UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSTGRADO

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

Autor:
Ing. SILVIA CRISTINA GARCÍA SAMAMÉ

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

Chiclayo, Perú
2018

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

POR

SILVIA CRISTINA GARCÍA SAMAMÉ

Tesis presentada a la Escuela de Postgrado de la Universidad Católica Santo Toribio de Mogrovejo, para optar el Grado Académico de
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADO POR

_____

Mtro. Gregorio Manuel León Tenorio

Presidente de Jurado

_____

Mtro. María Ysabel Arangurí García

Secretario de Jurado

_____

Mtro. Ricardo David Imán Espinoza

Vocal/Asesor de Jurado

CHICLAYO, octubre 2018

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación se enfoca en la necesidad de enlazar la seguridad de la información con la gestión de las unidades ambientales de la región Lambayeque, el análisis de la situación actual aplicado a tres unidades ambientales demostró que carecen de mecanismos para fortalecer su nivel estructural y la seguridad de su información, trayendo consigo pérdidas económicas, insatisfacción de los usuarios y un deterioro de la imagen institucional.

Se planteó como objetivo general contribuir en la seguridad de la información de la gestión de las unidades ambientales de la región Lambayeque, proponiendo la elaboración de un modelo de seguridad de la información basado en estándares, metodologías y marcos de trabajo adaptados a la gestión de las unidades ambientales.

El modelo se validó por juicio de expertos midiendo su confiabilidad aplicando el alfa de Cronbach y la concordancia de su contenido en base a Kendall.

Finalmente, el modelo validado se aplicó a un caso de estudio para una unidad ambiental de la región Lambayeque, identificando 21 riesgos que fueron alineados con 23 controles propuestos, monitoreando 23 controles para medir su nivel de cumplimiento, quedando demostrado que la seguridad de la información logra contribuir a la gestión de las unidades ambientales.

PALABRAS CLAVE: seguridad de la información, gestión de unidades ambientales, controles de seguridad.

ABSTRACT

This research focuses on the need to link information security with the management of the environmental units of the Lambayeque region, the analysis of the current situation applied to three environmental units showed that they lack mechanisms to strengthen their structural level and security of your information, bringing economic losses, user dissatisfaction and a deterioration of the institutional image.

The general objective was to contribute to the information security of the management of the environmental units of the Lambayeque region, proposing the development of an information security model based on standards, methodologies and frameworks adapted to the management of the environmental units.

The model was validated by expert judgment, measuring its reliability by applying Cronbach's alpha and concordance of its content based on Kendall.

Finally, the validated model was applied to a case study for an environmental unit of the Lambayeque region, identifying 21 risks that were aligned with 23 proposed controls, monitoring 23 controls to measure their level of compliance, demonstrating that the security of information manages to contribute to the management of environmental units.

Keywords: information security, management of environmental units, security controls.

INTRODUCCIÓN

Actualmente, se puede observar cómo diversas actividades humanas han originado una degradación ambiental significativa; trayendo consigo problemas de inestabilidad social, pérdida de los recursos naturales y económicos, incumplimiento de leyes, desorden documentario y administrativo. Por tal motivo, las organizaciones se ven obligadas a buscar los mecanismos más adecuados para contrarrestar sus amenazas, puesto que son las principales receptoras, generadoras y proveedoras de información.

Existen empresas en el ámbito internacional que experimentaron desastres como pérdidas de datos o fugas de información, teniendo la necesidad de implementar sistemas de seguridad más efectivos, se mencionan algunos casos: el 12 de febrero del 2005, la Torre Windsor (Madrid) sufrió un incendio que se propagó por los pisos superiores y devastó varias empresas arruinando información relevante para ellas. Una de las empresas afectadas fue Deloitte, dedicada a los servicios de consultoría, impuestos, asesoría jurídica, asesoría financiera y auditoría; decidió calmar los ánimos de sus clientes diciendo que "*Trabajamos con ordenadores portátiles y la mayoría los tenemos en casa, no hemos perdido demasiado*", esta afirmación tranquilizó a los clientes porque no era lógico que una empresa tenga uno de sus activos más importantes, la información, en portátiles y al

alcance de cualquier desastre. Otro caso fue la plataforma de almacenamiento online Dropbox, en el año 2012 sufrió un hackeo por parte de piratas informáticos, accediendo a las cuentas de varios usuarios llegando a apropiarse ilícitamente de sus datos y contraseñas. Por este motivo, Dropbox pidió sus usuarios que cambiasen su contraseña como medida preventiva, porque las credenciales de la aplicación estaban en peligro. Días después de ese comunicado, el medio especializado Motherboard informó que la aplicación había vuelto a ser hackeada, exponiendo la privacidad de más de 68 mil millones de usuarios. Se debe hacer conciencia que este tipo de situaciones pueden ocasionar daños incalculables para las empresas, por lo que es necesario el uso de herramientas que pueden mitigar dichos daños (Empresa Replicalia "Business Continuity as a Service" 2014).

En el ámbito nacional existen empresas que también experimentaron grandes pérdidas de información, como es el caso del incendio en el Banco de la Nación durante la marcha de los cuatro suyos en el año 2000, donde murieron seis personas y el perito argentino Ramón Montiel sostuvo que la explosión fue provocada. Si bien lo que más preocupa cuando ocurre un incendio en una entidad del Estado, son las vidas humanas y las pérdidas materiales que tienen que ver con el almacenamiento de información. El periodista Juan Carlos Tafur cuestionó que existían archivos físicos y no digitales de las facturas de compra en entidades del gobierno, proponiendo que, para evitar la pérdida de información todos los documentos deberían tener una versión en PDF y ser automáticamente subida a un servidor. Otro caso suscitado fue el 04 de noviembre del 2012, cuando un desperfecto en el servidor informático del Organismo Supervisor de las Contrataciones del Estado (OSCE) hizo colapsar el denominado Sistema Electrónico de Adquisiciones y Contrataciones del Estado (Seace). Se perdieron casi 800 mil archivos digitales relacionados a los procesos, las buenas pro, los contratos, las cartas-fianza y la absolución de consultas; la información estaba relacionada a 1.746 entidades del estado de los años 2009 al 2012 y también estaba vinculada a los casos Coopex-Rodolfo Orellana, al Caso Lava

Jato, el Caso Antalsis, entre otros. Cuando todo ocurrió, los ingenieros del OSCE Carlos Oliveros, Wilber Peña y Helmer Suca constituyeron un comité de crisis en la Oficina de Informática. Luego, pidieron ayuda a las empresas HP proveedora del hardware de sus servidores, GMD (empresa de Outsourcing de procesos de negocios, tecnología de la información (TI) y transformación digital) que les daba mantenimiento. Esta última consultora encontró que los discos habían colapsado y ya no tenían espacio para almacenar datos, se tuvo que prestarle al OSCE un disco duro para almacenar la información del 2012, pero quedaba claro que no se podía acceder a la data de los años 2009-2011.

En la región Lambayeque, los casos más comunes relacionados con la seguridad de la información, están ligados a la gestión de la información ambiental de las entidades públicas; principalmente en los sectores de agricultura, pesquería y minería. En estos sectores siempre ha existido un manejo deficiente del marco normativo, de personal capacitado y de sus recursos financieros. Debido a estas irregularidades en el año 2004 se promulgó la Ley N°28245 - ley marco del sistema nacional de gestión ambiental, teniendo como finalidad que las entidades públicas mediante la reestructuración de un área ambiental puedan orientar, coordinar, evaluar y garantizar la aplicación de políticas, planes y programas destinados a la protección del ambiente. Sin embargo, en las áreas ambientales ya establecidas, aún se pueden identificar los siguientes problemas: existe gran volumen de documentos y su alta rotación dificulta el registro de cada uno de sus movimientos; la información no se encuentra completamente digitalizada, esto implica que esté expuesta al deterioro, pérdida o algún tipo de amenaza que altere su contenido soportado en formato físico. Es necesario implementar controles de seguridad que garanticen la integridad, confidencialidad y disponibilidad de información durante la gestión de las unidades ambientales, a su vez, el uso sostenible de los recursos naturales a través de un marco jurídico legal sobre el cual se pueda alcanzar una rentabilidad y, por ende, el crecimiento económico del país.

Bajo el análisis de la situación problemática descrita anteriormente, se formuló la siguiente interrogante: ¿De qué manera se puede contribuir en la seguridad de la información de la gestión de las unidades ambientales de la región Lambayeque?, en respuesta a esta interrogante se planteó la siguiente hipótesis: mediante el desarrollo de un modelo de seguridad de la información basado en metodologías, normas y marcos de trabajo, se contribuye en la seguridad de la información de la gestión de las unidades ambientales de la región Lambayeque.

Para demostrar la validez del modelo, se estableció como objetivo general: Contribuir en la seguridad de la información de las unidades ambientales de la región Lambayeque. Para lograr este objetivo, fue necesario apoyarse en el cumplimiento de los siguientes objetivos específicos: determinar la armonización de los estándares, metodologías y marcos de trabajo relacionados a seguridad de la información, aumentar las respuestas proactivas frente a los riesgos identificados durante gestión de las unidades ambientales y validar el modelo propuesto aplicado a un caso de estudio.

La investigación se justifica desde el punto de vista legal, que esté sujeta a cumplir y mejorar lo establecido por la Ley N°28245 - ley marco del sistema nacional de gestión ambiental, Ley N°27446 - ley del sistema nacional de evaluación de impacto ambiental: orientada a la evaluación de los proyectos de inversión públicos, privados o de capital mixto, que por su naturaleza pudieran generar impactos ambientales negativos de carácter significativo. También, se debe cumplir con el D.S Supremo N°002-2009 MINAM - reglamento sobre transparencia, acceso a la información pública ambiental, participación y consulta ciudadana en asuntos ambientales. Además, se debe considerar el artículo 66° de la Ley N° 27806-2003 – ley de transparencia y acceso a la información, donde se establece que toda documentación incluida en el expediente administrativo de evaluación de impacto ambiental es de carácter público, a excepción de la información expresamente declarada como secreta, reservada o confidencial.

Desde el punto de vista económico, el modelo propuesto mejora la gestión de procedimientos en las unidades ambientales, permitiendo proporcionar óptimos servicios al usuario en cuanto a la entrega de información digital o impresa.

En el plano tecnológico, al aplicar conocimientos de seguridad de la información en las unidades ambientales, los documentos estuvieron menos expuestos a manipulación, reduciendo amenazas como deterioro o mal uso de información, logrando un monitoreo en tiempo real para su disponibilidad en la gestión de proyectos ambientales. De esta manera, se mejoró la calidad de los servicios que prestan y su eficacia en el desarrollo de sus actividades.

Finalmente, en el ámbito social, se apoyó en los proyectos planificados dirigidos a la mejora de la calidad de vida de los ciudadanos, ya que con una adecuada gestión de las unidades ambientales se logró planificar y aprovechar el uso de los recursos naturales y administrativos, en los mismos.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

Para dar un sustento a la propuesta planteada, se han seleccionado los siguientes antecedentes relacionados con el tema de investigación.

Inga (2013), da a conocer aquellas amenazas que surgen cuando no se dispone de información sistematizada, ni de un conocimiento claro de los términos ambientales a manejar. De este antecedente, se rescata el análisis realizado de las experiencias o iniciativas de algunos distritos en cuanto al manejo de información concerniente a la gestión ambiental. Queda demostrado que, gracias a la implementación de un sistema de gestión ambiental apoyado en mecanismos de seguridad, se provee de procedimientos operativos, administrativos y de una comunicación interna más formal y eficiente teniendo como resultado mayor objetividad a la toma de decisiones.

Narváez (2013) propone la implementación de un SGSI (Sistemas de gestión de seguridad de la información) centrando su análisis en el área de gestión de la Fiscalía General del Estado de Ecuador. Debido a que las investigaciones que realizan los fiscales son sumjstentadas en documentos físicos, la gran cantidad de información está soportada en medios impresos. El autor realiza una comparación de los estándares ISO/IEC 13335, ISO/IEC 20000, AC SI 33, la norma ISO/IEC 27001 y

de las metodologías COSO y OCTAVE. Se ha creído conveniente la selección de este antecedente, porque explica claramente que normas y metodologías se pueden adaptar según las necesidades de la organización y brinda un conjunto de indicadores que se utilizan diariamente en el área de gestión de la información.

Aguirre (2014) plantea una investigación orientada a mejorar la seguridad de la información de las entidades públicas, presentando un comparativo de las normas ISO 27000, MARGERIT, OCTAVE y COBIT 5. La importancia de esta tesis radica en la explicación de cómo utilizar cada norma y metodología orientadas a cumplir con los requerimientos legales, procesos institucionales críticos y mejorar la atención de los usuarios ligados a la organización.

Berríos y otros autores (2015) propone una investigación que tiene como objetivo, facilitar e incentivar a las pequeñas y medianas empresas a implementar procedimientos y herramientas que gestionen y protejan la confidencialidad, disponibilidad e integridad de la información utilizando procesos basados en gestión de riesgos. Este antecedente es importante porque propone un modelo sistema de gestión de la seguridad de basado en la ISO 27001, lo que permite tener una orientación para implementar un SGSI de manera sencilla, a un bajo costo y reduciendo los tiempos de implementación.

Alcántara (2015) propone una guía de implementación de la seguridad basado en la norma ISO/IEC 27001 para apoyar la seguridad en los sistemas informáticos de las comisarias, se enfoca en determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dichas instituciones. Esta investigación demuestra que al incorporar la norma ISO/IEC 27001 se logra detectar las anomalías en la seguridad de la información, el plan de tratamiento de riesgos disminuye los niveles de riesgos con respecto a los activos de información, con el plan de capacitación y concientización se puede

incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución.

Por último, Picón (2016) desarrolló un proyecto que al igual que la investigación actual, tiene como finalidad diseñar un sistema de gestión de seguridad de la información utilizando la Norma ISO/IEC 27001:2013. El autor considera la utilización de la norma para aquellas organizaciones que necesitan establecer objetivos y principios de seguridad que garanticen la continuidad de su negocio. Brinda una serie de controles que deben implementarse en la entidad a corto, mediano o largo plazo con el fin de garantizar la correcta gestión de la seguridad de la información y de ésta manera, poder mitigar la materialización de riesgos que pueden afectarla de manera negativa.

1.2 Base Teórico Conceptual

En este apartado se hace referencia a los conceptos que están directamente ligados al sustento de la investigación y dan soporte al modelo propuesto.

1.2.1 Gobierno de TI

Actualmente, el gobierno de TI es una prioridad en la mayoría de las empresas, ya que al ser implantado demuestra su efectividad y rendimiento a la hora de obtener el máximo valor de las TI.

"*El gobierno de TI, al igual que otros temas de gobierno, es responsabilidad del comité de dirección y de los ejecutivos. No es una disciplina o actividad aislada, es una parte integral del gobierno de la empresa. Consiste en el liderazgo, estructuras y procesos organizacionales que aseguran que las TI de la organización sostienen y extienden las estrategias y los objetivos de la organización*" (IT Governance Institute, 2003:12).

Roussey (2003) refiere que el gobierno de TI alinea las tecnologías de información para una adecuada supervisión, monitoreo, control y dirección de los procesos y/o funciones de las entidades, con el fin de lograr el cumplimiento de la misión, visión o metas estratégicas.

En la presente investigación, al enlazar el gobierno de TI con la seguridad de la información, se logra dar respuesta a las distintas preocupaciones de las partes interesadas externas e internas vinculadas con todas las funciones de las unidades ambientales (UA).

El propósito del gobierno de TI, es dirigir sus esfuerzos para garantizar que se cumplan los siguientes objetivos:

- Alineación de TI con la empresa y la realización de sus objetivos.
- Uso de TI para permitir a la empresa seguir explotando las oportunidades y maximizando los beneficios.
- Uso responsable de los recursos de TI.
- Gestión adecuada de los riesgos relacionados con TI.

La figura 1 presenta la interacción de objetivos y actividades de TI desde una perspectiva de gobierno de TI y se puede aplicar entre las diferentes capas dentro de la empresa.

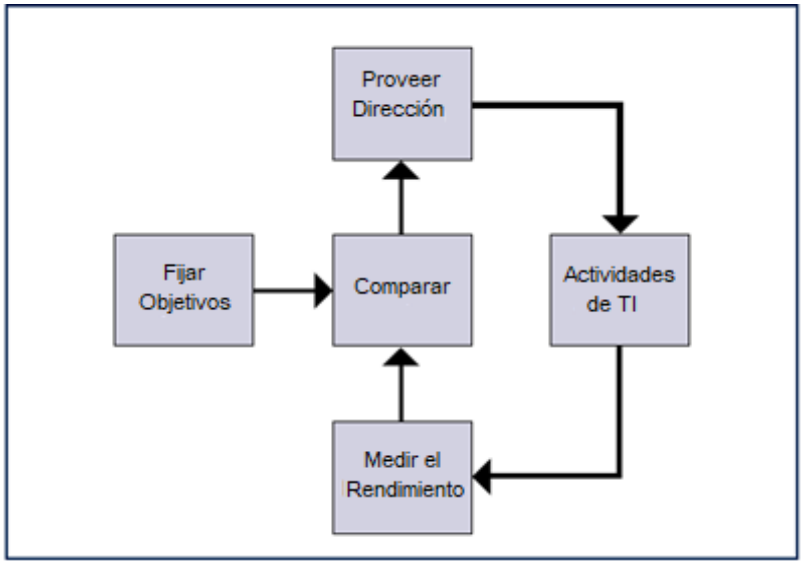


Figura 1. Interacción de objetivos y actividades de IT
Fuente: IT Governance Institute, 2003:13

Las actividades del gobierno de TI se pueden agrupar en cinco áreas de enfoque que son ilustradas en la figura 2.

Figura 2 Áreas de enfoque del Gobierno de TI
Fuente: ITGI, 2007-Cobit 4.1 pág. 06

A continuación, se describe brevemente cada área de enfoque:

- **Alineamiento estratégico:** Garantiza la alineación entre los planes del negocio y de TI, define, mantiene y valida la propuesta de valor de TI, y alinea las operaciones de TI con las operaciones de la empresa.

- **Entrega de valor:** Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios promedios en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

- **Administración de recursos:** Es la asignación adecuada de los recursos de TI para las aplicaciones, la información, infraestructura y personas; incluyendo temas claves como la optimización de conocimiento y de infraestructura.

- **Administración de riesgos:** Se requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito del riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riegos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

- **Medición del desempeño:** Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio.

Para el IT Governance Institute (2003), el gobierno de TI es importante por las siguientes razones:

- Provee oportunidades para obtener una ventaja competitiva y ofrece un medio para aumentar la productividad.

- Para transformar la empresa y crear valor agregado a productos y servicios que se han convertido en una competencia comercial universal.

- Es fundamental para administrar recursos empresariales, tratar con proveedores y clientes, y permitir transacciones cada vez más globales y desmaterializadas.

- También es clave para registrar y difundir el conocimiento empresarial.

Finalmente, para Muñoz y Ulloa (2011), el gobierno de TI dirige a la empresa hacia el logro de sus objetivos mediante el uso eficiente de sus recursos, logrando que la empresa aproveche al máximo su información, sus beneficios y gane ventajas competitivas.

1.2.2 Sistema de gestión de seguridad de la información

SGSI o ISMS por sus siglas en inglés (Information System Management System) "*es un sistema de gestión para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, de esta manera un SGSI lo que busca es poder mantener la confidencialidad, integridad y disponibilidad de la información mientras minimiza los riesgos de seguridad de la información*". (Aguirre 2014:29).

El propósito de un SGSI, "*es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y*

adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías." (ISO 27001).

El SGSI no es un sistema estático, deberá ser revisado y mejorado continuamente, documentando aquellos procedimientos que regulan el propio funcionamiento del SGSI, con el fin de establecer un enfoque adecuado para la seguridad de la información de las organizaciones.

Según el IT Governance Institute (2008), la seguridad de la información es la protección de los aspectos integrales de la información durante su ciclo de vida dentro de una organización.

En relación a lo mencionado por el IT Governance Institute (2008), se considera a la información como el activo más importante que posee toda entidad, independientemente de la forma en que se guarde o transmita, protegiéndola de las constantes amenazas que podrían ser: errores, omisiones, fraudes, accidentes y daños intencionales ligados a los actores de la seguridad. Dichas amenazas, pueden desencadenar incidentes como la pérdida, la inaccesibilidad, la alteración o la divulgación indebida de la información; poniendo en peligro la gestión de las organizaciones.

Para Gaona (2013), "*los actores de seguridad son todas las personas que están involucradas en el manejo de información, ya sea digitalmente o de forma física dentro de una organización*."

Teniendo en cuenta lo mencionado por Gaona (2013) y que existen vulnerabilidades y amenazas que atentan contra la seguridad de información, es necesario garantizar la conservación de los activos de información minimizando los riesgos potenciales a los cuales se encuentran expuestos.

La empresa Ernst & Young (2011), en su artículo seguridad de la información en un mundo sin fronteras dice que "*la seguridad de la información busca un equilibrio entre el nivel de seguridad y el costo. Debe estar alineada estratégicamente con la agenda de negocios y basarse en la tolerancia al riesgo de una organización*"

Otra definición, es la otorgada por la ISO 27001, la cual define que "*la seguridad de la información consiste en preservar la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización*".

La presente investigación, toma en cuenta los atributos antes mencionados, ya que en base a ellos se realizó la valoración de activos identificados por la organización. A continuación, definiremos cada atributo según (Borghello 2001):

- **Confidencialidad:** Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

- **Integridad:** Busca que el contenido de la información permanezca inalterado, a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

- **Disponibilidad:** Busca asegurar el acceso confiable y oportuno a los datos o recursos para ser procesada por las

personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

Para los autores Navarro y González (2002), la seguridad de la información sigue dependiendo del elemento humano, de la cultura de seguridad, de la formación e información, y de la motivación de las personas, a veces en mucha mayor medida que de cuantiosas inversiones en sofisticados dispositivos o software de control de accesos.

El objetivo de la seguridad información, al igual que la presente investigación es desarrollar, implementar y gestionar un programa de seguridad de la información que logre los cinco resultados básicos identificados en la publicación Information Security Governance: Guidance for Information Security Managers (2008), los cuales son:

- Alineación estratégica de la seguridad de la información con la estrategia comercial para respaldar los objetivos de la organización.
- Gestión efectiva del riesgo mediante la ejecución de medidas apropiadas para gestionar y mitigar los riesgos y reducir los posibles impactos en los recursos de información a un nivel aceptable.

- Entrega de valor optimizando las inversiones en seguridad de la información en apoyo de los objetivos de la organización.

- Gestión de recursos mediante el uso de conocimiento e infraestructura de seguridad de la información de manera eficiente y efectiva.

- Medición del desempeño midiendo, monitoreando y reportando las métricas de gobierno de seguridad de la información para asegurar el logro de los objetivos de la organización.

1.2.2.1 Estándar y marco de trabajo para el SGSI

Actualmente, existen estándares y marcos de trabajo que permiten la implementación y mantenimiento de un sistema de gestión de seguridad de la información. A continuación, se detallan los que han sido considerados para el desarrollo del modelo propuesto:

Norma ISO/IEC 27001

La ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Esta norma fue publicada el 15 de octubre de 2005 y revisada el 25 de septiembre de 2013; en ella se especifican los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, incluyendo los requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización.

A continuación, la figura 3 muestra un diagrama de relación de la reorganización de las cláusulas principales de la versión 2005 a la publicada en 2013.

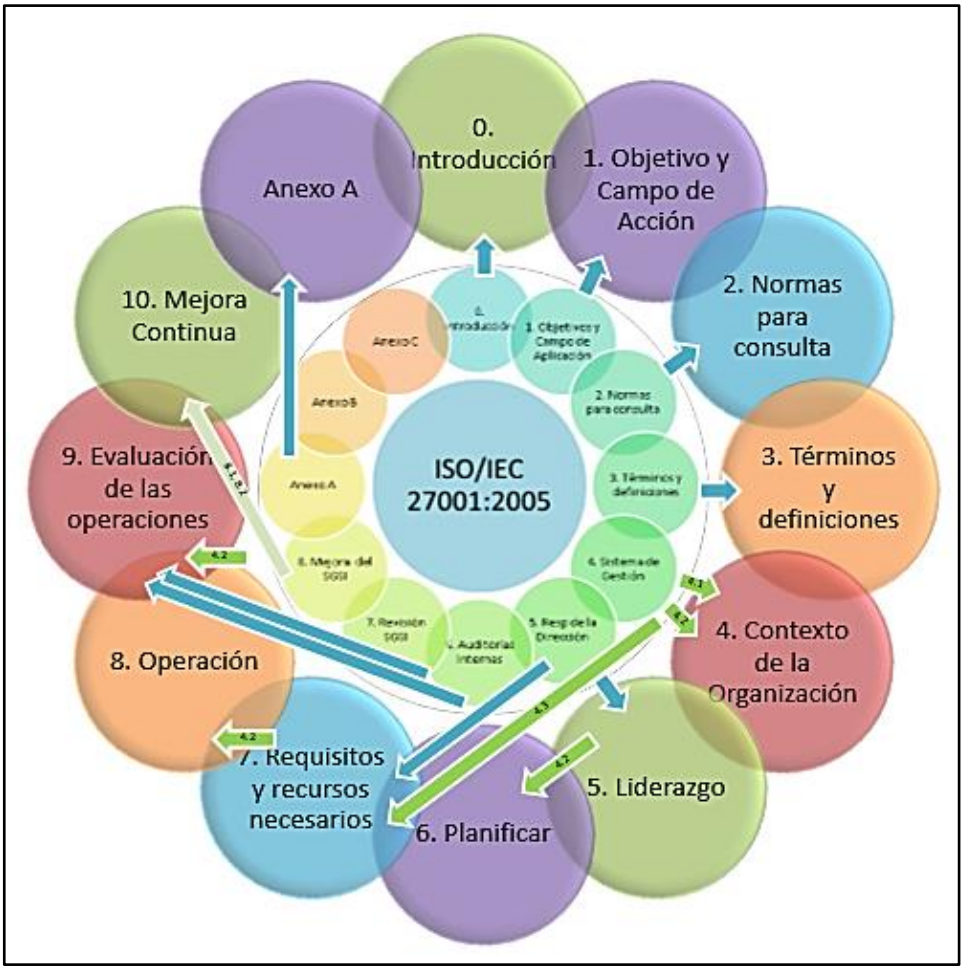


Figura 3. Comparación de la ISO/IEC 27001:2005 e ISO/IEC 27001:2013
Fuente: Adaptada de la ISO 27000

La última edición de la versión 2013 fue publicada el 25 de septiembre de 2013. Desde el 12 de noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014.
En el año 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015) y en diciembre de 2015 una segunda modificación (ISO/IEC 27001:2014/Cor.2:2015)

La norma 27001:2014 está conformada por 10 cláusulas y el anexo A, el cual se utiliza para el desarrollo de cada una de las cláusulas. Excluir cualquiera de los requisitos especificados en las cláusulas 4 a 10 no es aceptable cuando una organización declara conformidad

con esta norma. El proceso de gestión de seguridad de la información comienza desde la cláusula 4 y los siguientes se describen a continuación:

Cláusula 4 - Contexto de la organización

Se determina los aspectos externos e internos de la organización, las necesidades y expectativas de las partes interesadas y el alcance de todo el SGSI.

Cláusula 5 - Liderazgo

Se establece una política de seguridad de información, los roles y responsabilidades organizacionales.

Cláusula 6 - Planificación

Se determinan los riesgos y oportunidades que necesitan ser tratados, se valora cada riesgo identificado y se define un proceso de tratamiento de riesgos de seguridad de la información. La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Cláusula 7 - Soporte

Se debe determinar y proporcionar los recursos, competencias y habilidades necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

Cláusula 8 - Operación

La organización debe controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información. Se realiza la evaluación de riesgos y se aplica el proceso de tratamiento de riesgos de seguridad de la información.

Cláusula 9 - Evaluación del desempeño

Se realiza la auditoría interna y se monitorea, analiza y evalúa la efectividad del sistema de gestión de seguridad de la información.

Cláusula 10 - Mejoras

La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

Se considera esta norma como estándar base del modelo desarrollado, ya que según la resolución ministerial Nº 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana **"NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"**, en todas las entidades integrantes del Sistema Nacional de Informática.

COBIT 5 para seguridad de la información

Un marco de trabajo que también se orienta a mantener la seguridad de la información, es COBIT 5 para seguridad de la información, el cual está formado por tres secciones y ocho apéndices detallados a continuación:

Sección I - Profundiza en el tema de seguridad de la información y describe brevemente cómo la arquitectura de COBIT 5 puede ser adaptada a necesidades específicas de seguridad de la información.

Sección II - Profundiza en el uso de los catalizadores de COBIT 5 para implementar seguridad de la información. En esta sección se introduce el concepto de catalizadores específicos para seguridad, los cuales se explican utilizando ejemplos prácticos. En los apéndices se proporciona una guía detallada sobre estos catalizadores.

Sección III - Profundiza en cómo adaptar COBIT 5 para seguridad de la información a un entorno empresarial. Esta sección contiene guías de cómo se pueden implementar las iniciativas de seguridad de la información y proporciona un mapeo con otros estándares y marcos dentro del área de seguridad de la información.

Los apéndices contienen guías detalladas basadas en los catalizadores introducidos en la sección II:

- **Apéndice A** - Guía detallada acerca de los principios, políticas y marcos catalizadores.

- **Apéndice B** - Guía detallada acerca de los procesos catalizadores.

- **Apéndice C** - Guía detallada acerca de las estructuras organizativas catalizadoras.

- **Apéndice D** - Guía detallada acerca la cultura, ética y comportamientos catalizadores.

- **Apéndice E** - Guía detallada acerca de la información catalizadora.

- **Apéndice F**- Guía detallada acerca de los servicios, infraestructura, y aplicaciones catalizadoras.

- **Apéndice G** - Guía detallada acerca de las personas, habilidades y competencias catalizadoras.

- **Apéndice H** - Mapeos detallados de COBIT 5 para seguridad de la información con otros estándares de seguridad de la información.

Los apéndices antes mencionados, fueron considerados en el desarrollo del modelo durante la creación de las plantillas propuestas.

1.2.3 Gestión de riesgos de TI

Cuando se habla de riesgos, nos referimos a la probabilidad de que se produzca un evento, dando como resultado consecuencias negativas para una organización.

"*La gestión de riesgos es un proceso que utiliza los resultados del análisis de riesgos, ayudándonos a seleccionar y establecer las medidas de seguridad apropiadas para controlar o eliminar los riesgos identificados*." (Gaona 2013). En este concepto se manifiesta que el análisis de riesgos ayuda a identificar las necesidades de seguridad sobre los distintos activos del sistema, para determinar la vulnerabilidad del mismo ante amenazas y estimar el impacto potencial que podría ser causado por la pérdida de confidencialidad, integridad, disponibilidad de la información y recursos del sistema.

Según la ISO 27005:2008, existen distintas opciones de tratamiento del riesgo, las cuales son:

- **Mitigarse:** Implementando controles para los riesgos.
- **Aceptarse:** No es necesaria la implementación de controles.
- **Evitarse:** Adoptar medidas para prevenir el riesgo.
- **Transferirse:** Por ejemplo, pasar el riesgo a terceros por contrato o una compañía aseguradora.

Según la ISO 27000, al realizar la gestión de riesgos, se obtiene los siguientes beneficios:

- Asegurar la continuidad operacional de la organización.
- Manejar apropiadamente las amenazas y riesgos críticos.

- Mantener una estrategia de protección y reducción de riesgos.
- Minimizar el impacto con reducción de costos que incluyen perdidas de dinero, tiempo y mano de obra.

Para alcanzar los beneficios de la gestión de riesgos, es necesario considerar algunos estándares y metodologías ajustados a los riesgos identificados de cada organización.

1.2.3.1 Estándares y metodología para la gestión de riesgos

En este apartado se detallan los estándares y metodologías consideradas para complementar el desarrollo de las fases del modelo propuesto.

ISO/IEC 27005

"Gestión de riesgos de seguridad de la información", la primera edición de esta norma fue publicada el 15 de junio de 2008 y la segunda edición fue publicada el 1 de junio de 2011. Este estándar ofrece un marco que ayuda en la gestión del riesgo de la seguridad de la información.

A continuación, la figura 4 muestra el proceso de gestión del riesgo en la seguridad de la información.

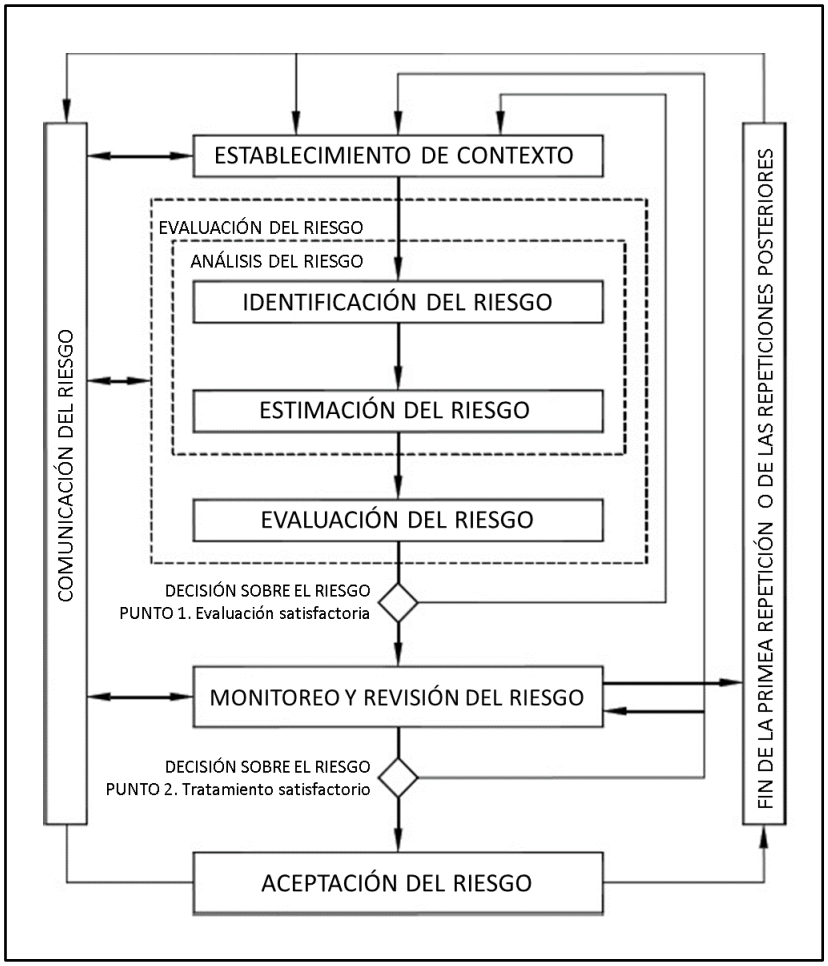


Figura 4. Proceso de gestión de riesgos en seguridad de la información – ISO/IEC 27005
Fuente: ISO/IEC 27005:2011

La norma está conformada por 12 cláusulas y 6 anexos; y su implementación comienza a partir de la cláusula 7, detallada a continuación:

Cláusula 7 - Establecimiento del contexto

Se describe toda la información que interviene en el desempeño de la organización, con la finalidad de establecer los objetivos y el alcance de la gestión del riesgo de la seguridad de la información.

Cláusula 8 - Valoración del riesgo

Se identifican los riegos y se priorizan según los objeticos de la organización. Consta de las siguientes actividades:

- Análisis del riesgo que consiste en la identificación y estimación del riesgo.
- Evaluación del riesgo, se valora la lista de riesgos identificados.

Cláusula 9 - Tratamiento del riesgo

Se seleccionan los controles para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo.

Cláusula 10 - Aceptación del riesgo

Se toma la decisión de aceptar los riesgos y se justifica la decisión de cada riesgo aceptado.

Cláusula 11 - Comunicación del riesgo

La información acerca del riesgo se debe intercambiar y/o compartir entre la persona que toma la decisión y las otras partes involucradas.

Cláusula 12 - Monitoreo y Revisión del riesgo

Los riesgos y sus factores se deben monitorear con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana.

ISO/IEC 31000

"Gestión del riesgo. Principios y directrices", este estándar proporciona una guía para los programas de auditoría interna o externa, no establece directrices concretas para el tratamiento de riesgos, sino que da orientaciones para la implantación de un sistema de gestión del riesgo.

A continuación, en la figura 5 se muestra el proceso de gestión del riesgo.

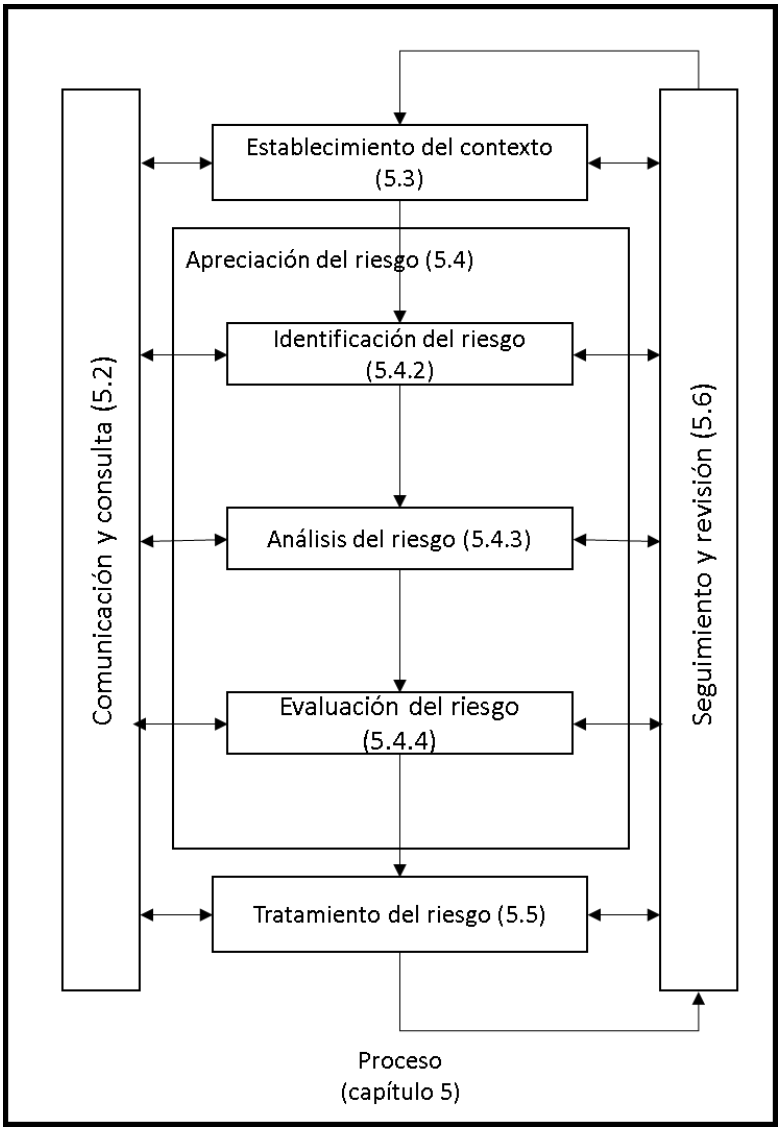


Figura 5. Proceso de gestión del riesgo de la ISO 31000
Fuente: ISO 31000:2016

MAGERIT

"Metodología de análisis y gestión de riesgos de los sistemas de información", se trata de una metodología promovida por el CSAE (Consejo superior de administración electrónica, Madrid - España) que persigue una aproximación metódica al análisis de riesgos. Según el ministerio de hacienda y administraciones públicas - España, los objetivos de la aplicación de este modelo son:

- Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de paralizarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

En la figura 6 se muestran los pasos del proceso de análisis y gestión de riesgos según MAGERIT.

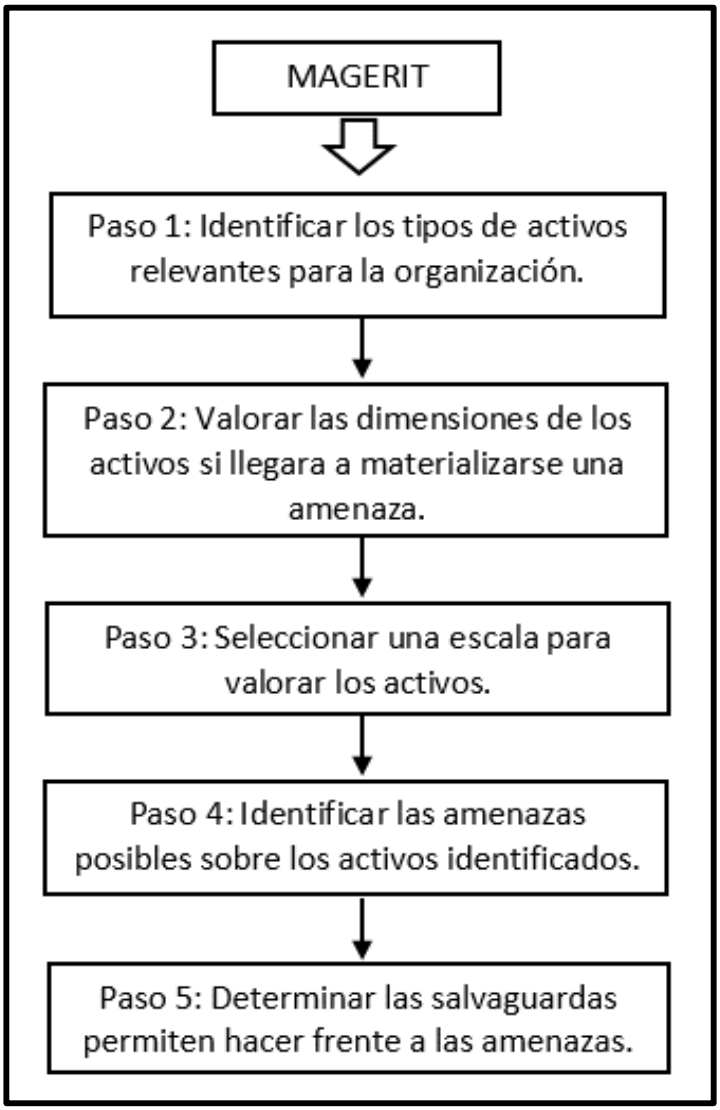


Figura 6. Proceso de análisis y gestión de riesgos.
Fuente: MAGERIT versión 3.0

1.2.4 Sistema de gestión ambiental – SGA

Según Pérez (2006) citado por Jaramillo (2012:06) dice que un sistema de gestión ambiental "*es una herramienta que permite controlar el nivel del desempeño ambiental y establece un proceso estructurado que proporciona orden y coherencia, contribuyendo con logros económicos, pero sobre todo a mejorar la calidad de vida*".

Para Collazos (2005:394), un sistema de gestión ambiental es "*el marco o método de trabajo que utiliza una organización para acometer un determinado comportamiento gerencial de acuerdo a las metas prefijadas en respuesta a normas, riesgos ambientales y presiones socioeconómicas en constante cambio en el tiempo y bajo esquemas de competitividad*".

La ley N°28245 "ley marco del sistema nacional de gestión ambiental", manifiesta que un sistema de gestión ambiental debe constituirse sobre la base de las instituciones estatales, órganos y oficinas de los distintos ministerios, organismos públicos descentralizados e instituciones públicas a nivel nacional, regional y local que ejerzan competencias y funciones sobre el ambiente y los recursos naturales; contando con la participación del sector privado y la sociedad civil. Según lo manifestado por la ley, en su artículo 02, estableció que cada entidad pública debía reestructurar su unidad ambiental, con la finalidad de adecuar su nivel jerárquico e incluir dentro de su ámbito las actividades de su competencia.

Según Collazos (2005), los objetivos de un SGA son:

- **Verificación de la conformidad legal**
  Se pretende garantizar el cumplimiento de las normas legales del medio ambiente.

- **Diseño de la política y procedimientos operativos**
  Trata de establecer las políticas y procedimientos operativos necesarios y adecuados para alcanzar los objetivos de la organización.

- **Determinación y gestión de riesgos ambientales y administrativos**
  Esto implica que, si el SGA identifica, interpreta y previene los efectos medioambientales derivados de proyectos, también la organización debe manejar apropiadamente los riesgos que surjan como consecuencia de dichas acciones.

- **Establecimiento de la organización**
  El SGA debe establecer la cantidad y calidad de insumos y recursos humanos necesarios para el cumplimiento de las metas y objetivos trazados.

- **Mejora interna**
  Consiste en la renovación de métodos, acciones y equipos, así como la actualización de conceptos y estructuras que permitan el mejoramiento y/o la reestructuración interna de la organización.

- **Obtención de la certificación de gestión ambiental**
  La obtención de certificación de calidad ambiental demuestra la eficacia del desarrollo de SGA adoptado, así como sus ventajas económicas alcanzadas.

Para la implementación y mejora continua de un SGA se propone la norma **NTP-ISO 14001:2015 "Sistemas de gestión ambiental. Requisitos con orientación para su uso" 4ª Edición,** publicada el 20 de noviembre de 2015. Dicho estándar proporciona a las organizaciones un marco para proteger el medio ambiente y responder a las condiciones ambientales cambiantes, siempre guardando el equilibrio con las necesidades socioeconómicas y administrativas. Aplicar la norma ISO 14001 será diferente en cada organización, ya que depende del contexto en el que se encuentre la empresa.

La NTP-ISO 14001:2015, al igual que la ISO 27001:2014, está conformada por 10 cláusulas, pero con 3 anexos: anexo A, anexo B y anexo C. El proceso del sistema de gestión ambiental comienza en la cláusula 4 y se describen a continuación:

Cláusula 4 - Contexto de la organización

Se determinan las cuestiones externas e internas que son pertinentes para el propósito de la organización y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión ambiental.

Cláusula 5 - Liderazgo

Se establece una política ambiental de dentro del alcance del sistema de gestión ambiental de la organizacional.

Cláusula 6 - Planificación

Se determinan los riesgos y oportunidades que necesitan ser tratados, se valora cada riesgo identificado y se define un proceso de tratamiento de riesgos según los impactos ambientales identificados.

Cláusula 7 - Soporte

Se debe determinar y proporcionar los recursos, competencias y habilidades necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de ambiental.

Cláusula 8 - Operación

La organización debe controlar los procesos necesarios para cumplir los requisitos del sistema de gestión ambiental y para implementar las acciones determinadas en el tratamiento de riesgos.

Cláusula 9 - Evaluación del desempeño

Se realiza la auditoría interna y se monitorea, analiza y evalúa la efectividad del sistema de gestión ambiental.

Cláusula 10 - Mejoras

La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión ambiental.

En el documento de la ISO 14001:20015 se detallan las ventajas que obtienen las empresas al implementar las cláusulas de la referida norma, las cuales son:

- ✓ Generar una política ambiental claramente definida y adecuada al tamaño y naturaleza de la organización.

- ✓ Permite mantener el cumplimiento de la legislación y anticiparse a una normativa cada vez más exigente en temas ambientales.

- ✓ Permite predecir problemas y riesgos ambientales o mitigarlos cuando éstos son inevitables.

- ✓ Promueve una mejor estructura organizacional de los procesos y actividades desarrolladas, lo que se traduce en ahorros indirectos significativos de tiempo y recursos.

- ✓ Provee de procedimientos operativos y administrativos y de una comunicación interna más formal y eficiente teniendo como resultado mayor objetividad a las tomas de decisiones.

- ✓ Permite mejorar las prácticas ambientales deficientes en la gestión de residuos, evitando costos y posibles daños ambientales asociados.

- ✓ Se genera un modelo de gestión aplicable a otros ámbitos de la empresa.

- ✓ Ofrece un marco flexible, pero estandarizado, para la gestión y la posibilidad de una futura certificación, permitiéndole una mejor posición y competitividad en los mercados, y por lo tanto mayores utilidades.

- ✓ Mejora la imagen pública demostrando compromiso, transparencia y un buen desempeño ambiental lo que da mayor confianza a la comunidad.

1.2.5 Unidades ambientales (UA)

Actualmente, las unidades ambientales funcionan como oficinas descentralizadas donde la población accede a la información sobre los diferentes componentes del ambiente, tales como: aire, agua, suelo, biodiversidad, residuos sólidos, indicadores ambientales, mapas temáticos, informes sobre el estado del ambiente, legislación ambiental e incluso proyectos ambientales ejecutados.

El objetivo de las unidades ambientales es crear e impulsar el desarrollo de políticas, acciones y estrategias planificadas que contribuyan a promover el proceso sostenible, la protección efectiva del medio ambiente y el tratamiento adecuado de los procedimientos de gestión de la referida unidad.

Según lo manifestado por la Ley Nº28245 - ley marco del sistema nacional de gestión ambiental, cada entidad pública debe elaborar su propuesta de reestructuración de sus unidades ambientales, con la finalidad de adecuar su nivel jerárquico e incluir dentro de su ámbito las actividades de su competencia. Por tal motivo, la presente tesis se enfoca en proponer un modelo orientado a mejorar la gestión de las unidades ambientales de la región Lambayeque.

A continuación, se muestran las funciones básicas dentro de una unidad ambiental.

Tabla 1. Funciones de la unidad ambiental
Fuente: Elaboración propia

N°	Función	Personal responsable
01	Supervisar el desempeño de la unidad ambiental. Planificar, monitorear, dirigir y desarrollar los programas de gestión ambiental de la institución y su presupuesto.	Responsable ambiental
02	Ejecutar los programas de gestión ambiental de acuerdo a lo planificado.	Especialista ambiental
03	Llevar a cabo los muestreos de recursos naturales agua, suelo, aire y ruido en el ámbito donde se realizan estudios y monitoreos de áreas intervenidas.	Técnico ambiental
04	Resguardar los documentos del archivo y supervisar el cumplimiento del trámite documentario que se genera como resultado de la gestión de la unidad ambiental.	Asistente administrativo y de archivo
05	Apoyar en las actividades relacionadas con la búsqueda de información, fotocopiado y atención al usuario.	Personal de apoyo

La información generada durante las funciones de la unidad ambiental, es registrada por el asistente administrativo, resguardada en el archivo y entregada o prestada según la solicitud del ciudadano y/o alguna entidad interesada.

CAPÍTULO II MATERIALES Y MÉTODOS

1.1 Diseño de la investigación

El tipo de estudio es no experimental transversal de tipo descriptivo.

El diseño de contrastación de la hipótesis es del tipo cuasi experimental porque la muestra no ha sido tomada probabilísticamente.

Se pretende evaluar el efecto que genera la ejecución de un modelo de seguridad de la información sobre la gestión de las unidades ambientales, por lo que se usará un modelo preprueba/posprueba con un solo grupo:

G O1 X O2

Donde:

- ✓ G = Caso de estudio seleccionado.
- ✓ O1 = Contribuir en la seguridad de la información de la gestión de las unidades ambientales de la región Lambayeque, antes de aplicar el modelo de seguridad de la información.
- ✓ X = Modelo de seguridad de información basado en normas, metodologías y marcos de trabajo.

- ✓ O2 = Contribuir en la seguridad de la información de la gestión de las unidades ambientales de la región Lambayeque, después de aplicar el modelo de seguridad de la información.

1.2 Población y muestra

La población inicial para la investigación, fueron las entidades públicas que cuentan con su unidad ambiental dentro de la región Lambayeque, las cuales son:

- Junta de Usuarios
- Gerencia Regional de Transportes y Comunicaciones.
- Gerencia Ejecutiva de Energía y Minas.
- PEOT - Proyecto Especial Olmos Tinajones.
- Gerencia Ejecutiva de Vivienda y Saneamiento.
- Gerencia Regional de Desarrollo Productivo.
- SERFOR - Servicio Forestal Nacional

De acuerdo a la accesibilidad a las unidades ambientales, sólo se consideraron tres (03) entidades públicas dentro de la región Lambayeque, las cuales se detallan en el Anexo 1.

1.3 Métodos y técnicas de recolección de datos

Los métodos empleados fueron:

a) Observación activa: se analizaron las funciones administrativas y de la UA, lo que permitió conocer el procesamiento de la información con el fin de resaltar los puntos críticos y determinar los riesgos a los que está expuesta la información solicitada por usuarios y/o por entidades externas.

b) Estudio de casos: se estudió la seguridad de la información de la gestión de proyectos ambientales de las tres (03) entidades seleccionadas en la región Lambayeque.

Se utilizaron las siguientes técnicas:

a) Encuesta: se aplicó una encuesta al responsable ambiental y al personal de la UA, para determinar el cumplimiento de las cláusulas establecidas por la norma ISO 27001:2014.

b) Análisis bibliográfico: se revisó bibliografía referente a la seguridad de la información, a la gestión de proyectos ambientales y a las funciones de la UA.

c) Análisis de documentos: los documentos revisados fueron:
   - Plan estratégico institucional.
   - Visión, misión, objetivos estratégicos y organigrama.
   - La estructura de la organización, funciones y responsabilidades.
   - Normas y políticas adoptadas por la entidad.
   - Sistemas de información y los procesos de toma de decisiones.

El cuestionario fue el instrumento empleado en la encuesta aplicada.

1.4 Técnicas de procesamiento de datos

Con el fin de obtener un diagnóstico de cómo se gestiona la seguridad de la información en la gestión de las unidades ambientales, se aplicó una encuesta al gerente y al personal de las tres (03) entidades seleccionadas de la región Lambayeque.

Los resultados de la encuesta se analizaron y procesaron mediante el uso de hojas del cálculo. En base a la información recolectada y luego del análisis relacionado con la seguridad de la información y la gestión de unidades ambientales, se procedió con el diseño de un modelo de seguridad de la información.

Para evaluar la validez del modelo, se usó la herramienta estadística SPSS (Paquete Estadístico para las Ciencias Sociales). Finalmente, se

aplicó el modelo propuesto a un caso de estudio, con el fin de probar su contribución en la seguridad de la información en la gestión de las unidades ambientales.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

1.1 Diagnóstico de la situación actual de las unidades ambientales con respecto a la seguridad de la información

Se aplicó una encuesta al gerente y responsables del manejo de información de las unidades ambientales de las tres (03) entidades seleccionadas, con el fin de diagnosticar si tanto la organización como la unidad de gestión ambiental cumplen con las cláusulas señaladas por la NTP ISO/IEC 27001:2014, según lo aprobado por la resolución ministerial Nº 004-2016-PCM.

En el Anexo 2, se muestra la encuesta que fue aplicada a los encargados del manejo de la información de las unidades ambientales, el resultado se observa en el gráfico de la figura 7.

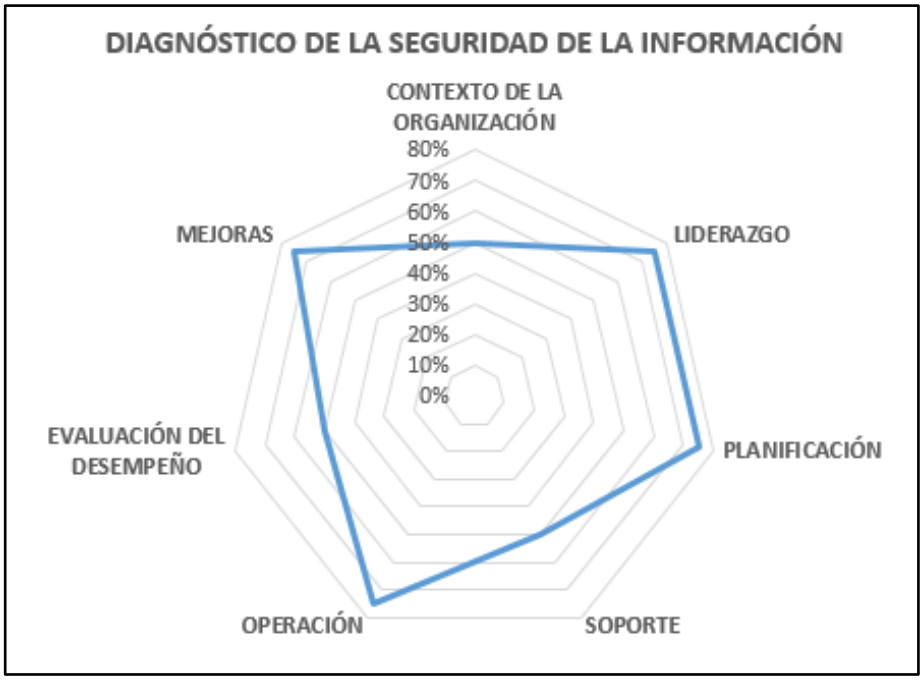


Figura 7. Diagnóstico de la seguridad de la información en las UA
Fuente: Elaboración propia

A continuación, se detalla el resultado del cuestionario aplicado a cada una de las cláusulas de la ISO 27001:2014.

Con respecto al **contexto de la organización**, los encuestados señalaron que conocen y han identificado los factores, situaciones y personas externas e internas relacionados al contexto de la organización; sin embargo, el 50% manifestó que aún no han establecido un sistema de gestión de la seguridad de la información (SGSI) para su institución.

El 75% no ha demostrado **liderazgo** en mejorar ni en establecer políticas para la seguridad de la información a pesar que todas las instituciones encuestadas ya habían asignado responsabilidades para el manejo de la misma.

Con respecto a la **planificación**, nuevamente un 75% manifiesta que no cuentan con un plan que les permite cumplir con los objetivos de

seguridad de la información necesarios para su unidad de gestión ambiental.

En cuanto a la fase de **soporte**, el 50% de las instituciones cumplen con los solicitado por la norma; sin embargo, al otro 50% el único requisito que les falta cumplir es el de documentar y actualizar la información completamente.

El 75% de los encuestados no cumple con la fase de **operación**, ya que no entregan un informen final de los riesgos ocurridos ni han constituido un plan de tratamiento de riesgos.

La totalidad de las instituciones analizadas no cumplen con la **evaluación del desempeño** y eficacia en cuanto a la seguridad de la información, no han identificado los temas que necesitan ser analizados, monitoreados y mejorados. Tampoco han implementado un programa de auditoría interna que les permita mejorar los procesos y/o funciones de la organización y de la unidad ambiental.

En cuanto a las **mejoras** en la seguridad de la información, el 75% manifestó que su unidad ambiental reacciona eficazmente ante cualquier no conformidad identificada y solo utilizan la información documentada como guía para determinar qué aspectos deben ir mejorando continuamente.

1.2 Análisis de estándares, marcos de trabajos y metodologías relacionados con seguridad de la información

Para el desarrollo del modelo de seguridad de la información propuesto, se analizaron los siguientes estándares, marcos de trabajo y metodologías: NTP ISO/IEC 27001:2014, NTP ISO/IEC 31000:2011 (revisada el 2016), NTP ISO 27005:2008, COBIT 5 para seguridad de la información y MAGERIT. (Anexo 3)

Como resultado del análisis, se detallan las fases que dan soporte a las necesidades de las unidades ambiental:

FASE I - CONTEXTO DE LA ORGANIZACIÓN

"El término contexto deriva del latín contextus, que significa lo que rodea a un acontecimiento o hecho. Por lo tanto, el contexto es un marco, un ambiente, un entorno, un conjunto de fenómenos, situaciones y circunstancias (como el tiempo y el lugar), que rodean a la organización." (ISO 14001:2015). El objetivo de esta fase es identificar los aspectos externos e internos que pueden afectar el rendimiento de la organización y conocer los requisitos de las partes interesadas en el desarrollo del sistema de gestión de seguridad de la información.

1.1 Identificación de contextos

Para la identificación de aspectos externos e internos, se usaron los mencionados en la NTP ISO 31000:2016 cláusula 5.3.

- **Identificación del contexto externo**

  El contexto externo contiene las condiciones locales y nacionales que se interrelacionan con una organización. Para este caso, su identificación permite conocer todo lo que rodea a las unidades de gestión ambiental. Entre los aspectos a identificar se tienen los siguientes:

  - **Social y cultural:** lugar donde los individuos se desarrollan en determinadas condiciones de vida y está determinado o relacionado a los grupos a los que pertenece.

  - **Político:** define los derechos, obligaciones y fines en los que debe basarse el funcionamiento de la organización.

- **Financiero:** conjunto de elementos relacionados con la economía que influyen en el rendimiento de las organizaciones.

- **Reglamentario:** son las exigencias legales como normas y lineamientos, su incumplimiento puede llevar a las organizaciones a estar expuestas a sanciones poniendo en riesgo su funcionamiento.

➢ **Identificación del contexto interno**

Se refiere a las condiciones dentro de la organización que influyen en el desenvolvimiento de su unidad de gestión ambiental. Se deben identificar los siguientes aspectos internos:

1. **Estructura de la organización, funciones y responsabilidades:** permite lograr un adecuado control para alcanzar las metas y objetivos planteadas por la organización.

2. **Objetivos y estrategias:** permitan mejorar el rendimiento y cumplimiento de los lineamientos ambientales y administrativos.

3. **Recursos y conocimientos:** son los elementos necesarios que dan soporte al rendimiento de las unidades de gestión ambiental.

4. **Cultura de la organización:** permiten identificar el comportamiento de los actores relacionados a la organización, orientada a brindar buen servicio al usuario.

1.2 Necesidades y expectativas de las partes interesadas

Para el desarrollo de esta actividad, COBIT 5 para seguridad de la información – Sección II apéndice E.1, explica lo siguiente:

Las **partes interesadas** son las entidades o personas interesadas que tienen mayor importancia para la organización o se ven afectadas por su desempeño.

Las **necesidades** vienen a ser los requisitos que tienen carácter obligatorio y comprenden el cumplimiento legal, contractual y reglamentario interno (directivas y políticas) y las e**xpectativas** son aquellos requisitos que surgen de los logros esperados respecto a los resultados de la operación de la organización.

1.3 Alcance del sistema de gestión de seguridad de la información

El alcance del SGSI es definir claramente que información quiere proteger la organización, independientemente de dónde se halle, cómo se almacene o quién pueda acceder a la misma. Según lo establecido en la cláusula 4.1 y 4.2 de la ISO 27001:2014, para determinar el alcance, la organización debe considerar los aspectos externos e internos; las partes interesadas relevantes al SGSI; los procesos o funciones que estarían incluidos dentro de los límites del SGSI y documentar lo siguiente:

- **Procesos / funciones:** identificar los procesos o funciones donde se maneja la información a resguardar.
- **Responsables:** los que están a cargo del tratamiento de la información.
- **Infraestructura de TI:** conjunto de dispositivos físicos y aplicaciones de software que intervienen durante el manejo de la información.

FASE II – LIDERAZGO

Según COBIT 5 “el liderazgo utiliza comunicaciones, disposiciones, reglas y normas con objeto de influir en los comportamientos dentro de la institución”. Para Maxwell (2009) “el liderazgo representa la facultad

de mejorar a las personas de un área, a través de la guía u orientación de un líder, que se define como aquel que tiene esa capacidad de influencia a través de la cual sus subordinados mejoran sus aptitudes y capacidades.

2.1 Asegurar el liderazgo y compromiso

La ISO 27001:2014 cláusula 5.1 propone una lista de funciones que deben cumplirse por la gerencia para demostrar liderazgo y compromiso con respecto al SGSI.

2.2 Establecer políticas y objetivos de seguridad de la información

Según la ISO 27001:2014 - numeral 5.2, se debe establecer una política de seguridad de la información que sea apropiada para el propósito de la organización, la cual debe estar documentada, debe ser comunicada y estar disponible a las partes interesadas externas e internas. COBIT 5 para seguridad de la información, determina que toda política de seguridad implementada en la organización, debe contener la definición de la política, el alcance, los objetivos de seguridad de la información (ISO 27001:2014) y los controles de seguridad.

A continuación, se detalla una lista de políticas planteadas por COBIT 5 para seguridad de la información, sección II – apéndice A.3:

- **Políticas de la seguridad de la información:** conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo sus objetivos de seguridad.

- **Política de control de accesos:** la implementación de una política de control de acceso ayuda a prevenir el robo y la divulgación no autorizada de la información.

- **Política de seguridad de la información del personal:** se debe verificar si todo el personal de seguridad de la información tiene las habilidades pertinentes para desempeñar los puestos críticos de seguridad de información.

- **Política de seguridad física y ambiental:** el objetivo de esta política es proporcionar orientación sobre la protección de ubicaciones físicas y los controles ambientales que proporcionen capacidad a las operaciones de soporte.

- **Política de privacidad y confidencialidad:** enfocada a proteger la información que es enviada a través de servicios o dispositivos de almacenamiento de la organización.

- **Política de integridad de la información:** su implementación permite conservar la exactitud de los atributos de la información durante la transmisión, el procesamiento y el almacenamiento de la misma.

- **Política de respaldo y restauración de información:** asegura que la información de la organización, los datos de los usuarios y clientes se mantengan protegidos contra la alteración o divulgación de manera accidental o malintencionada.

2.3 Definir roles y responsabilidades

La alta dirección debe asignar la responsabilidad y la autoridad para asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de la ISO 27001:2014. Se ha considerado el formato que ofrece COBIT 5 para seguridad de la información sección II Apéndice C, con el siguiente nivel de implicación:

(A) Responsable de que se haga
(R) Responsable de hacerlo
(C) Consultado
(I) Informado

FASE III - PLANIFICACIÓN

Para Robert A. (1998), la planificación es un proceso sistemático de desarrollo e implementación que se sigue para determinar los objetivos y las metas de una organización y las estrategias que permitirán alcanzarlos. Según la ISO 27001:2014 cláusula 6, esta fase tiene como objetivo identificar los riesgos y las oportunidades que necesitan ser tratados, prevenir o reducir efectos indeseados y lograr la mejora continua.

3.1 Identificación del riesgo

Se consideran los puntos mencionados en la ISO 27005:2008, descritos a continuación:

- **Identificación de activos**

  Un activo es todo aquello que tiene valor para la organización y por lo tanto requiere de protección. Los tipos de activos pueden ser: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (UNE 71504:2008). En la tabla 02 se presenta una lista de clasificación de activos propuesta por MAGERIT y la ISO 27005:2008. Se debe tener en cuenta que la organización puede identificar otros activos según el giro del negocio.

Tabla 2. Clasificación de los tipos de activos

MAGERITT	ISO 27005:2008
Esenciales - Información - Servicios	**Primarios** - Actividades y Procesos del negocio - Información
- Arquitectura del Sistema - Datos / Información - Claves Criptográficas - Servicios - Aplicaciones informáticas (Software) - Equipamiento informático (Hardware) - Redes de comunicaciones - Soporte de Información - Equipamiento Auxiliar - Instalaciones - Personal	**De soporte** - Hardware - Software - Redes - Personal - Ambientes físicos - Organización

- **<u>Identificación de amenazas y vulnerabilidades</u>**

La amenaza es una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Agrupando la información de la ISO 27005:2008 y MAGERIT capítulo 5, se ofrece una lista de amenazas y vulnerabilidades que pueden ser complementadas con las propias de la organización.

- **<u>Valoración de activos</u>**

Para la valoración de activos se tendrán en cuenta las dimensiones básicas mencionadas por MAGERIT, que son:

- **Disponibilidad (D):** acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO 27000)

- **Integridad (I):** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (ISO 27000)

- **Confidencialidad (C):** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO 27000)

3.2 Análisis del riesgo

Según la ISO 27001:2014, para realizar un análisis de riesgos se debe valorar la probabilidad y el impacto de los riesgos identificados como si estos fueran a materializarse. La probabilidad se define como la ocurrencia de que suceda el riesgo; esta puede ser medida con criterios de frecuencia desde raro, improbable, posible, probable y casi seguro. El impacto son las consecuencias que puede ocasionar a la organización la materialización del riesgo. Bajo el criterio de impacto, el riesgo se debe medir a partir de: Insignificante, menor, moderado, mayor y catastrófico.

3.3 Evaluación del riesgo

Según la ISO/IEC Guía 73:2002, la evaluación del riesgo es el proceso de comparación de los resultados del análisis del riesgo para determinar si el riesgo o su magnitud son aceptables o tolerables. La mencionada guía define el riesgo tolerable como la disponibilidad de una organización o de las partes interesadas para soportar el riesgo después de su tratamiento y, define la aceptación del riesgo como la decisión informada en favor de tomar un riesgo particular. En esta fase, la norma 27001:2014 pide la priorización de los riesgos analizados, para lo cual se usará el mapa de calor ubicando los riesgos según su impacto y probabilidad.

3.4 Tratamiento del riesgo

"El tratamiento del riesgo implica la selección una o más opciones para modificar los riesgos, una vez realizada la implementación, los

tratamientos proporcionan o modifican los controles". (ISO/IEC 31000:2016).

La norma ISO/IEC 27005:2008 propone las siguientes estrategias para el de tratamiento del riesgo:

- **Mitigar el riesgo:** disminuir el impacto y probabilidad del riesgo, seleccionando e implementación de controles.

- **Aceptar el riesgo:** los daños ocasionados por la materialización del riesgo no son significativos y no es necesario implementar controles adicionales.

- **Evitar el riesgo:** tomar medidas necesarias para prevenir la materialización del riesgo, se puede lograr mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes.

- **Transferir el riesgo:** el riesgo se transfiere a otra de las partes que pueda manejar de manera más eficaz el riesgo en particular.

FASE IV - SOPORTE

El desarrollo de esta fase se apoya en COBIT 5 para seguridad de la información apéndice G y tiene como objetivo definir los recursos que necesita la organización para implementar un SGSI.

4.1 Identificación de recursos para el tratamiento de riesgos

Se considera como recursos a los instrumentos y personas necesarias para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información.

La norma ISO 27001:2014 establece que la organización cumpla lo siguiente:

- Determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información.
- Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuada.
- Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas.
- Retener información documentada apropiada como evidencia de competencia.

4.2 Determinar la comunicación de controles

La comunicación de controles debe ser de dos tipos:

La **comunicación externa** es el conjunto de actividades generadoras de mensajes dirigidos a crear, mantener y mejorar la relación con los diferentes públicos objetivo del negocio.

La **comunicación interna** está dirigida al personal de la organización para dar respuesta a sus nuevas necesidades, crear un clima de confianza y motivación, dar a conocer la situación de la empresa.

FASE V - OPERACIÓN

Esta fase consta de una sola actividad descrita a continuación:

5.1 Planificación y control operacional

Para el desarrollo de esta actividad, la norma ISO 27001:2014 establece que la organización debe:

- Planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información.
- Implementar planes para lograr los objetivos de seguridad de la información.
- Mantener información documentada para demostrar que los procesos se han llevado a cabo tal como fueron planificados.
- Controlar los cambios planeados y revisar las consecuencias de cambios no intencionados para mitigar cualquier efecto adverso.

FASE VI - EVALUACIÓN DEL DESEMPEÑO

La evaluación del desempeño constituye una función esencial que debe efectuarse en toda organización, es un instrumento que se utiliza para comprobar el grado de cumplimiento de los objetivos propuestos a nivel individual y organizacional, al evaluar el desempeño la organización obtiene información para la toma de decisiones. Según la ISO 27001:2014, para cumplir con esta fase, la organización debe evaluar el desempeño y la efectividad del SGSI mediante la actividad detallada a continuación:

6.1 Monitoreo, análisis y evaluación del SGSI

Según la norma ISO 27001:2014, la organización debe determinar lo siguiente:

- Qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información.
- Los métodos para monitoreo, análisis y evaluación.
- Cuándo el monitoreo debe ser realizado.
- Quién debe monitorear.
- Cuándo los resultados del monitoreo deben ser analizados y evaluados.
- Quién debe analizar y evaluar estos resultados.

6.2 Auditoría interna

La Auditoría interna es una actividad que tiene por objetivo examinar y evaluar si los requisitos de la organización están en conformidad con el SGSI, mejorar las procesos y funciones de la organización velando por la preservación de la integridad de la información. La organización debe cumplir con las siguientes especificaciones requeridas por la ISO 27001:2014, numeral 9.2:

- Planificar e implementar uno o varios programas de auditoría interna, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación.
- Definir el alcance de cada auditoría y seleccionar a los auditores.
- Reportar a los gerentes los resultados de las auditorías.
- Documentar información como evidencia del (de los) programa(s) de auditoría y los resultados de la auditoría.

Métodos de auditoría

Las auditorías se realizarán a discreción del equipo auditor, bajo los siguientes métodos:

- Entrevistas de auditoría.
- Inspección de ambientes dentro del alcance de la auditoría.
- Pruebas de controles de seguridad de información (muestras, simulaciones)

Responsabilidades de auditoría

- Convocante: dirección de la alta dirección – Gerente general.
- Ejecutor: equipo auditor – Auditor líder y especialistas que puedan ser convocados por este.
- Participantes: todo el personal y terceros que puedan ser convocados a discreción del auditor, como parte de su investigación.

FASE VII – MEJORA CONTINUA

Esta fase se basa en la ISO 27001:2014 numeral 10.0 y en COBIT 5 para seguridad de la información, donde manifiesta que la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

1.3 Desarrollo del modelo propuesto

Según lo estipulado en la resolución ministerial Nº 004-2016-PCM, se tomó como estándar base las fases mencionadas en la ISO 27001:20014, las cuales se complementaron con otras metodologías para crear plantillas que fueron adaptadas a las necesidades de las unidades ambientales de la región Lambayeque.

En la figura 8 se muestra la estructura base del modelo de seguridad de la información propuesto, indicando las actividades que conforman cada fase.

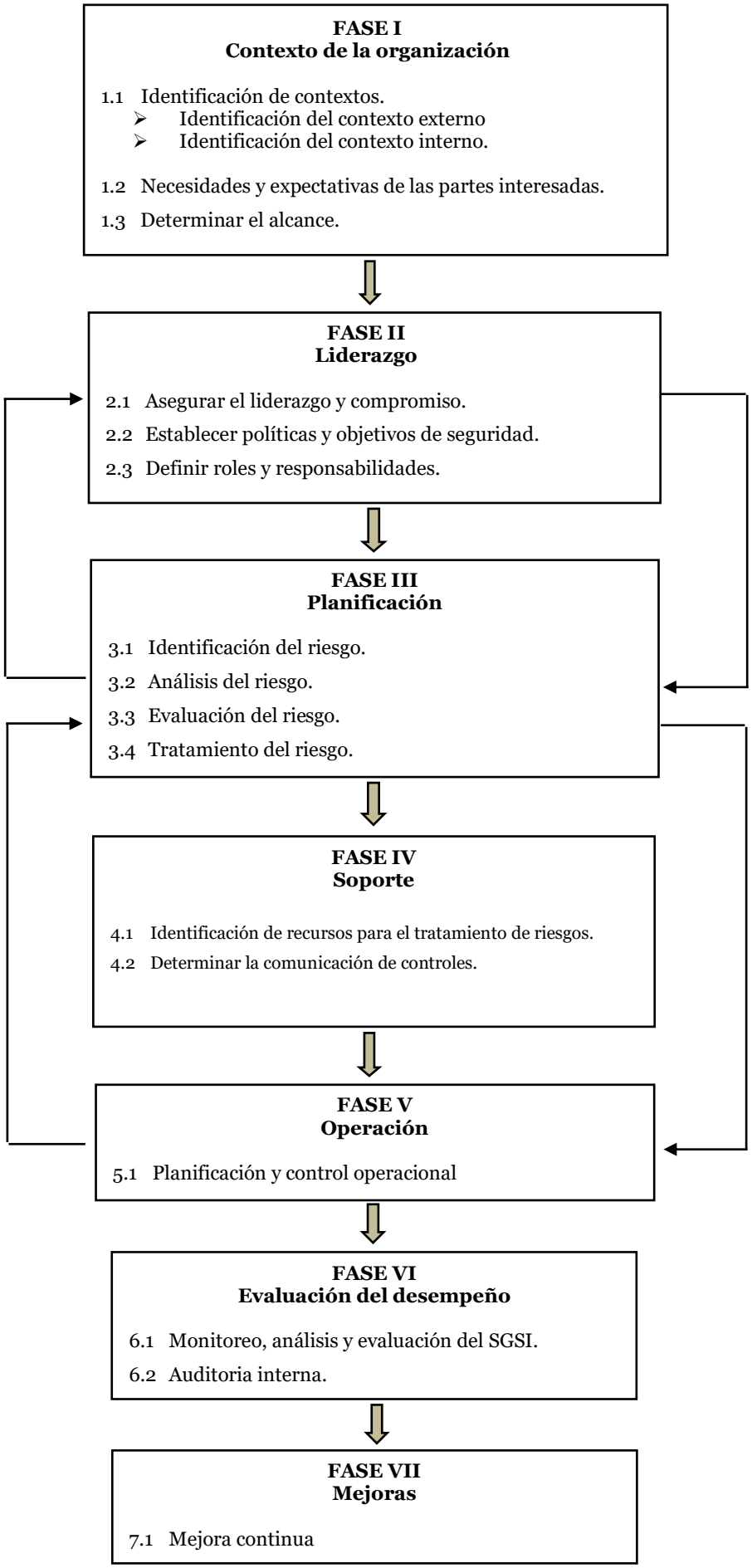


Figura 8. Modelo propuesto para la seguridad de la información.

FASE I - Contexto de la organización

En esta fase se deben identificar los aspectos externos e internos que se relacionan con el rendimiento de la unidad de gestión ambiental. También es necesario conocer las necesidades y las personas interesadas que intervienen en el desarrollo del sistema de gestión de seguridad de la información.

1.1 Identificación de contextos

- **Identificación del contexto externo**

Los aspectos a identificar, son los propuestos en la siguiente tabla:

Tabla 3. Plantilla para la identificación del contexto externo

<table>
<tr><th colspan="3">FASE I – CONTEXTO DE LA ORGANIZCIÓN</th></tr>
<tr><td colspan="2">Nombre del documento
Identificación del contexto externo</td><td>Doc. N° 01</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td>Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="3">Objetivo
Identificar los aspectos externos que afectan el rendimiento de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se puede hacer uso de técnicas e instrumentos como: entrevistas, análisis de documentos y cuestionarios.</td></tr>
<tr><th>N°</th><th>Entorno</th><th>Aspectos identificados</th></tr>
<tr><td>01</td><td>Social y cultural</td><td>Aspectos referentes al estilo de vida, el contexto geográfico, demográfico, grupos de interés sociales, empresas ejecutoras y otros organismos de la región relacionados a las unidades de gestión ambiental.</td></tr>
<tr><td>02</td><td>Político</td><td>Instituciones y aspectos políticos que se relacionan con el cumplimiento de los objetivos ambientales de las entidades públicas y el fortalecimiento de los mecanismos en la gestión ambiental.</td></tr>
<tr><td>03</td><td>Financiero</td><td>Elementos y/o instituciones relacionados con la economía que influyen en el rendimiento de las unidades de gestión ambiental.</td></tr>
<tr><td>04</td><td>Reglamentario</td><td>Conjunto de exigencias legales como normas y lineamientos que facilitan la gestión ambiental, las organizaciones que no cumplen lo dispuesto en el reglamento están expuestas a sanciones poniendo en riesgo su funcionamiento.</td></tr>
<tr><td colspan="3">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

- **Identificación del contexto interno**

Para la identificación de este contexto, es necesario primero revisar las siguientes fuentes de información:

- Plan estratégico institucional.
- Visión, misión, objetivos estratégicos.
- La estructura de la organización, funciones y responsabilidades.
- Normas y políticas adoptadas por la institución.
- Organigrama de institución.
- Sistemas de información y los procesos de toma de decisiones.

Después de revisar las fuentes de información antes mencionadas, se procede a identificar los aspectos internos de la siguiente tabla:

Tabla 4. Plantilla para la identificación del contexto interno

<table>
<tr><th colspan="3">FASE I - CONTEXTO DE LA ORGANIZACIÓN</th></tr>
<tr><td colspan="2">Nombre del documento
Identificación del contexto interno</td><td>Doc. N° 02</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td>Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="3">Objetivo
Identificar los aspectos internos que afectan el rendimiento de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se debe hacer uso del análisis de las fuentes de información de la entidad.</td></tr>
<tr><th>N°</th><th>Entorno</th><th>Aspectos identificados</th></tr>
<tr><td>01</td><td>Estructura de la organización, funciones y responsabilidades</td><td>Son todas las actividades, roles o tareas que la empresa debe realizar, las cuales le permitan establecer sus funciones para alcanzar las metas y objetivos de la gestión de proyectos ambientales.</td></tr>
<tr><td>02</td><td>Objetivos y estrategias</td><td>Es el propósito hacia donde la organización quiere llegar a través de un conjunto de actividades.</td></tr>
<tr><td>03</td><td>Recursos y conocimientos</td><td>Son las capacidades, competencias, documentos, procedimientos e infraestructura tecnológica necesarios para el rendimiento de las unidades de gestión ambiental.</td></tr>
<tr><td>04</td><td>Cultura de la organización</td><td>Conjunto de conocimientos, actitudes y experiencias que puede ser: miembros de la unidad de gestión ambiental, administrativos y áreas que otorgan información.</td></tr>
<tr><td colspan="3">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

1.2 Necesidades y expectativas de las partes interesadas

Para el desarrollo de esta actividad, es necesario incluir las partes interesadas externas e internas identificadas en el contexto de la organización, se deben realizar reuniones para definir los requisitos de la seguridad de información que representan necesidades o expectativas de las partes interesadas.

La plantilla de la tabla 5 se debe llenar utilizando un indicador de relación entre la parte interesada y cada necesidad/tipo de información:

- A—Aprobador:
- O—Origen (emisor)
- I— Informado del tipo de información
- U—Destino: usuario de la información

Tabla 5. Identificación de las partes interesadas

FASE I - CONTEXTO DE LA ORGANIZACIÓN											
Nombre del documento Identificación de las partes interesadas								**Doc. N°**		03	
Registrado por: **Aprobado por:**								**Fecha de registro** dd/mm/aaaa			
Objetivo Identificar las necesidades de las partes interesadas relacionadas con la entidad.											
Descripción Para la recolección de información se puede hacer uso de técnicas e instrumentos como entrevistas y cuestionarios.											
Parte interesada	**Necesidades / tipos de información**										
	Sistema de gestión de seguridad de la información	Mejoras en seguridad de la información	Políticas de seguridad de la información	Plan de acción para riesgos	Plan de seguridad de la información	Información documentada según las normas	Informe del análisis de riesgos	Programas de capacitación	Programa de auditoría interna	Revisiones del desempeño de la seguridad de la información	Plan de mejora continua
INTERNA											
Gerente de desarrollo olmos											
Responsable ambiental											
Especialista ambiental											
Encargado de archivo											
Personal de apoyo											
Responsable de TI											
EXTERNA											
Gobierno regional											
Empresas ejecutoras privadas											
Usuarios solicitantes de información.											
Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.											

Estos requisitos deben ser reevaluados en cada ciclo de operación, ya que las necesidades de la organización, sus acuerdos o las leyes aplicables pueden cambiar durante ese periodo.

1.3 Alcance del sistema de gestión de seguridad de la información

En esta actividad se deben considerar los aspectos externos e internos, las partes interesadas relevantes al SGSI y los procesos o funciones incluidos dentro de los límites del SGSI. Para cumplir con esta actividad, la unidad de ambiental debe documentar lo siguiente:

Tabla 6. Plantilla para el alcance del SGSI

<table>
<tr><th colspan="3">FASE I - CONTEXTO DE LA ORGANIZACIÓN</th></tr>
<tr><td colspan="2">Nombre del documento
Alcance del SGSI</td><td>Doc. N°
04</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td>Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="3">Objetivo
Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se debe hacer uso del TUPA.</td></tr>
<tr><td>Proceso/funciones</td><td colspan="2">Detallar los procesos o funciones donde se maneja la información a resguardar.</td></tr>
<tr><td>Responsables</td><td colspan="2">Personal a cargo del tratamiento de la información.</td></tr>
<tr><td>Infraestructura de TI</td><td colspan="2">Es el conjunto de dispositivos físicos y aplicaciones de software que intervienen durante el manejo de la información.</td></tr>
<tr><td colspan="3">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

FASE II – Liderazgo

En esta fase primero se identifican las funciones relacionadas con el liderazgo, después se seleccionan las políticas de seguridad a implementar, finalmente se establecen los roles y responsabilidades de las personas que intervendrán en el desarrollo del SGSI.

2.1 Asegurar el liderazgo y compromiso

Para desarrollar esta actividad, se consideran las funciones de seguridad de información mínimas requeridas por la norma 27001:2014 a partir de las cuales se identifica la participación de la gerencia general. Para ello, se debe llenar la plantilla de la tabla 07, marcando con una X según el cumplimiento

de la función. Finalmente, se debe especificar la(s) función(s) que falta por cumplir.

Tabla 7. Plantilla para determinar el liderazgo

<table>
<tr><th colspan="6">FASE II - LIDERAZGO</th></tr>
<tr><td colspan="4">Nombre del documento
Cumplimiento del liderazgo</td><td>Doc.
N°</td><td>05</td></tr>
<tr><td colspan="4">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="6">Objetivo
Identificar: Si = la gerencia cumple con las funciones de liderazgo, No= la gerencia no cumple con las funciones de liderazgo, Parcial= la función está incompleta.</td></tr>
<tr><td colspan="6">Descripción
Para la recolección de información se debe hacer uso de entrevistas aplicadas a la gerencia</td></tr>
<tr><th>N°</th><th>Funciones</th><th>Si</th><th>No</th><th>Parcial</th></tr>
<tr><td>01</td><td>Asegura que la política y los objetivos de seguridad de la información sean establecidos y compatibles con la dirección estratégica de la organización.</td><td></td><td></td><td></td></tr>
<tr><td>02</td><td>Asegurar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización.</td><td></td><td></td><td></td></tr>
<tr><td>03</td><td>Asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.</td><td></td><td></td><td></td></tr>
<tr><td>04</td><td>Comunicar la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.</td><td></td><td></td><td></td></tr>
<tr><td>05</td><td>Asegurar que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).</td><td></td><td></td><td></td></tr>
<tr><td>06</td><td>Dirigir y apoyar a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información</td><td></td><td></td><td></td></tr>
<tr><td>07</td><td>Promover la mejora continua.</td><td></td><td></td><td></td></tr>
<tr><td>08</td><td>Apoyar otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.</td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

2.2 Establecer políticas y objetivos de seguridad de la información

En este apartado se ha considerado una lista de políticas que cubren las necesidades de la unidad ambiental, teniendo en cuenta que también se pueden adaptar otras políticas de interés. El formato a seguir es el mostrado en la tabla 8.

Tabla 8. Plantilla para políticas de seguridad de la información

<table>
<tr><td colspan="6">FASE II - LIDERAZGO</td></tr>
<tr><td colspan="4">Nombre del documento
Establecimiento de políticas de seguridad de la información.</td><td>Doc. Nº</td><td>06</td></tr>
<tr><td colspan="4">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="6">Objetivo
Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.</td></tr>
<tr><td colspan="6">Descripción
Para la recolección de información se puede hacer uso de entrevistas y análisis de documentos.</td></tr>
<tr><td>Nº</td><td>Políticas de seguridad</td><td>Definición</td><td>Alcance</td><td>Objetivo</td><td>Controles de seguridad</td></tr>
<tr><td>01</td><td>Políticas de la seguridad de la información</td><td>Establecer controles para la gestión de seguridad de la información dentro de una organización.</td><td rowspan="4">Identificar las áreas donde se aplicarán las políticas y las personas involucras en el cumplimiento de la misma.</td><td rowspan="4">Objetivo de seguridad de la información.</td><td rowspan="4">Controles de seguridad de la información según la lista de controles de la ISO 27001.</td></tr>
<tr><td>02</td><td>Política de seguridad de los recursos humanos</td><td>Esta política ayuda en la asignación y cumplimiento de las responsabilidades del personal dentro de una organización.</td></tr>
<tr><td>03</td><td>Política de gestión de activos</td><td>Gestionar y administrar los activos de la organización durante sus procesos o funciones.</td></tr>
<tr><td>04</td><td>Política de control de accesos</td><td>Es la autorización que se otorga a las personas para acceder a las instalaciones o sistemas que contienen información.</td></tr>
</table>

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. Nº**	06
Registrado por: **Aprobado por:**				**Fecha de registro** dd/mm/aaaa	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se puede hacer uso de entrevistas y análisis de documentos.					
Nº	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
05	Política de seguridad física y ambiental	En esta política se debe detallar: -Protección de ubicaciones físicas: por ejemplo, los atributos de construcción. -Controles ambientales: normas de control medioambiental y normas de control de acceso físico (para empleados, proveedores, visitantes)	Identificar las áreas donde se aplicarán las políticas y las personas involucras en el cumplimiento de la misma.	Objetivo de seguridad de la información.	Controles de seguridad de la información según la lista de controles de la ISO 27001.
06	Política de respaldo y restauración de información	Detallar las medidas convenientes para asegurar que la información de la unidad de gestión ambiental, los datos del personal y de los usuarios; esté protegida contra pérdida, alteración o divulgación de manera accidental o malintencionada, ya sea por fallas de los equipos y/o redes.			
07	Política de seguridad de las comunicaciones	Se encarga de prevenir que algún usurario y/o entidad no autorizada, pueda acceder de forma inteligible a información.			

<table>
<tr><th colspan="6">FASE II - LIDERAZGO</th></tr>
<tr><td colspan="4">Nombre del documento
Establecimiento de políticas de seguridad de la información.</td><td>Doc. Nº</td><td>06</td></tr>
<tr><td colspan="4">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="6">Objetivo
Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.</td></tr>
<tr><td colspan="6">Descripción
Para la recolección de información se puede hacer uso de entrevistas y análisis de documentos.</td></tr>
<tr><th>Nº</th><th>Políticas de seguridad</th><th>Definición</th><th>Alcance</th><th>Objetivo</th><th>Controles de seguridad</th></tr>
<tr><td>08</td><td>Política de gestión de Incidentes de seguridad de la información</td><td>Todos los miembros de una organización deben anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios.</td><td rowspan="3">Identificar las áreas donde se aplicarán las políticas y las personas involucras en el cumplimiento de la misma.</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>09</td><td>Política de cumplimiento</td><td>Definir tareas y responsabilidades de modo que se ajusten a la normativa aplicable según el giro del negocio.</td></tr>
<tr><td>10</td><td>Política de privacidad</td><td>Se debe dar a conocer las condiciones que rigen el tratamiento y protección de datos personales que son enviados a través de servicios o dispositivos de almacenamiento de la unidad de gestión ambiental.</td><td>Objetivo de seguridad de la información.</td><td>Controles de seguridad de la información según la lista de controles de la ISO 27001.</td></tr>
<tr><td colspan="6">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

2.3 Definir roles y responsabilidades

La gerencia general en la tabla 9, debe asignar a cada rol sus responsabilidades, indicando el nivel de implicación que tienen en la unidad ambiental.

Tabla 9. Plantilla para identificar roles y responsabilidades

<table>
<tr><th colspan="3">FASE II - LIDERAZGO</th></tr>
<tr><td colspan="2">Nombre del documento
Roles y responsabilidades</td><td>Doc. Nº
07</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td>Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="3">Objetivo
Identificar los roles y las responsabilidades de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se debe hacer uso del análisis documentario de la unidad ambiental.</td></tr>
<tr><th>Rol</th><th>Responsabilidad</th><th>Nivel de implicancia</th></tr>
<tr><td>Identificar el rol o cargo del personal de la unidad ambiental</td><td>Identificar las responsabilidades o funciones asociadas a cada rol del personal de la unidad ambiental.</td><td>Indicar el nivel de implicación del personal en la unidad ambiental mediante la siguiente calificación:

(A) Responsable de que se haga.
(R) Responsable de hacerlo.
(C) Consultado.
(I) Informado.</td></tr>
<tr><td colspan="3">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

FASE III – Planificación

En esta fase es necesario considerar los aspectos externos e internos del numeral 1.1 y las necesidades y expectativas de las partes interesadas del numeral 1.2. El objetivo es identificar los riesgos y las oportunidades que necesitan ser tratados, prevenir o reducir efectos indeseados y lograr la mejora continua.

3.1 Identificación del riesgo

Para el desarrollo de esta actividad, primero es necesario identificar y valorar los activos, para luego identificar sus vulnerabilidades y amenazas.

- **<u>Identificación de activos</u>**

  Se entiende por activo, todo aquello que tiene valor para la organización y por lo tanto requiere de protección. Para el desarrollo de esta actividad, se hará uso de la lista de clasificación de activos (ver tabla 2) y se deberá llenar la plantilla N°10.

Tabla 10. Plantilla para la identificación de activos

FASE III – PLANIFICACIÓN					
Nombre del documento Identificación de activos.				**Doc. N°**	08
Registrado por: **Aprobado por:**				**Fecha de registro** dd/mm/aaaa	
Objetivo: Identificar los activos presentes en la unidad ambiental.					
Descripción: Para la recolección de información se puede hacer uso de la observación directa.					
N°	**Tipo de activo**	**Activo**	**Código_activo**	**Descripción**	**Responsable**
01	Hardware	Son los elementos físicos de hardware que soportan la ejecución de las aplicaciones informáticas y el procesamiento o la transmisión de la información.	[HW_activo]	Mencionar la función del activo.	Personal a cargo del activo.
02	Software	Son los programas o aplicativos que gestionan, analizan y transforman los datos, permitiendo la explotación de la información para la prestación de los servicios.	[SW_activo]		
03	Datos	Es la información que permite a la organización prestar sus servicios. Puede ser almacenada en equipos o bases de datos, o transferida en medios de transmisión de datos.	[D_activo]		
04	Servicios	Son las funciones que satisfacen una o varias necesidades de los usuarios.	[S_activo]		
05	Soportes de información	Se consideran los dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.	[Media_activo]		
06	Instalaciones	Son los lugares donde se hospedan los sistemas de información y comunicaciones.	[L_activo]		
07	Personal	Son las personas que laboran en la organización relacionadas con los sistemas de información.	[P_activo]		

- **Valoración de activos**

La organización debe asignar un valor al activo que puede perjudicarse ante la presencia de amenazas. Para la valoración de activos se tendrán en cuenta las siguientes dimensiones:

- **Disponibilidad (D):** es el acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO 27000)

- **Integridad (I):** mantenimiento de la exactitud y completitud de la información. (ISO 27000)

- **Confidencialidad (C):** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO 27000)

La valoración de cada activo se hace en base al valor de los siguientes criterios:

Tabla 11. Criterios para evaluar la disponibilidad

VALOR	DISPONIBILIDAD (D)
1	La inaccesibilidad a la información no afecta las funciones de la unidad ambiental.
2	La inaccesibilidad permanente durante una semana podría impedir la ejecución de las funciones de la unidad ambiental.
3	La inaccesibilidad permanente durante una hora podría impedir la ejecución de las funciones de la unidad ambiental.
4	La inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las funciones de la unidad ambiental.

Tabla 12. Criterios para evaluar la integridad

VALOR	INTEGRIDAD (I)
1	La modificación no autorizada puede repararse fácilmente o no afecta a las actividades de la unidad ambiental.
2	La modificación no autorizada puede repararse aunque podría ocasionar un perjuicio a la unidad ambiental.
3	La modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo a la unidad ambiental.
4	La modificación no autorizada no podría repararse, impidiendo la realización de las funciones de la unidad ambiental.

Tabla 13. Criterios para evaluar la confidencialidad

VALOR	CONFIDENCIALIDAD (C)
1	La información conocida y/o utilizada por un grupo de personas para realizar su trabajo dentro de la unidad ambiental, no es relevante.
2	La información conocida y/o utilizada por todo el personal dentro de unidad ambiental, no trasciende de la función afectada.
3	La información conocida y/o utilizada por un grupo muy reducido de personas dentro de la entidad, el incidente implica a otras funciones.
4	La información conocida y/o utilizada sin autorización por cualquier persona, dentro y fuera de la entidad, podría ocasionar un grave perjuicio.

La suma de las tres dimensiones determinará el nivel de criticidad del activo valorado según la tabla 14:

Tabla 14. Valoración del nivel de criticidad de activos

Valor	Nivel
1 - 3	Muy bajo
4 - 6	Bajo
7- 9	Alto
10 - 12	Muy alto

Mediante la plantilla de la tabla 15, se debe realizar la valoración de los activos:

Tabla 15. Plantilla para la valoración de activos

FASE III – PLANIFICACIÓN						
Nombre del documento Valoración de activos.					**Doc. N°**	09
Registrado por: **Aprobado por:**					**Fecha de registro** dd/mm/aaaa	
Objetivo: Identificar el nivel de criticidad de cada activo.						
Descripción: Para el desarrollo de esta actividad se extraen los activos de la plantilla de identificación de activos.						
N°	**Activo**	**Criterio**			**Total**	**Nivel**
		(D)	**(I)**	**(C)**		
01	Computadora de escritorio	3	2	4	9	Alto
02	Impresora	2	4	2	8	Alto
03	….	….	….	….	….	….
Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.						

- **<u>Identificación de amenazas y vulnerabilidades</u>**

A partir de los activos detallados anteriormente, se deben identificar las vulnerabilidades y amenazas asociadas. La lista de la tabla 16 servirá de ayuda para que la unidad ambiental identifique sus amenazas y vulnerabilidades; sin embargo, también puede adicionar otras a partir de experiencias vividas o casos de otras organizaciones del mismo giro del negocio.

Tabla 16. Lista de amenazas y vulnerabilidades

ACTIVO	AMENAZAS	VULNERABILIDADES
Hardware	Incumplimiento en el mantenimiento del sistema de información.	Mantenimiento insuficiente /instalación fallida de los medios de almacenamiento.
	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.	Falta de esquemas de reemplazo periódico, susceptibilidad a la humedad, el polvo y la suciedad.
	Radiación electromagnética	Sensibilidad a la radiación electromagnética
	Error en el uso	Falta de control de cambio con configuración eficiente.
	Pérdida del suministro de energía	Susceptibilidad a las variaciones de tensión.
	Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura.
	Hurto de medios o documentos	Almacenamiento sin protección.
		Copia no autorizada
		Falta de cuidado en la disposición final.
Software	Falsificación de derechos	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.
	Abuso de los derechos	Falta o insuficiencia de la prueba del software
		Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.
		Distribución errada de los derechos de acceso.
		Incompatibilidad
	Corrupción de datos	Ataque informático humano.
	Error en el uso	Interface de usuario complicada.
		Falta de documentación.
		Fechas incorrectas

ACTIVO	AMENAZAS	VULNERABILIDADES
	Manipulación con software	Descarga y uso no controlados de software
		Falta de copias de respaldo
Personal	Incumplimiento en la disponibilidad del personal.	Suplantación de identidad
	Error en el uso	Uso incorrecto de software y hardware
		Entrenamiento insuficiente en seguridad
		Falta de conciencia acerca de la seguridad
	Procesamiento ilegal de los datos	Falta de mecanismos de monitoreo
	Hurto de medios o documentos	Trabajo no supervisado del personal externo o de limpieza
	Destrucción de equipo o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
Ambientes físicos	Inundación	Ubicación en un área susceptible de inundación.
	Pérdida del suministro de energía	Red energética inestable
	Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación
Información	Incumplimiento en el mantenimiento de la información.	Información no registrada bajo control .
		Uso inadecuado de la información almacenada.
		Desgaste por manipulación
	Negación de acciones	Falta de asignación adecuada de responsabilidades en la seguridad de la información.

Para la identificación de amenazas y vulnerabilidades se plantea la siguiente plantilla:

Tabla 17. Plantilla de identificación de amenazas y vulnerabilidades

<table>
<tr><td colspan="4">FASE III – PLANIFICACIÓN</td></tr>
<tr><td colspan="2">Nombre del documento
Identificación de amenazas y vulnerabilidades.</td><td>Doc. Nº</td><td>10</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="4">Objetivo
Identificar las amenazas y vulnerabilidades de cada activo identificado.</td></tr>
<tr><td colspan="4">Descripción
Para el desarrollo de esta actividad se ubica el activo identificado en la lista de amenazas y vulnerabilidades.</td></tr>
<tr><td>Nº</td><td>Activo</td><td>Amenaza</td><td>Vulnerabilidad</td></tr>
<tr><td>01</td><td>Computadora de escritorio</td><td>Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.</td><td>Falta de esquemas de reemplazo periódico, susceptibilidad a la humedad, el polvo y la suciedad.</td></tr>
<tr><td>02</td><td>....</td><td>....</td><td>.....</td></tr>
<tr><td colspan="4">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

3.2 Análisis del riesgo

Para realizar esta actividad, se debe valorar la probabilidad y el impacto de las amenazas y vulnerabilidades con el fin de medir su grado de riesgo, para lo cual se usará la siguiente valoración:

- **<u>Valoración de la probabilidad e impacto del riesgo</u>**

Tabla 18. Valoración de probabilidad de ocurrencia

Valor	Probabilidad	Descripción
1	Raro	El evento no se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir una vez cada 5 años.
3	Posible	El evento puede ocurrir al menos una vez cada 2 años.
4	Probable	El evento puede ocurrir una vez al año.
5	Casi seguro	El evento puede ocurrir más de una vez al año.

Tabla 19. Valoración del impacto

Valor	Intensidad	Descripción
1	Insignificante	No altera la ejecución ni el rendimiento de las funciones de la unidad ambiental.
2	Menor	Afecta la ejecución de las funciones de la unidad ambiental.
3	Moderado	Se continua con la ejecución de las funciones, pero afecta el rendimiento de las mismas.
4	Mayor	Se suspenden temporalmente las funciones a reforzar.
5	Catastrófico	Se cierra la unidad ambiental hasta su reestructuración.

- **Valoración de la magnitud del riesgo**

Para determinar la magnitud del riesgo se tiene que:

Riesgo = Probabilidad x Impacto

Se utiliza la siguiente escala del 1 al 25.

Tabla 20. Magnitud del impacto

VALOR	MAGNITUD
1 – 5	Baja
6 – 10	Media
11 – 15	Alta
16 – 25	Critica

A continuación, la tabla 21 muestra la plantilla para realizar el análisis de riesgos.

Tabla 21. Plantilla para el análisis del riesgo

FASE III – PLANIFICACIÓN								
Nombre del documento Análisis del riesgo.							**Doc. Nº**	11
Registrado por: **Aprobado por:**							**Fecha de registro** dd/mm/aaaa	
Objetivo Determinar el análisis del riesgo.								
Descripción Para el desarrollo de esta actividad se hace uso del resultado de la plantilla de identificación de amenazas y vulnerabilidades.								
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**Valor (PXI)**	**Código de riesgo**	**Magnitud**
01	Computadora de escritorio	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.	Susceptibilidad a la humedad, el polvo y la suciedad.	4	3	12	R01	Alta
02	Información de la organización	Modificación no autorizada	Copia no controlada.	3	3	9	R02	Media
03	….	….	….	…	…	…	….	….
Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.								

3.3 Evaluación del riesgo

En esta actividad se priorizarán los riesgos identificados ubicándolos según su impacto y probabilidad en el mapa de calor.

Probabilidad						
	5 Casi seguro	5	10	15	20	25
	4 Probable	4	8	12	16	20
	3 Posible	3	6	9	12	15
	2 Improbable	2	4	6	8	10
	1 Raro	1	2	3	4	5
		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
		Impacto				

Figura 05. Mapa de calor

Después de la priorización de los riesgos, se identificará la tolerancia al riesgo, para el cual se tiene la tabla 22:

Tabla 22. Identificación de tolerancia al riesgo.

Valor del riesgo	Tolerancia al riesgo	Descripción
1 – 6	Aceptable	El riesgo es aceptable tal y como existe.
7 – 13	Tolerable	El riesgo es tratado basado en la mitigación.
14 – 25	No tolerable	El riesgo es inaceptable por pérdidas aprox. de $. 300.000.00

Finalmente, en la tabla 23 se agregará el valor del riesgo relacionado con la tolerancia al riesgo, para determinar si el riesgo es aceptable, tolerable, moderado o no tolerable.

Tabla 23. Plantilla para la evaluación del riesgo

FASE III – PLANIFICACIÓN							
Nombre del documento Evaluación del riesgo.						**Doc. N°**	12
Registrado por: **Aprobado por:**						**Fecha de registro** dd/mm/aaaa	
Objetivo Determinar la evaluación del riesgo.							
Descripción Para el desarrollo de esta actividad se hace uso del resultado de la plantilla del análisis del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**	**Observación**
R01	Alta	Computadora de escritorio	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.	Susceptibilidad a la humedad, el polvo y la suciedad.	12	Tolerable	
R02	Media	Información de la organización	Modificación no autorizada	Copia no controlada	9	Tolerable	
R03	…	….	…..	…..	…..	…..	
Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.							

3.4 Tratamiento del riesgo

Para cada riesgo evaluado, teniendo en cuenta su magnitud y tolerancia, se debe seleccionar la estrategia de tratamiento del riesgo mencionadas a continuación:

Tabla 24. Estrategias para el tratamiento del riesgo

Estrategias para el tratamiento del riesgo	Definición
Aceptar el riesgo	Los daños ocasionados por la materialización del riesgo no son significativos y no es necesario implementar controles adicionales.
Mitigar	Disminuir el impacto y la probabilidad del riesgo implementación de controles.
Evitar el riesgo	Prevenir la materialización del riesgo retirando una actividad o un conjunto de actividades planificadas o existentes.
Transferir	Subcontratar un servicio que pueda manejar de manera más eficaz el riesgo en particular.

Finalmente, para el tratamiento del riesgo se deberá llenar la plantilla de la tabla 25.

Tabla 25. Plantilla para el tratamiento del riesgo

FASE III – PLANIFICACIÓN					
Nombre del documento Tratamiento del riesgo.				**Doc. Nº**	13
Registrado por: **Aprobado por:**				**Fecha de registro** dd/mm/aaaa	
Objetivo Determinar la evaluación del riesgo.					
Descripción Para el desarrollo de esta actividad se hacer uso de las amenazas identificadas en el análisis del riesgo y de los controles mencionados en la tabla 29.					
Código de riesgo	**Magnitud**	**Tolerancia**	**Amenaza**	**Estrategia**	**Controles**
R01	Baja	Tolerable	Amenazas identificas	Mitigar	Seleccionar los controles necesarios para las amenazas identificadas.
R2	Baja	Aceptable	Error en el uso de equipos	Mitigar	Mantener la revisión periódica del activo para asegurar su continua disponibilidad.
R3	……	……	……	…….	……..
Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.					

FASE IV - SOPORTE

Esta fase tiene como objetivo definir los recursos que se necesitan para implementar un SGSI.

4.1 Identificación de recursos para el tratamiento de riesgos

Determinar los recursos y las personas necesarias para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información. Mediante la plantilla de la tabla 26, se deberán identificar y describir los recursos necesarios para un SGSI:

Tabla 26. Plantilla para la identificación de recursos

FASE IV - SOPORTE							
Nombre del documento Identificación de recursos.						**Doc. N°**	14
Registrado por: **Aprobado por:**						**Fecha de registro** 15/12/2017	
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.							
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R1	Alta	Computadora de escritorio	Pérdida del suministro de energía.	Transferir	Proteger los equipos contra las fallas en los servicios de suministro.	Solicitar la contratación del servicio de suministro.	- Personal experto en suministro de energía.

4.2 Determinar la comunicación de controles

Dar a conocer las personas responsables que intervienen en la comunicación de los controles a implementarse, utilizando la siguiente plantilla:

Tabla 27. Plantilla para la comunicación de controles

<table>
<tr><th colspan="6">FASE IV - SOPORTE</th></tr>
<tr><td colspan="4">Nombre del documento
Comunicación de controles.</td><td>Doc. N°</td><td>15</td></tr>
<tr><td colspan="4">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
22/12/2017</td></tr>
<tr><td colspan="6">Objetivo: Dar a conocer a la gerencia y al personal de la organización los controles a implementar.</td></tr>
<tr><td colspan="6">Descripción
Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.</td></tr>
<tr><th>Controles</th><th>Actividades</th><th>Riesgos asociados</th><th>A quien comunicar</th><th>Quien debe comunicar</th><th>Tipo de comunicación</th></tr>
<tr><td>Lista de controles a implementar.</td><td>Actividades seleccionadas para lograr la implementación de los controles.</td><td>Lista de riesgos a tratar.</td><td>Área o persona a quien comunicar el control a implementar</td><td>Responsable de comunicar el control a implementar</td><td>Documento escrito, e-amil,</td></tr>
</table>

FASE V - OPERACIÓN

5.1 Planificación y control operacional

Para el desarrollo de esta actividad se debe llenar la siguiente plantilla:

Tabla 28. Plantilla de control operacional

<table>
<tr><th colspan="4">FASE V - OPERACIÓN</th></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="2">Nombre del documento
Control operacional</td><td>Doc. N°</td><td>16</td></tr>
<tr><td colspan="2">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="4">Objetivo
Alinear los controles seleccionados con los objetivos de seguridad establecidos por la organización, a fin de que estos últimos sean cumplidos.</td></tr>
<tr><td colspan="4">Descripción
Para el desarrollo de esta actividad se deben usar los controles mencionados en el tratamiento de riesgos.</td></tr>
<tr><th>Objetivo de seguridad</th><th>Control de seguridad</th><th>Actividades</th><th>Responsable</th></tr>
<tr><td>Objetivos de seguridad establecidos.</td><td>Controles seleccionados en el tratamiento de riesgos</td><td>Listar las actividades para implementar los controles y cumplir con los objetivos de seguridad.</td><td>Persona responsable del cumplimiento del control de seguridad</td></tr>
<tr><td>……</td><td>……</td><td>……</td><td>……</td></tr>
</table>

FASE VI - EVALUACIÓN DEL DESEMPEÑO

Para el desarrollo de esta fase, primero se califican los controles utilizando la tabla 29, con el fin de evaluar el cumplimiento de los controles propuestos. Lo que permitirá realizar las actividades de monitoreo y auditoria interna.

Tabla 29. Valoración del nivel de cumplimiento

Valor	Estado	Descripción
1	Cumple satisfactoriamente	Es gestionado, se está cumpliendo como solicita la norma, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
2	Cumple parcialmente	Se está haciendo de manera parcial, no está documentado, se definió pero no se gestiona.
3	No cumple	No existe y/o no se está haciendo.
4	No aplica	El control no es aplicable para la entidad. En el campo observaciones indicar la justificación respectiva de su no aplicabilidad.

6.1 Monitoreo, análisis y evaluación del SGSI

Para realizar esta actividad se debe llenar la siguiente plantilla:

Tabla 30. Plantilla de monitoreo

<table>
<tr><td colspan="5">FASE VI - EVALUACIÓN DEL DESEMPEÑO</td></tr>
<tr><td colspan="3">Nombre del documento
Monitoreo del SGSI</td><td>Doc. N°</td><td>17</td></tr>
<tr><td colspan="3">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="5">Objetivo
Establecer un plan de monitoreo.</td></tr>
<tr><td colspan="5">Descripción
Para el desarrollo de esta actividad se puede tener una entrevista con la gerencia y el área de sistemas.</td></tr>
<tr><td>N°</td><td>Controles</td><td>Valor del control</td><td>Estado</td><td>Periodo</td></tr>
<tr><td>01</td><td>Controles propuestos</td><td>Calificación del cumplimiento del control</td><td>Desempeño del control</td><td>Pendiente/culminado</td></tr>
<tr><td>02</td><td>……..</td><td>……..</td><td>……..</td><td>……..</td></tr>
<tr><td colspan="5">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

6.2 Auditoría interna

La tabla 31 ofrece una plantilla para la realización de la auditoría interna.

Tabla 31. Plantilla para la auditoria interna

<table>
<tr><td colspan="9">FASE VI - EVALUACIÓN DEL DESEMPEÑO</td></tr>
<tr><td colspan="7">Nombre del documento
Auditoría interna del SGSI</td><td>Doc. Nº</td><td>18</td></tr>
<tr><td colspan="7">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="9">Objetivo
Establecer un plan de auditoria.</td></tr>
<tr><td colspan="9">Descripción
Para el desarrollo de esta actividad se puede tener una entrevista con la gerencia y el área de sistemas.</td></tr>
<tr><td>Nº</td><td>Acción</td><td>Involucrados</td><td>Recursos</td><td>Tareas</td><td>Efectividad</td><td>Inicio</td><td>Cierre</td><td>Resultado</td></tr>
<tr><td>01</td><td>Actividades a realizar</td><td>Responsables y convocado</td><td>Ubicación de los recursos y tecnología a utilizar</td><td>Tareas a realizar durante la auditoria</td><td>Resultado esperado</td><td>dd/mm/año inicio de la auditoria</td><td>dd/mm/año fin de la auditoria</td><td>Realizado</td></tr>
<tr><td>02</td><td>.....</td><td>.....</td><td>.....</td><td>.....</td><td>.....</td><td>.....</td><td>.....</td><td>.....</td></tr>
</table>

FASE VII – MEJORA CONTINUA

Para el desarrollo de esta fase, se debe llenar la siguiente plantilla:

Tabla 32. Plantilla para mejora continua

<table>
<tr><td colspan="6">FASE VII - MEJORA CONTINUA</td></tr>
<tr><td colspan="4">Nombre del documento
Mejora continua</td><td>Doc. N°</td><td>19</td></tr>
<tr><td colspan="4">Registrado por:
Aprobado por:</td><td colspan="2">Fecha de registro
dd/mm/aaaa</td></tr>
<tr><td colspan="6">Objetivo
Establecer un plan de mejora continua.</td></tr>
<tr><td colspan="6">Descripción
Para el desarrollo de esta actividad se debe tener en cuenta los controles que no han sido cumplidos.</td></tr>
<tr><td>N°</td><td>Plan de acción</td><td>Riesgos involucrados</td><td>Controles</td><td>Fecha inicio</td><td>Fecha fin</td></tr>
<tr><td>01</td><td>Planes propuestos</td><td>Riesgos detectados</td><td>Controles propuestos que contrarrestan los riesgos</td><td>Inicio del plan</td><td>Fin del plan</td></tr>
<tr><td>02</td><td>….</td><td>……</td><td>……</td><td>…..</td><td>…..</td></tr>
<tr><td colspan="6">Conclusiones: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.</td></tr>
</table>

1.4 Evaluación de indicadores

Para contrastar la hipótesis se evaluarán los siguientes indicadores:

1.4.1 Armonización de las metodologías, estándares y normas de seguridad de la información

Para la evaluación de este indicador, se consideraron tres etapas para la comparación y armonización de las metodologías, estándares y normas de seguridad de la información, las cuales se describen a continuación:

Etapa 1

Identificar las leyes, estándares, metodologías y marcos de trabajo relacionados con la seguridad de la información.

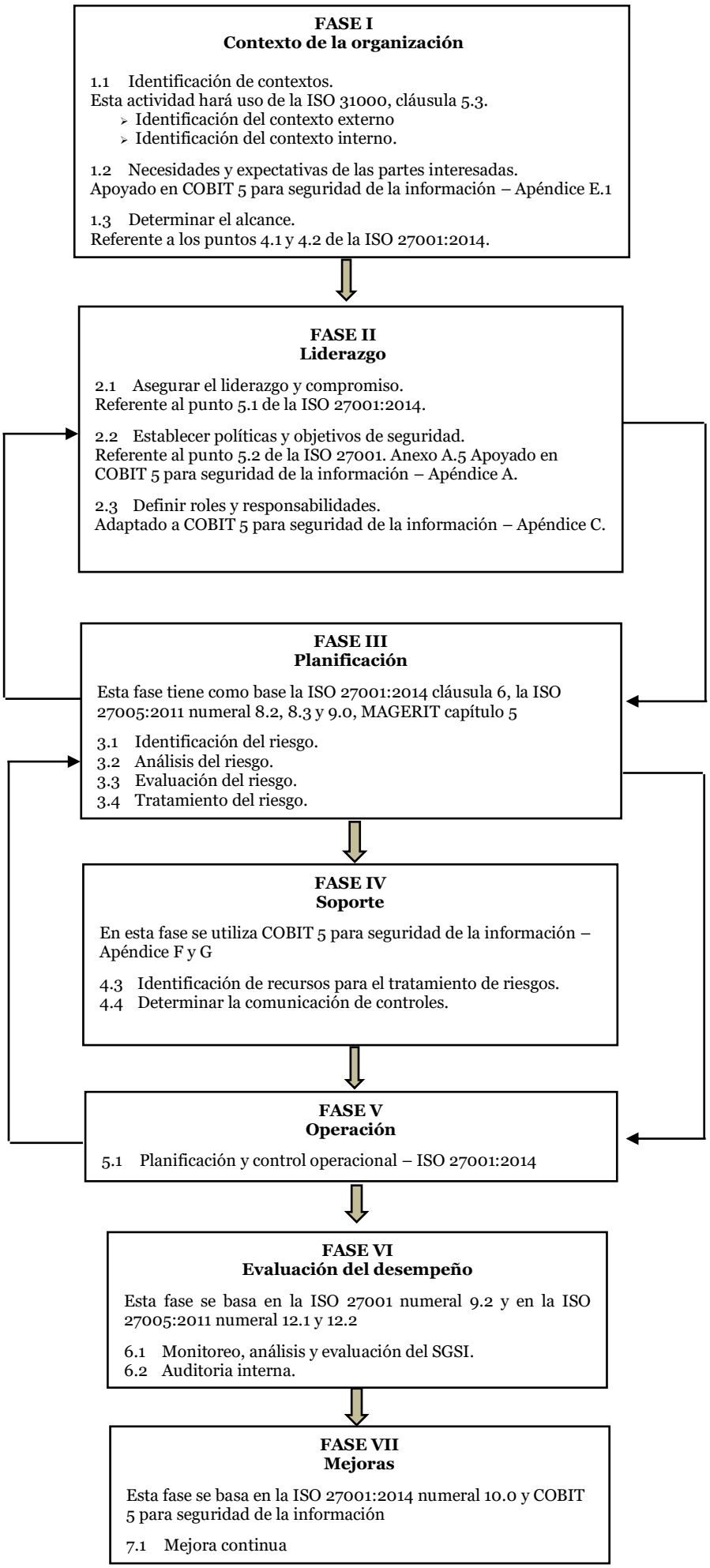
Etapa 2

Comparar cada uno de los estándares y metodologías relacionadas con la seguridad de la información (Anexo 3), realizando un análisis detallado de cada una de sus actividades (Capitulo III, numeral 1.2), seleccionando los elementos comunes entre sí y agrupándolos de acuerdo a las necesidades de las unidades ambientales.

Etapa 3

Esquematizar una estructura del modelo orientado a seguridad de la información, especificando los ítems de los estándares, metodologías y marcos de trabajo que apoyaron el desarrollo del modelo propuesto.

A continuación, se muestra el detalle de la estructura propuesta.


FASE I
Contexto de la organización
1.1 Identificación de contextos.
Esta actividad hará uso de la ISO 31000, cláusula 5.3.
Identificación del contexto externo
Identificación del contexto interno.
1.2 Necesidades y expectativas de las partes interesadas.
Apoyado en COBIT 5 para seguridad de la información – Apéndice E.1
1.3 Determinar el alcance.
Referente a los puntos 4.1 y 4.2 de la ISO 27001:2014.
FASE II
Liderazgo
2.1 Asegurar el liderazgo y compromiso.
Referente al punto 5.1 de la ISO 27001:2014.
2.2 Establecer políticas y objetivos de seguridad.
Referente al punto 5.2 de la ISO 27001. Anexo A.5 Apoyado en COBIT 5 para seguridad de la información – Apéndice A.
2.3 Definir roles y responsabilidades.
Adaptado a COBIT 5 para seguridad de la información – Apéndice C.
FASE III
Planificación
Esta fase tiene como base la ISO 27001:2014 cláusula 6, la ISO 27005:2011 numeral 8.2, 8.3 y 9.0, MAGERIT capítulo 5
3.1 Identificación del riesgo.
3.2 Análisis del riesgo.
3.3 Evaluación del riesgo.
3.4 Tratamiento del riesgo.
FASE IV
Soporte
En esta fase se utiliza COBIT 5 para seguridad de la información – Apéndice F y G
4.3 Identificación de recursos para el tratamiento de riesgos.
4.4 Determinar la comunicación de controles.
FASE V
Operación
5.1 Planificación y control operacional – ISO 27001:2014
FASE VI
Evaluación del desempeño
Esta fase se basa en la ISO 27001 numeral 9.2 y en la ISO 27005:2011 numeral 12.1 y 12.2
6.1 Monitoreo, análisis y evaluación del SGSI.
6.2 Auditoria interna.
FASE VII
Mejoras
Esta fase se basa en la ISO 27001:2014 numeral 10.0 y COBIT 5 para seguridad de la información
7.1 Mejora continua

1.4.2 Validez del modelo de seguridad de la información

Se tiene como objetivo general: contribuir en la seguridad de la información de la gestión de proyectos ambientales de las unidades de gestión ambiental en la región Lambayeque, para demostrar el cumplimiento de este objetivo, se realiza la validación del modelo propuesto mediante el uso de dos instrumentos:

Primero: Se sometió el modelo de seguridad de la información a la evaluación de tres expertos con el fin de medir el nivel de confiabilidad del modelo. Se procesaron los resultados del juicio de expertos, aplicando Alfa de Crombach, obteniendo un nivel de confiabilidad del 64% como lo refiere los resultados del cálculo siguiente:

Tabla 33. Estadístico de confiabilidad Alfa de Cronbach

Alfa de Cronbach	Alfa de Cronbach basados en elementos estandarizados	N elementos
0,641	0,583	21

Fuente: Elaboración propia

Tabla 34. Valores para estimar el nivel confiabilidad

VALOR	CONCLUSIÓN
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabilidad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy Confiable
0,72 a 0,99	Excelente confiabilidad
1.0	Confiabilidad perfecta

En base a la tabla anterior, se puede considerar que el coeficiente de confiabilidad obtenido es confiable.

El segundo instrumento es la prueba de concordancia de Kendall, para la validación de contenidos, el cual arrojó el siguiente resultado:

- Nivel de significancia de 0.05, es decir con 95% de confianza.

-Distribución chi-cuadrada ($\chi 2$) con N – 1 grados de libertad.

-k = 3

H0: No existe concordancia entre las opiniones de los evaluadores (W = 0).

H1: Existe concordancia entre las opiniones de los evaluadores (W > 0).

Tabla 35. Estadístico de prueba W de Kendall

	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
N	17	17	17	17
W	0.198	0.381	0.381	0.198
$\chi 2$	16.128	12.667	12.943	12.667
gl	2	2	2	2
p	0.000	0.002	0.002	0.002

Fuente: Elaboración propia

W es mayor que cero, se rechaza la hipótesis nula y se concluye que existe concordancia entre las opiniones de los evaluadores con respecto a la suficiencia, claridad, coherencia y relevancia y, que este valor es significativo.

1.4.3 Número de riesgos detectados y controles detectados

Según el diagnóstico de la situación problemática de las unidades ambientales, se manifestó (Ver anexo 02, preguntas 06 y 07) que no cuentan con políticas y controles de seguridad establecidos para la protección de la información, respondiendo de manera reactiva a cualquier tipo de amenaza.

Sin embargo, para medir el indicador de número de políticas y controles de seguridad identificados, se implementó para el caso de estudio el

modelo propuesto validado por juicio de expertos, logrando identificar 10 políticas de seguridad y 40 controles de seguridad (Ver anexo 04, tabla N°41) según las necesidades manifestadas por la unidad de gestión ambiental.

CONCLUSIONES

1. Se ha logrado proponer un modelo de seguridad de la información basado en estándares y metodologías adaptadas a las TI que soportan las funciones para contribuir en la seguridad de la información de las unidades de ambientales de la región Lambayeque.

2. Mediante el juicio de 3 profesionales expertos, se ha validado el modelo propuesto en seguridad de la información, logrando su aceptación y permitiendo que sea aplicado al entorno de las unidades ambientales.

3. Se ha calificado la implementación del modelo de seguridad de la información validado, aplicándolo a un caso de estudio en una unidad ambiental, identificando 6 riesgos críticos y 12 riesgos de magnitud alta.

4. En base al análisis de los riesgos, se ha logrado obtener una plantilla estándar que contiene todos los parámetros necesarios para la gestión de la seguridad de la información en el contexto de las unidades ambientales.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre, David. 2014. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Lima. Pontificia Universidad Católica del Perú.

Alcántara, Julio. 2015. Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo. Universidad Católica Santo Toribio de Mogrovejo.

Berríos Mesía, César Augusto, Rocha Cam y Martín Augusto. 2015. Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001. Lima. Universidad Peruana de Ciencias Aplicadas.

Borghello, Cristian. 2001. Seguridad Informática: sus implicancias e implementación. Tesis de Licenciatura en Sistemas. Argentina. Universidad Tecnológica Nacional.

Cateriano Pedro. 2016. Resolución ministerial Nº 004-2016-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Lima. Diario el Peruano.
http://busquedas.elperuano.com.pe/normaslegales/aprueban-el-uso-bligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

Collazos, Jesús. 2005. Manual de evaluación ambiental de proyectos. Lima. San Marcos.

Duque Rubiela. 2010. Metodologías de gestión de riesgos. Colombia. Universidad de Caldas.

Ernst & Young. 2011. Seguridad de la información en un mundo sin fronteras. Fecha de acceso: noviembre 23, 2017. México.
http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf

Gaona, Karina. 2013. Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicada a la empresa pesquera e industrial Bravito en la ciudad de Machala. Universidad Politécnica Salesiana sede Cuenca.

IT Governance Institute. 2006. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2nd Edition. USA.

IT Governance Institute. 2008. Information Security Governance: Guidance for Information Security Managers. USA.

ISACA. COBIT 5 para seguridad de la información. 2012.

INDECOPI. 2014. NTP-ISO/IEC 27001. "Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición". Lima.

INACAL. 2011. NTP-ISO/IEC 31000. "Gestión del riesgo. Principios y directrices". Lima.

INACAL. 2015. NTP-ISO/IEC 14001. Sistemas de gestión ambiental. Requisitos con orientación para su uso. 4ª Edición. Lima.

INDECOPI. 2008. ISO/IEC 27005. Gestión de riesgos de seguridad de la información.

Inga, Deysi. 2013. El sistema de gestión ambiental local en el distrito de San Borja. Lima. Pontificia Universidad Católica del Perú.

Jaramillo, Pablo. 2012. Propuesta para la implementación de un sistema de gestión ambiental conforme a la norma ISO 14001:2004, en la "asociación agroindustrial lojana de alimentos" ubicada en la ciudad de Loja, Ecuador. Universidad de Católica de Loja.

Narváez, Iván. 2013. Aplicación de la norma ISO 27001 para la implementación de un SGSI en la Fiscalía General del Estado. Pontificia Universidad Católica del Ecuador.

Peso Navarro, Emilio del Ramos y Miguel Ángel. 2004. La seguridad de los datos de carácter personal. Madrid. Ediciones Díaz de Santos.

Picón, Ingrid. 2016. Elaboración de un plan de implementación de la ISO/IEC 27001:2013. Colombia. Instituto colombiano para la evaluacion de la educación – ICFES.

MEF. 2014. Resolución ministerial NTP-ISO/IEC 17799:2007 https://www.mef.gob.pe/es/por-instrumento/resolucion-inisterial/11070-resolucion-ministerial-n-081-2014-ef-44/file

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. 2012. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I. Madrid. Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones.

Zavaleta, Deyvis. 2016. Implementación de un Sistema de Gestión de Seguridad de la Información aplicando NTP ISO/IEC 27001:2014 en el sector Hospitalario. Lima. Universidad Weiner.

ANEXO 1

DESCRIPCIÓN DE ENTIDADES PÚBLICAS CON UNIDAD AMBIENTAL EN LA REGIÓN LAMBAYEQUE

DATOS GENERALES	ENTIDAD 1	ENTIDAD 2	ENTIDAD 3	ENTIDAD 4
Sector	Transporte	Agrícola	Producción	Actividades de otras asociaciones
Actividad relacionada	Elaboración de proyectos ambientales			
Fecha de creación	09 de febrero de 1998.	04 de Julio del 2003	2002	13 de octubre de 1972
Dirección	KM. 9 carretera Pimentel Chiclayo	Calle Las Violetas N° 148 Urb. Los Libertadores	Laureles N° 171 Urb. Los Libertadores	Juan Buendía N° 145 Urb. Patazca Chiclayo
Representante legal	Ing. César Antonio Zeña Santamaría	Juan Saavedra Tineo	Lic. Juan Pablo Santamaría Baldera	Jorge Alberto Figueroa Roque
Misión	Mejorar y ampliar la infraestructura vial, garantizar el adecuado funcionamiento del transporte público terrestre y las comunicaciones con el fin de contribuir al desarrollo integral, armónico y sostenible de la región.	Contribuir al desarrollo sostenible de su ámbito de influencia, mediante la explotación racional de sus recursos y potencialidades existentes, aprovechando en forma sustentable el uso multipropósito del recurso hídrico, con un enfoque de inclusión social y adaptación al cambio climático.	Ejecutar acciones de coordinación, evaluación y control de actividades pesqueras (extracción, procesamiento y acuicultura) comprendidas dentro de su ámbito, promoviendo su competitividad y desarrollo mediante el uso racional de los recursos y protección del medio ambiente, contribuyendo al desarrollo sostenible de la Región Lambayeque.	Somos una Organización representativa de los usuarios de agua de uso agrario del Valle Chancay-Lambayeque. Realizamos una gestión integrada del recurso hídrico; a través de una eficiente administración, operación y mantenimiento del sistema hidráulico; y actividades de promoción agraria generando el bienestar de nuestros usuarios.
Visión	Ser en una institución líder cuya gestión eficiente en los servicios de transportes y comunicaciones contribuya al desarrollo integral y sostenible de la región Lambayeque.	Ser la organización líder en la gestión y ejecución de proyectos hidráulicos e hidroenergéticos, orientados a garantizar la sostenibilidad de la oferta hídrica en todos los valles de la región y/a impulsar el desarrollo y la inversión en el norte del país.	Ser un organismo estatal eficiente para promover el desarrollo integral y sostenido de los sub sectores pesquería, industria y MYPE's de la región Lambayeque. Mantener una cultura ética basada en el fomento y la práctica de los valores, utilizando los recursos y las competencias asignadas con eficacia y eficiencia.	Ser la mejor junta a nivel nacional, reconocida por su vocación integradora, eficiente gestión del recurso hídrico y promoción de la agro exportación y gestión empresarial; que brinda sus servicios de calidad a sus usuarios, generando su bienestar y contribuyendo a la protección del medio ambiente y al desarrollo sostenible del Valle Chancay - Lambayeque.

DATOS GENERALES	ENTIDAD 1	ENTIDAD 2	ENTIDAD 3	ENTIDAD 4
Valores	Compromiso, colaboración, capacidad, servicio.	Compromiso, colaboración, responsabilidad, servicio.	Servicio, compromiso, responsabilidad.	Servicio, compromiso, responsabilidad.
Objetivos estratégicos	- Ejecutar políticas orientadas a facilitar la administración de los servicios de transporte público, de personas y carga, a nivel regional. - Conducir y controlar las actividades relacionadas con la circulación y educación vial, a nivel regional en el ámbito de su competencia. - Mantener actualizado los registros administrativos y normatividad vigente en materia de transporte y tránsito de personas y carga. - Controlar y fiscalizar el cumplimiento de la normatividad y reglamentación vinculada al transporte y tránsito terrestre, en el ámbito regional.	Contribuir, apoyar y promover el desarrollo armónico e integral de las áreas seleccionadas en el ámbito de su jurisdicción y otras que le encargue el Gobierno Regional Lambayeque. Formular y proponer lineamientos de política integral y estrategias que instrumenten la implementación de los Proyecto Olmos, Tinajones y proyectos del plan de desarrollo hidráulico regional. Elaborar un sistema de seguimiento y evaluación que mida el grado de avance y logros de los Proyectos Olmos y Tinajones, de los proyectos del plan de desarrollo hidráulico regional, del planeamiento estratégico, del plan operativo e implementación de políticas y estrategias. Apoyar y coordinar con las instituciones pertinentes, acciones, programas y proyectos orientados al	- Promover el desarrollo de la acuicultura. - Conseguir la formalización de la totalidad de productores acuícolas. - Acceder a créditos por parte del Fondo Nacional de Desarrollo Pesquero - FONDEPES. - Mejorar el asesorando a los acuicultores para un eficiente manejo piscícola.	- Operar y mantener la infraestructura hidráulica a su cargo, promoviendo su desarrollo. - Distribuir el agua en el sector hidráulico menor de acuerdo a la disponibilidad de los recursos hídricos y los programas aprobados. - Cobrar las tarifas de agua y administrarlas adecuadamente. - Recaudar la retribución económica y transferirla a la Autoridad Nacional del Agua. - Supervisar el cumplimiento de las obligaciones de los usuarios de agua del sector hidráulico.

DATOS GENERALES	ENTIDAD 1	ENTIDAD 2	ENTIDAD 3	ENTIDAD 4
		afianzamiento y sostenibilidad del recurso hídrico.		
Área de TI	- Difusión de los datos de trabajos en las diferentes oficinas en la página web de la institución. - Descargar en el sistema de cómputo documentos relacionados con licencias de conducir. - Almacenar actas de examen de manejo. - Almacenar las sanciones de suspensión, inhabilitación y cancelación de las licencias de conducir en la tarjeta de registro del conductor. - Digitar y procesar documentos de seguridad vial, construcción y reparación de carreteras, entro otros.	- Se establece un cronograma para el respaldo mensual de la información. - Realización y aplicación del plan de contingencia. - Actualización y publicación de la información en la página web. - Mantenimiento preventivo y correctivo de equipos. - Atención a los usuarios en asignación y préstamo de equipos de cómputo.	- Actualización y publicación en la página web de los múltiples trabajos ejecutados en las diferentes oficinas. - Registrar y procesar información de los diferentes proyectos propuestos y ejecutados. - Atención en la asignación y préstamo de equipos de cómputo. - Control y respaldo de información.	- Evaluar e informar sobre aplicativos informáticos necesarios en diversas oficinas orgánicas. - Planificar, programar, ejecutar y supervisar el mantenimiento preventivo y correctivo de los recursos informáticos: físicos, lógicos y de comunicación. - Formular, implementar y supervisar la aplicación efectiva de los planes de contingencia.

ANEXO 02

ENCUESTA PARA DIAGNÓSTICAR LA SEGURIDAD DE LA INFORMACIÓN

Institución :

_____

Cargo :

_____

Nombre :

_____

Fecha : _____

Marque con una "X" en la casilla que crea conveniente:

SI = cumple con la pregunta señalada.

NO = no cumple con la pregunta señala.

PARCIAL = la actividad en la pregunta señalada está incompleta**.**

PREGUNTAS	SI	PARCIAL	NO
1. ¿La organización ha determinado los aspectos externos e internos que son relevantes para establecer el contexto organizacional?			
2. ¿La organización ha establecido un sistema de gestión de seguridad de la información? (SGSI)			
3. ¿La organización tiene los recursos adecuados (incluidos humanos, tecnológicos y financieros) para el establecimiento, implementación, mantenimiento y mejora continua del SGSI?			
4. ¿La organización ha demostrado su compromiso con la mejora de la seguridad de la información?			
5. ¿Se han identificado las partes interesadas y los requisitos más importantes para la seguridad de la información ambiental?			
6. ¿Se han establecido políticas de seguridad de la información en la unidad de gestión ambiental?			
7. ¿Se han establecido controles de seguridad de la información en la unidad de gestión ambiental?			
8. ¿Se han asignado responsabilidades en cuanto al manejo de la información ambiental?			
9. ¿La unidad de gestión ambiental ha establecido un plan de acción para hacer frente a los riesgos identificados?			
10. ¿La unidad de gestión ambiental dispone de un plan para alcanzar los objetivos de la seguridad de la información?			
11. ¿La organización ha tomado las medidas necesarias para determinar la competencia de las personas encargadas del manejo y rendimiento del SGSI?			

PREGUNTAS	SI	PARCIAL	NO
12.¿La unidad de gestión ambiental ha promovido la concientización de la seguridad del información; de manera que todos los que trabajan bajo el control de la organización son conscientes de los requisitos que les afectan?			
13. ¿La organización ha establecido, mantenido y controlado la información documentada como lo requiere la norma 27001?			
14. ¿La unidad de gestión ambiental trata y documenta su información como lo requiere la norma 27001 y 14001?			
15. ¿La organización ha establecido un plan que contenga la evaluación, tratamiento de riesgos y los resultados finales de la seguridad de la información de todas sus áreas?			
16. ¿La unidad de gestión ambiental entrega un informe final a la organización sobre los resultados del análisis de sus riesgos ?			
17. ¿La organización ha determinado que temas necesitan ser capacitados, monitoreados, analizados y evaluados con el fin de establecer el desempeño y eficacia del SGSI?			
18. ¿La organización ha establecido, implementado y mantenido un programa de auditoría interna de seguridad de información ambiental y ha documentado la evidencia de los resultados?			
19. ¿La gerencia ha llevado a cabo revisiones de cómo se realiza la seguridad de la información en la organización?			
20. ¿La unidad de gestión ambiental reacciona eficazmente ante cualquier no conformidad identificada dentro de su seguridad de la información y mantiene información documentada en su caso?			
21. ¿La unidad de gestión ambiental realiza mejoras continuas de su sistema de seguridad para mejorar el desempeño de la gestión ambiental?			

ANEXO 03

COMPARACIÓN DE ESTÁNDARES, MARCOS DE TRABAJO Y METODOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN.

<table>
<tr><th>ISO 27001</th><th>COBIT 5 para seguridad de la información</th><th>ISO 27005</th><th>MAGERIT</th></tr>
<tr><td>FASE I - Contexto de la organización
1.1 Entender la organización y su contexto.
1.2 Comprender las necesidades y expectativas de las partes interesadas.
1.3 Determinación del alcance del sistema de gestión de la seguridad de la información.

FASE II – Liderazgo
1.5 Liderazgo y compromiso.
1.6 Política de seguridad.
1.7 Roles, responsabilidades y autoridades organizacionales</td><td>1.1 Definir marcos de trabajo.
1.2 Establecer principios y políticas de la información adaptándolos al entorno de la empresa.
1.3 Determinar las funciones de seguridad de la información en la organización.
1.4 Establecer un modelo de cultura organizacional.
1.5 Asegurar el liderazgo y compromiso.</td><td>FASE I – Establecimiento del contexto
1.1 Definir el alcance y los límites.
1.2 Desarrollar criterios de evaluación de riesgo, criterios de impacto, criterios de la aceptación del riesgo.
1.3 Establecer y mantener las responsabilidades en la organización.</td><td>FASE I – Proyecto de análisis de riesgo
1.1 Estudio de oportunidad.
1.2 Determinación del alcance del proyecto.
1.3 Planificación del proyecto.
1.4 Lanzamiento del proyecto.</td></tr>
<tr><td>FASE III – Planificación
3.1 Acciones para tratar los riesgos y las oportunidades.
3.2 Objetivos de seguridad de la información y planificación para conseguirlos.</td><td>1.6 Realizar el análisis de riesgos manteniendo un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas)</td><td>FASE II – Valoración del riesgo
2.1 Análisis del riesgo
2.2 Estimación del riesgo
2.2 Evaluación del riesgo</td><td>FASE II - Método de análisis de riesgo
2.1 Caracterización de los activos.
2.2 Caracterización de las amenazas.
2.3 Caracterización de las salvaguardas.
2.4 Estimación del estado de riesgo.</td></tr>
</table>

ISO 27001	COBIT 5 para seguridad de la información	ISO 27005	MAGERIT
FASE IV – Soporte 4.1 Proporcionar recursos. 4.2 Asegurar la competencia del personal. 4.3 Concientización 4.4 Comunicación externa e interna. 4.5 Información documentada	1.7 Definir un modelo de servicios, infraestructura y aplicaciones. 1.8 Determinar y asegurar un modelo de personas, habilidades y competencias relacionados a la seguridad de la información.	----------	
FASE V - Operación 5.1 Planificación y control operacional. 5.2 Evaluación de riesgos de seguridad de la información. 5.3 Tratamiento de riesgos de seguridad de la información.	1.9 Formular y mantener un plan de tratamiento del riesgo de la seguridad de la información.	**FASE III - Tratamiento del riesgo** 3.1 Reducción del riesgo 3.2 Retención del riesgo 3.3 Evitación del riesgo 3.4 Transferencia del riesgo **FASE IV - Aceptación del riesgo**	**FASE 3 - Plan de seguridad** 3.1 Identificación de proyectos de seguridad. 3.2 Planificación de los proyectos de seguridad 3.3 Ejecución del plan
FASE VI - Evaluación del desempeño 6.1 Monitoreo, medición, análisis y evaluación. 6.2 Auditoría interna 6.3 Revisión por la gerencia.	1.10 Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. 1.11 Realizar auditorías internas al SGSI a intervalos planificados.	**FASE V - Monitoreo y revisión del riesgo** 5.1 Monitoreo y revisión de los factores de riesgo 5.2 Monitoreo, revisión y mejora de la gestión del riesgo.	
FASE VII – Mejoras 7.1 No conformidades y acción correctivas. 7.2 Mejora continua.	5.3 Corregir las no conformidades para prevenir recurrencias. 5.4 Promover una cultura de seguridad y de mejora continua.		

ANEXO 4

APLICACIÓN DEL MÉTODO PROPUESTO

A continuación, se muestra la aplicación del modelo propuesto a la unidad ambiental de una de las entidades seleccionadas de la región Lambayeque.

FASE I - Contexto de la organización

El Proyecto Especial Olmos Tinajones – PEOT es una unidad ejecutora del Gobierno Regional, está compuesta por la Gerencia de Desarrollo Tinajones y la Gerencia de Desarrollo Olmos, esta última a través de su unidad de gestión ambiental se encarga de supervisar la elaboración de expedientes técnicos; supervisar las obras que deberían ser ejecutadas en el marco del contrato para la construcción, operación y mantenimiento de las obras trasvase; realizar la evaluación y gestión de proyectos ambientales.

1.1 Identificación de contextos

- **Identificación del contexto externo**

Tabla 36. Identificación del contexto externo

<table>
<tr><th colspan="3">FASE I - CONTEXTO DE LA ORGANIZACION</th></tr>
<tr><td colspan="2">Nombre del documento
Identificación del contexto externo</td><td>Doc. N° 01</td></tr>
<tr><td colspan="2">Registrado por: Responsable ambiental de la UA
Aprobado por: Gerente de desarrollo olmos.</td><td>Fecha de registro
04/12/2017</td></tr>
<tr><td colspan="3">Objetivo
Identificar los aspectos externos que afectan el rendimiento de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se hizo uso de entrevistas, estudio de casos y análisis de documentos.</td></tr>
<tr><th>N°</th><th>Entorno</th><th>Aspectos identificados</th></tr>
<tr><td>01</td><td>Social y cultural</td><td>- Representantes de comunidades aledañas a cada obra.
- Empresas ejecutoras privadas.
- Gerencias del gobierno regional.
- Sectores poblacionales de bajos recursos.</td></tr>
<tr><td>02</td><td>Político</td><td>- Políticas ambientales.
- Directivos en el Gobierno Regional y sus demás gerencias.
- Cambios en el gobierno central.</td></tr>
<tr><td>03</td><td>Financiero</td><td>- Gobierno Regional de Lambayeque.
- Ministerio de economía y finanzas – MEF.</td></tr>
<tr><td>04</td><td>Reglamentario</td><td>- Emisión de ordenanzas regionales.</td></tr>
</table>

FASE I - CONTEXTO DE LA ORGANIZACION		
Nombre del documento Identificación del contexto externo	**Doc. N°**	01
Registrado por: Responsable ambiental de la UA **Aprobado por:** Gerente de desarrollo olmos.	**Fecha de registro** 04/12/2017	
Objetivo Identificar los aspectos externos que afectan el rendimiento de la unidad ambiental.		
Descripción Para la recolección de información se hizo uso de entrevistas, estudio de casos y análisis de documentos.		

N°	Entorno	Aspectos identificados
		- Cuestiones legales por el MEF que limitan el ámbito de los proyectos.

Conclusiones: Los cambios en las normativas legales, representantes políticos de gobiernos locales, regionales y/o nacionales son los aspectos más relevantes que influyen en el desarrollo de las funciones de las unidad ambiental.

➢ Identificación del contexto interno

Tabla 37. Plantilla para la identificación del contexto interno

FASE I - CONTEXTO DE LA ORGANIZACIÓN		
Nombre del documento Identificación del contexto interno	**Doc. N°**	02
Registrado por: Responsable ambiental de la UA **Aprobado por:** Gerente de desarrollo olmos.	**Fecha de registro** 04/12/2017	
Objetivo Identificar los aspectos internos que afectan el rendimiento de la unidad ambiental.		
Descripción Para la recolección de información se hizo uso del análisis de las fuentes de información de la entidad.		

N°	Entorno	Aspectos identificados
	Estructura de la organización, funciones y responsabilidades	**Gerencia de Desarrollo Olmos** Gerente de Desarrollo Olmos **Control y monitoreo del contrato** Abogado especialista en contratos de obras. Ingeniero de contratos. **Gestión ambiental y ordenamiento territorial** Responsable ambiental Especialista ambiental Especialista forestal Especialista sociólogo Asistente administrativo y de archivo Personal de apoyo (2)

Fig 1. Organigrama de la Gerencia de Desarrollo Olmos

FASE I - CONTEXTO DE LA ORGANIZACIÓN			
Nombre del documento Identificación del contexto interno		**Doc. N°**	02
Registrado por: Responsable ambiental de la UA **Aprobado por:** Gerente de desarrollo olmos.		**Fecha de registro** 04/12/2017	
Objetivo Identificar los aspectos internos que afectan el rendimiento de la unidad ambiental.			
Descripción Para la recolección de información se hizo uso del análisis de las fuentes de información de la entidad.			
N°	**Entorno**	**Aspectos identificados**	
		<u>Funciones y responsabilidades</u> - Gerente de desarrollo olmos: supervisar y monitorear el desempeño y desarrollo de las funciones de las oficinas de: control y monitoreo del contrato y gestión ambiental y ordenamiento territorial. - Abogado especialista en contratos de obras: se encarga de la normativa legal incluida en los contratos de obras. - Ingeniero de contratos: lideras procesos de licitación, evaluar y monitorear el desempeño de las contratas, proponer planes de acción para abordar temas de administración de contratos. - Responsable ambiental: encargado de la unidad ambiental, planifica, monitorea, dirige y desarrolla los programas de gestión Ambiental de la institución y su presupuesto. - Especialista ambiental: ejecuta los programas de gestión ambiental de acuerdo a lo planificado. - Especialista forestal: ejecuta los programas relacionados con los planes de desarrollo forestal incluidos en los programas de manejo ambiental de acuerdo a lo planificado. - Especialista sociólogo: desarrolla los programas sociales establecidos en los programas o planes de manejo ambiental del ámbito de intervención de la institución. - Asistente administrativo y de archivo: encargado del resguardo del archivo y del trámite documentario que se genera como resultado de la gestión de la unidad ambiental - Personal de apoyo: apoya en las actividades relacionadas con la búsqueda de información, fotocopiado y atención al usuario.	
02	Objetivos estratégicos	- Contribuir, apoyar y promover el desarrollo armónico e integral de las áreas seleccionadas en el ámbito de su jurisdicción, y otras que le encargue el Gobierno Regional Lambayeque. - Formular y Proponer al Presidente del Gobierno Regional de Lambayeque, para su aprobación, los lineamientos de política integral y las estrategias que instrumenten la implementación de los Proyecto Olmos, Tinajones y Proyectos del Plan de Desarrollo Hidráulico Regional.	

<table>
<tr><th colspan="3">FASE I - CONTEXTO DE LA ORGANIZACIÓN</th></tr>
<tr><td colspan="2">Nombre del documento
Identificación del contexto interno</td><td>Doc. N° 02</td></tr>
<tr><td colspan="2">Registrado por: Responsable ambiental de la UA
Aprobado por: Gerente de desarrollo olmos.</td><td>Fecha de registro
04/12/2017</td></tr>
<tr><td colspan="3">Objetivo
Identificar los aspectos internos que afectan el rendimiento de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se hizo uso del análisis de las fuentes de información de la entidad.</td></tr>
<tr><td>N°</td><td>Entorno</td><td>Aspectos identificados</td></tr>
<tr><td></td><td></td><td>- Elaborar un Sistema de Seguimiento y Evaluación que mida el grado de avance y logros de los Proyectos Olmos y Tinajones, de los Proyectos del Plan de Desarrollo Hidráulico Regional, del Planeamiento Estratégico del PEOT, del Plan Operativo e implementación de Políticas y Estrategias.
- Apoyar, promover y coordinar con las instituciones pertinentes, acciones, programas y proyectos orientados al afianzamiento y sostenibilidad del recurso hídrico en las cuencas aportantes y receptoras, a fin de propender al equilibrio entre oferta y demanda del recurso.</td></tr>
<tr><td>03</td><td>Recursos y conocimientos</td><td>Los recursos que dan soporte al rendimiento de la unidad ambiental son: el archivo documentario y la infraestructura tecnológica que está conformada por computadoras de escritorio, switch, impresoras, hub y computadoras portátiles.</td></tr>
<tr><td>04</td><td>Cultura de la organización</td><td>En el PEOT, la cultura organizacional se ve reflejado en lo siguiente:
<u>Misión</u>
Contribuir al desarrollo sostenible de su ámbito de influencia, mediante la explotación racional de sus recursos y potencialidades existentes, aprovechando en forma sustentable el uso multipropósito del recurso hídrico, con un enfoque de inclusión social y adaptación al cambio climático.
<u>Visión</u>
Ser la Organización Líder en la gestión y ejecución de Proyectos Hidráulicos e Hidroenergéticos, orientados a garantizar la sostenibilidad de la oferta hídrica en todos los valles de la región y/a impulsar el desarrollo y la inversión en el Norte del país.
<u>Valores:</u>
El ambiente de trabajo y reclutamiento de personal se rige bajo los siguientes valores: compromiso, colaboración, responsabilidad, servicio.</td></tr>
<tr><td colspan="3">Conclusiones: Se han identificado todos los aspectos internos que influyen en el desempeño de las funciones de la unidad ambiental. En el PEOT su unidad ambiental recibe el nombre de Gestión ambiental y ordenamiento territorial.</td></tr>
</table>

1.2 Necesidades y expectativas de las partes interesadas

Tabla 38. Identificación de las partes interesadas

FASE I - CONTEXTO DE LA ORGANIZACIÓN											
Nombre del documento Identificación de las partes interesadas							**Doc. N°**	03			
Registrado por: Responsable ambiental. **Aprobado por:** Gerente de desarrollo olmos.							**Fecha de registro** 04/12/2017				
Objetivo Identificar las necesidades de las partes interesadas relacionadas con la UA.											
Descripción Para la recolección de información se usaron técnicas e instrumentos como entrevistas y cuestionarios.											
Parte interesada	**Necesidades / tipos de información**										
	Sistema de gestión de seguridad de la información	Mejoras en seguridad de la información	Políticas de seguridad de la información	Plan de acción para riesgos	Plan de seguridad de la información	Información documentada según las normas	Informe del análisis de riesgos	Programas de capacitación	Programa de auditoría interna	Revisiones del desempeño de la seguridad de la información	Plan de mejora continua
INTERNA											
Gerente de desarrollo olmos	A		A					A	A	A	A
Responsable ambiental		O		O	U	U	O	A			
Especialista ambiental						O					
Asistente administrativo y de archivo						U	O			O	
Personal de apoyo							O	I		O	
Responsable de TI			O	O	O		A			U	O
EXTERNA											
Gobierno regional	A					I					
Empresas ejecutoras privadas						I					
Usuarios solicitantes de información.						U					
Conclusiones: Se ha utilizado un indicador de relación entre la parte interesada y la necesidad/tipo de información.											

1.3 Alcance del sistema de gestión de seguridad de la información

Tabla 39. Plantilla para el alcance del SGSI

<table>
<tr><th colspan="3">FASE I - CONTEXTO DE LA ORGANIZACIÓN</th></tr>
<tr><td colspan="2">Nombre del documento
Alcance del SGSI</td><td>Doc. N°
04</td></tr>
<tr><td colspan="2">Registrado por: Responsable ambiental, responsable de centro de cómputo.
Aprobado por: Gerente de desarrollo olmos.</td><td>Fecha de registro
11/12/2017</td></tr>
<tr><td colspan="3">Objetivo
Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.</td></tr>
<tr><td colspan="3">Descripción
En esta actividad se consideraron los aspectos externos e internos, las partes interesadas relevantes al SGSI y los procesos o funciones incluidos dentro de los límites del SGSI.</td></tr>
<tr><td>Proceso/funciones</td><td colspan="2">- Funciones de la unidad de gestión ambiental:
- Planificar, monitorear, dirigir y desarrollar los programas de Gestión Ambiental de la institución y su presupuesto.
- Ejecutar los programas de Gestión Ambiental.
- Trámite documentario para acceder a la información ambiental.
- Registro y archivamiento de la documentación ambiental.
- Entrega de la información ambiental solicitada por el ciudadano y/o alguna entidad interesada.</td></tr>
<tr><td>Responsables</td><td colspan="2">- Gerente de desarrollo olmos
- Responsable ambiental
- Especialista ambiental
- Asistente administrativo y de archivo.
- Personal de apoyo
- Responsable de TI</td></tr>
<tr><td>Infraestructura de TI</td><td colspan="2">- 04 Computadoras de escritorio.
- 01 switch.
- 01 impresora.
- 02 computadoras portátiles.
- 01 fotocopiadora.
- 01 scanner
- 01 UPS</td></tr>
<tr><td colspan="3">Conclusiones: El modelo de seguridad de la información cubre las todas las funciones de la unidad ambiental, incluyendo a los responsables de cada función que vienen a ser los miembros de la gerencia de Desarrollo Olmos – Chiclayo.</td></tr>
</table>

FASE II – Liderazgo

2.1 Asegurar el liderazgo y compromiso

Tabla 40. Plantilla para determinar el liderazgo

FASE II - LIDERAZGO				
Nombre del documento Cumplimiento del liderazgo		**Doc. N°**		05
Registrado por: Responsable ambiental. **Aprobado por:** Gerente de desarrollo olmos.		**Fecha de registro** 11/12/2017		
Objetivo Identificar: Si = la gerencia cumple con las funciones de liderazgo, No= la gerencia no cumple con las funciones de liderazgo, Parcial= la función está incompleta.				
Descripción Para la recolección de información solo se aplicó a la gerencia la presente plantilla con las funciones a continuación mencionadas.				
N°	**Funciones**	**Si**	**No**	**Parcial**
01	Asegura que la política y los objetivos de seguridad de la información sean establecidos y compatibles con la dirección estratégica de la organización.		X	
02	Asegurar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización.	X		
03	Asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.	X		
04	Comunicar la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.	X		
05	Asegurar que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).		X	
06	Dirigir y apoyar a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información		X	
07	Promover la mejora continua.			X
08	Apoyar otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.	X		
Conclusiones: La gerencia no cumple con todas las funciones solicitadas por la ISO 27001:2014. Para cumplir completamente con la fase de liderazgo, se debe culminar con las funciones referidas en los puntos 01, 05, 06 y 07.				

2.2 Establecer políticas y objetivos de seguridad de la información

Tabla 41. Plantilla para políticas de seguridad de la información

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
01	Políticas de la seguridad de la información	Lista de controles para la gestión de seguridad de la información en la unidad ambiental.	Las políticas deben ser implementadas en toda la organización y comunicada a todo el personal del Proyecto Especial Olmos – Tinajones.	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	1. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes. 2. Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.
02	Política de seguridad de los recursos humanos	Debe orientarse al cumplimiento de los	La política debe ser implementada en la	Asegurar que el personal comprenda	3. El área de RR. HH debe reclutar personal que esté con el perfil establecido para cumplir

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
		roles y responsabilidades del personal que interviene en la unidad ambiental.	unidad ambiental y comunicada a todo el personal del Proyecto Especial Olmos – Tinajones.	sus responsabilidades y son capaces en los roles para los que se consideran.	todas las funciones de la unidad ambiental. 4. Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro la unidad ambiental. 5. El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental. 6. Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
03	Política de gestión de activos	Identificar y proteger los activos destinados a las funciones de la unidad ambiental.	La política debe ser implementada en la unidad ambiental y comunicada a todo el personal del Proyecto Especial Olmos –	Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas asegurando que la información recibe un nivel apropiado de protección.	7. Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. 8. Implementar mecanismos de mantenimiento para conservar la integridad de la información física. 9. Escanear todas las solicitudes y expedientes que ingresan a la unidad ambiental.
04	Política de control de accesos	Se refiere a la autorización que se otorga a todo el personal del PEOT,	Las políticas deben ser implementadas en toda la organización y comunicada a todo el personal del	Limitar el acceso a la información y a las instalaciones de procesamiento de	10. Establecer segregación de funciones para separar el personal del servicio de

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
		para acceder a las instalaciones o sistemas que contienen información.	Proyecto Especial Olmos – Tinajones.	información ambiental.	información y personal con funciones administrativas. 11. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
05	Política de seguridad física y ambiental	Se deben analizar y evaluar las ubicaciones físicas del PEOT, establecer controles ambientales que proporcionen capacidad a las operaciones de soporte, que pueden ser: las normas de	La política debe ser implementada en toda la organización y comunicada a todo el personal del Proyecto especial Olmos – Tinajones.	1. Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	12. Definir y usar perímetros de seguridad para proteger áreas que contengan información confidencial e instalaciones de manejo de información. 13. La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
		control medioambiental y las normas de control de acceso físico (para empleados o visitantes)			14. Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones. 15. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. 16. Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.
				2. Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las	17. La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
				operaciones de la organización.	18. Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. 19. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
06	Política de respaldo y restauración de información	Mantener la disponibilidad de la información, asegurando que la información de la unidad de gestión ambiental, los datos de los usuarios y del	La política debe ser implementada en la unidad de gestión ambiental, debe ser comunicada a la gerencia de desarrollo olmos y al personal que interviene en	Proteger contra la perdida de datos.	20. Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que, ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
		personal se mantenga protegida contra la pérdida, alteración o divulgación de manera accidental o malintencionada, ya sea por fallas de los equipos y/o redes.	el tratado de la información.		21. La oficina del centro de cómputo junto con el especialista ambiental debe realizar respaldos de la información periódicamente.
07	Política de seguridad de las comunicaciones	Proteger la información que sale de la unidad de gestión ambiental, por cualquier medio de transferencia.	La política debe ser implementada en la unidad de gestión ambiental, debe ser comunicada a la gerencia de desarrollo olmos y al personal que interviene en el tratado de la información.	Mantener la seguridad de la información transferida dentro de la unidad de gestión ambiental y con cualquier entidad externa.	22. Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
08	Política de gestión de incidentes de seguridad de la información	Mantener el nivel del funcionamiento del servicio de la unidad de gestión ambiental, minimizando en lo posible el impacto negativo, de forma que la calidad del servicio y la disponibilidad de información se mantengan.	La política debe ser implementada en la unidad de gestión ambiental, debe ser comunicada a la gerencia de desarrollo olmos y al personal que interviene en el tratado de la información.	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	23. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
09	Política de cumplimiento	Cumplir con la resolución ministerial N°004-2016-PCM referente a la seguridad de la información.	La política debe ser implementada en toda la organización y comunicada a todo el personal del Proyecto Especial Olmos – Tinajones.	1. Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales	24. Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.

FASE II - LIDERAZGO					
Nombre del documento Establecimiento de políticas de seguridad de la información.				**Doc. N°**	06
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Gerente de desarrollo olmos y el responsable ambiental.				**Fecha de registro** 11/12/2017	
Objetivo Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.					
Descripción Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.					
N°	**Políticas de seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles de seguridad**
				relacionadas con seguridad de la información y de cualquier requisito de seguridad.	
				2. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.	25. Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas. 26. Revisar periódicamente la base de datos del personal para su actualización correspondiente.
10	Política de privacidad	Cumplir con lo estipulado por la ley	La política debe ser implementada en la	Proteger la información	27. Implementar controles de acceso para evitar la

<table>
<tr><th colspan="6">FASE II - LIDERAZGO</th></tr>
<tr><td colspan="4">Nombre del documento
Establecimiento de políticas de seguridad de la información.</td><td>Doc.
N°</td><td>06</td></tr>
<tr><td colspan="4">Registrado por: Responsable de centro de cómputo.
Aprobado por: Gerente de desarrollo olmos y el responsable ambiental.</td><td colspan="2">Fecha de registro
11/12/2017</td></tr>
<tr><td colspan="6">Objetivo
Identificar las políticas de seguridad de acuerdo a las necesidades de la unidad ambiental.</td></tr>
<tr><td colspan="6">Descripción
Para la recolección de información se hizo uso de análisis de documentos relacionados con seguridad de la información.</td></tr>
<tr><th>N°</th><th>Políticas de seguridad</th><th>Definición</th><th>Alcance</th><th>Objetivo</th><th>Controles de seguridad</th></tr>
<tr><td></td><td></td><td>Nº 27806, ley de transparencia y acceso a la información pública.</td><td>unidad de gestión ambiental y comunicada a todo el personal del Proyecto Especial Olmos – Tinajones.</td><td>ambiental y personal de los empleados, usuarios y entidades externas del uso indebido y divulgación no autorizada.</td><td>incorporación ajena a la unidad de gestión ambiental.</td></tr>
<tr><td colspan="6">Conclusiones: Se estableció para la unidad ambiental un total de diez (10) políticas de seguridad, doce (12) objetivos y cuarenta controles de seguridad de la información (40).</td></tr>
</table>

2.3 Definir roles y responsabilidades

Tabla 42. Plantilla para identificar roles y responsabilidades

<table>
<tr><th colspan="3">FASE II - LIDERAZGO</th></tr>
<tr><td colspan="2">Nombre del documento
Roles y responsabilidades</td><td>Doc. Nº 07</td></tr>
<tr><td colspan="2">Registrado por: Responsable ambiental.
Aprobado por: Gerente de desarrollo olmos.</td><td>Fecha de registro
11/12/2017</td></tr>
<tr><td colspan="3">Objetivo
Identificar los roles y responsabilidades del personal que intervendrá en seguridad de la información de la unidad ambiental.</td></tr>
<tr><td colspan="3">Descripción
Para la recolección de información se hizo uso del análisis documentario de la unidad ambiental.</td></tr>
<tr><td>Rol</td><td>Responsabilidad</td><td>Nivel de implicancia</td></tr>
<tr><td>Gerente de desarrollo olmos</td><td>Supervisar y monitorear el desarrollo e implementación del sgsi.</td><td>I</td></tr>
<tr><td>Responsable ambiental.</td><td>Identificar y comunicar amenazas para la seguridad de la información, comportamientos deseables y cambios necesarios para tratar estos puntos.</td><td>C</td></tr>
<tr><td>Asistente administrativo y de archivo.</td><td>Supervisar el registro de la información entrante y la entrega de información solicitada.</td><td>R</td></tr>
<tr><td>Director de seguridad de la información</td><td>Recoger toda la información concerniente a la seguridad de la información de la organización.</td><td>R</td></tr>
<tr><td>Comité de Gestión de Riesgos.</td><td>Evaluar, optimizar, financiar y monitorizar el riesgo de todos los orígenes con el propósito de incrementar el valor de la empresa a corto y largo plazo para las partes interesadas</td><td>A</td></tr>
<tr><td>Comité de seguridad de la información.</td><td>Responsabilidad general para la gestión de esfuerzos en seguridad de la información</td><td>A</td></tr>
<tr><td colspan="3">Conclusiones: según lo examinado por Cobit 5 para seguridad de la información, se cree conveniente la creación de tres (03) roles: director de seguridad de la información, comité de gestión de riesgos y un comité de seguridad de la información.</td></tr>
</table>

FASE III - Planificación

3.1 Identificación del riesgo

Identificación de activos

Tabla 43. Plantilla para la identificación de activos

IDENTIFICACIÓN DE ACTIVOS					
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.				**Doc. Nº**	08
Objetivo: Identificar los activos presentes en la unidad ambiental.				**Fecha de registro** 14/12/2018	
Descripción: Para la recolección de información se hizo uso de la observación directa.					
Nº	**Tipo de activo**	**Activo**	**Código**	**Descripción**	**Responsable**
1	Hardware	Computadora de escritorio	[HW_pc]	Equipo de cómputo utilizado por el personal de la unidad ambiental.	Unidad ambiental
2	Hardware	Impresora	[HW_impr]	Equipo de cómputo utilizado por la gerencia de desarrollo Olmos y la unidad ambiental.	Unidad ambiental
3	Hardware	Fotocopiadora	[HW_fcp]	Equipo de cómputo usado por la gerencia de desarrollo Olmos y la unidad ambiental.	Unidad ambiental
4	Hardware	Escáner	[HW_scan]	Equipo de cómputo usado por la gerencia de desarrollo Olmos y la unidad ambiental.	Unidad ambiental
5	Hardware	Plotter	[HW_plot]	Equipo de cómputo utilizado por el personal de la unidad ambiental.	Unidad ambiental
6	Soportes de información	Disco duro externo	[Media_disk_ex]	Dispositivo físico para almacenar información en la gerencia de desarrollo Olmos y la unidad ambiental.	Unidad ambiental

IDENTIFICACIÓN DE ACTIVOS					
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.				**Doc. N°**	08
Objetivo: Identificar los activos presentes en la unidad ambiental.				**Fecha de registro** 14/12/2018	
Descripción: Para la recolección de información se hizo uso de la observación directa.					
N°	**Tipo de activo**	**Activo**	**Código**	**Descripción**	**Responsable**
7	Soportes de información	CD	[MEDIA_cd]	Dispositivo físico para almacenar información en la unidad ambiental o entregarla según la solicitud de los usuarios.	Unidad ambiental
8	Soportes de información	DVD	[MEDIA_dvd]	Dispositivo físico para almacenar información en la unidad ambiental o entregarla según la solicitud de los usuarios.	Unidad ambiental
9	Soportes de información	Memoria USB	[MEDIA_usb]	Dispositivo físico para almacenar información en la gerencia de desarrollo olmos o la unidad ambiental.	Unidad ambiental
10	Soportes de información	Expedientes impresos	[MEDIA_exp]	Información ambiental almacenada en la unidad de gestión ambiental, entregada según la solicitud de los usuarios internos y externos de la organización.	Unidad ambiental
11	Software	Ofimática	[SW_office]	Licencias para utilizar un software adquirido a terceros.	Centro de cómputo
12	Software	Cliente de correo electrónico	SW_email	Software para acceso a correo eléctrico.	Unidad ambiental
13	Software	Anti virus	[SW_av]	Antivirus instalado en la unidad ambiental.	Unidad ambiental
14	Datos	Fichero	[D_files]	Información digital almacenada en las pc's de la unidad ambiental.	Unidad ambiental
15	Datos	Copias de respaldo	[D_backup]	Información generada en las pc's de la unidad ambiental.	Unidad ambiental

IDENTIFICACIÓN DE ACTIVOS						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.					**Doc. N°**	08
Objetivo: Identificar los activos presentes en la unidad ambiental.					**Fecha de registro** 14/12/2018	
Descripción: Para la recolección de información se hizo uso de la observación directa.						
N°	**Tipo de activo**	**Activo**	**Código**	**Descripción**	**Responsable**	
16	Datos	Credenciales (contraseñas)	[D_password]	Contraseñas para que el personal de la unidad ambiental acceda a la información digital almacenada.	Unidad ambiental y gerencia de desarrollo olmos	
17	Datos	Datos de validación de credenciales	[D_contr_acc]	Datos personales para crear las identificaciones del personal.	Unidad ambiental	
18	Datos	Registro de actividad	[D_reg_act]	Programación de actividades establecidas por la gerencia de desarrollo olmos y la unidad ambiental.	Unidad ambiental	
19	Servicios	Servicios externos	[S_us_ext]	Servicio de entrega de información ambiental otorgado a los usuarios y/o entidades.	Unidad ambiental	
20	Servicios	Correo electrónico	[S_CE]	Cuentas de correo para el personal.	Unidad ambiental	
21	Instalaciones	Ambientes físicos	[L]	Oficinas destinadas para la unidad ambiental.	Gerencia de desarrollo Olmos	
22	Personal	Usuarios internos	[P_ui]	Personal que labora en la unidad ambiental.	Unidad ambiental	
Conclusiones: Se han identificado veintidós (22) activos relacionados con las funciones de la unidad ambiental.						

Valoración de activos

Tabla 44. Plantilla para la valoración de activos

VALORACIÓN DE ACTIVOS						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.					**Doc. N°**	09
Objetivo Identificar el nivel de criticidad de cada activo.					**Fecha de registro** 14/12/2018	
Descripción Para el desarrollo de esta actividad se extraen los activos de la plantilla de identificación de activos.						
N°	**Activo**	**Criterio**			**Total**	**Nivel**
		(D)	**(I)**	**(C)**		
1	Computadora de escritorio	4	2	3	9	Alto
2	Impresora	2	1	1	4	Bajo
3	Fotocopiadora	1	1	1	3	Muy bajo
4	Escáner	1	1	1	3	Muy bajo
5	Plotter	1	1	1	3	Muy bajo
6	Disco duro externo	3	2	4	9	Alto
7	CD	3	2	4	9	Alto
8	DVD	3	2	4	9	Alto
9	Memoria USB	3	2	4	9	Alto
10	Expedientes impresos	4	4	4	12	Muy alto
11	Ofimática	2	1	3	6	Bajo
12	Cliente de correo electrónico	2	2	4	8	Alto
13	Anti virus	2	2	1	5	Bajo
14	Fichero	4	2	3	9	Alto
15	Copias de respaldo	1	2	4	7	Alto
16	Credenciales (contraseñas)	3	2	4	9	Alto
17	Datos de validación de credenciales.	1	1	1	3	Muy bajo
18	Registro de actividad	2	2	3	7	Alto
19	Servicios externos	4	3	3	10	Muy alto
20	Correo electrónico	2	2	4	8	Alto
21	Ambientes físicos	3	2	4	9	Alto
22	Usuarios internos	3	3	3	9	Alto

<table>
<tr><th colspan="6">VALORACIÓN DE ACTIVOS</th></tr>
<tr><td colspan="4">Registrado por: Responsable ambiental.
Aprobado por: Responsable de centro de cómputo.</td><td>Doc. N°</td><td>09</td></tr>
<tr><td colspan="4">Objetivo
Identificar el nivel de criticidad de cada activo.</td><td colspan="2">Fecha de registro
14/12/2018</td></tr>
<tr><td colspan="6">Descripción
Para el desarrollo de esta actividad se extraen los activos de la plantilla de identificación de activos.</td></tr>
<tr><td rowspan="2">N°</td><td rowspan="2">Activo</td><td colspan="3">Criterio</td><td rowspan="2">Total</td><td rowspan="2">Nivel</td></tr>
<tr><td>(D)</td><td>(I)</td><td>(C)</td></tr>
<tr><td colspan="6">Conclusiones: Se identificaron trece (13) activos con nivel de criticidad alto y seis (06) activos de criticidad muy alta.</td></tr>
</table>

Identificación de amenazas y vulnerabilidades

Tabla 45. Plantilla de identificación de amenazas y vulnerabilidades

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES			
Registrado por: Responsable de la unidad ambiental. **Aprobado por:** Responsable de centro de cómputo.		**Doc. N°**	10
Objetivo Identificar las amenazas y vulnerabilidades de cada activo identificado.		**Fecha de registro** 14/12/2017	
Descripción Para el desarrollo de esta actividad, se ubica el activo identificado en la lista de amenazas y vulnerabilidades.			
N°	**Activo**	**Amenaza**	**Vulnerabilidad**
1	Computadora de escritorio	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.
		Reducción en el funcionamiento óptimo de los equipos.	Procedimientos inadecuados de mantenimiento.
2	Impresora	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.
3	Fotocopiadora	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.
		Destrucción del equipo o los medios, polvo.	Falta de esquemas de reemplazo y mantenimiento periódico.
4	Escáner	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.
5	Plotter	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES			
Registrado por: Responsable de la unidad ambiental. **Aprobado por:** Responsable de centro de cómputo.		**Doc. N°**	10
Objetivo Identificar las amenazas y vulnerabilidades de cada activo identificado.		**Fecha de registro** 14/12/2017	
Descripción Para el desarrollo de esta actividad, se ubica el activo identificado en la lista de amenazas y vulnerabilidades.			

N°	Activo	Amenaza	Vulnerabilidad
		Error en el uso de equipos.	Falta de capacitación al personal.
6	Disco duro externo	Hurto de medios o documentos.	Almacenamiento sin protección.
7	CD	Hurto de medios o documentos.	Almacenamiento sin protección.
8	DVD	Hurto de medios o documentos.	Almacenamiento sin protección.
9	Memoria USB	Hurto de medios o documentos.	Almacenamiento sin protección.
10	Expedientes impresos	Hurto de medios o documentos.	Falta de control de acceso al personal.
			Almacenamiento sin protección.
		Incumplimiento en el mantenimiento de la información.	Desgaste por manipulación.
11	Ofimática	Indisponibilidad en el uso de comandos.	Error en la activación del producto.
12	Cliente de correo electrónico	Error en el uso del software de correo electrónico.	Configuración incorrecta de parámetros.
			Interfaz de usuario complicada.
13	Anti virus	Uso limitado del antivirus.	Error en la activación del producto.
14	Fichero	Modificación y/o eliminación no autorizada.	Falta de control de acceso al personal.
15	Copias de respaldo	Hurto de medios o documentos.	Copia no controlada.
			Falta de control de acceso al personal.
16	Credenciales (contraseñas)	Falsificación de derechos.	Gestión deficiente de las contraseñas.
			Falta de control de acceso al personal.
17	Datos de validación de credenciales.	Incongruencia en la integridad de los datos personales.	Datos registrados incorrectamente.

<table>
<tr><th colspan="4">IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES</th></tr>
<tr><td colspan="2">Registrado por: Responsable de la unidad ambiental.
Aprobado por: Responsable de centro de cómputo.</td><td>Doc. Nº</td><td>10</td></tr>
<tr><td colspan="2">Objetivo
Identificar las amenazas y vulnerabilidades de cada activo identificado.</td><td colspan="2">Fecha de registro
14/12/2017</td></tr>
<tr><td colspan="4">Descripción
Para el desarrollo de esta actividad, se ubica el activo identificado en la lista de amenazas y vulnerabilidades.</td></tr>
<tr><th>Nº</th><th>Activo</th><th>Amenaza</th><th>Vulnerabilidad</th></tr>
<tr><td>18</td><td>Registro de actividad</td><td>Procesamiento ilegal de datos.</td><td>Falta de mecanismos de monitoreo al personal.</td></tr>
<tr><td rowspan="3">19</td><td rowspan="3">Servicios externos</td><td rowspan="3">Indisponibilidad y daño de información o de equipos.</td><td>Falta de control de acceso al personal.</td></tr>
<tr><td>No existen copias de respaldo.</td></tr>
<tr><td>Falta de capacitación al personal.</td></tr>
<tr><td rowspan="2">20</td><td rowspan="2">Correo electrónico</td><td>Falsificación de derechos.</td><td>Falta de mecanismos de identificación y autenticación, como la autenticación de usuario.</td></tr>
<tr><td>Error en el uso del correo.</td><td>Falta de políticas sobre el uso del correo electrónico.</td></tr>
<tr><td rowspan="3">21</td><td rowspan="3">Ambientes físicos</td><td>Inundación.</td><td>Ubicación en un área susceptible de inundación.</td></tr>
<tr><td>Pérdida del suministro de energía.</td><td>Red energética inestable.</td></tr>
<tr><td>Hurto de equipo</td><td>Falta de protección física de las puertas y ventanas de la edificación.</td></tr>
<tr><td rowspan="5">22</td><td rowspan="5">Usuarios internos</td><td rowspan="2">Incumplimiento en la disponibilidad del personal.</td><td>Falta de presupuesto.</td></tr>
<tr><td>Ausencia del personal en el área designada.</td></tr>
<tr><td>Negación de acciones</td><td>Falta de asignación adecuada de responsabilidades en la seguridad de la información.</td></tr>
<tr><td rowspan="2">Error en el uso de equipos e información.</td><td>Uso incorrecto de software y hardware.</td></tr>
<tr><td>Entrenamiento insuficiente en seguridad de la información.</td></tr>
<tr><td colspan="4">Conclusiones: Se obtuvieron treinta y un (31) amenazas con sus vulnerabilidades relacionadas a cada activo identificado.</td></tr>
</table>

3.2 Análisis del riesgo

Valoración de la probabilidad e impacto del riesgo

Tabla 46. Valoración de probabilidad de ocurrencia

Valor	Probabilidad	Descripción
1	Raro	El evento no se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir una vez cada 5 años.
3	Posible	El evento puede ocurrir al menos una vez cada 2 años.
4	Probable	El evento puede ocurrir una vez al año.
5	Casi seguro	El evento puede ocurrir más de una vez al año.

Tabla 47. Valoración del impacto

Valor	Intensidad	Descripción
1	Insignificante	No altera la ejecución ni el rendimiento de las funciones de la unidad ambiental.
2	Menor	Afecta la ejecución de las funciones de la unidad ambiental.
3	Moderado	Se continua con la ejecución de las funciones, pero afecta el rendimiento de las mismas.
4	Mayor	Se suspenden temporalmente las funciones a reforzar.
5	Catastrófico	Se cierra la unidad ambiental hasta su reestructuración.

Valoración de la magnitud del riesgo

Tabla 48. Magnitud del impacto

VALOR	MAGNITUD
1 – 5	Baja
6 – 10	Media
11 – 15	Alta
16 – 25	Critica

Tabla 49. Plantilla para el análisis del riesgo

ANÁLISIS DEL RIESGO								
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.							**Doc. N°**	11
Objetivo Determinar el análisis del riesgo.							**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se usaron los resultado de la plantilla de identificación de amenazas y vulnerabilidades, y se calificó cada amenaza según su probabilidad, impacto y magnitud.								
N°	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**Valor (PXI)**	**Código de riesgo**	**Magnitud**
1	Computadora de escritorio	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	4	3	12	R1	Alta
		Mal funcionamiento de los equipos.	Procedimientos inadecuados de mantenimiento.	4	2	8	R2	Media
2	Impresora	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.	4	2	8	R3	Media
3	Fotocopiadora	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	4	3	12	R4	Alta
		Destrucción del equipo o los medios, polvo.	Falta de esquemas de reemplazo y mantenimiento periódico.	3	3	9	R5	Media
4	Escáner	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.	4	2	8	R6	Media
5	Plotter	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	4	3	12	R7	Alta

ANÁLISIS DEL RIESGO

Registrado por: Responsable ambiental.
Aprobado por: Responsable de centro de cómputo.

Doc. N° 11

Objetivo
Determinar el análisis del riesgo.

Fecha de registro
15/12/2017

Descripción
Para el desarrollo de esta actividad se usaron los resultado de la plantilla de identificación de amenazas y vulnerabilidades, y se calificó cada amenaza según su probabilidad, impacto y magnitud.

N°	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PXI)	Código de riesgo	Magnitud
		Error en el uso de equipos.	Falta de capacitación al personal.	4	3	12	R8	Alta
6	Disco duro externo	Hurto de medios o documentos.	Almacenamiento sin protección.	2	5	10	R9	Media
7	CD	Hurto de medios o documentos.	Almacenamiento sin protección.	4	4	16	R10	Crítica
8	DVD	Hurto de medios o documentos.	Almacenamiento sin protección.	4	4	16	R11	Crítica
9	Memoria USB	Hurto de medios o documentos.	Almacenamiento sin protección.	5	3	15	R12	Alta
10	Expedientes y solicitudes impresas.	Hurto de medios o documentos.	Falta de control de acceso al personal.	4	4	16	R13	Crítica
		Incumplimiento en el mantenimiento de la información.	Desgaste por manipulación.	3	4	12	R14	Alta
11	Ofimática	Indisponibilidad en el uso del software.	Error en la activación del producto.	4	1	4	R15	Baja
12	Cliente de correo electrónico	Error en el uso del software de correo electrónico.	Configuración incorrecta de parámetros.	3	2	6	R16	Media

ANÁLISIS DEL RIESGO

Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.	**Doc. N°** 11
Objetivo Determinar el análisis del riesgo.	**Fecha de registro** 15/12/2017

Descripción
Para el desarrollo de esta actividad se usaron los resultado de la plantilla de identificación de amenazas y vulnerabilidades, y se calificó cada amenaza según su probabilidad, impacto y magnitud.

N°	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PXI)	Código de riesgo	Magnitud
			Interfaz de usuario complicada.					
13	Anti virus	Abuso de derechos.	Error en la activación del producto.	4	3	12	R17	Alta
14	Fichero	Modificación y/o eliminación no autorizada.	Falta de control de acceso al personal.	4	3	12	R18	Alta
15	Copias de respaldo	Hurto de medios o documentos.	Copia no controlada. Falta de control de acceso al personal.	2	4	8	R19	Media
16	Credenciales (contraseñas)	Falsificación de derechos.	Gestión deficiente de las contraseñas. Falta de control de acceso al personal.	3	3	9	R20	Media
17	Datos de validación de credenciales.	Incongruencia en la integridad de los datos personales.	Datos registrados incorrectamente.	3	3	9	R21	Media
18	Registro de actividad	Procesamiento ilegal de datos.	Falta de mecanismos de monitoreo al personal.	4	3	12	R22	Alta

ANÁLISIS DEL RIESGO

Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.	**Doc. N°** 11
Objetivo Determinar el análisis del riesgo.	**Fecha de registro** 15/12/2017

Descripción
Para el desarrollo de esta actividad se usaron los resultado de la plantilla de identificación de amenazas y vulnerabilidades, y se calificó cada amenaza según su probabilidad, impacto y magnitud.

N°	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PXI)	Código de riesgo	Magnitud
19	Servicios externos	Indisponibilidad y daño de información o de equipos.	Falta de control de acceso al personal.	4	4	16	R23	Crítica
			No existen copias de respaldo.					
			Falta de capacitación al personal.					
20	Correo electrónico	Falsificación de derechos.	Falta de autenticación de usuario.	3	2	6	R24	Media
		Error en el uso del correo.	Falta de políticas sobre el uso del correo electrónico.	3	3	9	R25	Media
21	Ambientes físicos	Inundación.	Ubicación en un área susceptible de inundación.	3	5	15	R26	Alta
		Pérdida del suministro de energía.	Red energética inestable.	4	3	12	R27	Alta
		Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación.	2	5	10	R28	Media
	Usuarios internos		Falta de presupuesto.	4	3	12	R29	Alta

ANÁLISIS DEL RIESGO

Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo.	**Doc. N°** 11
Objetivo Determinar el análisis del riesgo.	**Fecha de registro** 15/12/2017

Descripción
Para el desarrollo de esta actividad se usaron los resultado de la plantilla de identificación de amenazas y vulnerabilidades, y se calificó cada amenaza según su probabilidad, impacto y magnitud.

N°	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PXI)	Código de riesgo	Magnitud
22		Incumplimiento en la disponibilidad del personal.	Ausencia del personal en el área designada.					
		Negación de acciones	Falta de asignación adecuada de responsabilidades en la seguridad de la información.	4	4	16	R30	Crítica
		Error en el uso de equipos e información.	Uso incorrecto de software y hardware.	4	4	16	R31	Crítica
			Entrenamiento insuficiente en seguridad de la información.					

Conclusiones: De los 31 riesgos identificados, se observa que existen seis (06) riesgos de magnitud critica relacionados a la perdida de dispositivos de almacenamiento. Del mismo modo, se observan doce (12) riesgos de magnitud alta relacionados a la pérdida del suministro de energía y a la falta de control de acceso del personal.

3.3 Evaluación del riesgo

Priorización de los riesgos ubicados en el mapa de calor.

Probabilidad						
	5 Casi seguro			R12,		
	4 Probable	R15	R2, R3, R6	R1, R4, R7, R8, R17, R18 R22, R27, R29	R10, R11, R13, R23, R30, R31	
	3 Posible		R16, R24,	R5, R20, R21, R25	R14	R26
	2 Improbable			R9	R19	R28
	1 Raro					
		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
		Impacto				

Figura 05. Mapa de calor

Del mapa de calor se observa que existen un (01) riesgo de magnitud baja, trece (12) riegos de magnitud media, doce (12) de magnitud alta y seis (06) riesgos de magnitud critica.

Tabla 50. Identificación de tolerancia al riesgo.

Valor del riesgo	Tolerancia al riesgo	Descripción
1 – 6	Aceptable	El riesgo es aceptable tal y como existe.
7 – 13	Tolerable	El riesgo es tratado basado en la mitigación.
14 – 25	No tolerable	El riesgo es inaceptable por pérdidas aprox. de $. 200.000.00

Tabla 51. Plantilla para la evaluación del riesgo

EVALUACIÓN DEL RIESGO						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo					**Doc. N°**	12
Objetivo Determinar la evaluación del riesgo.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**
R1	Alta	Computadora de escritorio	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	12	No tolerable
R2	Media		Reducción en el funcionamiento óptimo de los equipos.	Procedimientos inadecuados de mantenimiento.	8	Tolerable
R3	Media	Impresora	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.	8	Tolerable
R4	Alta	Fotocopiadora	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	12	No tolerable
R5	Media		Destrucción del equipo o los medios, polvo.	Falta de esquemas de reemplazo y mantenimiento periódico.	9	Tolerable
R6	Media	Escáner	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad.	8	Tolerable
R7	Alta	Plotter	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.	12	No tolerable

EVALUACIÓN DEL RIESGO						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo					**Doc. N°**	12
Objetivo Determinar la evaluación del riesgo.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**
R8	Alta		Error en el uso de equipos.	Falta de capacitación al personal.	12	No tolerable
R9	Media	Disco duro externo	Hurto de medios o documentos.	Almacenamiento sin protección.	10	Tolerable
R10	Crítica	CD	Hurto de medios o documentos.	Almacenamiento sin protección.	16	No tolerable
R11	Crítica	DVD	Hurto de medios o documentos.	Almacenamiento sin protección.	16	No tolerable
R12	Alta	Memoria USB	Hurto de medios o documentos.	Almacenamiento sin protección.	15	No tolerable
R13	Crítica	Solicitudes y expedientes impresos	Hurto de medios o documentos.	Falta de control de acceso al personal. Almacenamiento sin protección.	16	No tolerable
R14	Alta		Incumplimiento en el mantenimiento de la información.	Desgaste por manipulación.	12	No tolerable
R15	Baja	Ofimática	Indisponibilidad en el uso de comandos.	Error en la activación del producto.	4	Aceptable

EVALUACIÓN DEL RIESGO						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo					**Doc. N°**	12
Objetivo Determinar la evaluación del riesgo.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**
R16	Media	Cliente de correo electrónico	Error en el uso del software de correo electrónico.	Configuración incorrecta de parámetros. Interfaz de usuario complicada.	6	Tolerable
R17	Alta	Anti virus	Desactualización de antivirus	Error en la activación del producto.	12	No tolerable
R18	Alta	Fichero	Modificación y/o eliminación no autorizada.	Falta de control de acceso al personal.	12	No tolerable
R19	Media	Copias de respaldo	Hurto de medios o documentos.	Copia no controlada. Falta de control de acceso al personal.	8	Tolerable
R20	Media	Credenciales (contraseñas)	Falsificación de derechos.	Gestión deficiente de las contraseñas. Falta de control de acceso al personal.	9	Tolerable
R21	Media	Datos de validación de credenciales.	Incongruencia en la integridad de los datos personales.	Datos registrados incorrectamente.	9	Tolerable

EVALUACIÓN DEL RIESGO						
Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo					**Doc. N°**	12
Objetivo Determinar la evaluación del riesgo.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**
R22	Alta	Registro de actividad	Procesamiento ilegal de datos.	Falta de mecanismos de monitoreo al personal.	12	No tolerable
R23	Crítica	Servicios externos	Indisponibilidad y daño de información o de equipos.	Falta de control de acceso al personal. No existen copias de respaldo. Falta de capacitación al personal.	16	No tolerable
R24	Media	Correo electrónico	Falsificación de derechos.	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.	6	Tolerable
R25	Media		Error en el uso del correo.	Falta de políticas sobre el uso del correo electrónico.	9	Tolerable
R26	Alta	Ambientes físicos	Inundación.	Ubicación en un área susceptible de inundación.	15	No tolerable
R27	Alta		Pérdida del suministro de energía.	Red energética inestable.	12	No tolerable
R28	Media		Hurto de equipo	Falta de protección física de las puertas y ventanas de la edificación.	10	Tolerable

EVALUACIÓN DEL RIESGO

Registrado por: Responsable ambiental. **Aprobado por:** Responsable de centro de cómputo	**Doc. N°**	12
Objetivo Determinar la evaluación del riesgo.	**Fecha de registro** 15/12/2017	

Descripción
Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.

Código de riesgo	Magnitud	Activo	Amenaza	Vulnerabilidad	Valor (PXI)	Tolerancia
R29	Alta	Usuarios internos	Incumplimiento en la disponibilidad del personal.	Falta de presupuesto. Ausencia del personal en el área designada.	12	No tolerable
R30	Crítica		Negación de acciones	Falta de asignación adecuada de responsabilidades en la seguridad de la información.	16	No tolerable
R31	Crítica		Error en el uso de equipos e información.	Uso incorrecto de software y hardware. Entrenamiento insuficiente en seguridad de la información.	16	No tolerable

Conclusiones: Se evaluaron 31 riesgos identificados.

3.4 Tratamiento del riesgo

Tabla 52. Plantilla para el tratamiento de riesgos

<table>
<tr><th colspan="7">TRATAMIENTO DE RIESGOS</th></tr>
<tr><td colspan="5">Registrado por: Responsable de centro de cómputo.
Aprobado por: Responsable ambiental.</td><td>Doc. N°</td><td>13</td></tr>
<tr><td colspan="5">Objetivo
Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.</td><td colspan="2">Fecha de registro
15/12/2017</td></tr>
<tr><td colspan="7">Descripción
Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.</td></tr>
<tr><th>Código de riesgo</th><th>Magnitud</th><th>Tolerancia</th><th>Activo</th><th>Amenaza</th><th>Estrategia</th><th>Controles</th></tr>
<tr><td>R1</td><td>Alta</td><td>No tolerable</td><td rowspan="2">Computadora de escritorio</td><td>Pérdida del suministro de energía.</td><td>Transferir</td><td>Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.</td></tr>
<tr><td>R2</td><td>Media</td><td>Tolerable</td><td>Mal funcionamiento de los equipos</td><td>Mitigar</td><td>Realizar el soporte técnico preventivo y correctivo de los equipos para asegurar su disponibilidad e integridad continuas.</td></tr>
<tr><td>R3</td><td>Media</td><td>Tolerable</td><td>Impresora</td><td>Polvo, corrosión</td><td>Mitigar</td><td>Realizar el soporte técnico preventivo y correctivo de los equipos para asegurar su disponibilidad e integridad continuas.</td></tr>
<tr><td>R4</td><td>Alta</td><td>No tolerable</td><td>Fotocopiadora</td><td>Pérdida del suministro de energía.</td><td>Transferir</td><td>Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.</td></tr>
</table>

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R5	Media	Tolerable		Destrucción del equipo o los medios, polvo.	Mitigar	Realizar el soporte técnico preventivo y correctivo de los equipos para asegurar su disponibilidad e integridad continuas.
R6	Media	Tolerable	Escáner	Polvo, corrosión	Mitigar	Realizar el soporte técnico preventivo y correctivo de los equipos para asegurar su disponibilidad e integridad continuas.
R7	Alta	No tolerable	Plotter	Pérdida del suministro de energía.	Transferir	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
R8	Alta	No tolerable		Error en el uso de equipos.	Mitigar	El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental.
R9	Media	Tolerable	Disco duro externo	Hurto de medios o documentos. Disco duro	Mitigar	La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.
R10	Crítica	No tolerable	CD	Hurto de medios o documentos.	Mitigar	La información digital debe estar protegida para reducir los riesgos de

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
						amenazas y peligros de acceso no autorizado.
R11	Crítica	No tolerable	DVD	Hurto de medios o documentos.	Mitigar	La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.
R12	Alta	No tolerable	Memoria USB	Hurto de medios o documentos.	Mitigar	La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.
R13	Crítica	No tolerable	Solicitudes y expedientes impresos	Hurto de medios o documentos.	Mitigar	Establecer segregación de funciones para separar el personal del servicio de información y personal con funciones administrativas.
R14	Alta	No tolerable		Incumplimiento en el mantenimiento de la información.	Mitigar	Implementar mecanismos de mantenimiento para conservar la integridad de la información física.
R15	Baja	Aceptable	Ofimática	Indisponibilidad en el uso de comandos.	Aceptar	Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R16	Media	Tolerable	Cliente de correo electrónico	Error en el uso del software de correo electrónico.	Mitigar	Establecer capacitaciones antes de la instalación de un software en la unidad ambiental.
R17	Alta	No tolerable	Anti virus	Desactualización de antivirus	Mitigar	Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.
R18	Alta	No tolerable	Fichero	Modificación y/o eliminación no autorizada.	Mitigar	Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro la unidad ambiental.
R19	Media	Tolerable	Copias de respaldo	Hurto de medios o documentos.	Mitigar	La oficina del centro de cómputo con el responsable ambiental deben realizar respaldos de la información periódicamente.
R20	Media	Tolerable	Credenciales (contraseñas)	Falsificación de derechos.	Mitigar	Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
R21	Media	Tolerable	Datos de validación de credenciales.	Incongruencia en la integridad de los datos personales.	Aceptar	Revisar periódicamente la base de datos del personal para su actualización correspondiente.

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R22	Alta	No tolerable	Registro de actividad	Procesamiento ilegal de datos.	Mitigar	Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.
R23	Crítica	No tolerable	Servicios externos	Indisponibilidad y daño de información o de equipos.	Transferir	Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.
R24	Media	Tolerable	Correo electrónico	Falsificación de derechos.	Mitigar	Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
R25	Media	Tolerable		Error en el uso del correo.	Mitigar	Proteger adecuadamente la información incluida en la mensajería electrónica.

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R26	Alta	No tolerable	Ambientes físicos	Inundación.	Transferir	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
R27	Alta	No tolerable		Pérdida del suministro de energía.	Transferir	Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.
R28	Media	Tolerable		Hurto de equipo.	Mitigar	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones. Definir y usar perímetros de seguridad para proteger áreas que contengan información confidencial e instalaciones de manejo de información.
R29	Alta	No tolerable	Usuarios internos	Poca disponibilidad de personal.	Mitigar	El área de RR.HH debe reclutar personal que esté con el perfil establecido para cumplir todas las funciones de la unidad ambiental.
R30	Crítica	No tolerable		Negación de acciones	Mitigar	Establecer responsabilidades y procedimientos de gestión para asegurar una

TRATAMIENTO DE RIESGOS						
Registrado por: Responsable de centro de cómputo. **Aprobado por:** Responsable ambiental.					**Doc. N°**	13
Objetivo Alinear cada una de las amenazas con los controles adecuados para tratar los riesgos identificados.					**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se hizo uso del resultado de la plantilla del análisis del riesgo.						
Código de riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
						respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
R31	Crítica	No tolerable		Error en el uso de equipos e información.	Mitigar	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
Conclusiones: Se asignó un control correspondiente, a cada una de las treinta y un amenazas identificadas.						

FASE IV – SOPORTE

4.1 Identificación de recursos para el tratamiento de riesgos

Tabla 53. Plantilla para la identificación de recursos

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R1	Alta	Computadora de escritorio	Pérdida del suministro de energía.	Transferir	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Solicitar la contratación del servicio de suministro.	- Personal experto en suministro de energía. - UPS
R4	Alta	Fotocopiadora	Pérdida del suministro de energía.	Transferir	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Solicitar la contratación del servicio de suministro.	- Personal experto en suministro de energía. - UPS
R7	Alta	Plotter	Pérdida del suministro de energía.	Transferir	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por	Solicitar la contratación del servicio de suministro.	- Personal experto en suministro de energía.

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
					fallas en los servicios de suministro.		- UPS
R8	Alta		Error en el uso de equipos.	Mitigar	El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental.	Programa de capacitación con la empresa que suministra el equipo.	Profesional experto para capacitar al personal de la unidad ambiental.
R10	Crítica	CD	Hurto de medios o documentos.	Mitigar	La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
R11	Crítica	DVD	Hurto de medios o documentos.	Mitigar	La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.

IDENTIFICACION DE RECURSOS		
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos	**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.	**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.		

Código de riesgo	Magnitud	Activo	Amenaza	Estrategia	Controles	Actividades	Recursos
R12	Alta	Memoria USB	Hurto de medios o documentos.	Mitigar	La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
R13	Crítica	Solicitudes y expedientes impresos	Hurto de medios o documentos.	Mitigar	Establecer segregación de funciones para separar el personal del servicio de información y personal con funciones administrativas.	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
R14	Alta		Incumplimiento en el mantenimiento de la información.	Mitigar	Implementar mecanismos de mantenimiento para conservar la integridad de la información física.	Solicitar capacitaciones para el mantenimiento de información	Personal experto en el mantenimiento de información.
					Escanear todas las solicitudes y expedientes que ingresan a la unidad ambiental.	Solicitar escáner y asignación de personal.	- Escáner. - Personal encargado del escaneo.

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R17	Alta	Anti virus	Desactualización de antivirus	Mitigar	Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.	Solicitar configuración y actualización de antivirus para la seguridad de la información.	Personal de soporte del centro de cómputo.
R18	Alta	Fichero	Modificación y/o eliminación no autorizada.	Mitigar	Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro la unidad ambiental.	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
R22	Alta	Registro de actividad	Procesamiento ilegal de datos.	Mitigar	Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.	El responsable ambiental debe revisar el procesamiento y manejo de la información del	Contratar profesional en seguridad de la información para capacitar al personal de la unidad ambiental

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
						registro de actividades.	
R23	Crítica	Servicios externos	Indisponibilidad y daño de información o de equipos.	Transferir	Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.	Solicitud para selección de proveedor en recuperación de la información.	Personal experto en recuperación de información y restauración del sistema.
R26	Alta	Ambientes físicos	Inundación	Transferir	Se debe diseñar y aplicar protección física contra	Solicitud para selección y	Personal experto en

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
					desastres naturales, ataques maliciosos o accidentes.	contratación de empresas en seguridad de instalaciones.	seguridad de instalaciones.
R27	Alta		Pérdida del suministro de energía.	Transferir	Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.	Solicitud para selección y contratación de empresas en suministro eléctrico.	Personal experto en suministro eléctrico
R29	Alta	Usuarios internos	Poca disponibilidad de personal.	Mitigar	El área de RR.HH debe reclutar personal que esté con el perfil establecido para cumplir todas las funciones de la unidad ambiental.	Solicitar al área de RR.HH cubrir todas las plazas.	Base de datos de personal calificado.

IDENTIFICACION DE RECURSOS							
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos						**Doc. N°**	14
Objetivo Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.						**Fecha de registro** 15/12/2017	
Descripción Para el desarrollo de esta actividad se deben elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							
Código de riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R30	Crítica	Usuarios internos	Negación de acciones	Mitigar	Establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	El responsable ambiental debe supervisar el procesamiento y manejo de la información.	Contratar un profesional en seguridad de la información para capacitar al personal orientado a mejorar los procedimientos del manejo de información, así como el uso adecuado de la misma.
R31	Crítica		Error en el uso de equipos e información.	Mitigar	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Revisar y actualizar el inventario de activos de la unidad ambiental.	Inventario de activos. Personal asignado para la actualización del inventario.

4.2 Determinar la comunicación de controles

Tabla 54. Plantilla para la comunicación de controles

<table>
<tr><th colspan="6">COMUNICACIÓN DE CONTROLES</th></tr>
<tr><td colspan="4">Registrado por: Responsable de centro de cómputo
Aprobado por: Gerente de desarrollo olmos</td><td>Doc. Nº</td><td>15</td></tr>
<tr><td colspan="4">Objetivo
Dar a conocer al personal de la gerencia de desarrollo los controles a implementar.</td><td colspan="2">Fecha de registro
22/12/2017</td></tr>
<tr><td colspan="6">Descripción
Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.</td></tr>
<tr><th>Controles</th><th>Actividades</th><th>Riesgos asociados</th><th>A quien comunicar</th><th>Quien debe comunicar</th><th>Tipo de comunicación</th></tr>
<tr><td>Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.</td><td>Solicitar la contratación del servicio de suministro</td><td>R1, R4, R7</td><td>Área de administración</td><td>Responsable de centro de cómputo</td><td>Documento escrito.</td></tr>
<tr><td>El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental.</td><td>Pactar un programa de capacitación con la empresa que suministra el equipo.</td><td>R8</td><td>Al gerente de desarrollo olmos.</td><td>El responsable ambiental.</td><td>Reuniones informativas</td></tr>
<tr><td>La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.</td><td>Solicitar el uso de credenciales por área y usuario.</td><td>R10, R11</td><td>Al personal de la unidad ambiental.</td><td>El responsable ambiental.</td><td>Charlas informativas</td></tr>
</table>

COMUNICACIÓN DE CONTROLES					
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos				**Doc. Nº**	15
Objetivo Dar a conocer al personal de la gerencia de desarrollo los controles a implementar.				**Fecha de registro** 22/12/2017	
Descripción Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.	Solicitar el uso de credenciales por área y usuario.	R12	A todo el personal de la gerencia de desarrollo olmos.	El gerente de desarrollo olmos.	Documento escrito.
Establecer segregación de funciones para separar el personal del servicio de información y personal con funciones administrativas.	Solicitar el uso de credenciales por área y usuario.	R13	Área de RR.HH	El responsable ambiental.	Documento escrito.
Implementar mecanismos de mantenimiento para conservar la integridad de la información física.	Solicitar capacitaciones para el mantenimiento de información.	R14	El gerente de desarrollo olmos.	El responsable ambiental.	Reunión informativa
Escanear todas las solicitudes y expedientes que ingresan a la unidad ambiental.	Solicitar escáner y asignación de personal.	R14	Al personal de la unidad ambiental.	El responsable ambiental.	Correo electrónico
Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.	Solicitar actualización de antivirus para la seguridad de la información.	R17	Responsable de centro de cómputo	El gerente de desarrollo olmos.	Documento físico

COMUNICACIÓN DE CONTROLES					
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos				**Doc. Nº**	15
Objetivo Dar a conocer al personal de la gerencia de desarrollo los controles a implementar.				**Fecha de registro** 22/12/2017	
Descripción Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro la unidad ambiental.	Comprar, instalar y configurar un servidor de archivos.	R18	El gerente de desarrollo olmos.	El responsable ambiental.	Reunión informativa
Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.	El responsable ambiental debe revisar el procesamiento y manejo de la información del registro de actividades.	R22	Responsable de centro de cómputo	El responsable ambiental.	Reunión informativa
Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.	Solicitud para selección de proveedor en recuperación de la información.	R23	Responsable de centro de cómputo	El gerente de desarrollo olmos.	Documento escrito
Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Solicitud para selección y contratación de empresas.	R26	Área de administración	El gerente de desarrollo olmos.	Documento escrito

COMUNICACIÓN DE CONTROLES					
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos				**Doc. Nº**	15
Objetivo Dar a conocer al personal de la gerencia de desarrollo los controles a implementar.				**Fecha de registro** 22/12/2017	
Descripción Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.	Solicitud para selección y contratación de empresas.	R27	Área de administración	El gerente de desarrollo olmos.	Documento escrito
El área de RR.HH debe reclutar personal que esté con el perfil establecido para cumplir todas las funciones de la unidad ambiental.	Solicitar al área de RR.HH cubrir todas las plazas.	R29	El gerente de desarrollo olmos.	El responsable ambiental.	Reunión informativa
Establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	El responsable ambiental debe supervisar el procesamiento y manejo de la información.	R30	Responsable de centro de cómputo	El responsable ambiental.	Reunión informativa
Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Revisar y actualizar el inventario de activos de la unidad ambiental.	R31	El gerente de desarrollo olmos. Jefe cómputo	El responsable ambiental.	Reunión informativa
Conclusiones: Se obtuvieron dieciséis controles para ser comunicados en la gerencia de desarrollo olmos y unidad ambiental.					

FASE V - OPERACIÓN

5.1 Planificación y control operacional

Para el desarrollo de esta actividad se debe llenar la siguiente plantilla:

Tabla 55. Plantilla de control operacional

<table>
<tr><th colspan="4">PLANIFICACIÓN Y CONTROL OPERACIONAL</th></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="2">Registrado por: Responsable de centro de cómputo
Aprobado por: Gerente de desarrollo olmos y especialista ambiental.</td><td>Doc. Nº</td><td>16</td></tr>
<tr><td colspan="2">Objetivo
Asignar a cada control un responsable de su ejecución, para lograr el cumplimiento de los objetos de seguridad de la información.</td><td colspan="2">Fecha de registro
28/12/2017</td></tr>
<tr><td colspan="4">Descripción
Para el desarrollo de esta actividad se deben usar los controles mencionados en el tratamiento de riesgos.</td></tr>
<tr><th>Objetivo de seguridad</th><th>Control</th><th>Actividades</th><th>Responsable</th></tr>
<tr><td rowspan="2">Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td><td>1. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td><td rowspan="2">Realizar reuniones con el gerente de desarrollo olmos, el responsable ambiental y de centro de cómputo</td><td rowspan="2">Control 1: Responsable de centro de cómputo.

Control 2: Responsable ambiental.</td></tr>
<tr><td>2. Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.</td></tr>
<tr><td rowspan="2">Asegurar que el personal comprenda sus responsabilidades y son capaces en los roles para los que se consideran.</td><td>3. El área de RR. HH debe reclutar personal que esté con el perfil establecido para cumplir todas las funciones de la unidad ambiental.</td><td>- Solicitar al área de RR. HH cubrir todas las plazas.</td><td rowspan="2">Control 3, 5:
Área de RR. HH

Control 4: gerente de desarrollo olmos.</td></tr>
<tr><td>4. Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro de la unidad ambiental.</td><td>- Programa de capacitación con la empresa que suministra el equipo.</td></tr>
</table>

PLANIFICACIÓN Y CONTROL OPERACIONAL			
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y especialista ambiental.		**Doc. Nº**	16
Objetivo Asignar a cada control un responsable de su ejecución, para lograr el cumplimiento de los objetos de seguridad de la información.		**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se deben usar los controles mencionados en el tratamiento de riesgos.			
	5. El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental.		
Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas asegurando que la información recibe un nivel apropiado de protección.	6. Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Revisar y actualizar el inventario de activos de la unidad ambiental.	Control 6, 7: Responsable de centro de cómputo.
	7. Implementar mecanismos de mantenimiento para conservar la integridad de la información física.	Solicitar capacitaciones para el mantenimiento de información.	
	8. Escanear todas las solicitudes y expedientes que ingresan a la unidad ambiental.	Solicitar escáner y asignación de personal.	Control 8: Responsable ambiental.
Limitar el acceso a la información y a las instalaciones de procesamiento de información ambiental.	9. Establecer segregación de funciones para separar el personal del servicio de información y personal con funciones administrativas.	Solicitar el uso de credenciales por área y usuario.	Control 9: Área de RR. HH
Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	10. La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.	Solicitar el uso de credenciales por área y usuario.	Control 10: Área de RR. HH
	11. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Solicitud para selección y contratación de empresas.	Control 11, 12: Área de administración

PLANIFICACIÓN Y CONTROL OPERACIONAL			
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y especialista ambiental.		**Doc. Nº**	16
Objetivo Asignar a cada control un responsable de su ejecución, para lograr el cumplimiento de los objetos de seguridad de la información.		**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se deben usar los controles mencionados en el tratamiento de riesgos.			
	12. Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.		
Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	13. La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.	Solicitar el uso de credenciales por área y usuario.	Control 13: Área de RR. HH
	14. Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Solicitar la contratación del servicio de suministro	Control 14: Área de administración
Proteger contra la perdida de datos.	15. Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.	Solicitud para selección de proveedor en recuperación de la información.	Control 15: Área de RR. HH
Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	16. Establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	El responsable ambiental debe supervisar el procesamiento y manejo de la información.	Control 16: Responsable de centro de cómputo.

PLANIFICACIÓN Y CONTROL OPERACIONAL			
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y especialista ambiental.		**Doc. Nº**	16
Objetivo Asignar a cada control un responsable de su ejecución, para lograr el cumplimiento de los objetos de seguridad de la información.		**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se deben usar los controles mencionados en el tratamiento de riesgos.			
Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	17. Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.	Solicitar actualización de antivirus para la seguridad de la información.	Control 17: Responsable de centro de cómputo.
Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.	18. Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.	El responsable ambiental debe revisar el procesamiento y manejo de la información del registro de actividades.	Control 18: Responsable ambiental.

FASE VI - EVALUACIÓN DEL DESEMPEÑO

Valoración de los controles propuestos

Tabla 56. Valoración del nivel de cumplimiento de los controles

Valor	Estado	Descripción
1	Cumple satisfactoriamente	Es gestionado, se está cumpliendo como solicita la norma, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
2	Cumple parcialmente	Se está haciendo de manera parcial, no está documentado, se definió pero no se gestiona.
3	No cumple	No existe y/o no se está haciendo.
4	No aplica	El control no es aplicable para la entidad. En el campo observaciones indicar la justificación respectiva de su no aplicabilidad.

6.1 Monitoreo, análisis y evaluación del SGSI

Tabla 57. Plantilla de monitoreo

<table>
<tr><td colspan="5">MONITOREO DEL SGSI</td></tr>
<tr><td colspan="3">Registrado por: Responsable de centro de cómputo
Aprobado por: Gerente de desarrollo olmos y responsable ambiental.</td><td>Doc. N°</td><td>17</td></tr>
<tr><td colspan="3">Objetivo
Establecer una evaluación de monitoreo.</td><td colspan="2">Fecha de registro
28/12/2017</td></tr>
<tr><td colspan="5">Descripción
Para el desarrollo de esta actividad se debe aplicar el check-list al gerente de desarrollo olmos.</td></tr>
<tr><td>N°</td><td>Controles</td><td>Valor del control</td><td>Estado</td><td>Periodo</td></tr>
<tr><td>1</td><td>Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td><td>2</td><td>Cumple parcialmente</td><td>Mensual</td></tr>
<tr><td>2</td><td>Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.</td><td>2</td><td>Cumple parcialmente</td><td>Anual</td></tr>
<tr><td>3</td><td>El área de RR. HH debe reclutar personal que esté con el perfil establecido para cumplir todas las funciones de la unidad ambiental.</td><td>1</td><td>Cumple satisfactoriamente</td><td>Cada 10 meses</td></tr>
<tr><td>4</td><td>Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro de la unidad ambiental.</td><td>2</td><td>Cumple parcialmente</td><td>Cada 6 meses</td></tr>
</table>

MONITOREO DEL SGSI				
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y responsable ambiental.			**Doc. N°**	17
Objetivo Establecer una evaluación de monitoreo.			**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se debe aplicar el check-list al gerente de desarrollo olmos.				
N°	**Controles**	**Valor del control**	**Estado**	**Periodo**
5	El personal debe ser capacitado antes de instalar y asignar el uso de un equipo a la unidad ambiental.	1	Cumple satisfactoriamente	Cada 6 meses
6	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	2	Cumple parcialmente	Anual
7	Implementar mecanismos de mantenimiento para conservar la integridad de la información física.	2	Cumple parcialmente	Cada 6 meses
8	Escanear todas las solicitudes y expedientes que ingresan a la unidad ambiental.	1	Cumple satisfactoriamente	Quincenal
9	Establecer segregación de funciones para separar el personal del servicio de información y personal con funciones administrativas.	1	Cumple satisfactoriamente	Anual
10	La unidad ambiental debe asegurar que solo se permita el acceso al personal autorizado.	1	Cumple satisfactoriamente	Diariamente

MONITOREO DEL SGSI				
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y responsable ambiental.			**Doc. N°**	17
Objetivo Establecer una evaluación de monitoreo.			**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se debe aplicar el check-list al gerente de desarrollo olmos.				
N°	**Controles**	**Valor del control**	**Estado**	**Periodo**
11	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	1	Cumple satisfactoriamente	Anual
12	Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.	2	Cumple parcialmente	Cada 6 meses
13	La información digital debe estar protegida para reducir los riesgos de amenazas y peligros de acceso no autorizado.	1	Cumple satisfactoriamente	Cada 6 meses
14	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	2	Cumple parcialmente	Cada 6 meses
15	Implementar procedimientos de copias de respaldo y recuperación de información para asegurar que ante cualquier falla en el sistema o almacén, estos pueden recuperarse y restaurarse completamente.	1	Cumple satisfactoriamente	Mensual

MONITOREO DEL SGSI				
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y responsable ambiental.			**Doc. N°**	17
Objetivo Establecer una evaluación de monitoreo.			**Fecha de registro** 28/12/2017	
Descripción Para el desarrollo de esta actividad se debe aplicar el check-list al gerente de desarrollo olmos.				
N°	**Controles**	**Valor del control**	**Estado**	**Periodo**
16	Establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	1	Cumple satisfactoriamente	Mensual
17	Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.	2	Cumple parcialmente	Mensual
18	Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.	2	Cumple parcialmente	Mensual
Conclusiones: De los 18 controles identificados se observa que: 9 controles se cumplen satisfactoriamente, 9 se están cumpliendo parcialmente y 2 no se cumplen.				

6.2 Auditoria interna

La tabla 58 ofrece una plantilla para la realización de la auditoría interna.

Tabla 58. Plantilla para la auditoria interna

<table>
<tr><th colspan="9">AUDITORIA INTERNA DEL SGSI</th></tr>
<tr><td colspan="7">Registrado por: Empresa externa.
Aprobado por: Gerente de desarrollo olmos.</td><td>Doc. Nº</td><td>18</td></tr>
<tr><td colspan="7">Objetivo
Establecer un plan de auditoria.</td><td colspan="2">Fecha de registro
08/01/2018</td></tr>
<tr><td colspan="9">Descripción
Para el desarrollo de esta actividad se puede contratar un servicio externo.</td></tr>
<tr><th>Nº</th><th>Acción</th><th>Involucrados</th><th>Recursos</th><th>Tareas</th><th>Efectividad</th><th>Inicio</th><th>Cierre</th><th>Resultado</th></tr>
<tr><td>01</td><td>Reunión de inicio de auditoría</td><td>Responsable:
Auditor interno del SGSI
Convocado:
- Gerente de desarrollo olmos
- Responsable ambiental.
- Jefe de centro de cómputo</td><td>Ubicación:
Sala de reuniones de la consultora
Tecnología:
Laptop con acceso controlado (auditor) a registros de operación del SGSI</td><td>1. Presentar el Plan de Auditoría (final)

2. Ejecutar la reunión de auditoría</td><td>Resultado esperado:
Compromiso de asistencia de los involucrados y su personal a las reuniones de auditoría</td><td>08/01/2018</td><td>08/01/2018</td><td>Realizado</td></tr>
<tr><td>02</td><td>Auditoría al representante de la gerencia de desarrollo olmos</td><td>Responsable:
Auditor interno del SGSI
Convocado:
- Gerente de desarrollo olmos</td><td>Ubicación:
Sala de reuniones de la consultora
Tecnología:
Laptop con acceso controlado (auditor) a registros</td><td>1. Ejecutar la reunión de auditoría.

2. Solicitar evidencia complementaria, si</td><td>Resultado esperado:
-Asistencia de los convocados.
- Evidencias</td><td>08/01/2018</td><td>08/01/2018</td><td>Realizado</td></tr>
</table>

AUDITORIA INTERNA DEL SGSI								
Registrado por: Empresa externa. **Aprobado por:** Gerente de desarrollo olmos.						**Doc. N°**	18	
Objetivo Establecer un plan de auditoria.						**Fecha de registro** 08/01/2018		
Descripción Para el desarrollo de esta actividad se puede contratar un servicio externo.								
N°	**Acción**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
			de operación del SGSI	corresponde	solicitadas durante la reunión.			
03	Auditoría al responsable de la seguridad de información	**Responsable:** Auditor interno del SGSI **Convocado:** - Jefe de centro de cómputo	**Ubicación:** Sala de reuniones de la consultora **Tecnología:** Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría. 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** -Asistencia de los convocados. - Evidencias solicitadas durante la reunión.	09/01/2018	09/01/2018	Realizado
04	Auditoría a los representantes de las funciones	**Responsable:** Auditor interno del SGSI **Convocado:** -Responsable ambiental -Especialista ambiental -Encargado de archivo	**Ubicación:** Sala de reuniones de la consultora **Tecnología:** Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría. 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** -Asistencia de los convocados. - Evidencias solicitadas durante la reunión.	10/01/2018	12/01/2018	Realizado

AUDITORIA INTERNA DEL SGSI								
Registrado por: Empresa externa. **Aprobado por:** Gerente de desarrollo olmos.							**Doc. N°**	18
Objetivo Establecer un plan de auditoria.							**Fecha de registro** 08/01/2018	
Descripción Para el desarrollo de esta actividad se puede contratar un servicio externo.								
N°	**Acción**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
		-Personal de apoyo						
05	Inspección a ambientes de trabajo de los procesos	**Responsable:** Auditor interno del SGSI **Convocado:** -Responsable ambiental -Especialista ambiental -Encargado de archivo -Personal de apoyo	**Ubicación:** Sala de reuniones de la consultora **Tecnología:** Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría. 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** -Asistencia de los convocados. - Evidencias solicitadas durante la reunión.	15/02/2018	15/02/2018	Realizado
06	Inspección al centro de datos	**Responsable:** Auditor interno del SGSI **Convocado:** -Encargado de archivo.	**Ubicación:** Lugar de almacenamiento	1. Ejecutar la reunión de auditoría. 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** -Asistencia de los convocados. - Evidencias solicitadas durante la reunión.	16/02/2018	18/02/2018	Realizado

AUDITORIA INTERNA DEL SGSI								
Registrado por: Empresa externa. **Aprobado por:** Gerente de desarrollo olmos.						**Doc. N°**	18	
Objetivo Establecer un plan de auditoria.						**Fecha de registro** 08/01/2018		
Descripción Para el desarrollo de esta actividad se puede contratar un servicio externo.								
N°	**Acción**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
07	Reunión de fin de auditoría	**Responsable:** Auditor interno del SGSI **Convocado:** -Gerente de desarrollo Olmos. -Responsable ambiental -Especialista ambiental -Encargado de archivo -Personal de apoyo	**Ubicación:** Sala de reuniones de la consultora **Tecnología:** Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Presentar los resultados de auditoría 2. Suscribir el acta de cierre de la auditoría.	**Resultado esperado:** -Asistencia de los convocados. - Acta de cierre de auditoría.	19/02/2018	19/02/2018	Realizado

FASE VII – MEJORA CONTINUA

Tabla 59. Plantilla para mejora continua

MEJORA CONTINUA					
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y responsable ambiental.				**Doc. Nº**	19
Objetivo Establecer un plan de mejora continua.				**Fecha de registro** 20/02/2018	
Descripción Para el desarrollo esta plantilla se utilizaron los controles evaluados en la actividad de monitoreo.					
Nº	**Actividades**	**Riesgos involucrados**	**Controles**	**Fecha inicio**	**Fecha fin**
1	Realizar reuniones con el gerente de desarrollo olmos, el responsable ambiental y de centro de cómputo	Los riesgos considerados como altos y críticos	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	20/02/2018	23/02/2018
2	Reunión con el responsable ambiental y de centro de cómputo	Los riesgos considerados como altos y críticos	Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	23/02/2018	24/02/2018
3	Configurar un servidor de archivos.	R18	Se deben definir y asignar todas las responsabilidades de la seguridad de la información dentro de la unidad ambiental.	26/02/2018	26/03/2018
4	Revisar y actualizar el inventario de activos de la unidad ambiental.	R31	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	27/02/2018	28/02/2018

MEJORA CONTINUA					
Registrado por: Responsable de centro de cómputo **Aprobado por:** Gerente de desarrollo olmos y responsable ambiental.				**Doc. Nº**	19
Objetivo Establecer un plan de mejora continua.				**Fecha de registro** 20/02/2018	
Descripción Para el desarrollo esta plantilla se utilizaron los controles evaluados en la actividad de monitoreo.					
Nº	**Actividades**	**Riesgos involucrados**	**Controles**	**Fecha inicio**	**Fecha fin**
5	Reforzar las capacitaciones para el mantenimiento de información.	R14	Implementar mecanismos de mantenimiento para conservar la integridad de la información física.	01/03/2018	05/03/2018
6	Solicitar la revisión periódica del suministro.	R27	Se debe diseñar y aplicar la revisión, instalación y mantenimiento del suministro eléctrico.	05/03/2018	08/03/2018
07	Revisar el funcionamiento del UPS	R1, R4, R7	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	09/03/2018	12/03/2018
08	Actualizar el antivirus para la seguridad de la información.	R17	Implementar procedimientos para asegurar el cumplimiento del uso de productos de software patentados.	12/03/2018	14/03/2018
09	El responsable ambiental debe revisar periódicamente el procesamiento y manejo de la información del registro de actividades.	R22	Revisar el cumplimiento del procesamiento y procedimientos de información dentro de la unidad ambiental, con las políticas y normas de seguridad apropiadas.	14/03/2018	17/03/2018
Conclusiones: Se han considerado los controles que cumplen parcialmente con su desempeño.					

ANEXO 5

PLANTILLA PARA LA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

FECHA :
NOMBRES Y APELLIDOS :
FORMACIÓN ACADÉMICA :
AREAS DE EXPERIENCIA PROFESIONAL:
TIEMPO DE EXPERIENCIA :
CARGO ACTUAL :
INSTITUCIÓN :

Objetivo de la investigación : Contribuir en la seguridad de la información de las unidades ambientales de la región Lambayeque.

Objetivo del juicio de expertos : Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad de las plantillas propuestas en la gestión de la unidad ambiental de su institución.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1 No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1 No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

CUESTIONARIO PARA VALIDACIÓN DEL

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I Contexto de la organización	Identificación de contextos.					
	Necesidades y expectativas de las partes interesadas.					
	Determinar el alcance.					
II Liderazgo	Asegurar el liderazgo y compromiso.					
	Establecer políticas y objetivos de seguridad.					
	Definir roles y responsabilidades.					
III Planificación	Identificación del riesgo.					
	Análisis del riesgo.					
	Evaluación del riesgo.					
	Tratamiento del riesgo.					

IV Soporte	Definir un modelo de recursos.					
	Determinar un modelo de competencia del personal.					
	Determinar la comunicación externa e interna.					
V Operación	Planificación y control operacional.					
VI Evaluación del desempeño	Monitoreo, análisis y evaluación del SGSI.					
	Auditoria interna.					
VII Mejoras	Mejora continua					

ANEXO 6

VALIDACION DEL MODELO POR JUICIO DE EXPERTOS

EXPERTO 1

PLANTILLA PARA LA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

FECHA	: 23 de marzo 2018
NOMBRES Y APELLIDOS	: Luis Martín García Cabrera.
FORMACIÓN ACADÉMICA	: Ingeniero de Sistemas.

AREAS DE EXPERIENCIA PROFESIONAL: Analista programador, seguimiento y control de proyectos, gestión de tecnologías de información.

TIEMPO DE EXPERIENCIA	: 14 años
CARGO ACTUAL	: Jefe del área de TI.
INSTITUCIÓN	: Ministerio Público – Fiscalía de Lambayeque.

Objetivo de la investigación	: Contribuir en la seguridad de la información de las unidades ambientales de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en la gestión de la unidad ambiental de su institución.

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I Contexto de la organización	Identificación de contextos.	4	4	4	4	
	Necesidades y expectativas de las partes interesadas.	3	4	4	4	Se podría separar las necesidades y expectativas
	Determinar el alcance.	4	4	4	4	
II Liderazgo	Asegurar el liderazgo y compromiso.	3	4	4	4	
	Establecer políticas y objetivos de seguridad.	4	4	4	4	
	Definir roles y responsabilidades.	3	4	4	4	
III Planificación	Identificación del riesgo.	4	4	4	4	
	Análisis del riesgo.	4	4	4	4	
	Evaluación del riesgo.	4	4	4	4	
	Tratamiento del riesgo.	4	4	4	4	

IV Soporte	Definir un modelo de recursos.	4	4	4	4	
	Determinar un modelo de competencia del personal.	3	4	4	4	Se podría agregar un modelo de objetivos (solo sugerencia)
	Determinar la comunicación externa e interna.	4	4	4	3	
V Operación	Planificación y control operacional.	3	4	4	4	
VI Evaluación del desempeño	Monitoreo, análisis y evaluación del SGSI.	4	4	4	4	
	Auditoria interna.	4	4	4	4	
VII Mejoras	Mejora continua	4	4	4	4	

EXPERTO 2

PLANTILLA PARA LA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

FECHA	: 23 DE MARZO
NOMBRES Y APELLIDOS	: VICTOR EDUARDO MARCOS CORREA
FORMACIÓN ACADÉMICA	: INGENIERO DE SISTEMAS
AREAS DE EXPERIENCIA PROFESIONAL:	TECNOLOGIAS DE INFORMACION
TIEMPO DE EXPERIENCIA	: 9 AÑOS.
CARGO ACTUAL	: ESPECIALISTA SIG - RADA
INSTITUCIÓN	: ADMINISTRACION LOCAL DE AGUA CHANCAY - LAMBAYEQUE

Objetivo de la investigación	: Contribuir en la seguridad de la información de las unidades ambientales de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en la gestión de la unidad ambiental de su institución.

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I Contexto de la organización	Identificación de contextos.	4	4	4	4	
	Necesidades y expectativas de las partes interesadas.	4	4	4	4	
	Determinar el alcance.	4	4	4	4	
II Liderazgo	Asegurar el liderazgo y compromiso.	4	4	4	3	
	Establecer políticas y objetivos de seguridad.	3	3	4	3	
	Definir roles y responsabilidades.	3	3	4	3	
III Planificación	Identificación del riesgo.	4	4	4	4	
	Análisis del riesgo.	4	4	4	4	
	Evaluación del riesgo.	4	4	4	4	
	Tratamiento del riesgo.	4	4	4	4	

IV Soporte	Definir un modelo de recursos.	3	3	3	3	SE PODRIA ADICIONAR UNA LISTA DE RECURSOS
	Determinar un modelo de competencia del personal.	3	3	3	3	ESTABLECER UNA LISTA DE COMPETENCIAS
	Determinar la comunicación externa e interna.	3	4	4	3	
V Operación	Planificación y control operacional.	3	3	4	4	
VI Evaluación del desempeño	Monitoreo, análisis y evaluación del SGSI.	4	4	4	4	
	Auditoria interna.	4	4	4	4	
VII Mejoras	Mejora continua	4	4	4	4	

Ing. Victor Eduardo Marcos Correa
PROFESIONAL ALA CHINCHAY - LAMBAYEQUE
CIP N° 115172

EXPERTO 3

PLANTILLA PARA LA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE. Para tal fin, se anexa el cuestionario de validación.

FECHA	: 26 de marzo 2018
NOMBRES Y APELLIDOS	: MIGUEL ANGEL DIAZ ESPINO
FORMACIÓN ACADÉMICA	: INGENIERO EN COMPUTACIÓN Y SISTEMAS
AREAS DE EXPERIENCIA PROFESIONAL:	GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN
TIEMPO DE EXPERIENCIA	: 20 AÑOS
CARGO ACTUAL	: ESPECIALISTA EN SISTEMAS DE INFORMACIÓN
INSTITUCIÓN	: PROYECTO ESPECIAL OLMOS TINAJONES
Objetivo de la investigación	: Contribuir en la seguridad de la información de las unidades ambientales de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en la gestión de la unidad ambiental de su institución.

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LAS UNIDADES AMBIENTALES DE LA REGIÓN LAMBAYEQUE

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I Contexto de la organización	Identificación de contextos.	4	3	4	4	
	Necesidades y expectativas de las partes interesadas.	4	4	4	4	
	Determinar el alcance.	3	4	4	4	- Falta que información es la que se auditara
II Liderazgo	Asegurar el liderazgo y compromiso.	2	2	4	4	- Definir lo que se busca en esta fase
	Establecer políticas y objetivos de seguridad.	4	4	4	4	
	Definir roles y responsabilidades.	3	4	4	4	- Mostrar modelo de matriz
III Planificación	Identificación del riesgo.	4	4	4	4	
	Análisis del riesgo.	3	3	4	4	- Mostrar matriz de análisis
	Evaluación del riesgo.	3	3	4	4	- Mostrar matriz de evaluación

	Tratamiento del riesgo.	4	4	4	4	
IV Soporte	Definir un modelo de recursos.	4	4	4	4	
	Determinar un modelo de competencia del personal.	3	4	4	4	- Falta Matriz de Modelo
	Determinar la comunicación externa e interna.	3	3	4	4	- Definir algunos actores
V Operación	Planificación y control operacional.	4	4	4	4	
VI Evaluación del desempeño	Monitoreo, análisis y evaluación del SGSI.	4	4	4	4	
	Auditoria interna.	4	4	4	4	
VII Mejoras	Mejora continua	4	4	4	4	

PROYECTO ESPECIAL CONMEMORACIONES
OFICINA DE ADMINISTRACIÓN
Ing. Miguel Díaz Espino
CENTRO DE COMPUTO

COMPARACIÓN DE LOS RESULTADO DE LA VALIDACIÓN DEL JUICIO DE EXPERTOS

FASE	ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3			
		SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE
I Contexto de la organización	Identificación de contextos.	4	4	4	4	4	4	4	4	4	3	4	4
	Necesidades y expectativas de las partes interesadas.	3	4	4	4	4	4	4	4	4	4	4	4
	Determinar el alcance.	4	4	4	4	4	4	4	4	3	4	4	4
II Liderazgo	Asegurar el liderazgo y compromiso.	3	4	4	4	4	4	4	3	2	2	4	4
	Establecer políticas y objetivos de seguridad.	4	4	4	4	3	3	4	3	4	4	4	4
	Definir roles y responsabilidades.	3	4	4	4	3	3	4	3	3	4	4	4
III Planificación	Identificación del riesgo.	4	4	4	4	4	4	4	4	4	4	4	4
	Análisis del riesgo.	4	4	4	4	4	4	4	4	3	3	4	4
	Evaluación del riesgo.	4	4	4	4	4	4	4	4	3	3	4	4
	Tratamiento del riesgo.	4	4	4	4	4	4	4	4	4	4	4	4

FASE	ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3			
		SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE
IV Soporte	Definir un modelo de recursos.	4	4	4	4	3	3	3	3	4	4	4	4
	Determinar un modelo de competencia del personal.	3	4	4	4	3	3	3	3	3	4	4	4
	Determinar la comunicación externa e interna.	4	4	4	3	3	4	4	3	3	3	4	4
V Operación	Planificación y control operacional.	3	4	4	4	3	3	4	4	4	4	4	4
VI Evaluación del desempeño	Monitoreo, análisis y evaluación del SGSI.	4	4	4	4	4	4	4	4	4	4	4	4
	Auditoria interna.	4	4	4	4	4	4	4	4	4	4	4	4
VII Mejoras	Mejora continua	4	4	4	4	4	4	4	4	4	4	4	4

De la comparación de los resultados de la validación del modelo de seguridad de la información para la gestión de las unidades ambientales de la región Lambayeque, los tres expertos coincidieron que las actividades de: asegurar el liderazgo y compromiso, definir roles y responsabilidades, determinar un modelo de competencia del personal y determinar la comunicación externa e interna; deben mejorar en la categoría de suficiencia, incrementando ítems para poder evaluar las actividades completamente.