I] Talleres	{5,1}					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{5,5}	{0,98}	{0,90}			
[ADM_P] Personal de administración y logístico	{3,4}	{1,3}	{0,88}			
[JADM_P] Jefatura de administración	{5,1}	{1,3}	{0,88}			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{4,2}	{1,3}	{0,88}			
[JUNI_P] Jefe de Unidad	{5,1}	{1,3}	{0,88}			
[SYMA_P] Personal SyMA	{3,4}	{1,3}	{0,88}			
[JSYMA_P] Jefatura SyMA	{5,1}	{1,3}	{0,88}			
[TOP_P] Tópico	{3,4}	{1,3}	{0,88}			
[OPE_P] Personal Operaciones	{3,4}	{1,3}	{0,88}			
[JOPE_P] Jefatura de Operaciones	{5,1}	{1,3}	{0,88}			
[CIV_P] Personal Ing. Civil	{3,4}	{1,3}	{0,88}			
[SGI_P] Personal SGI	{3,4}	{1,3}	{0,88}			
[CDOM_P] Coordinaciones O&M	{5,1}	{1,3}	{0,88}			

8.2. FASE: [CURRENT] SITUACIÓN ACTUAL

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{3,4}	{2,1}	{2,1}			
[OS_SW] Sistema Operativo	{2,2}	{0,38}	{0,62}			
[OFIMATICA_SW] Ofimática	{0,53}	{0,85}	{0,38}			
[OTR_SW] Otros Software	{0,65}	{0,38}	{0,62}			
[PI_SW] PI Process Book	{3,4}	{2,1}	{2,1}			
[SCADA_SW] Sistema Tiempo Real	{3,4}	{2,1}	{2,1}			
[MAXIMO_SW] Maximo	{3,4}	{2,1}	{2,1}			
[PSOFT_SW] PeopleSoft	{3,4}	{2,1}	{2,1}			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{3,4}	{2,1}	{2,1}			
[GPS_SW] Sistema de Frecuencia	{3,4}	{2,1}	{2,1}			
[ANTIVIRUS_SW] Antivirus	{3,4}	{2,1}	{2,1}			
[HW] Hardware	{4,9}	{2,2}	{0,71}			
[DOM_HW] Controlador de Dominio Windows 2012 Server	{4,6}	{1,3}	{0,47}			
[FILE_HW] Servidor de Archivos	{4,8}	{1,6}	{0,52}			
[PI_HW] Servidor PI	{4,9}	{1,3}	{0,47}			

[BACKUP_HW] Servidor Copias de Seguridad	{4,9}	{1,3}	{0,47}			
[SPRINTER_HW] Servidor de Impresión	{3,8}	{2,2}	{0,47}			
[NVR_HW] Servidor de Grabación CCTV-NVR	{4,9}	{1,3}	{0,47}			
[STATION_HW] Estaciones de Trabajo	{4,3}	{1,7}	{0,71}			
[PRINTER_HW] Equipos de Impresión	{3,8}	{1,3}	{0,58}			
[PROYECTOR_HW] Proyectores Salas de Reuniones	{1,4}	{0,22}	{0,47}			
[CAM_HW] Cámaras de Video Vigilancia	{3,8}	{0,41}	{0,47}			
[COM] Comunicaciones	{4,4}	{1,2}	{0,45}	{2,3}		
[ANT_COM] Antena (Enlace Microondas)	{4,4}	{0,44}	{0,44}	{0,43}		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{4,4}	{0,45}	{0,45}	{0,43}		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{3,8}	{1,2}	{0,45}	{2,3}		
[SWSCADA_COM] Switch SCADA	{3,8}	{1,2}	{0,45}	{2,3}		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{3,8}	{0,45}	{0,45}	{2,3}		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{3,8}	{0,45}	{0,45}	{2,3}		
[SWCAM_COM] Switch Cámaras de Video vigilancia	{3,8}	{0,45}	{0,45}	{2,3}		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{3,8}	{0,45}	{0,45}	{2,3}		
[FOTALL_COM] Media Converter - Fibra óptica talleres	{3,8}	{0,45}	{0,45}	{2,3}		
[PKSHA_COM] Packet Shaper 2500	{3,8}	{0,45}	{0,45}	{2,3}		
[ROUTER_COM] Router Cisco	{4,2}	{1,2}	{0,45}	{2,3}		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{3,8}	{1,2}	{0,45}	{2,3}		
[REP_COM] Repetidoras	{2,6}	{0,45}	{0,45}	{1,7}		
[RAD_COM] Radios	{1,3}	{0,45}	{0,45}	{1,1}		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{3,9}	{2,6}	{2,6}	{3,2}	{3,0}	
[MAIL_S] Correo Electrónico	{3,2}	{2,7}	{2,8}	{2,8}	{3,0}	
[STELF_S] Telefonía IP (Servicio)	{3,8}	{2,1}	{0,98}	{2,1}	{2,7}	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{0,93}	{0,01}	{0,29}			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{4,2}					
[OTR_AUX] Otros Equipos Auxiliares	{0,91}		{0,51}			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{3,4}					
[ZONA_SERV_I] Sala de Servidores	{3,4}					
[ZONA_REU_I] Sala de Reuniones	{1,6}					
[ZONA_ALM_I] Almacén	{3,4}					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{3,4}					
[ZONA_OFTALL_I] Oficinas Talleres	{3,4}					
[ZONA_CONTROL_I] Sala Control	{3,4}					
[ZONA_TALL_I] Talleres	{3,4}					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{3,5}	{0,64}	{0,51}			
[ADM_P] Personal de administración y logístico	{1,7}	{0,71}	{0,49}			
[JADM_P] Jefatura de administración	{3,2}	{0,71}	{0,49}			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{2,5}	{0,71}	{0,54}			
[JUNI_P] Jefe de Unidad	{3,2}	{0,71}	{0,49}			
[SYMA_P] Personal SyMA	{1,4}	{0,71}	{0,49}			
[JSYMA_P] Jefatura SyMA	{3,4}	{0,71}	{0,49}			
[TOP_P] Tópico	{1,4}	{0,71}	{0,54}			
[OPE_P] Personal Operaciones	{1,4}	{0,71}	{0,49}			
[JOPE_P] Jefatura de Operaciones	{3,2}	{0,71}	{0,49}			

[CIV_P] Personal Ing. Civil	{1,4}	{0,71}	{0,49}			
[SGI_P] Personal SGI	{1,4}	{0,71}	{0,49}			
[CDOM_P] Coordinaciones O&M	{3,2}	{0,71}	{0,49}			

8.3. FASE: [Target] SITUACIÓN OBJETIVO

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{2,6}	{1,4}	{1,4}			
[OS_SW] Sistema Operativo	{1,4}	{0,24}	{0,48}			
[OFIMATICA_SW] Ofimática	{0,36}	{0,71}	{0,24}			
[OTR_SW] Otros Software	{0,49}	{0,24}	{0,48}			
[PI_SW] PI Process Book	{2,6}	{1,4}	{1,4}			
[SCADA_SW] Sistema Tiempo Real	{2,6}	{1,4}	{1,4}			
[MAXIMO_SW] Maximo	{2,6}	{1,4}	{1,4}			
[PSOFT_SW] PeopleSoft	{2,6}	{1,4}	{1,4}			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{2,6}	{1,4}	{1,4}			
[GPS_SW] Sistema de Frecuencia	{2,6}	{1,4}	{1,4}			
[ANTIVIRUS_SW] Antivirus	{2,6}	{1,4}	{1,4}			
[HW] Hardware	{4,1}	{1,6}	{0,59}			
[DOM_HW] Controlador de Dominio Windows 2012 Server	{3,8}	{0,93}	{0,31}			
[FILE_HW] Servidor de Archivos	{3,8}	{1,0}	{0,40}			
[PI_HW] Servidor PI	{4,1}	{0,93}	{0,31}			
[BACKUP_HW] Servidor Copias de Seguridad	{4,1}	{0,93}	{0,31}			
[SPRINTER_HW] Servidor de Impresión	{2,9}	{1,6}	{0,31}			
[NVR_HW] Servidor de Grabación CCTV-NVR	{4,1}	{0,93}	{0,31}			
[STATION_HW] Estaciones de Trabajo	{3,4}	{1,1}	{0,59}			
[PRINTER_HW] Equipos de Impresión	{3,1}	{0,93}	{0,47}			
[PROYECTOR_HW] Proyectores Salas de Reuniones	{0,91}	{0,06}	{0,31}			
[CAM_HW] Cámaras de Video Vigilancia	{2,9}	{0,29}	{0,31}			
[COM] Comunicaciones	{3,9}	{0,94}	{0,35}	{1,8}		
[ANT_COM] Antena (Enlace Microondas)	{3,9}	{0,34}	{0,34}	{0,33}		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{3,8}	{0,35}	{0,35}	{0,33}		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{3,2}	{0,94}	{0,35}	{1,8}		
[SWSCADA_COM] Switch SCADA	{3,2}	{0,94}	{0,35}	{1,8}		
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{3,2}	{0,35}	{0,35}	{1,8}		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{3,2}	{0,35}	{0,35}	{1,8}		
[SWCAM_COM] Switch Cámaras de Video vigilancia	{3,2}	{0,35}	{0,35}	{1,8}		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{3,2}	{0,35}	{0,35}	{1,8}		
[FOTALL_COM] Media Converter - Fibra óptica talleres	{3,2}	{0,35}	{0,35}	{1,8}		
[PKSHA_COM] Packet Shaper 2500	{3,2}	{0,35}	{0,35}	{1,8}		
[ROUTER_COM] Router Cisco	{3,6}	{0,94}	{0,35}	{1,8}		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{3,2}	{0,94}	{0,35}	{1,8}		
[REP_COM] Repetidoras	{2,0}	{0,35}	{0,35}	{1,2}		
[RAD_COM] Radios	{0,95}	{0,35}	{0,35}	{0,92}		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{3,2}	{2,1}	{2,1}	{2,6}	{2,3}	
[MAIL_S] Correo Electrónico	{2,6}	{2,1}	{2,2}	{2,2}	{2,3}	
[STELF_S] Telefonía IP (Servicio)	{3,2}	{1,5}	{0,88}	{1,6}	{2,2}	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{0,78}	{0,01}	{0,16}			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{3,5}					
[OTR_AUX] Otros Equipos Auxiliares	{0,75}		{0,39}			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{2,7}					
[ZONA_SERV_I] Sala de Servidores	{2,7}					
[ZONA_REU_I] Sala de Reuniones	{0,97}					
[ZONA_ALM_I] Almacén	{2,7}					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{2,7}					
[ZONA_OFTALL_I] Oficinas Talleres	{2,7}					
[ZONA_CONTROL_I] Sala Control	{2,7}					
[ZONA_TALL_I] Talleres	{2,7}					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{3,0}	{0,53}	{0,40}			
[ADM_P] Personal de administración y logístico	{1,1}	{0,60}	{0,38}			
[JADM_P] Jefatura de administración	{2,7}	{0,60}	{0,38}			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{2,0}	{0,60}	{0,43}			
[JUNI_P] Jefe de Unidad	{2,7}	{0,60}	{0,38}			
[SYMA_P] Personal SyMA	{0,97}	{0,60}	{0,38}			
[JSYMA_P] Jefatura SyMA	{2,9}	{0,60}	{0,38}			
[TOP_P] Tópico	{0,97}	{0,60}	{0,43}			
[OPE_P] Personal Operaciones	{0,97}	{0,60}	{0,38}			
[JOPE_P] Jefatura de Operaciones	{2,7}	{0,60}	{0,38}			
[CIV_P] Personal Ing. Civil	{0,97}	{0,60}	{0,38}			
[SGI_P] Personal SGI	{0,97}	{0,60}	{0,38}			
[CDOM_P] Coordinaciones O&M	{2,7}	{0,60}	{0,38}			

8.4. FASE: [PILAR] RECOMENDACIÓN

[E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[SW] Software	{1,9}	{0,91}	{0,91}			
[OS_SW] Sistema Operativo	{0,94}	{0,09}	{0,33}			
[OFIMATICA_SW] Ofimática	{0,23}	{0,56}	{0,09}			
[OTR_SW] Otros Software	{0,35}	{0,09}	{0,33}			
[PI_SW] PI Process Book	{1,9}	{0,91}	{0,91}			
[SCADA_SW] Sistema Tiempo Real	{1,9}	{0,91}	{0,91}			
[MAXIMO_SW] Maximo	{1,9}	{0,91}	{0,91}			
[PSOFT_SW] PeopleSoft	{1,9}	{0,91}	{0,91}			
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{1,9}	{0,91}	{0,91}			
[GPS_SW] Sistema de Frecuencia	{1,9}	{0,91}	{0,91}			
[ANTIVIRUS_SW] Antivirus	{1,9}	{0,91}	{0,91}			
[HW] Hardware	{3,2}	{0,93}	{0,30}			
[DOM_HW] Controlador de Dominio Windows 2012 Server	{2,9}	{0,76}	{0,16}			
[FILE_HW] Servidor de Archivos	{3,2}	{0,74}	{0,14}			
[PI_HW] Servidor PI	{3,2}	{0,76}	{0,16}			
[BACKUP_HW] Servidor Copias de Seguridad	{3,2}	{0,76}	{0,16}			
[SPRINTER_HW] Servidor de Impresión	{2,0}	{0,93}	{0,16}			
[NVR_HW] Servidor de Grabación CCTV-NVR	{3,2}	{0,76}	{0,16}			
[STATION_HW] Estaciones de Trabajo	{2,9}	{0,78}	{0,30}			
[PRINTER_HW] Equipos de Impresión	{2,2}	{0,76}	{0,30}			
[PROYECTOR_HW] Proyectores Salas de Reuniones	{0,73}	{0,01}	{0,16}			
[CAM_HW] Cámaras de Video Vigilancia	{2,0}	{0,11}	{0,16}			
[COM] Comunicaciones	{2,7}	{0,70}	{0,11}	{0,93}		
[ANT_COM] Antena (Enlace Microondas)	{2,7}	{0,10}	{0,11}	{0,11}		
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{2,6}	{0,11}	{0,11}	{0,11}		
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{2,0}	{0,70}	{0,11}	{0,93}		
[SWSCADA_COM] Switch SCADA	{2,0}	{0,70}	{0,11}	{0,93}		

[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{2,0}	{0,11}	{0,11}	{0,93}		
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{2,0}	{0,11}	{0,11}	{0,93}		
[SWCAM_COM] Switch Cámaras de Video vigilancia	{2,0}	{0,11}	{0,11}	{0,93}		
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{2,0}	{0,11}	{0,11}	{0,93}		
[FOTALL_COM] Media Converter - Fibra óptica talleres	{2,0}	{0,11}	{0,11}	{0,93}		
[PKSHA_COM] Packet Shaper 2500	{2,0}	{0,11}	{0,11}	{0,93}		
[ROUTER_COM] Router Cisco	{2,5}	{0,70}	{0,11}	{0,93}		
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{2,0}	{0,70}	{0,11}	{0,93}		
[REP_COM] Repetidoras	{0,96}	{0,11}	{0,11}	{0,81}		
[RAD_COM] Radios	{0,71}	{0,11}	{0,11}	{0,69}		

[S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	{2,4}	{0,97}	{0,98}	{1,5}	{1,4}	
[MAIL_S] Correo Electrónico	{1,8}	{1,2}	{1,2}	{1,2}	{1,4}	
[STELF_S] Telefonía IP (Servicio)	{2,2}	{0,86}	{0,63}	{0,86}	{0,97}	

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	{0,58}	{0,01}	{0,01}			
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{2,5}					
[OTR_AUX] Otros Equipos Auxiliares	{0,58}		{0,18}			

[I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	{1,7}					
[ZONA_SERV_I] Sala de Servidores	{1,6}					
[ZONA_REU_I] Sala de Reuniones	{0,77}					
[ZONA_ALM_I] Almacén	{1,6}					
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{1,6}					
[ZONA_OFTALL_I] Oficinas Talleres	{1,6}					
[ZONA_CONTROL_I] Sala Control	{1,6}					
[ZONA_TALL_I] Talleres	{1,6}					

[P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	{1,9}	{0,28}	{0,19}			
[ADM_P] Personal de administración y logístico	{0,77}	{0,35}	{0,17}			
[JADM_P] Jefatura de administración	{1,6}	{0,35}	{0,17}			
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{0,95}	{0,35}	{0,18}			
[JUNI_P] Jefe de Unidad	{1,6}	{0,35}	{0,17}			
[SYMA_P] Personal SyMA	{0,76}	{0,35}	{0,17}			
[JSYMA_P] Jefatura SyMA	{1,6}	{0,35}	{0,17}			
[TOP_P] Tópico	{0,76}	{0,35}	{0,18}			
[OPE_P] Personal Operaciones	{0,76}	{0,35}	{0,17}			
[JOPE_P] Jefatura de Operaciones	{1,6}	{0,35}	{0,17}			
[CIV_P] Personal Ing. Civil	{0,76}	{0,35}	{0,17}			
[SGI_P] Personal SGI	{0,76}	{0,35}	{0,17}			
[CDOM_P] Coordinaciones O&M	{1,6}	{0,35}	{0,17}			

8.5. [D] DISPONIBILIDAD

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{5,7}	{3,4}	{2,6}	{1,9}
[OS_SW] Sistema Operativo	{4,5}	{2,2}	{1,4}	{0,94}
[OFIMATICA_SW] Ofimática	{1,0}	{0,53}	{0,36}	{0,23}
[OTR_SW] Otros Software	{1,6}	{0,65}	{0,49}	{0,35}
[PI_SW] PI Process Book	{5,7}	{3,4}	{2,6}	{1,9}
[SCADA_SW] Sistema Tiempo Real	{5,7}	{3,4}	{2,6}	{1,9}
[MAXIMO_SW] Maximo	{5,7}	{3,4}	{2,6}	{1,9}
[PSOFT_SW] PeopleSoft	{5,7}	{3,4}	{2,6}	{1,9}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{5,7}	{3,4}	{2,6}	{1,9}
[GPS_SW] Sistema de Frecuencia	{5,7}	{3,4}	{2,6}	{1,9}
[ANTIVIRUS_SW] Antivirus	{5,7}	{3,4}	{2,6}	{1,9}
[HW] Hardware	{6,8}	{4,9}	{4,1}	{3,2}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{6,4}	{4,6}	{3,8}	{2,9}
[FILE_HW] Servidor de Archivos	{6,8}	{4,8}	{3,8}	{3,2}
[PI_HW] Servidor PI	{6,8}	{4,9}	{4,1}	{3,2}
[BACKUP_HW] Servidor Copias de Seguridad	{6,8}	{4,9}	{4,1}	{3,2}
[SPRINTER_HW] Servidor de Impresión	{5,6}	{3,8}	{2,9}	{2,0}
[NVR_HW] Servidor de Grabación CCTV-NVR	{6,8}	{4,9}	{4,1}	{3,2}
[STATION_HW] Estaciones de Trabajo	{6,5}	{4,3}	{3,4}	{2,9}
[PRINTER_HW] Equipos de Impresión	{6,0}	{3,8}	{3,1}	{2,2}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{3,2}	{1,4}	{0,91}	{0,73}
[CAM_HW] Cámaras de Video Vigilancia	{5,6}	{3,8}	{2,9}	{2,0}
[COM] Comunicaciones	{6,5}	{4,4}	{3,9}	{2,7}
[ANT_COM] Antena (Enlace Microondas)	{6,5}	{4,4}	{3,9}	{2,7}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{6,3}	{4,4}	{3,8}	{2,6}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SWSCADA_COM] Switch SCADA	{5,7}	{3,8}	{3,2}	{2,0}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{5,7}	{3,8}	{3,2}	{2,0}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{5,7}	{3,8}	{3,2}	{2,0}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{5,7}	{3,8}	{3,2}	{2,0}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{5,7}	{3,8}	{3,2}	{2,0}
[PKSHA_COM] Packet Shaper 2500	{5,7}	{3,8}	{3,2}	{2,0}
[ROUTER_COM] Router Cisco	{6,2}	{4,2}	{3,6}	{2,5}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{5,7}	{3,8}	{3,2}	{2,0}
[REP_COM] Repetidoras	{4,5}	{2,6}	{2,0}	{0,96}
[RAD_COM] Radios	{3,4}	{1,3}	{0,95}	{0,71}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{6,2}	{3,9}	{3,2}	{2,4}
[MAIL_S] Correo Electrónico	{5,6}	{3,2}	{2,6}	{1,8}
[STELF_S] Telefonía IP (Servicio)	{5,9}	{3,8}	{3,2}	{2,2}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{2,6}	{0,93}	{0,78}	{0,58}
[SAI_AUX] Sistema de Alimentación Ininterrumpida	{6,2}	{4,2}	{3,5}	{2,5}
[OTR_AUX] Otros Equipos Auxiliares	{2,6}	{0,91}	{0,75}	{0,58}

[I] INSTALACIONES

Activo	[potencial]	[current]	[target]	[pilar]
[EDI_I] Edificio	{5,1}	{3,4}	{2,7}	{1,7}
[ZONA_SERV_I] Sala de Servidores	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_REU_I] Sala de Reuniones	{3,3}	{1,6}	{0,97}	{0,77}
[ZONA_ALM_I] Almacén	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_OFADM_I] Oficinas Casa de Máquinas	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_OFTALL_I] Oficinas Talleres	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_CONTROL_I] Sala Control	{5,1}	{3,4}	{2,7}	{1,6}
[ZONA_TALL_I] Talleres	{5,1}	{3,4}	{2,7}	{1,6}

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{5,5}	{3,5}	{3,0}	{1,9}
[ADM_P] Personal de administración y logístico	{3,4}	{1,7}	{1,1}	{0,77}
[JADM_P] Jefatura de administración	{5,1}	{3,2}	{2,7}	{1,6}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{4,2}	{2,5}	{2,0}	{0,95}
[JUNI_P] Jefe de Unidad	{5,1}	{3,2}	{2,7}	{1,6}
[SYMA_P] Personal SyMA	{3,4}	{1,4}	{0,97}	{0,76}
[JSYMA_P] Jefatura SyMA	{5,1}	{3,4}	{2,9}	{1,6}
[TOP_P] Tópico	{3,4}	{1,4}	{0,97}	{0,76}
[OPE_P] Personal Operaciones	{3,4}	{1,4}	{0,97}	{0,76}
[JOPE_P] Jefatura de Operaciones	{5,1}	{3,2}	{2,7}	{1,6}
[CIV_P] Personal Ing. Civil	{3,4}	{1,4}	{0,97}	{0,76}
[SGI_P] Personal SGI	{3,4}	{1,4}	{0,97}	{0,76}
[CDOM_P] Coordinaciones O&M	{5,1}	{3,2}	{2,7}	{1,6}

8.6. [I] INTEGRIDAD DE LOS DATOS

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{4,5}	{2,1}	{1,4}	{0,91}
[OS_SW] Sistema Operativo	{0,88}	{0,38}	{0,24}	{0,09}
[OFIMATICA_SW] Ofimática	{3,0}	{0,85}	{0,71}	{0,56}
[OTR_SW] Otros Software	{0,88}	{0,38}	{0,24}	{0,09}
[PI_SW] PI Process Book	{4,5}	{2,1}	{1,4}	{0,91}
[SCADA_SW] Sistema Tiempo Real	{4,5}	{2,1}	{1,4}	{0,91}
[MAXIMO_SW] Maximo	{4,5}	{2,1}	{1,4}	{0,91}
[PSOFT_SW] PeopleSoft	{4,5}	{2,1}	{1,4}	{0,91}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{4,5}	{2,1}	{1,4}	{0,91}
[GPS_SW] Sistema de Frecuencia	{4,5}	{2,1}	{1,4}	{0,91}
[ANTIVIRUS_SW] Antivirus	{4,5}	{2,1}	{1,4}	{0,91}
[HW] Hardware	{4,5}	{2,2}	{1,6}	{0,93}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{3,7}	{1,3}	{0,93}	{0,76}
[FILE_HW] Servidor de Archivos	{3,7}	{1,6}	{1,0}	{0,74}
[PI_HW] Servidor PI	{3,7}	{1,3}	{0,93}	{0,76}
[BACKUP_HW] Servidor Copias de Seguridad	{3,7}	{1,3}	{0,93}	{0,76}
[SPRINTER_HW] Servidor de Impresión	{4,5}	{2,2}	{1,6}	{0,93}
[NVR_HW] Servidor de Grabación CCTV-NVR	{3,7}	{1,3}	{0,93}	{0,76}
[STATION_HW] Estaciones de Trabajo	{3,7}	{1,7}	{1,1}	{0,78}
[PRINTER_HW] Equipos de Impresión	{3,7}	{1,3}	{0,93}	{0,76}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{0,63}	{0,22}	{0,06}	{0,01}
[CAM_HW] Cámaras de Video Vigilancia	{0,88}	{0,41}	{0,29}	{0,11}
[COM] Comunicaciones	{3,4}	{1,2}	{0,94}	{0,70}
[ANT_COM] Antena (Enlace Microondas)	{0,87}	{0,44}	{0,34}	{0,10}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{0,88}	{0,45}	{0,35}	{0,11}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{3,4}	{1,2}	{0,94}	{0,70}
[SWSCADA_COM] Switch SCADA	{3,4}	{1,2}	{0,94}	{0,70}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{0,88}	{0,45}	{0,35}	{0,11}

[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{0,88}	{0,45}	{0,35}	{0,11}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{0,88}	{0,45}	{0,35}	{0,11}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{0,88}	{0,45}	{0,35}	{0,11}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{0,88}	{0,45}	{0,35}	{0,11}
[PKSHA_COM] Packet Shaper 2500	{0,88}	{0,45}	{0,35}	{0,11}
[ROUTER_COM] Router Cisco	{3,4}	{1,2}	{0,94}	{0,70}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{3,4}	{1,2}	{0,94}	{0,70}
[REP_COM] Repetidoras	{0,88}	{0,45}	{0,35}	{0,11}
[RAD_COM] Radios	{0,88}	{0,45}	{0,35}	{0,11}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,0}	{2,6}	{2,1}	{0,97}
[MAIL_S] Correo Electrónico	{5,0}	{2,7}	{2,1}	{1,2}
[STELF_S] Telefonía IP (Servicio)	{4,1}	{2,1}	{1,5}	{0,86}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{0,37}	{0,01}	{0,01}	{0,01}
[SAI_AUX] Sistema de Alimentación Ininterrumpida				
[OTR_AUX] Otros Equipos Auxiliares				

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{0,98}	{0,64}	{0,53}	{0,28}
[ADM_P] Personal de administración y logístico	{1,3}	{0,71}	{0,60}	{0,35}
[JADM_P] Jefatura de administración	{1,3}	{0,71}	{0,60}	{0,35}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{1,3}	{0,71}	{0,60}	{0,35}
[JUNI_P] Jefe de Unidad	{1,3}	{0,71}	{0,60}	{0,35}
[SYMA_P] Personal SyMA	{1,3}	{0,71}	{0,60}	{0,35}
[JSYMA_P] Jefatura SyMA	{1,3}	{0,71}	{0,60}	{0,35}
[TOP_P] Tópico	{1,3}	{0,71}	{0,60}	{0,35}
[OPE_P] Personal Operaciones	{1,3}	{0,71}	{0,60}	{0,35}
[JOPE_P] Jefatura de Operaciones	{1,3}	{0,71}	{0,60}	{0,35}
[CIV_P] Personal Ing. Civil	{1,3}	{0,71}	{0,60}	{0,35}
[SGI_P] Personal SGI	{1,3}	{0,71}	{0,60}	{0,35}
[CDOM_P] Coordinaciones O&M	{1,3}	{0,71}	{0,60}	{0,35}

8.7. [C] CONFIDENCIALIDAD DE LOS DATOS

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software	{4,5}	{2,1}	{1,4}	{0,91}
[OS_SW] Sistema Operativo	{1,6}	{0,62}	{0,48}	{0,33}
[OFIMATICA_SW] Ofimática	{0,92}	{0,38}	{0,24}	{0,09}
[OTR_SW] Otros Software	{1,6}	{0,62}	{0,48}	{0,33}
[PI_SW] PI Process Book	{4,5}	{2,1}	{1,4}	{0,91}
[SCADA_SW] Sistema Tiempo Real	{4,5}	{2,1}	{1,4}	{0,91}
[MAXIMO_SW] Maximo	{4,5}	{2,1}	{1,4}	{0,91}
[PSOFT_SW] PeopleSoft	{4,5}	{2,1}	{1,4}	{0,91}
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	{4,5}	{2,1}	{1,4}	{0,91}
[GPS_SW] Sistema de Frecuencia	{4,5}	{2,1}	{1,4}	{0,91}
[ANTIVIRUS_SW] Antivirus	{4,5}	{2,1}	{1,4}	{0,91}
[HW] Hardware	{1,3}	{0,71}	{0,59}	{0,30}
[DOM_HW] Controlador de Dominio Windows 2012 Server	{0,88}	{0,47}	{0,31}	{0,16}
[FILE_HW] Servidor de Archivos	{0,88}	{0,52}	{0,40}	{0,14}
[PI_HW] Servidor PI	{0,88}	{0,47}	{0,31}	{0,16}
[BACKUP_HW] Servidor Copias de Seguridad	{0,88}	{0,47}	{0,31}	{0,16}

[SPRINTER_HW] Servidor de Impresión	{0,88}	{0,47}	{0,31}	{0,16}
[NVR_HW] Servidor de Grabación CCTV-NVR	{0,88}	{0,47}	{0,31}	{0,16}
[STATION_HW] Estaciones de Trabajo	{1,3}	{0,71}	{0,59}	{0,30}
[PRINTER_HW] Equipos de Impresión	{1,3}	{0,58}	{0,47}	{0,30}
[PROYECTOR_HW] Proyectores Salas de Reuniones	{0,88}	{0,47}	{0,31}	{0,16}
[CAM_HW] Cámaras de Video Vigilancia	{0,88}	{0,47}	{0,31}	{0,16}
[COM] Comunicaciones	{0,88}	{0,45}	{0,35}	{0,11}
[ANT_COM] Antena (Enlace Microondas)	{0,88}	{0,44}	{0,34}	{0,11}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{0,88}	{0,45}	{0,35}	{0,11}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{0,88}	{0,45}	{0,35}	{0,11}
[SWSCADA_COM] Switch SCADA	{0,88}	{0,45}	{0,35}	{0,11}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{0,88}	{0,45}	{0,35}	{0,11}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{0,88}	{0,45}	{0,35}	{0,11}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{0,88}	{0,45}	{0,35}	{0,11}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{0,88}	{0,45}	{0,35}	{0,11}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{0,88}	{0,45}	{0,35}	{0,11}
[PKSHA_COM] Packet Shaper 2500	{0,88}	{0,45}	{0,35}	{0,11}
[ROUTER_COM] Router Cisco	{0,88}	{0,45}	{0,35}	{0,11}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{0,88}	{0,45}	{0,35}	{0,11}
[REP_COM] Repetidoras	{0,88}	{0,45}	{0,35}	{0,11}
[RAD_COM] Radios	{0,88}	{0,45}	{0,35}	{0,11}

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,0}	{2,6}	{2,1}	{0,98}
[MAIL_S] Correo Electrónico	{5,0}	{2,8}	{2,2}	{1,2}
[STELF_S] Telefonía IP (Servicio)	{3,0}	{0,98}	{0,88}	{0,63}

[AUX] EQUIPAMIENTO AUXILIAR

Activo	[potencial]	[current]	[target]	[pilar]
[MOB_AUX] Mobiliario	{0,66}	{0,29}	{0,16}	{0,01}
[SAI_AUX] Sistema de Alimentación Ininterrumpida				
[OTR_AUX] Otros Equipos Auxiliares	{0,89}	{0,51}	{0,39}	{0,18}

[P] PERSONAL

Activo	[potencial]	[current]	[target]	[pilar]
[TI_P] Coordinador TI	{0,90}	{0,51}	{0,40}	{0,19}
[ADM_P] Personal de administración y logístico	{0,88}	{0,49}	{0,38}	{0,17}
[JADM_P] Jefatura de administración	{0,88}	{0,49}	{0,38}	{0,17}
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	{0,88}	{0,54}	{0,43}	{0,18}
[JUNI_P] Jefe de Unidad	{0,88}	{0,49}	{0,38}	{0,17}
[SYMA_P] Personal SyMA	{0,88}	{0,49}	{0,38}	{0,17}
[JSYMA_P] Jefatura SyMA	{0,88}	{0,49}	{0,38}	{0,17}
[TOP_P] Tópico	{0,88}	{0,54}	{0,43}	{0,18}
[OPE_P] Personal Operaciones	{0,88}	{0,49}	{0,38}	{0,17}
[JOPE_P] Jefatura de Operaciones	{0,88}	{0,49}	{0,38}	{0,17}
[CIV_P] Personal Ing. Civil	{0,88}	{0,49}	{0,38}	{0,17}
[SGI_P] Personal SGI	{0,88}	{0,49}	{0,38}	{0,17}
[CDOM_P] Coordinaciones O&M	{0,88}	{0,49}	{0,38}	{0,17}

8.8. [A] AUTENTICIDAD DE LOS USUARIOS Y DE LA INFORMACIÓN

[E] EQUIPAMIENTO

Activo	[potencial]	[current]	[target]	[pilar]
[SW] Software				
[OS_SW] Sistema Operativo				
[OFIMATICA_SW] Ofimática				
[OTR_SW] Otros Software				

[PI_SW] PI Process Book				
[SCADA_SW] Sistema Tiempo Real				
[MAXIMO_SW] Maximo				
[PSOFT_SW] PeopleSoft				
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras				
[GPS_SW] Sistema de Frecuencia				
[ANTIVIRUS_SW] Antivirus				
[HW] Hardware				
[DOM_HW] Controlador de Dominio Windows 2012 Server				
[FILE_HW] Servidor de Archivos				
[PI_HW] Servidor PI				
[BACKUP_HW] Servidor Copias de Seguridad				
[SPRINTER_HW] Servidor de Impresión				
[NVR_HW] Servidor de Grabación CCTV-NVR				
[STATION_HW] Estaciones de Trabajo				
[PRINTER_HW] Equipos de Impresión				
[PROYECTOR_HW] Proyectores Salas de Reuniones				
[CAM_HW] Cámaras de Video Vigilancia				
[COM] Comunicaciones	{4,5}	{2,3}	{1,8}	{0,93}
[ANT_COM] Antena (Enlace Microondas)	{0,88}	{0,43}	{0,33}	{0,11}
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	{0,88}	{0,43}	{0,33}	{0,11}
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SWSCADA_COM] Switch SCADA	{4,5}	{2,3}	{1,8}	{0,93}
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	{4,5}	{2,3}	{1,8}	{0,93}
[SWCAM_COM] Switch Cámaras de Video vigilancia	{4,5}	{2,3}	{1,8}	{0,93}
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	{4,5}	{2,3}	{1,8}	{0,93}
[FOTALL_COM] Media Converter - Fibra óptica talleres	{4,5}	{2,3}	{1,8}	{0,93}
[PKSHA_COM] Packet Shaper 2500	{4,5}	{2,3}	{1,8}	{0,93}
[ROUTER_COM] Router Cisco	{4,5}	{2,3}	{1,8}	{0,93}
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	{4,5}	{2,3}	{1,8}	{0,93}
[REP_COM] Repetidoras	{3,9}	{1,7}	{1,2}	{0,81}
[RAD_COM] Radios	{3,4}	{1,1}	{0,92}	{0,69}

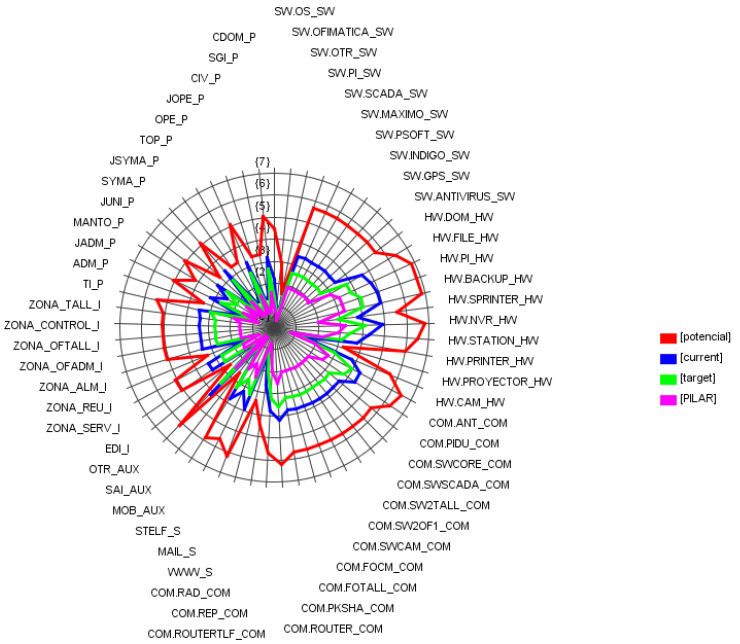
[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,6}	{3,2}	{2,6}	{1,5}
[MAIL_S] Correo Electrónico	{5,0}	{2,8}	{2,2}	{1,2}
[STELF_S] Telefonía IP (Servicio)	{4,1}	{2,1}	{1,6}	{0,86}

8.9. [T] TRAZABILIDAD DEL SERVICIO Y DE LOS DATOS

[S] SERVICIOS

Activo	[potencial]	[current]	[target]	[pilar]
[WWW_S] Internet	{5,3}	{3,0}	{2,3}	{1,4}
[MAIL_S] Correo Electrónico	{5,3}	{3,0}	{2,3}	{1,4}
[STELF_S] Telefonía IP (Servicio)	{4,8}	{2,7}	{2,2}	{0,97}


SW.OS_SW
SW.OFIMATICA_SW
SW.OTR_SW
SW.PI_SW
SW.SCADA_SW
SW.MAXIMO_SW
SW.PSOFT_SW
SW.INDIGO_SW
SW.GPS_SW
SW.ANTIVIRUS_SW
HW.DOM_HW
HW.FILE_HW
HW.PI_HW
HW.BACKUP_HW
HW.SPRINTER_HW
HW.NVR_HW
HW.STATION_HW
HW.PRINTER_HW
HW.PROYECTOR_HW
HW.CAM_HW
COM.ANT_COM
COM.PIDU_COM
COM.SWCORE_COM
COM.SWSCADA_COM
COM.SW2TALL_COM
COM.SW2OF1_COM
COM.SWCAM_COM
COM.FOCM_COM
COM.FOTALL_COM
COM.PKSHA_COM
COM.ROUTER_COM
COM.ROUTERTLF_COM
COM.REP_COM
COM.RAD_COM
WWW_S
MAIL_S
STELF_S
MOB_AUX
SAI_AUX
OTR_AUX
EDI_I
ZONA_SERV_I
ZONA_REU_I
ZONA_ALM_I
ZONA_OFADM_I
ZONA_OFTALL_I
ZONA_CONTROL_I
ZONA_TALL_I
TI_P
ADM_P
JADM_P
MANTO_P
JUNI_P
SYMA_P
JSYMA_P
TOP_P
OPE_P
JOPE_P
CIV_P
SGI_P
CDOM_P
{7}
{6}
{5}
{4}
{3}
{2}
{1}
[potencial]
[current]
[target]
[PILAR]

ANEXO N° 10: RESUMEN DE RIESGOS

ANÁLISIS DE RIESGOS

PROYECTO: [01] UPH. CARHUAQUERO

1. DATOS DEL PROYECTO

PROYECTO:	UPH. Carhuaquero
DESCRIPCIÓN:	PLAN DE SEGURIDAD DE LA INFORMACIÓN APLICADO A LA CENTRAL HIDROELÉCTRICA CARHUAQUERO
RESPONSABLE:	LEONARDO CELIS FIGUEROA
ORGANIZACIÓN:	ORAZUL ENERGY PERU S.A.
VERSIÓN:	1
FECHA:	1/11/2017
BIBLIOTECA:	[std] Biblioteca INFOSEC (6.6.2016)

2. LICENCIA

[edu] USAT
Universidad Católica
Santo Toribio de Mogrovejo
Chiclayo - PERÚ
[... 31.12.2017]

3. DIMENSIONES

- [D] Disponibilidad
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad del servicio y de los datos
- [V] Valor

4. DOMINIOS DE SEGURIDAD

- [base] Base

5. FACTORES AGRAVANTES | ATENUANTES

- [base] Base
  - [101.a] Público en general
  - [102.d] Personal propio con conflictos de interés
  - [102.g] Con ánimo de causar daño
  - [103.a] Moderadamente interesado
  - [103.b] Muy interesado
  - [106.c] Objetivo atractivo
  - [106.d] Objetivo muy atractivo
  - [104.a] Todo el personal está fuertemente motivado
  - [105.a] Se permite el acceso a Internet
  - [105.b] Se permite la ejecución de programas sin autorización previa
  - [105.c] Se permite la instalación de programas sin autorización previa
  - [105.d] Se permite la conexión de dispositivos removibles
  - [111.b] Conectado a un conjunto reducido y controlado de redes
  - [111.d] Conectado a Internet
  - [112.b] En un área de acceso abierto

6. VALORACIÓN DE LOS ACTIVOS

DOMINIO: [BASE] BASE

CAPA: [E] EQUIPAMIENTO

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[OS_SW] Sistema Operativo	[7](1)	[0]	[2]	[6]	[0]	[6]
[OFIMATICA_SW] Ofimática	[1](2)	[4]	[0]	[4]	[0]	[4]
[OTR_SW] Otros Software	[2]	[0]	[2]	[2]	[0]	[2]
[PI_SW] PI Process Book	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[SCADA_SW] Sistema Tiempo Real	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[MAXIMO_SW] Maximo	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[PSOFT_SW] PeopleSoft	[9](3)	[7](4)	[7]	[7]	[4]	[9]
[INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[GPS_SW] Sistema de Frecuencia	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[ANTIVIRUS_SW] Antivirus	[9](5)	[7](4)	[7]	[7]	[4]	[9]
[DOM_HW] Controlador de Dominio Windows 2012 Server	[10]	[7]	[0]	[6]	[0]	[10]
[FILE_HW] Servidor de Archivos	[10]	[7]	[0]	[6]	[0]	[10]
[PI_HW] Servidor PI	[10]	[7]	[0]	[6]	[0]	[10]
[BACKUP_HW] Servidor Copias de Seguridad	[10]	[7]	[0]	[6]	[0]	[10]
[SPRINTER_HW] Servidor de Impresión	[8]	[7]	[0]	[4]	[0]	[8]
[NVR_HW] Servidor de Grabación CCTV-NVR	[10]	[7]	[0]	[6]	[0]	[10]
[STATION_HW] Estaciones de Trabajo	[8]	[4]	[0]	[6]	[0]	[8]
[PRINTER_HW] Equipos de Impresión	[8]	[4]	[0]	[6]	[0]	[8]
[PROYECTOR_HW] Proyectores Salas de Reuniones	[4]	[0]	[0]	[0]	[0]	[4]
[CAM_HW] Cámaras de Video Vigilancia	[8]	[0]	[0]	[6]	[0]	[8]
[ANT_COM] Antena (Enlace Microondas)	[10]	[0]	[0]	[0]	[7]	[10]
[PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[10]	[0]	[0]	[0]	[7]	[10]
[SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso	[9]	[5]	[0]	[7]	[4]	[9]
[SWSCADA_COM] Switch SCADA	[9]	[5]	[0]	[7]	[4]	[9]
[SW2TALL_COM] Switch Oficinas Talleres 2 Piso	[9]	[0]	[0]	[7]	[0]	[9]
[SW2OF1_COM] Switch Oficinas Administrativas 1 Piso	[9]	[0]	[0]	[7]	[0]	[9]
[SWCAM_COM] Switch Cámaras de Video vigilancia	[9]	[0]	[0]	[7]	[0]	[9]
[FOCM_COM] Media Converter - Fibra óptica cerro la mesa	[9]	[0]	[0]	[7]	[0]	[9]
[FOTALL_COM] Media Converter - Fibra óptica talleres	[9]	[0]	[0]	[7]	[0]	[9]
[PKSHA_COM] Packet Shaper 2500	[9]	[0]	[0]	[7]	[0]	[9]
[ROUTER_COM] Router Cisco	[9]	[5]	[0]	[7]	[4]	[9]
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)	[9]	[5]	[0]	[7]	[4]	[9]
[REP_COM] Repetidoras	[7]	[0]	[0]	[6]	[0]	[7]
[RAD_COM] Radios	[5]	[0]	[0]	[5]	[0]	[5]

(1) [3.pi1] Probablemente afecte a un individuo
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.rto] RTO < 4 horas

(2) [1.pi1] Pudiera causar molestias a un individuo
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[1.adm] Pudiera impedir la operación efectiva de una parte de la organización

(3) [cei] Intereses Comerciales / Económicos:
[5.cei] Nivel 5
[5.cei.a] De interés significativo para la competencia
[da] Interrupción del servicio:
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[olm] Operaciones:
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[adm] Administración y Gestión:
[7.adm] Probablemente impediría la operación efectiva de la organización

(4) [4.pi1] Probablemente afecte a un grupo de individuos

[7.da2] Probablemente tenga un gran impacto en otras organizaciones
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(5) [1.pi1] Pudiera causar molestias a un individuo
[si] Seguridad:
[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.lg] Probablemente causaría una publicidad negativa generalizada
[7.rto] RTO < 4 horas

CAPA: [S] SERVICIOS

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[WWW_S] Internet	[8]	[7]	[7]	[8]	[8]	[8]
[MAIL_S] Correo Electrónico	[8]	[7]	[7]	[8]	[8]	[8]
[STELF_S] Telefonía IP (Servicio)	[7]	[5]	[3]	[5]	[5]	[0]

CAPA: [AUX] EQUIPAMIENTO AUXILIAR

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[MOB_AUX] Mobiliario	[5]	[0]	[0]	[2]	[0]	[5]
[SAI_AUX] Sistema de Alimentación Ininterrumpida	[9]	[7]	[0]	[0]	[7]	[9]
[OTR_AUX] Otros Equipos Auxiliares	[5]	[0]	[0]	[2]	[0]	[5]

CAPA: [I] INSTALACIONES

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[EDI_I] Edificio	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_SERV_I] Sala de Servidores	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_REU_I] Sala de Reuniones	[5]	[0]	[0]	[5]	[0]	[5]
[ZONA_ALM_I] Almacén	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_OFADM_I] Oficinas Casa de Máquinas	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_OFTALL_I] Oficinas Talleres	[8]	[0]	[0]	[6](1)	[0]	[7]
[ZONA_CONTROL_I] Sala Control	[8]	[0]	[0]	[8]	[0]	[8]
[ZONA_TALL_I] Talleres	[8]	[0]	[0]	[6](1)	[0]	[7]

(1) [ps] Seguridad de las personas

CAPA: [P] PERSONAL

Activo	[d]	[i]	[c]	[a]	[t]	[v]
[TI_P] Coordinador TI	[8]	[0]	[0]	[8]	[0]	[8]
[ADM_P] Personal de administración y logístico	[5]	[0]	[0]	[5]	[0]	[5]
[JADM_P] Jefatura de administración	[8]	[0]	[0]	[8]	[0]	[8]
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico	[5]	[0]	[0]	[5]	[0]	[5]
[JUNI_P] Jefe de Unidad	[8]	[0]	[0]	[8]	[0]	[8]
[SYMA_P] Personal SyMA	[5]	[0]	[0]	[5]	[0]	[5]
[JSYMA_P] Jefatura SyMA	[8]	[0]	[0]	[8]	[0]	[8]
[TOP_P] Tópico	[5]	[0]	[0]	[5]	[0]	[5]
[OPE_P] Personal Operaciones	[5]	[0]	[0]	[5]	[0]	[5]
[JOPE_P] Jefatura de Operaciones	[8]	[0]	[0]	[8]	[0]	[8]
[CIV_P] Personal Ing. Civil	[5]	[0]	[0]	[5]	[0]	[5]
[SGI_P] Personal SGI	[5]	[0]	[0]	[5]	[0]	[5]
[CDOM_P] Coordinaciones O&M	[8]	[0]	[0]	[8]	[0]	[8]

7. VALORACIÓN DE LOS DOMINIOS

Dominio de seguridad	***[d]***	***[i]***	***[c]***	***[a]***	***[t]***	***[v]***
[base] Base	[7]	[9]	[3]	[2]	[2]	[8]

8. RIESGO ACUMULADO

8.1. FASE: [Potencial]

8.1.1. DOMINIO: [BASE] BASE

Amenaza	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[I.*] Desastres industriales	D	[10]	P	{6,8}
[A.15] Modificación de la información	I	[8]	MA	{6,6}
[A.11] Acceso no autorizado	I	[8]	MA	{6,6}

8.2. FASE: [CURRENT] SITUACIÓN ACTUAL

8.2.1. DOMINIO: [BASE] BASE

Amenaza	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[A.15] Modificación de la información	I	[6]	P	{4,9}
[I.*] Desastres industriales	D	[8]	PP	{4,9}

8.3. FASE: [Target] SITUACIÓN OBJETIVO

8.3.1. DOMINIO: [BASE] BASE

Amenaza	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[A.15] Modificación de la información	I	[6]	P	{4,3}

8.4. FASE: [PILAR] RECOMENDACIÓN

8.4.1. DOMINIO: [BASE] BASE

Amenaza	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[I.*] Desastres industriales	D	[6]	PP	{3,2}
[A.15] Modificación de la información	I	[4]	P	{3,1}

9. RIESGO REPERCUTIDO

9.1. FASE: [Potencial]

9.1.1. DOMINIO: [BASE] BASE

Activo	*Amenaza*	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[10]	P	{6,8}
[HW.STATION_HW] Estaciones de Trabajo	[A.6] Abuso de privilegios de acceso	D	[8]	MA	{6,5}
[HW.STATION_HW] Estaciones de Trabajo	[A.11] Acceso no autorizado	D	[8]	MA	{6,5}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[9]	P	{6,5}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[10]	P	{6,4}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.6] Corte del suministro eléctrico	D	[9]	P	{6,3}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.5] Avería de origen físico o	D	[9]	P	{6,3}

	lógico				

9.2. FASE: [CURRENT] SITUACIÓN ACTUAL

9.2.1. DOMINIO: [BASE] BASE

Activo	*Amenaza*	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[8]	PP	{4,9}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[8]	PP	{4,9}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[8]	PP	{4,9}
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[8]	PP	{4,8}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[8]	PP	{4,6}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.1] Fuego	D	[7]	PP	{4,5}
[HW.PI_HW] Servidor PI	[I.2] Daños por agua	D	[7]	PP	{4,5}
[HW.PI_HW] Servidor PI	[I.1] Fuego	D	[7]	PP	{4,5}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.1] Fuego	D	[7]	PP	{4,5}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.2] Daños por agua	D	[7]	PP	{4,5}

9.3. FASE: [Target] SITUACIÓN OBJETIVO

9.3.1. DOMINIO: [BASE] BASE

Activo	*Amenaza*	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[7]	PP	{4,1}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	PP	{3,9}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[7]	PP	{3,8}
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[7]	PP	{3,8}
[COM.PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[I.8] Fallo de servicios de comunicaciones	D	[6]	PP	{3,8}
[COM.ANT_COM] Antena (Enlace Microondas)	[E.2] Errores del administrador del sistema / de la seguridad	D	[6]	PP	{3,7}
[COM.ANT_COM] Antena (Enlace Microondas)	[I.8] Fallo de servicios de comunicaciones	D	[6]	PP	{3,7}
[COM.PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	PP	{3,7}

9.4. FASE: [PILAR] RECOMENDACIÓN

9.4.1. DOMINIO: [BASE] BASE

Activo	*Amenaza*	*Dimensión*	*Impacto*	*Probabilidad*	*Riesgo*
[HW.FILE_HW] Servidor de Archivos	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.PI_HW] Servidor PI	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.BACKUP_HW] Servidor Copias de Seguridad	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.NVR_HW] Servidor de Grabación CCTV-NVR	[I.*] Desastres industriales	D	[6]	PP	{3,2}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.*] Desastres industriales	D	[6]	MR	{2,9}
[HW.STATION_HW] Estaciones de Trabajo	[A.6] Abuso de privilegios de acceso	D	[4]	P	{2,9}
[HW.FILE_HW] Servidor de Archivos	[I.1] Fuego	D	[5]	PP	{2,8}
[HW.FILE_HW] Servidor de Archivos	[I.2] Daños por agua	D	[5]	PP	{2,8}
[HW.FILE_HW] Servidor de Archivos	[I.6] Corte del suministro eléctrico	D	[5]	PP	{2,8}
[HW.DOM_HW] Controlador de Dominio Windows 2012 Server	[I.5] Avería de origen físico o lógico	D	[5]	PP	{2,7}

10. ACTIVOS

10.1. DOMINIO: [BASE] BASE

Capa: [E] Equipamiento

[SW] Software
- [OS_SW] Sistema Operativo
- [OFIMATICA_SW] Ofimática
- [OTR_SW] Otros Software
- [PI_SW] PI Process Book
- [SCADA_SW] Sistema Tiempo Real
- [MAXIMO_SW] Maximo
- [PSOFT_SW] PeopleSoft
- [INDIGO_SW] Sistema Indigo - Monitoreo de Cámaras
- [GPS_SW] Sistema de Frecuencia
- [ANTIVIRUS_SW] Antivirus

[HW] Hardware
- [DOM_HW] Controlador de Dominio Windows 2012 Server
- [FILE_HW] Servidor de Archivos
- [PI_HW] Servidor PI
- [BACKUP_HW] Servidor Copias de Seguridad
- [SPRINTER_HW] Servidor de Impresión
- [NVR_HW] Servidor de Grabación CCTV-NVR
- [STATION_HW] Estaciones de Trabajo
- [PRINTER_HW] Equipos de Impresión
- [PROYECTOR_HW] Proyectores Salas de Reuniones
- [CAM_HW] Cámaras de Video Vigilancia

[COM] Comunicaciones
- [ANT_COM] Antena (Enlace Microondas)
- [PIDU_COM] Conversor Coaxial-Ethernet (Enlace Microondas)
- [SWCORE_COM] Switch Core Capa3 Oficinas administrativas 2 Piso
- [SWSCADA_COM] Switch SCADA
- [SW2TALL_COM] Switch Oficinas Talleres 2 Piso
- [SW2OF1_COM] Switch Oficinas Administrativas 1 Piso
- [SWCAM_COM] Switch Cámaras de Video vigilancia
- [FOCM_COM] Media Converter - Fibra óptica cerro la mesa

[FOTALL_COM] Media Converter - Fibra óptica talleres
[PKSHA_COM] Packet Shaper 2500
[ROUTER_COM] Router Cisco
[ROUTERTLF_COM] Gateway de voz (Telefonía IP)
[REP_COM] Repetidoras
[RAD_COM] Radios

Capa: [S] Servicios

[WWW_S] Internet
[MAIL_S] Correo Electrónico
[STELF_S] Telefonía IP (Servicio)

Capa: [AUX] Equipamiento Auxiliar

[MOB_AUX] Mobiliario
[SAI_AUX] Sistema de Alimentación Ininterrumpida
[OTR_AUX] Otros Equipos Auxiliares

Capa: [I] Instalaciones

[EDI_I] Edificio
[ZONA_SERV_I] Sala de Servidores
[ZONA_REU_I] Sala de Reuniones
[ZONA_ALM_I] Almacén
[ZONA_OFADM_I] Oficinas Casa de Máquinas
[ZONA_OFTALL_I] Oficinas Talleres
[ZONA_CONTROL_I] Sala Control
[ZONA_TALL_I] Talleres

Capa: [P] Personal

[TI_P] Coordinador TI
[ADM_P] Personal de administración y logístico
[JADM_P] Jefatura de administración
[MANTO_P] Personal Mantenimiento Mecánico y Eléctrico
[JUNI_P] Jefe de Unidad
[SYMA_P] Personal SyMA
[JSYMA_P] Jefatura SyMA
[TOP_P] Tópico
[OPE_P] Personal Operaciones
[JOPE_P] Jefatura de Operaciones
[CIV_P] Personal Ing. Civil
[SGI_P] Personal SGI
[CDOM_P] Coordinaciones O&M

ANEXO N° 11: FOTOS PROYECTOS Y CAPACITACIONES

- **CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN**

Figura 32: Capacitaciones Seguridad de la Información

Figura 33: Muestra caso de estudio - CH. Carhuaquero

- **MANTENIMIENTO DE UPS Y CABLEADOS DE ENERGÍA**

Figura 34: Controlador carga de baterías - Sistema fotovoltaico

Figura 35: Conexión directa al sistema fotovoltaico

Figura 36: Paneles Solares

Figura 37: Línea 10KV para mantenimiento – Lado A

Figura 38: Línea 10KV para mantenimiento – Lado B

Figura 39: Línea 10KV para mantenimiento – Lado C

Figura 40: Línea 10KV para mantenimiento – Lado D