UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

Modelo de gestión de riesgos para mejorar la seguridad de la información en los procesos de emergencia en el sector salud pública de la región Lambayeque

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

AUTOR

Miluska Natalia Nicho Gomez

ASESOR

Maria Ysabel Aranguri Garcia

https://orcid.org/0000-0001-9220-5801

Chiclayo, 2024

Modelo de gestión de riesgos para mejorar la seguridad de la información en los procesos de emergencia en el sector salud pública de la región Lambayeque

PRESENTADA POR

Miluska Natalia Nicho Gomez

A la Escuela de Posgrado 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

APROBADA POR

Héctor Miguel Zelada Valdivieso
PRESIDENTE

Gregorio Manuel León Tenorio
SECRETARIO

Maria Ysabel Aranguri Garcia
VOCAL

Dedicatoria

A mis padres, que con su esfuerzo y dedicación han podido brindarme la formación necesaria para poder proyectar mis metas e ideales y mantener siempre la constancia y paso firme hacia adelante. A mi hija, Valeria, que siempre ha sido la motivación importante para avanzar y lograr mis metas y objetivos.

Agradecimientos

Un agradecimiento especial a cada persona que, durante el transcurso de esta investigación, ha brindado su apoyo en cada peldaño que he ido avanzando.
Un agradecimiento a Dios por permitirme disfrutar de mi familia, gozar de buena salud, poseer la motivación suficiente para poder culminar cada meta que me propongo.

Modelo de gestión de riesgos para mejorar la seguridad de la información en los procesos de emergencia en el sector salud pública de la región Lambayeque.pdf

INFORME DE ORIGINALIDAD

20%	20%	4%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	6%
2	tesis.usat.edu.pe Fuente de Internet	3%
3	www.essalud.gob.pe Fuente de Internet	2%
4	repository.unad.edu.co Fuente de Internet	2%
5	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	1%
6	idoc.pub Fuente de Internet	1%
7	repository.unipiloto.edu.co Fuente de Internet	1%
8	docplayer.es Fuente de Internet	<1%

Índice

Resumen

Los hospitales del sector Salud Pública de la región Lambayeque, dentro del servicio de atención de Emergencia, evidencian retraso en la atención, baja capacidad de respuesta de los aplicativos informáticos, sobredemanda de atención y afectación en la calidad de la misma. Parte del surgimiento de esta serie de problemas es, porque no están suficientemente capacitados en seguridad de la información, además existe la falta de identificación de requerimientos y controles, es por ello que se requiere un nivel de mejora para la misma. Los servicios de emergencia forman parte fundamental de los diferentes establecimientos de salud, este nivel de importancia requiere que el manejo de la información no presente inconvenientes en relación a la seguridad de la misma, por lo que se requiere tomar medidas para brindar un mejor servicio, logrando así ayudar con el cumplimiento de la misión de la organización. Tomar prioridad a los activos importantes dentro del servicio de atención de Emergencia, permite que la información del personal junto a la del paciente esté resguardada, no alterada y con disponibilidad las 24 horas del día, los 7 días de la semana. Es por ello que en este informe plantea un modelo que permite llevar a cabo una evaluación de vulnerabilidades, activos y amenazas operacionalmente críticas, a través de la armonización de diferentes normas y metodologías como NTP ISO 27005, COBIT 5 para Riesgos, Magerit y Octave, para adaptarlas a la necesidad del contexto evaluado. Aquí se resalta la importancia de la participación de todos los miembros activos dentro del área de Emergencia de los hospitales del sector Salud Pública, ya que a través de los diferentes roles que se les asignen en el modelo propuesto de la evaluación de la Gestión del Riesgo, podrá ser llevado con éxito el mismo.

Palabras claves: estándares, seguridad de la información, gestión de riesgo, emergencias, activo, amenaza.

Abstract

The hospitals of the Public Health sector of the Lambayeque region, within the Emergency care service, showing delays in care, low response capacity, over-demand for care and affectation in the quality of care. Part of the emergence of this series of problems is because they are not sufficiently trained in information security, requiring a level of improvement for it. The emergency services are a fundamental part of the different health establishments, this level of importance requires that the handling of the information does not present inconveniences in relation to its security, for which it is necessary to take measures to provide a better service, thus achieving help with the fulfillment of the mission of the organization. Giving priority to important assets within the Emergency care service allows staff information along with that of the patient to be protected, not altered and available 24 hours a day, 7 days a week. That is why this report proposes a model that allows carrying out an assessment of operationally critical vulnerabilities, assets and threats, through the harmonization of different standards and methodologies such as NTP ISO 27005, COBIT, Magerit and Octave, to adapt them. to the need of the evaluated context. Here the importance of the participation of all active members within the Emergency area of hospitals in the Public Health sector is highlighted, since through the different roles assigned to them in the proposed model of Risk Management evaluation, it can be successfully carried out.

Keywords: standards, information security, risk management, emergencies, asset, threat.

1. Introducción

Los hospitales o centros médicos han mostrado un alto nivel de dependencia en sistemas de información para el cumplimiento de funciones en el ámbito clínico y administrativo. Estos centros hospitalarios realizan su labor a través de medios de diagnósticos modernos, los cuales conllevan un elevado mecanismo informatizado, esto representa el uso de diversas herramientas que, necesitan estar conectadas con sistemas externos, convirtiéndose en una situación compleja de controlar [1]. Si bien la tecnología genera valor en la eficiencia de los procesos principales de cualquier negocio, la misma está expuesta a diversos riesgos que podrían afectar la información que obtienen, procesan y reportan.

A nivel mundial han ocurrido diversos incidentes relacionados a este tema como, por ejemplo, la divulgación no autorizada de información crítica ocurrida en mayo de 2017, en un ataque dirigido a por lo menos 16 hospitales británicos [2]. Esto se produjo por la intromisión de un virus *malware*, que afectó a los sistemas Windows, a través del cifrado de todos sus archivos y de las unidades de red a las que estaban conectados. Así pues, el usuario no podía acceder a sus ficheros hasta que hubiera realizado el pago solicitado por los delincuentes cibernéticos. Este problema surgió debido a la falta de implementación de una gestión de riesgos que permitiera poner en salvaguarda la información. Este ataque cibernético tuvo como consecuencias el desviar ambulancias, suspender citas rutinarias, la cancelación de citas médicas, problemas informáticos graves y retrasos en cuatro de los establecimientos afectados, por lo que tuvieron que activar el plan para incidentes y mejoras, con el que lograron asegurar el mantenimiento de la seguridad, así como el bienestar de los pacientes. Todo ello generó un gasto aproximado de 100 millones de libras (137 millones de dólares, aproximadamente).

Un caso similar ocurrió en el Hospital Presbiteriano de Nueva York, en donde la información médica se encontraba alojada en servidores con acceso a la nube de Internet, sin contar con medidas de seguridad apropiadas. El ataque cibernético a este hospital ocasionó que la información de 6800 pacientes terminara en los buscadores web. Este ataque se produjo porque no se identificaron a tiempo situaciones de riesgo a las cuales han estado expuestas los servidores. Como consecuencia hubo sendas multas al hospital [2].

Un caso más de nivel internacional, es el ocurrido en el hospital Royal Melbourne en Australia, ocurrido en enero del 2016, el cual sufrió la introducción de un virus informático que causó un caos hospitalario de gran magnitud. Esto trajo como consecuencia que todos los procedimientos médicos que se llevaban a cabo en el sistema informático tuvieran que realizarse solamente en papel [3].

En una investigación realizada en EE. UU. [4], en 2017, se concluyó que, el ataque principal a un hospital es por el robo de la identidad médica y hurto de información de pacientes. Por su parte, en cuanto a las consecuencias, en esta investigación se plantean las siguientes: 1) Un daño dirigido hacia la práctica clínica que derivan en una falta de atención oportuna a los pacientes; 2) Un daño económico por el coste de restaurar sistemas y copias de seguridad; 3) Un daño reputacional hacia la organización derivado a partir de estos eventos.

El sector salud fue uno de los sectores más atacados en los últimos años. De acuerdo con la fuente en mención [5]: "Los cotos de un ciberataque son elevados aproximadamente unos 7.13 millones de dólares" [5].

En el contexto latinoamericano, una lista de hechos similares ocurrió en Brasil [6], en junio del 2018 en los hospitales de Barretos, Jales y Fernandópolis, los cuales se vieron afectados por la intromisión del ramsomware *Wannacry* [7]. Este acontecimiento comprometió la base de datos de los pacientes y degradó el funcionamiento de algunos aparatos, trayendo como consecuencia que miles de pacientes estuvieran desatendidos. En el caso del Hospital de Barretos, el rescate fue de 360 mil dólares para el hospital. Además del impacto financiero, también se vieron afectados los procesos de atención médica, ya que alrededor de 3000 consultas y pruebas fueron canceladas y 350 pacientes quedaron sin radioterapia. Según [8], ha referido que la cantidad de ataques a organismos de salud sigue creciendo a nivel acelerado, ya que el valor de la información de la misma, tiene un elevado nivel de búsqueda y pago en mercados clandestinos.

Colombia no es la excepción, el Hospital San Juan de Dios en Armenia sufrió un ataque el 29 de marzo del 2018 [9]. En donde lograron tener acceso al servidor y encriptar la información del servidor central de la entidad, la cual contenía información de los pacientes. Ante esta situación, la entidad se declaró en emergencia informática hasta el 2 de abril, donde realizaron procesos manuales de historia clínica. Logrando posteriormente recuperar el 98% de de la funcionalidad del servidor.

A nivel nacional, en marzo del 2019 ocurrieron incidentes de seguridad en hospitales del seguro social que habían migrado a un nuevo sistema de información Servicio de Salud Inteligente (ESSI), el cual registraba toda la información de los pacientes [10]. Durante el primer mes de operación, el sistema presentó múltiples fallas que ocasionaron la pérdida de información de pacientes, generando caos y demoras en la atención, conllevando a un deficiente manejo administrativo de los datos.

Otro caso a nivel nacional, es la fiscalización que se realizó en los años 2018-2019 en 40 establecimientos de salud [11], en la cual se detectaron irregularidades en el manejo de los

datos de sus pacientes. Una de ellas fue el incumplimiento sobre la confidencialidad hacia los datos sensibles, otra fue que no se cumplió con el debido proceso de brindar la información a los pacientes en relación a las cláusulas del tratamiento de sus datos (artículo 18 de la Ley de Protección de Datos Personales 'LPDP').

Adicional a ello, otra de las normas quebrantadas fue que incumplieron con, en lo que se refiere a medidas para la seguridad de la información, fue no haber implementado las medidas de seguridad requeridas. Ante ello, la misma organización sugirió a los referidos establecimientos, reforzar todas las medidas de seguridad. Cumpliendo ello, lograría garantizar el tratamiento adecuado de la información.

Prosiguiendo con la mención a los incidentes de seguridad, se mencionará los que han ocurrido a nivel local. Esta información fue proporcionada a través de entrevistas a uno de los integrantes del área administrativa perteneciente a uno de los centros hospitalarios, así como a los directores de TI de cada organización en estudio, tal es así que podemos citar una serie de problemáticas encontradas en diversos hospitales de la región: interrupción de la red hospitalaria, infraestructura inadecuada del área de TI, accesos irrestrictos de usuarios, poco nivel de seguridad de equipos informáticos y ausencia de comunicación entre áreas y departamentos. Como resultado de la entrevista, se concluyó que los hospitales han sido víctimas de ataques informáticos, incidentes de seguridad, etc., que han generado pérdida de información, interrupción del servicio y pérdidas económicas.

Una manera de contrarrestar estos resultados es, mediante la gobernanza de la seguridad de la información, que permita asegurar el resguardo de la información crítica. Sin embargo, se constató que los 4 hospitales a nivel local no tienen definido un modelo del mismo con ese nivel de enfoque, o tampoco manejan una bitácora de incidencias que afecten la misma, es decir, no documentan acciones para gestionarlas, algo necesario en una organización grande y compleja como lo es un hospital. También otra de las problemáticas encontradas es que no existe un área encargada de la Seguridad de la Información a nivel de redes asistenciales, lo cual es un punto crítico que debe tener atención total, ya que, sin una gestión de seguridad correcta, la organización se ve expuesta a una serie de vulnerabilidades cuyas consecuencias podrían verse reflejadas como en los casos mencionados con anterioridad.

De acuerdo a las diferentes opiniones emitidas por el personal directivo de TI de cada hospital en estudio, indicaron que una de las áreas más críticas corresponde al área de Emergencias, ya que es ahí donde la atención requiere realizarse de manera eficaz al poner en peligro inminente la vida de los pacientes, además de ello, el manejo de la información es

bastante sensible con respecto a otras áreas, por la cual el resguardo de la misma debe mantener altos niveles de seguridad (Ver Anexo 04).

Por lo antes expuesto, se plantea la siguiente interrogante: ¿De qué manera la implementación de un modelo de gestión de riesgos puede impactar en la seguridad de la información sobre los procesos de atención de emergencia del sector Salud pública de la región Lambayeque? Ante ello, se propuso como hipótesis que, si se implementa un modelo de gestión de riesgos contribuirá a la seguridad de la información en los procesos de atención de emergencia del sector Salud pública de hospitales de la región Lambayeque.

El objetivo general de la presente investigación es, desarrollar un modelo de gestión de riesgos para contribuir a la seguridad de la información en los procesos de atención de Emergencias para el Sector Salud pública de Lambayeque. Con este propósito, se planteó:

- Analizar comparativamente marcos de trabajo y normativas de riesgos de seguridad de la información a través de características que permitan armonizar la propuesta de un modelo de gestión de riesgos adaptado a la realidad del sector Salud Pública.
- Seleccionar las fases alineadas a los procesos de emergencias del sector Salud Pública, que permitan determinar el nuevo modelo de gestión de riesgos de Seguridad de la Información.
- Validar el modelo de gestión de riesgos basado en marcos de trabajo estandarizados, mediante juicio de expertos, para valorar el modelo adaptado.
- Implementar de manera parcial el modelo de Gestión de Riesgos para mejorar la Seguridad de la Información en los hospitales del sector Salud Pública de la región.

Con respecto a su justificación en el ámbito social, el presente trabajo presentó un modelo que, una vez implementado, permitirá que la información en salud se encuentre protegida, completa, correcta y disponible de manera oportuna para el personal de salud. En relación al ámbito científico, contribuye al conocimiento con lo cual se genera un antecedente para futuros investigadores, y la importancia de la aplicación de un modelo hacia el sector Salud. En el ámbito tecnológico, permite mejorar la gestión de Tecnologías de Información, al brindar mecanismos útiles que permitan proteger la confidencialidad de la información, al aplicar controles que contrarresten las amenazas que afecten a cada uno de ellos, de acuerdo al contexto del negocio. Y, por último, en el ámbito económico, logrará que, mediante la implementación del modelo, reducirá los riesgos a los cuales se encuentre expuesto la organización en estudio, disminuyendo toda actividad impropia que implique una posterior reparación económica para contrarrestar la materialización de cualquier amenaza.

2. Revisión de literatura

2.1 Antecedentes

Para fundamentar la alternativa de solución propuesta se muestra a continuación algunas investigaciones previas que dan soporte a la actual al presente estudio, teniendo:

Según Ordeñana [12] , hay una problemática existente en una institución dirigida al sector público, indicándose la exposición existente de sus recursos tangibles e intangibles, causando una serie de riesgos que influenciaron en las metas y objetivos organizacionales. Teniendo como conclusión que, la implementación de la Norma ISO/IEC ISO 27005 puede optimizar el tiempo de ejecución. En nuestra investigación se propone un modelo de gestión de riesgos dirigida hacia el hospital, que viene a ser igualmente de nivel público, la misma que tendremos en cuenta como base para nuestro modelo propuesto.

En el caso de Rovira [13], existe una serie de problemáticas que se manifiestan en distintas organizaciones, las cuales padecen con frecuencia ataques informáticos, teniendo como consecuencias perdidas, sanciones o hasta el mismo cierre de la empresa por la manipulación de la información. Se propuso el uso de marcos metodológicos que permitirá mejorar prácticas y gestión de las tecnologías de información. Al finalizar, se resaltó al marco COBIT, el cual permite abarcar toda la organización y gobierno de TI, al igual que en nuestro caso, estaremos limitándonos de acuerdo a los recursos disponibles, como al presupuesto del centro hospitalario.

En la investigación de Brand [14], hay una problemática existente en el área de tecnología de la empresa AXEDE S.A., ya que no disponen de adecuada gestión de controles de seguridad, tampoco cuentan con normas que ayuden a gestionar la Seguridad de la Información, lo que conlleva a una falta de confianza hacia los trabajadores y proveedores, quebrantando las normas propias del negocio. Es por ello que han buscado desarrollar un diseño de Sistema de Gestión de Seguridad de la Información sustentado en la norma NTC ISO/IEC 27001:2013, que busca el fortalecimiento de los procesos de la respectiva área, obteniendo como resultado una efectiva gestión de Seguridad de la Información, ya que se establecieron controles y planes de tratamiento de acuerdo a la norma planteada, implementando técnicas de protección de los activos de información en búsqueda del cumplimiento de los objetivos empresariales, y en colaboración con la presidencia, se logró minimizar los daños ante posibles culminaciones de amenazas. Respecto a este antecedente en relación con la investigación actual,

busca crear conciencia hacia su personal sobre Seguridad de la Información, logrando un fortalecimiento organizacional ante la materialización de un incidente de seguridad.

En el contexto nacional, de acuerdo con Mere [15], muestra una problemática existente en el sector Telecomunicaciones, debido a la incorrecta gestión de sus riesgos. Como solución, se propuso el desarrollo de una gestión de riesgos basado en estándares internacionales, que permita mantener el respectivo cumplimiento sobre las principales leyes, identificando posibles riesgos sobre la seguridad de la información, fortaleciendo los controles existentes e implementar nuevos. En esta investigación se hizo uso de otra norma para una correcta gestión de Riesgo, la ISO/IEC 31000 hacia una empresa del sector Telecomunicaciones, permitiendo influir en un manejo adecuado de riesgos, que vaya en relación a ese rubro laboral, a diferencia de nuestra investigación que tomará en cuenta la ISO 27005, ya que está dirigido específicamente a salvaguardar la información.

Según Carmona [16], muestra la importancia de implementar una adecuada gestión de seguridad de la información en el Instituto Nacional de Salud (OGITT), Lima, ya que entre sus riesgos identificados, está el de pérdida de archivos de investigación, así como otros riesgos en relación a la falta de concientización del personal y fallas en la infraestructura física de la organización, es por ello que esta investigación propone la evaluación de la gestión de riesgos en base a la norma NTP-ISO/IEC 27005:2018, ya que ésta proporciona directrices para la gestión de Riesgos para la Seguridad de la información, logrando identificar 104 activos de información, 38 de ellos en estado Muy Crítico y Crítico en la primera fase, derivándose éstos a distintos niveles de riesgo (Extremo, Alto, Mediano y Bajo), logrando reducir la amenazas a los que se encontraban expuestos en sus diferentes áreas.

García [17], en su investigación, muestra a través de indicadores estadísticos, que 4 de cada 10 empresas han sufrido una brecha de seguridad de la información entre los años 2016-2018, y menos del 1% cuenta con indicadores que evalúen la seguridad de la información. Como objetivo se propuso realizar la implementación de un modelo de gestión conforme a la norma ISO. Como resultado de esta implementación, se pudo conocer los riesgos de seguridad de información expuestos a distintos niveles de criticidad, se utilizó la metodología OCTAVE-S y la norma ISO/IEC 27005, misma que aplicamos a nuestra investigación, la cual ayudó obtener resultados satisfactorios.

Según Banda [18], en la región de Lambayeque se planteó como objetivo mejorar la seguridad de los activos de información mediante el desarrollo de un modelo basado en un enfoque de gestión de riesgos de TI. Obteniendo la identificación de escenarios de riesgos, proponiendo proyectos que permitan disminuir los niveles de riesgos existentes. La conexión

entre la presente tesis y este estudio es el uso de normas y estándares similares que apuntan al mismo objetivo.

En la investigación de Medianero [19], plantea el desarrollo de un Modelo de Gestión de Seguridad de la Información orientado a instituciones de salud, esto con el fin de apoyar los procesos de atención al paciente y la seguridad de la información. Se identificó, 26 riesgos clasificados en impacto critico 23.08% y alta magnitud 26.92%. A la vez, se dio la propuesta de 4 proyectos, demostrando que el modelo mejoró los procesos de atención al paciente. Esta investigación está relacionada con la tesis planteada, la cual también el caso de estudio tiene que ver con los hospitales del sector público, y viene a brindar un aporte hacia la Seguridad de la Información.

Según Villegas [20], esta investigación propuso una solución para los riesgos que rodean en forma constante a los activos críticos de los hospitales. Esta solución, al ser implementado, facilitarán la gestión de riesgos. Esta propuesta se convirtió en un modelo de gestión de riesgos TI que contribuya a la protección de los activos de información. Este estudio está relacionado con la investigación actual, ya que también está destinada a hospitales públicos, y ofrece una solución que ayudaría a reducir los riesgos asociados a los activos de información.

2.2 Bases teóricas

2.2.1 SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la norma española UNE 71504:2008 [21], "es la confianza que los sistemas de información deben estar libre de peligro o daño". Otra definición de acuerdo al informe del sitio web [24] es: "conjunto de medidas usadas para salvaguardar los datos de una organización". Se debe considerar que la seguridad de la información se define como asegurar el activo de información que está debidamente clasificado para su confidencialidad [25].

2.2.2 GESTIÓN DE RIESGOS

Según Rowe [22] "El riesgo es la posibilidad de sufrir daños o pérdidas. Es el potencial para darse cuenta de las consecuencias negativas no deseadas de un evento." Quiere decir que debe haber una situación en la que pueda ocurrir una acción indeseable, la cual es provocada por una persona o medio atmosférico, resultando por defecto un impacto o consecuencia negativa. Otra definición de riesgo se encuentra en Magerit [23], la cual indica que el riesgo es la valoración del nivel en que un peligro se materialice y perjudique a la organización. ISO/IEC

27005 define al riesgo, en este caso enfocado a la seguridad de información como “el potencial de que una amenaza explote las vulnerabilidades de los activos información” [24].

2.2.3 NORMAS Y METODOLOGÍAS DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En este apartado se recoge un conjunto de normas y metodologías de gestión de riesgos enfocado en la seguridad de la información, que a través de su respectivo análisis nos ayudará a brindar una propuesta de modelo enfocado en los servicios de atención de Emergencia para resguardar la información crítica y confidencial.

a) Norma NTP-ISO/IEC 27005

Esta norma brinda directrices generales para gestionar el riesgo de la seguridad de la información, siendo una guía para implementar de manera satisfactoria la seguridad de la información enfocada en riesgos aplicada a cualquier tipo de organización. Su estructura está conformada de la siguiente manera:

- Capítulo 7: Establecimiento del contexto, apoyado por el Anexo A.
- Capítulo 8: Evaluación del riesgo, apoyado por el anexo B, C, D y E.
- Capítulo 9: Tratamiento del riesgo, apoyado por el anexo F.
- Capítulo 10: Aceptación del riesgo.
- Capítulo 11: Comunicación del riesgo.
- Capítulo 12: Seguimiento y revisión del riesgo.

Cada actividad de la gestión del riesgo se organiza de la siguiente manera: Entrada, Acción, Guía de implementación y Salida.

b) Marco COBIT 5 para riesgos

COBIT 5 para riesgos es un marco que analiza los riesgos relacionados a TI. Entre sus beneficios está el brindar una guía para poner en práctica este marco, que va dirigido hacia las funciones de gobierno y gestión de riesgo en la organización a través del uso de siete facilitadores o habilitadores de COBIT 5:

- Principios, políticas y marcos: Ofrece una selección de principios, políticas y marcos de referencia relevantes para el gobierno y la gestión de riesgos en la organización.
- Procesos: Brinda una lista de procesos clave y procesos de soporte para el gobierno y la gestión del riesgo.
- Estructuras organizativas: Muestra una lista de roles organizacionales necesarios para el gobierno y la gestión del riesgo en la organización.
- Cultura, Ética y Conducta: Describe el comportamiento necesario para conseguir un adecuado gobierno y gestión del riesgo.
- Información: Se realiza cuando necesitan la información al asumir sus funciones, actividades y comunicación con los demás. Entre sus elementos tenemos a Perfil de riesgo, Plan de acción de riesgos, Plan de comunicación de riesgos, mapa de riesgos, etc.
- Servicios, Infraestructura y Aplicaciones: Se refiere a la lista de servicios, infraestructura y aplicaciones que se refieren para llevar a cabo una gestión adecuada del riesgo en la organización.
- Personas, Habilidades y Competencias: Trata sobre las distintas habilidades y competencias de los participantes de la gestión del riesgo.

c) Metodología MAGERIT

Magerit busca una aproximación metódica, para que los altos directivos tomen acuerdos considerando riesgos relacionados con TI y así determinar la seguridad de sus activos de información. Entre sus objetivos está el concientizar a los altos directivos sobre la importancia del análisis y gestión de riesgos, ofreciendo un método sistemático para sus análisis, planificando las medidas de protección necesarias para mitigar los riesgos y tenerlos bajo control.

d) Metodología OCTAVE

Es una técnica de evaluación de riesgos [25], desarrollada para organizaciones de más de 300 empleados, en la que fomenta la participación de reuniones o talleres entre personal y los analistas de riesgos, dividido en las siguientes etapas: La primera, “Crear perfiles de amenazas basadas en activos”, en la cual en los procesos 1 al 3 recopilan una serie de

conocimientos en lo que se refiere a activos, requisitos de seguridad, áreas de preocupación, estrategias de protección actuales y vulnerabilidades de la empresa, y en el proceso 4 prepara un perfil de amenaza con los activos críticos recopilados. La fase 2 denominada "Identificar las vulnerabilidades de la infraestructura", en la cual los procesos 5 y 6 revisan las vulnerabilidades de la empresa aplicada a los activos críticos y componentes clave pertenecientes a esos activos.

Por último, está la fase 3 "Desarrollar planes y estrategias de seguridad", en la cual los procesos 7 y 8 reúnen la información de los activos críticos, y crea estrategias de protección para contrarrestar esos riesgos, siendo éstos previamente aprobados por los altos directivos de la organización.

2.2.4 REFERENCIAS NORMATIVAS QUE RECONOCEN Y GARANTIZAN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN SALUD

2.2.4.1 Datos Personales

Son toda aquella información que permite identificar a una persona (nombre, dirección, etc), teniendo estos datos una relación directa con el conjunto de tareas desarrolladas en la actividad diaria, siendo los datos personales un derecho fundamental para reservar la intimidad personal y familiar ante cualquier tratamiento irregular [26].

2.2.4.2 Constitución Política del Perú

Siendo de vital importancia la protección de datos personales, dentro de la Constitución, en el artículo 2, citaremos algunos derechos:

> 6) Los servicios informáticos no suministren información que afecta la intimidad personal.
> 10) Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

La clasificación de los datos personales, en lo que se refiere a los artículos citados, guarda un estricto nivel de confidencialidad, el cual no puede ser vulnerado, ya que estamos quebrantando normas que recaerían en una estricta consecuencia legal para el responsable.

2.2.4.3 Ley de Protección de Datos Personales (LPDP) o Ley N.° 29733

La protección de datos personales es vital, sobre todo la que se maneja dentro del área de Emergencia, fundamentándose además en la ley N° 29733, en la cual encontramos como objetivo garantizar la protección de los datos personales, brindando el respectivo tratamiento, manteniendo el respeto por los derechos fundamentales [32].

2.2.4.4 Ley N.° 26842, Ley General de Salud

De acuerdo al Artículo 25, en ella indica que la información relativa al acto médico que se realiza es completamente privada. El profesional en el sector Salud, no puede divulgar la información del acto médico, ya que estaría penado e incurriría en no cumplir con los respectivos códigos de Ética Profesional [27].

2.2.4.5 Directiva Administrativa N° 294-MINSA/2020/OGTI

Hace referencia sobre el uso adecuado de los datos personales relacionados a la salud, con el fin de no violar la intimidad personal. También se basan en la Ley N° 26842 – Ley General de Salud, en donde decreta el que el personal de salud, debe salvaguardar la información relacionada. Dentro de sus referencias también se encuentra la Ley N.° 27806 – Ley de Transparencia y Acceso a la Información Pública [33].

2.2.5 SALUD PÚBLICA

La salud pública viene a tener como objetivo la salud de la población, organizada por las administraciones públicas en conjunto con la sociedad [28]. Está formada por los siguientes organismos:

- El Seguro Social de Salud (EsSalud)
- Fuerzas Armadas (FFAA) y Policía Nacional del Perú (PNP)
- Ministerio de Salud (Minsa)

2.2.5.1 Prestaciones de salud

Prestaciones son beneficios brindados por empresas públicas, privadas o por parte del Estado, ellas brindan a sus empleados o ciudadanía en general, servicios de diferentes tipos,

acordados por un convenio en ambos lados para hacer utilización de ello [29]. EsSalud es un organismo que brinda atención en lo que se refiere a prestaciones de salud, económicas y sociales. Entre las prestaciones de salud se brindan los diferentes servicios, los cuales se redactan en la siguiente imagen, originándose en el punto de Atención de Salud.

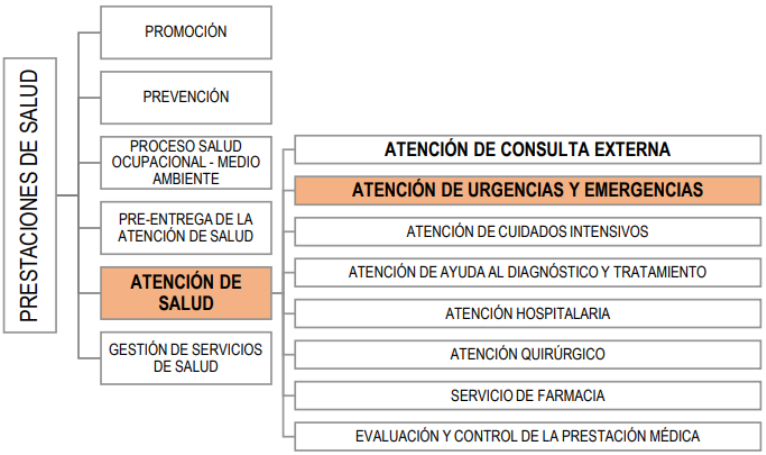


Ilustración 1: Actividades relacionadas a los servicios de Atención en Salud, resaltando la atención de Urgencias y Emergencias. [30]

Uno de los servicios que brinda las Prestaciones con atención de Salud, es Emergencia. Emergencia viene a ser una condición repentina que requiere atención prioritaria al poner en peligro la vida o salud del enfermo [30].

Los servicios que proporciona Emergencia se clasifican en 5 prioridades:

- Prioridad I - Resucitación: paciente que pone en riesgo su vida de manera súbita.
- Prioridad II - Emergencia: paciente que requiere atención médica de intensidad media dentro del rango de un tiempo riesgoso.
- Prioridad III - Urgencia: se refiere al enfermo cuyo riesgo de vida no está comprometida y solo requiere evaluación y atención médica.
- Prioridad IV - Urgencia menor: paciente que presenta una lesión comprometedora y cuyo cuidado en rangos periódicos.
- Prioridad V - Sin Urgencia: se refiere al paciente que no presenta compromiso de algún órgano o sistema y sin necesitar algún cuidado urgente.

3. Materiales y métodos

3.1 Diagnóstico de las empresas del sector Salud Pública

Los hospitales en el país, se localizan geográficamente de manera agrupada en distintas redes asistenciales. La red asistencial Lambayeque, denominada "Juan Aita Valle", agrupa al Almanzor Aguinaga Asenjo, Luis Heysen, Naylamp y Agustín Arbulú Neyra. La Red Asistencial mencionada, al estar dentro de los lineamientos de gobierno de EsSalud, presenta una descripción a nivel de organización, cuyo contenido lo podemos ver con más detalle en el Anexo 01. Allí mismo, se mencionan los 4 hospitales, de los cuales 3 son materia de nuestra investigación. Bajo nivel jerárquico, el área de Emergencias, denominado "Departamento de Emergencias y Áreas Críticas" se encuentra supervisado por la dependencia denominada Gerencia Clínica (ver Anexo 02).

EsSalud tiene como misión ofrecer servicios de salud, económico y social al sector asegurado, brindando una atención eficiente, que proporcione el cuidado económico de un servicio integral, y como visión está el buscar ser una institución de características modernas y en constante mejora, enfocándose en la población asegurada, ofreciéndole a ellos un acceso a la seguridad colectiva en temas de salud con ética, oportunidad y calidad. Entre sus principios está la "Solidaridad, Universalidad, Igualdad, Unidad, Integralidad y Autonomía" [31] .

De acuerdo a la encuesta dirigida a las respectivas organizaciones, con el fin de determinar un diagnóstico actual de riesgo, se planteó una serie de preguntas al área de TI (ver Anexo 03), observándose que el total de ellos no contaba con un modelo implementado de Gestión de Riesgos, eso quiere decir que no cuentan con una administración de Riesgos definida, el cual permita mejorar la Seguridad de la Información de la organización, así mismo tampoco cuentan con una bitácora de incidencias que afecten la seguridad de la misma.

Otro de los cuestionamientos fue si la empresa brinda capacitación o genera algún tipo de esquema de concientización en relación a la Seguridad de la Información, de la cual solo un hospital indicó que sí se realizaba, eso quiere decir que la totalidad encuestada no muestra su principal enfoque en brindar una orientación y reflexión sobre el tema, que permita concientizar al personal sobre la importancia de resguardar y proteger la información en cualquiera de sus áreas. En otra de las preguntas, el 67% sí toma medidas para mitigar los riesgos de seguridad de la información, lo cual está directamente relacionado con la normativa que Essalud dictamina

para todos los centros médicos. También, un 67% manifiesta que tiene planes y procedimientos para poner en resguardo las instalaciones, los edificios y las áreas restringidas, y el 100% guarda un acuerdo de confidencialidad al momento de compartir la información con otras organizaciones, lo cual es entendible, ya que se trata de datos privados del paciente. Así mismo, el 100% reveló que sí tienen normas para regular el acceso físico a las áreas de trabajo, hardware y medios de software, la cual está relacionada con el compendio de órdenes que emite Essalud, sin embargo, como se mencionó líneas arriba, no existe una herramienta que permita regular a nivel de cada empresa, los riesgos de seguridad de información que se pueda presentar.

En caso se presente una situación crítica en el negocio, los servicios complementarios de Emergencia que debe seguir operando fueron varios, destacando Rayos X, Hospitalización y Sala de Operaciones como los más mencionados, seguido de Traumashock, Laboratorio, TI y Diagnóstico, debido a que un paciente, para estos casos críticos en lo que su vida está en riesgo, tiene que tener como soporte las otras áreas mencionadas, y asegurar la estabilidad del asegurado. El servicio de Emergencia interactúa con casi todas las áreas del hospital para la transferencia de información, logrando ser una de las áreas con mayor relevancia en el centro médico. Por último, todos coinciden en que la Historia clínica es la información vital para la ejecución de los procesos del área de Emergencia. El análisis gráfico se visualiza en el anexo correspondiente (ver anexo 04).

A través del Manual de Operaciones del Hospital y Manual de Procedimientos del área de Emergencias, se determinaron los procesos más importantes de la atención de Emergencias, para establecer lineamientos que orienten y proporcionen criterios adecuados para la implementación de la Gestión del Riesgo. En el siguiente cuadro mostraremos los mismos, junto a los usuarios responsables en cada uno de ellos (ver Anexo 05). Entre los usuarios que destacan en los procesos de Emergencia, mencionamos al médico, enfermera(o), técnico de enfermería y tecnólogo. Información adicional sobre los hospitales, nuestro objeto de estudio, se encuentra en el siguiente Anexo (ver Anexo 06). Entre las funciones principales del servicio de Emergencia en la región Lambayeque tenemos las siguientes (ver Anexo 07). A continuación, se muestra una tabla que muestra la diferencia los servicios que ofrece Emergencias en diferentes hospitales (ver Anexo 08).

3.2 Tipo y nivel de Investigación

La presente investigación es Cuantitativa – Exploratoria, porque se ha formulado una hipótesis que oriente este estudio, se ha precisado las variables de la misma, definiéndolas conceptualmente, y también se ha definido operacionalmente las variables de la hipótesis. Así mismo se ha utilizado preguntas específicas con posibilidades de respuesta predeterminadas y estos datos se analizaron estadísticamente.

3.3 Diseño de Investigación

Se utilizó un método de diseño pretest – postest y un diseño de Contrastación Pretest y Posttest.

GE = O1 X O2

Donde:

- GE = Grupo Experimental
- O_1 = Seguridad de la información de los procesos de Emergencia en el sector Salud Pública de hospitales de la región Lambayeque, antes de aplicar el modelo de Gestión de Riesgos.
- X = Modelo de Gestión de Riesgos basado en normas y metodologías para mejorar la Seguridad de la Información.
- O_2 = Seguridad de la información de los procesos de Emergencia en el sector Salud Pública de hospitales de la región Lambayeque, después de aplicar el modelo de Gestión de Riesgos.

3.4 Población, muestra y muestreo

Los hospitales en consideración son los siguientes:

Nombre	Nivel	Ubicación
Hospital Almanzor Aguinaga Asenjo	III – 1	Av. Jorge Chavez - Chiclayo
Hospital Luis Heysen	II	Km 3.5 Carretera Pimentel
Hospital Naylamp	I	Francisco Bolognesi 14008

Tabla 1: Actividades relacionadas a los servicios de Atención en Salud, resaltando la atención de Urgencias y Emergencias. [30]

La población considerada para esta investigación tomó en cuenta inicialmente los trabajadores de los hospitales del sector Salud pública de la región Lambayeque. En ellos se determinó la cantidad de trabajadores del área de atención de Emergencias y del área de TI, que son los que llevarán a cabo la propuesta del modelo. En el caso de estudio que estamos desarrollando, la población accesible son los 3 hospitales del sector Salud Pública de la Región Lambayeque. En ellos se aplicará el cálculo de la muestra, y los instrumentos diseñados en esta investigación. Las áreas de los hospitales que fueron relevantes para el desarrollo del trabajo y la recopilación de la información, fueron las siguientes: Atención de Emergencia junto al área de TI que brinda soporte a ésta.

3.5 Técnicas e instrumentos de recolección de datos

Seguidamente, para obtener los aspectos relacionados, se aplicó como técnica la entrevista a una persona con un puesto dentro del área de Informes para poder recoger lo relacionado con el manejo de la información como parte de los procesos de emergencia. Se tomó en cuenta entrevistar a personas cuyo cargo en el centro de salud lleva una relación con el manejo de información relacionado a los procesos de emergencia: estos roles son el director de TI y servicio de admisión. Teniendo como técnicas:

a) **Análisis de información:** Se analizaron la norma NTP ISO 27005, marco COBIT 5 para Riesgos, metodología Magerit y metodología Octave, con la finalidad de sintetizar un modelo de gestión de riesgos de seguridad de la información, que permita guardar relación a los procesos de Emergencia de un hospital.

b) **Recopilación de datos:** se obtuvo la información en fuentes confiables para llegar al armado de la investigación, y que representaron un insumo para la misma. Entre la información que fue recopilada, está el Manual y Procedimientos del Proceso de Atención de Salud, con énfasis en atención de Urgencias y Emergencias, cuyo informe influyó en la obtención de mayor conocimiento respecto a los procesos que participan con Emergencias, y el flujo de información que viaja a través de ellos. Otra información obtenida fue con respecto al Manual de Operaciones (MOPE) del hospital en estudio, en la cual se extrae información como su finalidad, naturaleza jurídica y funciones, además de sus unidades orgánicas.

c) **Entrevista:** Se realizaron una serie de preguntas a un ingeniero de sistemas que pertenece al área de TI de uno de los establecimientos de salud, con el objeto de identificar los activos de información críticos, vulnerabilidad y amenazas. A su vez se tomó en cuenta interrogar al director del área de TI, para tener un panorama más amplio del contexto e infraestructura en que son manejados los procesos principales y los activos relacionados a la información. También se logró entrevistar a los usuarios respectivos de los procesos de Emergencia en estudio, para conocer a plenitud las labores que realiza, el flujo de la información y los activos informáticos imprescindibles para su funcionamiento.

d) **Encuesta**: Se estableció un conjunto de preguntas preparadas con una serie de alternativas sobre la gestión de riesgos, dirigido al director de TI de cada organización en estudio, que permitió establecer los activos y procesos más importantes, que ayudarán a la fase del Contexto de la organización de la Gestión de Riesgos.

3.6 Procedimientos para el procesamiento de datos

En base a las técnicas e instrumentos de recolección de datos mencionados, describiremos el procedimiento con el que se realizó el procesamiento de datos, se realizó encuestas de forma manual a los hospitales en estudio (ver anexo 15), respectivamente al responsable o director de cada área de TI, se establecieron preguntas abiertas y cerradas con la intención de recopilar los datos relevantes de la institución y una información general sobre activos de información en el área, siendo procesadas con el software ofimático Excel, comparando los resultados, finalizando con análisis y gráficos estadísticos.

Describiendo a detalle, en el caso de Análisis de información de las normas y metodologías mencionadas, se necesitó integrar, comparar y homogeneizar los diferentes procesos con las respectivas fases, alineadas a los procesos de Emergencia, consiguiendo así, un modelo armonizado. En lo que respecta a Recopilación de datos, se obtuvo un panorama claro en lo que respecta a los procesos de Emergencias del hospital, desde el ingreso hasta la salida del paciente, los documentos físicos y virtuales que fluyen durante todos los procesos; y en base al MOPE, se conoció la estructura de la organización, enfocándose principalmente en Emergencias, y las unidades jerárquicas tanto a nivel superior como inferior, así como una información general de la institución.

En el caso de la Entrevista, a través de los distintos usuarios, se logró unificar la información para proceder a clasificar los activos, conocer las amenazas y vulnerabilidades del área en estudio, y poder categorizar los riesgos en base a ello, así como dar a conocer las medidas de protección necesarias que vayan en armonía con la naturaleza de la institución. Por último, en el caso de Encuesta, se estableció una serie de preguntas abiertas y cerradas, elaborada a los directores de área de TI de la institución, así como obtener un conocimiento general de lo que tienen ellos en lo que respecta a sus activos informáticos y como estos brindan soporte a Emergencias, conociendo a partir de allí la importancia de establecer una Gestión de Riesgos para mejorar la Seguridad de la Información del área en estudio.

4. Resultados y Discusión

A continuación, vamos a hacer la presentación de los resultados de acuerdo al orden de los objetivos específicos.

4.1 Resultado para el objetivo específico 01

"Analizar comparativamente marcos de trabajo y normativas de riesgos de seguridad de la información, a través de características que permitan armonizar la propuesta de un modelo de gestión de riesgos adaptado a la realidad del sector Salud Pública."

En torno a este objetivo se obtuvieron los siguientes resultados: Análisis de Estándares, Marcos de Trabajo y Metodologías y la creación de un cuadro resumen con las características comunes para implementar en las fases de la Gestión del Riesgo, y crear un modelo armónico del mismo.

- Análisis de Estándares, Marcos de Trabajo y Metodologías: Se realizó una lectura y análisis de los documentos (NTP-ISO/IEC 27005, Cobit 5 para Riesgos, Magerit y Octave), contrastando la información de sus fases y procesos con la organización del área de Emergencias y el área de TI que brinda soporte a ésta.
- Creación de un cuadro resumen: Se elaboró un cuadro que establece las semejanzas y diferencias de las difentes fases y actividades de cada una de las normas y estándares (Ver Anexo 09).
- Modelo armónico: A través de la anterior etapa, se procedió con el proceso de homogeneización, propuesta adaptada de Pardo [32], en la que se estableció una armonía con los modelos referidos, estableciendo estructuras comunes en los procesos, permitiendo elaborar un cuadro que determine las fases y procesos a utilizar en nuestro Modelo de

gestión de riesgos con las normas y estándares que se tomarán en cuenta en cada una de ellos (Ver Anexo 10).

Seguidamente, vamos a describir con más detalle los resultados correspondientes:

Análisis de Estándares, Marcos de Trabajo y Metodologías

A) *Norma NTP-ISO/IEC 27005*

Esta norma técnica peruana brinda conceptos generales para gestionar el riesgo de Seguridad de la Información, acompañada de la descripción de sus actividades. La descripción de las fases se basa en la metodología ISO 31000, en la cual muestra una vista de alto nivel de la gestión del riesgo, y la cual, aplicado a la NTP-ISO/IEC 27005 sería de la siguiente manera:

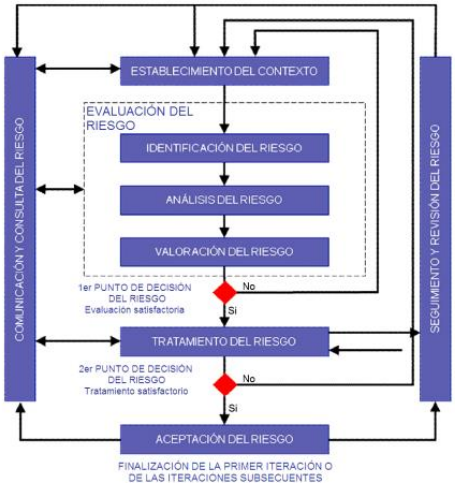


Ilustración 2. El proceso de gestión del Riesgo de seguridad de la Información según NTP - ISO 27005

Bajo ese enfoque hemos considerado aplicar 4 fases de la normativa para nuestro modelo de Gestión de Riesgos, la primera etapa, denominada “Establecimiento del contexto”, la cual busca recopilar toda la información relevante de la institución para una adecuada gestión del riesgo, en la cual la división de este proceso, Contexto Interno y Externo, fueron necesarias para conocer el alcance y límites de la misma.

La siguiente fase fue “Evaluación del riesgo”, esta etapa indica que, una vez recopilada la información de la fase anterior, se analicen los riesgos propios del área de Emergencia junto a la de TI, la cual brinda soporte a ésta. Seguidamente determinamos los procesos de Emergencia necesarios para nuestro análisis del riesgo, así como el área de TI en su totalidad, establecemos los activos de información, analizamos las amenazas y vulnerabilidades existentes, en el caso de estas últimas, la norma muestra ejemplo de las mismas, la cual nos ayudará a identificar vulnerabilidades en ambos espacios, luego de ello procedemos a

identificar los riesgos y darle su respectivo valor, finalizando esta etapa con la priorización de riesgos.

Luego tenemos la fase “Tratamiento del riesgo”, en la cual menciona proponer una lista de controles o medidas de protección adecuadas para minimizar, aceptar o evadir los riesgos, producto de la evaluación de las mismas para el área de Emergencias y TI. Finalmente tenemos la fase “Comunicación y consulta del riesgo”, la cual considera documentar toda la información, misma que fue obtenida durante las actividades de gestión del riesgo, y que será dirigida a los altos directivos de la institución. Todo el proceso de comunicación será llevado a cabo con el personal de las áreas que participan en el proceso de Gestión de Riesgos, como son los médicos, enfermeras del área de Emergencia, así como ingenieros y técnicos del área de TI, con el fin de que se obtenga una mayor comprensión del proceso que se está realizando.

B) Marco COBIT 5 para riesgos

De acuerdo a este marco [33], describe la manera en la que COBIT puede aplicarse hacia las necesidades de riesgo específicas, a través de siete facilitadores o habilitadores, los cuales hemos considerado 3 de ellos para nuestra investigación:

— Procesos: Habla sobre los procesos principales del riesgo (EDM03: Asegurar la optimización del riesgo, y APO12: Gestionar el riesgo), junto a otros procesos secundarios para la función de riesgos. En el caso de EDM03, implica el aseguramiento del apetito y la tolerancia al riesgo, de manera que sea comprensible para los implicados entre los que gestionan el riesgo. En APO12 encontramos actividades importantes como es el “Recopilar datos”, necesarios para identificar y recopilar datos relevantes sobre la institución y las áreas principales como son Emergencias y la estructura de TI que brinde soporte a sus procesos. Otro de los procesos a considerar fue “Definir un portafolio de acciones para la gestión de riesgos”, necesario para reducir el riesgo a un nivel aceptable para la institución. Otra de las actividades “Responder al riesgo” que implica establecer normas de protección que contrarresten los riesgos en ambas áreas mencionadas, y por último tenemos a “Evaluar la gestión de riesgos”, se trata de definir un conjunto de indicadores de riesgo que permitan la identificación y monitoreo del riesgo actual en ambas áreas.

— Cultura, Ética y Comportamiento: Se refiere a la conducta de la institución, que es una característica que influye para que el gobierno del riesgo sea exitoso.
— Información: Menciona a los elementos de información necesarios para que la gestión del riesgo sea eficiente y efectiva. Allí habla sobre Escenario de riesgos, en la cual consideramos a los actores (responsables) de que ocurra el riesgo, las amenazas existentes, los eventos y el activo que es afectado, tanto en el área de TI como en la de Emergencias, también vemos el Plan de acción de riesgos, en la cual define a los responsables de aprobar e implementar el plan, el conjunto de acciones propuestas, los recursos que implica y el tiempo necesario para su implementación.

En la siguiente imagen visualizamos un enfoque genérico de la metodología Cobit 5 para Riesgos, en la cual menciona como punto central a los habilitadores:

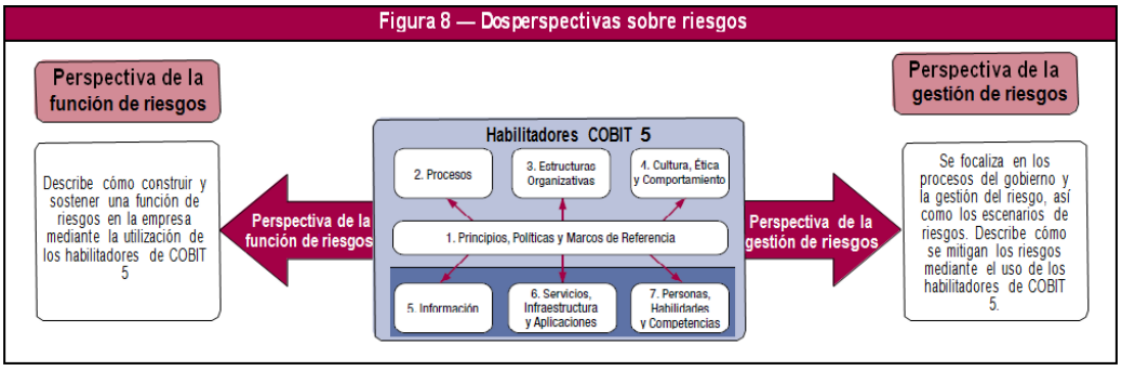


Ilustración 3: Las dos perspectivas ilustradas sobre gestión de riesgos (COBIT 5 para Riesgos)

C) Metodología MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) tiene como base la norma ISO 31000, en la cual hace mención al "Proceso de Gestión de los Riesgos" [23]. El siguiente gráfico muestra las diferentes etapas del marco de referencia mencionado, en la cual la fase que trata sobre la Implementación de la gestión de riesgos (fase 4.4), hace uso de la metodología Magerit.

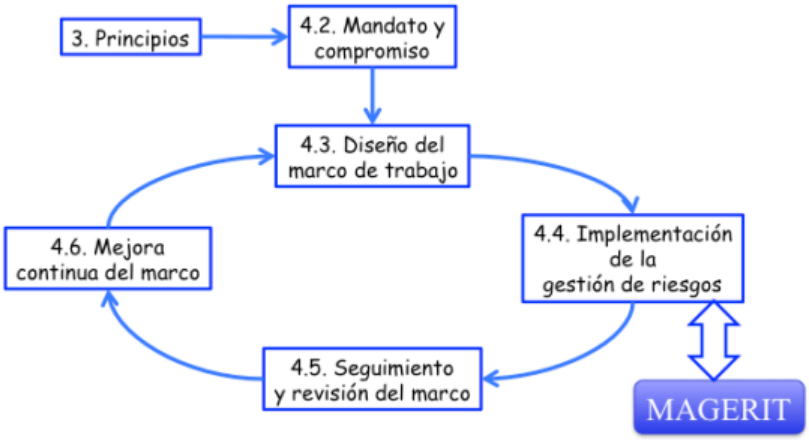


Ilustración 4. ISO 31000 - Marco de referencia para la gestión de riesgos, en la cual la etapa 4.4 hace referencia a la implementación de la metodología MAGERIT

Bajo este enfoque hemos considerado el catálogo de activos, amenazas y Salvaguardas, así como una guía para el análisis de riesgos, mismos que ayudaron al desarrollo de la propuesta del modelo. Mediante el catálogo de activos, clasificamos los mismos, y determinamos las dimensiones y criterios de valoración de Emergencias y la estructura de TI que brinde soporte a sus procesos, el catálogo de amenazas, implica que los analistas de riesgos (personal del hospital), tengan claro e identifiquen las amenazas presentes en la institución, luego el catálogo de Salvaguardas, la cual nos ayuda a establecer las nuevas medidas de protección, en acuerdo con los altos directivos de la institución. En lo que se refiere a análisis de riesgos, estableceremos un método sencillo del mismo a través de tablas, en la cual el personal de la institución tendrá un conocimiento del riesgo que ayudará en la priorización de los mismos para su posterior tratamiento.

D) Metodología OCTAVE

OCTAVE (Evaluación operativa crítica, de amenazas, activos y de vulnerabilidad), es una metodología de análisis y gestión de riesgos en la cual hace énfasis en realizar la gestión del riesgo de manera conjunta, a través de talleres o reuniones, dirigidos a través de un equipo de análisis. Esta metodología se ilustra a través del siguiente diagrama:

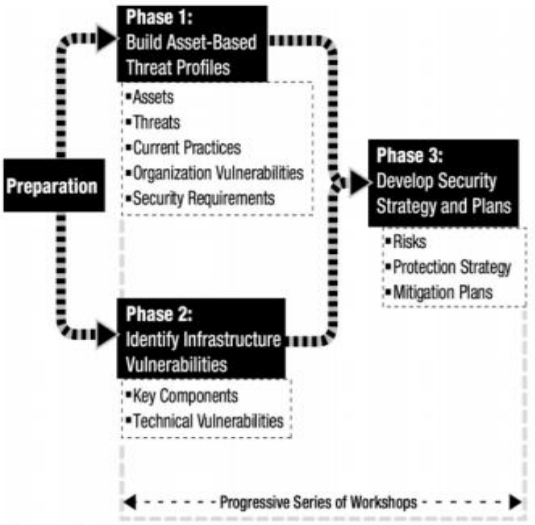


Ilustración 5: Método Octave (Fase 1: Crear perfiles basados en activos, Fase 2: Identificar vulnerabilidades de la infraestructura, Fase 3: Desarrollar planes y estrategias de seguridad.

Bajo esta perspectiva aplicaremos para nuestro trabajo de investigación, datos relacionados con la primera fase: "Crear perfiles basados en activos", en la cual personal de la institución buscará conocer dentro de Emergencias y la estructura de TI que brinde soporte a sus procesos, a los activos, los requisitos de seguridad por cada uno de ellos y si previamente existen estrategias de protección, en este caso relacionado con reglamentos de la institución o la Normativa de EsSalud, luego, aplicaremos lo redactado en la fase 2, "Identificar las vulnerabilidades de la infraestructura", en la cual para descubrir las vulnerabilidades, el personal buscará a los sistemas o activos que estén muy ligados a los activos críticos, para determinar el nivel de debilidad que rodea los mismos, y por último en la fase 3, "Desarrollar planes y estrategias de seguridad", en la cual el personal analizará el riesgo, agregando una medición cualitativa de ellos, en relación a su impacto, y a su vez desarrollar estrategias de protección para contrarrestar las mismas.

4.2 Resultado para el objetivo específico 02

"Seleccionar las fases alineadas a los procesos de emergencias del sector Salud Pública, que permitan determinar el nuevo modelo de gestión de riesgos de Seguridad de la Información". En torno a este objetivo se obtuvieron los siguientes resultados: a) Listado de los procesos de Emergencias del sector Salud Pública, b) propuesta del modelo de Solución, c) descripción del modelo detallado y d) plantillas desarrolladas.

a) Listado de los procesos de Emergencia

A través del Manual de Operaciones del Hospital y Manual de Procedimientos del área de Emergencias [34], se determinaron los procesos más importantes de la atención de Emergencias, para establecer lineamientos que orienten y proporcionen criterios adecuados para la implementación de la Gestión del Riesgo. En el siguiente cuadro mostraremos los mismos, junto a los usuarios responsables en cada uno de ellos (ver Anexo 05).

Como resultado de este análisis, haremos una propuesta que brindará el soporte necesario a las necesidades del área de Emergencias dentro del sector estudiado.

b) Propuesta del modelo de Solución

A continuación, se muestra el modelo desarrollado como resultado del análisis de los estándares y metodologías para la gestión de riesgos, las cuales fueron adaptadas a las necesidades particulares del área de Emergencia del sector Salud Pública, teniendo como base fundamental la norma NTP ISO 27005:2018.

La propuesta obedece a un modelo con una serie de fases que los establecimientos de salud deben implementar y así ejecutar una gestión de riesgos de Seguridad de la Información.

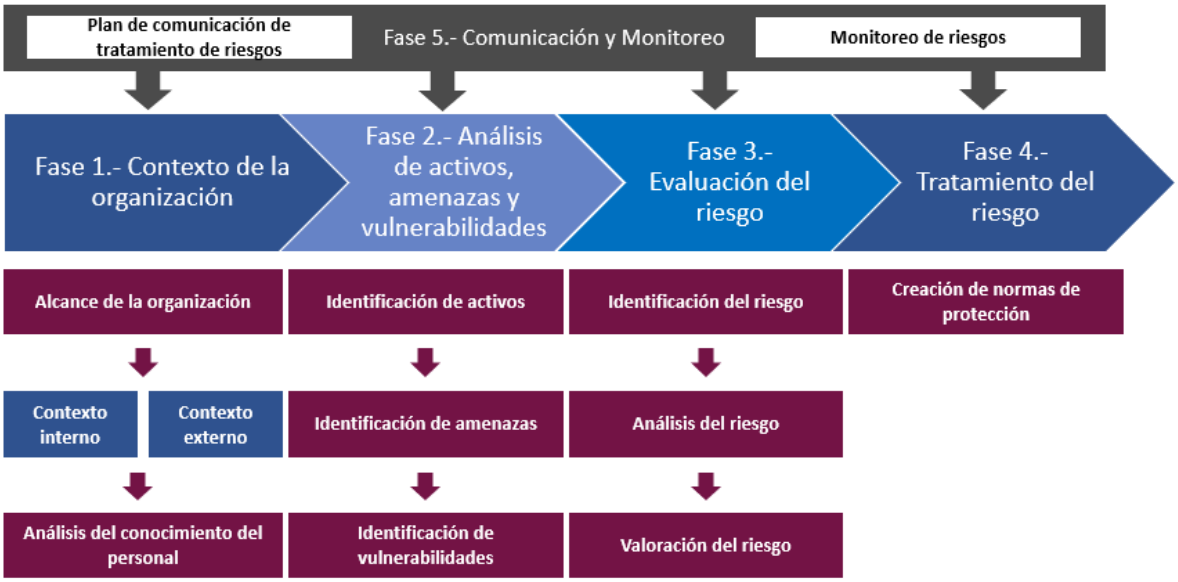


Ilustración 6: Fases y procesos considerados en el Modelo Propuesto
Fuente: Elaboración propia

Las etapas a considerar para el modelo propuesto fueron las siguientes:

- **Fase 1. Contexto de la Organización:** Considera toda la información relevante que pueda incidir en la implementación de gestión de Riesgos de Seguridad de la Información.
- **Fase 2. Identificación de activos, amenazas y vulnerabilidades:** Se dará uso a diversas orientaciones o catálogos de elementos que sirvan de guía para el reconocimiento rápido de activos, amenazas y vulnerabilidades.
- **Fase 3. Evaluación del riesgo:** Se considerará a los activos críticos, y en base a ello estimaremos el riesgo, tomando en cuenta la probabilidad e impacto.
- **Fase 4. Tratamiento del riesgo:** Se hará uso de normas de protección propuestas para contrarrestar los riesgos, que vayan en armonía con el contexto de la institución.
- **Fase 5. Comunicación y monitoreo:** Se elabora un plan de Tratamiento de Riesgos, que resguarden la protección de los activos, compartiéndolo con la parte directiva, asignando los recursos adecuados para ello, finalizando en un control y seguimiento al plan.

Fases del Modelo

Las plantillas, material que el participante de Gestión de Riesgos va a considerar para llevar a cabo la herramienta en mención, van a estar estructuradas en cabecera y contenido, detallados cada una de la siguiente manera:

- Cabecera, en la primera sección se nombra el código de la plantilla, iniciando con la inicial de fase "F", seguido del número del mismo y a qué proceso se refiere, luego está el nombre de la fase, acompañado del nombre del proceso, seguido del logo de la institución, luego redactamos el objetivo de la plantilla, la cual describe lo que pretende la institución en relación al proceso del modelo propuesto, y la fecha en que se realiza el recojo de la información, seguido del nombre de la persona responsable del desarrollo de la plantilla, y la aprobación del personal adecuado para el desarrollo.
- Información requerida: Se refiere al levantamiento de datos necesarios para cumplir con el objetivo de la fase.
- Contenido: Es toda la información que resulta del objetivo planteado de este proceso.
- Salidas: Es toda la información general producto del desarrollo de la plantilla.

Fase 1.- Contexto de la Organización

En esta fase se toma en cuenta toda causa o factor que pueda influir hacia los distintos escenarios de riesgo que puedan afectar la seguridad de la información, considerando el área de Emergencias y los procesos de soporte de TI para la misma. Es por ello que mencionaremos toda la información indispensable que repercuta en la gestión de riesgo mencionado. Esta sección ha sido dividida en dos procesos: Alcance de la organización y Análisis del conocimiento del personal, en el cual la principal importancia es reunir información de los activos críticos del área mencionada.

Proceso 1: Alcance de la organización

Se va a encargar de analizar el conjunto de normas y directrices en relación a la Seguridad de la Información que emite Essalud a todos los centros médicos, así como manuales, políticas o cualquier otro documento que marque limitaciones e influyan para la ejecución de la Gestión de Riesgos de Seguridad de la Información dentro del área de Emergencias. Varios

de estos documentos pueden obtenerse desde el portal de EsSalud o Ministerio de Salud (MINSA).

F-001-1	**Fase 1: Establecimiento del contexto** **Proceso 1: Alcance de la organización**	Logo de la Institución Fecha: __ / __ / ____
Objetivos	Conocer el conjunto de normas y directrices que rigen a cada organización, en relación al área de Emergencias y Seguridad de la Información, para poder alinearlas junto a una gestión de riesgos efectiva.	
Información requerida: Compendio normativo de EsSalud, Manual de procesos y procedimientos de Emergencias – EsSalud, Política Institucional de Protección de Datos Personales, Política Institucional de Seguridad de la Información u otros documentos relacionados con reglamentaciones del área de Emergencia y la Seguridad de la Información de la institución.		**Responsable:** **Aprobado por:**

Documento	**Secciones**	**Información**
Norma técnica de salud de los servicios de Emergencia. Fuente: Portal del MINSA	Normas o disposiciones específicas para los servicios de Emergencia.	**De la atención al paciente**: - Del Ingreso y Admisión - Triaje ...
Compendio normativo – EsSalud (Normas internas). Fuente: Portal de EsSalud	Lista de normas extraídas desde el portal de EsSalud en torno a Seguridad de la información	- 0003-GCIN-ESSALUD-2001 - Normas para el uso de computadoras personales y periféricos en ESSALUD. - 0005-GG-ESSALUD-2006 - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. ...
Política Institucional de Protección de Datos Personales. Fuente: Portal de EsSalud	Principios para la protección de datos personales	- Legalidad - Consentimiento ... ...
Política Institucional de Protección de Datos Personales. Fuente: Portal de EsSalud	Principios para la protección de datos personales	- Legalidad - Consentimiento ...
Política Institucional de Seguridad de la Información. Fuente: Portal de EsSalud	Objetivos Institucionales de Seguridad de la Información	- Proteger, salvaguardar y mantener la confidencialidad, integridad y disponibilidad de la información. - Incentivar y fortalecer una cultura en seguridad de la información al personal de EsSalud. ...
Salidas		
Lista de normas	Políticas o directrices existentes que refleje el alcance y limitaciones para la implementación de la Gestión de Riesgos de Seguridad de la Información.	

Tabla 1: Fase 1 – Establecimiento del Contexto

Fuente: Elaboración propia

1.a) Contexto Externo

De acuerdo con NTP ISO 27005, al hablar del contexto externo nos vamos a referir a distintos aspectos relacionados con lo económico, competitivo, a nivel de tecnología, etc. En lo que se refiere a COBIT 5 para Riesgos, menciona diversas situaciones que pueden influenciar el impacto de un evento y que la organización no puede controlar. Sobre ello vamos a determinar aspectos para los hospitales del sector salud pública como: Factor económico, social, ambiental y tecnológico.

- Factor económico: Considera al panorama económico, el nivel de empleabilidad, y la reducción de la morosidad (deudas tributarias) hacia Essalud, ya que, a través de los impuestos o aportes de los empleadores públicos y privados, hay una mejora en los servicios que ofrece Essalud, caso contrario, no contaría con los recursos necesarios, recursos humanos, instrumentos para la capacitación, etc.
- Factor social: Se refiere al nivel de acceso a servicios médicos e infraestructura tecnológica de la población, o cualquier otro dato demográfico (edad registrada en los sistemas de atención al paciente, sexo, tipo de aseguramiento, etc) que influya en el uso de una herramienta de Gestión de Riesgos.
- Factor ambiental: El nivel climático influye en la tasa de mortalidad, ya que aparecen diversas enfermedades o plagas. También se considera las enfermedades virales o epidemiológicas de gran magnitud, ello podría impactar en la implementación de la Gestión de Riesgos, por ejemplo, hacia el proceso de Triaje y Admisión a Emergencias, ya que la demanda de los servicios dentro del área afectaría a la calidad de la atención al paciente y cualquier implementación a realizar dentro del área.
- Factor tecnológico: Está influenciada por la calidad de la infraestructura tecnológica del sector salud, en especial del área de Emergencias, ya que el resultado de la implementación exitosa de una Gestión de Riesgos depende bastante de ello. También busca la información de módulos o aplicativos, hardware o software que da soporte a Emergencias.

<table>
<tr><td rowspan="2">F-001-1a</td><td colspan="2">Fase 1: Establecimiento del contexto</td><td rowspan="2">Logo de la Institución</td></tr>
<tr><td colspan="2">Sub Proceso 1a: Contexto Externo</td></tr>
<tr><td>Objetivos</td><td colspan="2">Determinar las limitaciones al más alto nivel de la institución para comprender en qué ambiente externo se encuentra para lograr sus objetivos.</td><td>Fecha: __ / __ / ____</td></tr>
<tr><td colspan="3">Información Requerida: Información respecto a la situación actual del país en el aspecto económico, social, ambiental y tecnológico en relación a factores que repercutan en el sector Salud.</td><td>Responsable:
Aprobado por:</td></tr>
<tr><td>Factores</td><td>Fuentes</td><td colspan="2">Información</td></tr>
<tr><td>Factor económico</td><td rowspan="4">- INEI
- Reportes a través de cada municipalidad o gobierno regional
- Links con fuente oficial
- Otras fuentes</td><td colspan="2">- La tasa del PBI
- El PEA (Población Económicamente Activa)
- La situación actual de la deuda del sector público y privado hacia Essalud.</td></tr>
<tr><td>Factor social</td><td colspan="2">Edad registrada en los sistemas de atención al paciente, sexo, tipo de aseguramiento, principales motivos de ingreso, especialidad más consultada, o cualquier información adicional, que permita determinar las características genéricas de pacientes que acceden a servicios médicos e infraestructura tecnológica.</td></tr>
<tr><td>Factor ambiental</td><td colspan="2">Informes del clima y la aparición de enfermedades virales, en la infraestructura de un hospital. Por ejemplo, el fenómeno del Niño, COVID-19, etc., influenciaron drásticamente la infraestructura hospitalaria o llevó de alguna manera daños a la institución.</td></tr>
<tr><td>Factor tecnológico</td><td colspan="2">Informes que describan la infraestructura tecnológica, plataformas tecnológicas y datos sobre los softwares institucionales como sistema operativo, software de oficina, antivirus, características generales de las computadoras, servidores. Lista de sistemas de la institución.</td></tr>
<tr><td colspan="4">Salidas</td></tr>
<tr><td>Listado de factores del contexto Externo</td><td colspan="3">Lista de factores que influyan para el uso de una herramienta de Gestión de Riesgos, de acuerdo al contexto externo.</td></tr>
</table>

Tabla 2: Fase 1 – Establecimiento del Contexto, Sub Proceso 1a) Contexto Externo
Fuente: Elaboración propia

1.b) Contexto Interno

Según COBIT 5 para Riesgos, en el ámbito del contexto interno, están incluidos las metas, objetivos, importancia de la institución, etc. De acuerdo a la NTP/ISO 27005, considera de vital importancia el análisis de la institución, por lo que se tendrá en cuenta sus datos organizacionales y estructura. Ambos marcos de trabajo resaltan el comprender cómo opera la institución para lograr sus objetivos. En cuanto a los hospitales del sector salud pública, consideraremos datos como: Misión, Visión, Objetivos, Principios, etc., así como objetivos

planteados dentro del área de Emergencias, datos que nos pueda ser útil para un mejor alcance y proyección sobre el uso de una herramienta de Gestión de riesgos. Los esquemas que a continuación se describan se desarrollarán en base con el nombre de “Hospital Nuestra Salud”.

Su plantilla va a estar organizada de la siguiente manera:

<table>
<tr><td rowspan="2">F-001-1B</td><td colspan="2">Fase 1: Establecimiento del contexto</td><td rowspan="2">Logo de la Institución</td></tr>
<tr><td colspan="2">Sub Proceso 1b: Contexto Interno</td></tr>
<tr><td>Objetivos</td><td colspan="2">Recolectar información sobre los principales datos organizacionales y sobre los procesos de Emergencia para comprender el funcionamiento del negocio.</td><td>Fecha: __ / __ / ____</td></tr>
<tr><td colspan="3" rowspan="2">Información Requerida: Plan Estratégico Institucional de EsSalud, MOPE y otras fuentes de información que describan al hospital en el aspecto del contexto interno.</td><td>Responsable:</td></tr>
<tr><td>Aprobado por:</td></tr>
<tr><td>Documento</td><td>Secciones</td><td colspan="2">Información</td></tr>
<tr><td rowspan="3">Plan Estratégico Institucional de EsSalud</td><td>Misión</td><td colspan="2">Brindar prestaciones de salud, económicas y sociales a nuestros asegurados con una gestión eficiente e innovadora que garantiza la protección financiera de las prestaciones integrales.</td></tr>
<tr><td>Visión</td><td colspan="2">Ser una institución moderna y en mejora continua, centrada en los asegurados, que garantiza el acceso a la seguridad social con ética, oportunidad y calidad.</td></tr>
<tr><td>Objetivos Estratégicos</td><td colspan="2">- Proteger financieramente las prestaciones que se brindan a los asegurados garantizando una gestión eficiente de los recursos.
- Brindar a los asegurados acceso oportuno a prestaciones integrales y de calidad acorde a sus necesidades.
…</td></tr>
<tr><td rowspan="3">MOPE: Manual de Operaciones del Hospital “Nuestra Salud”</td><td>Finalidad general de la institución</td><td colspan="2">Brindar prestaciones de salud especializadas a la población asegurada del ámbito nacional …</td></tr>
<tr><td>Funciones generales</td><td colspan="2">- Brindar atención integral de salud especializada mediante prestaciones de promoción, prevención de la enfermedad, atención ambulatoria, hospitalización de emergencia y de rehabilitación
…</td></tr>
<tr><td>Organigrama (ubicar el Servicio de Emergencia)</td><td colspan="2">Ver Anexo #</td></tr>
</table>

	Procesos Estratégicos de la institución	- Diseño y control de la capacidad operativa. ...
	Funciones del área del dpto de Emergencia y Áreas Críticas.	- Monitorear y evaluar la ejecución de técnicas, procedimientos, pruebas y otras acciones en torno a la calidad, seguridad del paciente y gestión de riesgos en los Servicios a su cargo. ...
	Organización del Área de Emergencias.	- Servicio de Emergencia Adultos. - Servicio de Emergencia Pediátrica. ...
Entrevista	Procesos de Emergencia	- Ingreso y atención de pacientes en triaje. - Admisión de pacientes en Emergencia. ...
Salidas		
Fuente	Descripción	
Datos generales de la institución	Información relevante que sea soporte para la implementación de la Gestión de Riesgos de Seguridad de la Información.	
Datos sobre el área de estudio	Información necesaria del área de Emergencias y los procesos de soporte de TI para la misma para poder seguir con la Gestión de Riesgos.	

Tabla 3: Fase 1 – Establecimiento del Contexto, Sub Proceso 1b) Contexto Interno
Fuente: Elaboración propia

Proceso 2: Análisis del conocimiento del personal

Una vez establecido qué procesos de Emergencias se va a considerar para la implementación de una gestión de Riesgos, será necesario recoger la información del personal que labora sobre los procesos seleccionados de Emergencias, y sobre los activos que son imprescindibles para el área de estudio y su respectiva clasificación:

— Información: Se refiere a la documentación física o electrónica que ayudan al cumplimiento de la misión de la organización.
— Redes: Hace mención a los recursos que establecen la conectividad de la institución.
— Software: Incluye lo que son aplicativos para el computador, como sistemas operativos, aplicaciones de base de datos, aplicaciones ofimáticas, antivirus, aplicaciones personalizadas, etc.
— Hardware: Se refiere a los dispositivos físicos que hacen uso de la tecnología de la información.
— Personal: Reúne a los trabajadores de la institución que cuentan con habilidades, formación, conocimiento y experiencia y brindan un servicio hacia la organización.

— Instalaciones: Espacio donde se dispone el almacenamiento de uno o más activos para ayudar con el control y funcionamiento de los mismos.

También en esta lista revisará si el activo exige cumplir con los requisitos de seguridad de los mismos (integridad, confidencialidad y disponibilidad).

— Confidencialidad: Se refiere a la exigencia de preservar la información confidencial a cualquier persona o trabajador que no tenga permiso para verla.
— Integridad: Resalta la importancia de mantener el activo de información de forma auténtica y precisa.
— Disponibilidad: Implica que el activo esté siempre disponible para su uso.

Adicionalmente, tomando en cuenta las fuentes de información anterior, se elaboró una tabla genérica, la cual resume los procesos de Emergencias de la institución, mediante el cual, se escogió dos procesos que serán objeto de nuestro estudio, y es allí donde identificamos los activos de información que apoyen estas etapas. La tabla sería la siguiente:

N° Proceso	**Descripción**
01	Ingreso y atención de pacientes en triaje
02	Admisión de pacientes en Emergencia
03	Atención del paciente en la unidad de Shock Trauma Prioridad I
04	Atención del paciente en área de Prioridad II de Emergencia
05	Ingreso y atención del paciente en sala de observación Estancia Corta / Unidad Cuidados Críticos / Cuidados Intermedios
06	Alta médica del Servicio de Emergencia
07	Alta Voluntaria
08	Transferencia del paciente a otros servicios de hospitalización
09	Referencia / Contrarreferencia a otros centros de salud
10	Monitoreo Clínico: Evaluación Médica
11	Monitoreo Clínico: Atención de Enfermería
12	Solicitud de Interconsultas
13	Solicitud de exámenes auxiliares
14	Emisión de constancia de atención
15	Constatación de fallecimiento: Emisión de informe de defunción / Emisión de certificado de defunción

Tabla 4: Lista de procesos de Emergencia a nivel general.
Fuente: Elaboración propia

Al listar los activos importantes por procesos de Emergencia que serán objeto de nuestro estudio, debemos tomar en cuenta que los mismos guarden relación con el activo principal o

estén subordinados a él, y seleccionar qué aspecto del requerimiento de seguridad es importante que se mantenga sobre el activo. El formato de plantilla de esta etapa sería el siguiente:

F-001-2	**Fase 1: Establecimiento del contexto** **Proceso 2: Análisis del conocimiento del personal**	Logo de la Institución
Objetivos	Recoger toda la información necesaria sobre los activos del área de estudio y relacionarlo con los procesos de Emergencia en el que se involucra.	Fecha: __ / __ / ____
Información Requerida: Información dirigida al personal sobre los activos que considera importantes para el desempeño que labora.		**Responsable:** **Aprobado por:**

Nombre del activo	**Categoría**	**Definición**	**Procesos de Emergencia**	**Relación con otros activos**	**Requerimientos de seguridad**		
					CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
Historia clínica física	Información	Documento médico de carácter obligatorio y legal que almacena la información médica del paciente y todos los procesos que realiza el personal que interviene en su salud.	Todos		*	*	*
ESSI	Software	Servicio de Salud Inteligente: Permite gestionar las historias clínicas, reduciendo de manera considerable el tiempo de atención.	- Ingreso y atención de pacientes según triaje	- PC de escritorio - Cable de data	*	*	*
…	…	…	…	…	…	…	…

Tabla 5: Fase 1 – Establecimiento del Contexto, Proceso 2: Análisis del Conocimiento del Personal
Fuente: Elaboración propia

Fase 2: Análisis de activos, amenazas y vulnerabilidades

En esta fase es cuando se reúne la información acumulada de la plantilla anterior y se da inicio a la identificación y valoración de activos, amenazas y vulnerabilidades de manera más personalizada, para las amenazas se tendrá en cuenta el catálogo de amenazas de Magerit

(ver Anexo 13) y la guía de Orientación de Octave, redactada en su Proceso 6: "Evaluar componentes seleccionados", que permitan continuar con la evaluación de riesgos, y resuma la información obtenida previamente.

Proceso 3: Identificación de activos

En este proceso recopilamos toda la información obtenida de la fase anterior, en la que se han definido los activos necesarios para el negocio. Revisaremos si estos activos presentan mención en las normas, manuales, metodologías, directivas, procedimientos u otros documentos normativos ya establecidos de la institución, en relación a Seguridad de la Información. Mientras más exista la necesidad de proteger los activos, el nivel de escala (valor) en lo que se refiere a requisitos de seguridad, se incrementará.

El valor de los activos también puede depender de su relación con los otros activos (establecido en la plantilla anterior), o llámese también activos inferiores, como si fueran dependientes, ya que se apoyan en ellos. De la última plantilla elaborada, también se concluirá si es un activo crítico. Mientras más requisitos de seguridad requiera el activo, mayor será su impacto. Para estimar el impacto debemos considerar a los activos con mayor importancia, cuyo valor resulta de la suma de las dimensiones de seguridad de la información de cada uno de ellos. La institución, al tratarse de un servicio de salud, tomará en cuenta el nivel de impacto como la proporción del daño que afecte la misión de la organización, como daños a la imagen institucional, la preservación de la vida y salud del paciente, la disponibilidad de los servicios, nivel financiero, su infraestructura, etc. El valor menor será 1 y el mayor será 5. La escala propuesta es la siguiente:

Escala	Significado	Definición
5	Muy alto	Daño irreparable a la organización.
4	Alto	Daño a la organización con posibilidad de recuperación en un largo plazo.
3	Medio	Daño que retrasa el avance de los objetivos de la organización.
2	Bajo	Daño leve a la organización con poca afectación en sus labores.
1	Muy bajo	Daño mínimamente considerable.

Tabla 6: Cuadro de impacto de amenazas

Fuente: Elaboración propia

Por ejemplo, mientras las tres dimensiones tengan un alto nivel de importancia, y la suma de las tres sea cercana a 15, se establecerá como impacto Muy Alto, es decir, nivel 5, caso contrario, si la suma de las dimensiones resulta ser un valor cercano a 0, el impacto será Muy bajo. A continuación, presentaremos la siguiente plantilla que define la lista de los activos con sus respectivos niveles de valoración, de acuerdo al criterio del personal de la institución. Los activos con mayor nivel de resultado, revelan mayor nivel de criticidad. A su costado se establecerá el valor del impacto del activo.

F-002 – 3	**Fase 2: Análisis de activos, amenazas y vulnerabilidades** **Proceso 3: Identificación de Activos**	Logo de la institución
Objetivos	Valorar los activos clasificados del proceso anterior, teniendo en cuenta la a las dimensiones de la seguridad de la información.	Fecha: ___ / ___ / _____
Información requerida: Lista de activos importantes de los procesos seleccionados de Emergencias.		Responsable: Aprobado por:

Código	**Activo**	**Normas o disposiciones relacionadas con el activo**	**Niveles de valoración del activo**			**Total**	**Impacto**
			Integridad [I]	**Disponibilidad [D]**	**Confidencialidad [C]**		
[I] – HCLF	Historia Clínica Física	- Gestión de la historia clínica…	5	5	5	15	5
[SW] - ESSI	ESSI	- Disposiciones para el acceso, registro y uso de la información …	5	4	5	14	5
…	…	…	…	…	…	…	…

Tabla 7: Fase 2 – Análisis de activos, amenazas y vulnerabilidad, Proceso 3: Identificación de activos
Fuente: Elaboración propia

Proceso 4: Identificación de amenazas

Una vez establecida la lista con los activos que han revelado mayor exigencia en lo que es requisito de seguridad, es necesario relacionar esos activos junto a las amenazas para conocer

el impacto y a qué activos puede dañar dentro de la misma. Las amenazas en resumen pueden ser clasificadas de la siguiente manera:

SIGLA	CATEGORÍA	DEFINICIÓN
[N]	De origen natural	Son acontecimientos que ocurren al no intervenir el personal, ya sea en forma intencional o no intencional
[I]	De origen industrial	Son acontecimientos que ocurren de forma no provocada, a consecuencia de la actividad del personal que realizan actividades de tipo industrial. En este caso, sí puede ser de manera accidental o deliberada.
[E]	Errores y fallos no intencionados	Son errores de manera no intencionada causada por el personal.
[A]	Ataques intencionados	Son ataques provocados de manera intencional por el personal.

Tabla 8: Cuadro de clasificación de amenazas
Fuente: Magerit

La manera más detallada para especificar los casos de amenazas, se pueden visualizar en el anexo 14, el cual se tomará en cuenta como referencia para conocer a qué dimensión de la seguridad de un activo está perjudicando.

Valoración de las amenazas

Para seguir con la identificación de amenazas, es necesario recurrir a una escala cuantitativa que se usará para este proceso. Es por ello que recurriremos a la “probabilidad” e “impacto” para poder dar una puntuación a esta amenaza. Para la probabilidad se usará como referencia un año, por lo que se ha establecido una valoración numérica para la posterior calificación del riesgo.

Escala numérica	Denominación	Probabilidad
5	Continuo	Todos los días
4	Recurrente	Semanal
3	Probable	Mensual
2	Poco Probable	Semestral
1	Algo Improbable	Anual

Tabla 9: Cuadro de probabilidad de amenazas
Fuente: Elaboración propia

Luego de ello, se usará una plantilla en la cual tomaremos en cuenta los activos críticos, y de acuerdo al catálogo sugerido en párrafos anteriores (Magerit), determinaremos qué amenaza podemos encontrar en ello, sobre todo los que atenten a los requisitos de seguridad establecidos en cada activo. Por ejemplo, si a un activo se ha determinado que hay que prevalecer su confidencialidad e integridad, relacionar qué amenazas puedan atentar contra esas dimensiones. Luego de ello, ver las consecuencias en caso la amenaza se materialice, la probabilidad que ello suceda dentro del intervalo de un año y el impacto que ocasionaría.

F-002	**Fase 2: Análisis de activos, amenazas y vulnerabilidades** **Proceso 4: Identificación de amenazas**	Logo de la Institución
Objetivos	Identificar las amenazas correspondientes a los activos críticos, los responsables de ese activo y la probabilidad con que ocurre el determinado evento.	Fecha: __ / __ / ____
Información Requerida: Lista de activos principales de los procesos analizados del área de Emergencias.		**Responsable:** **Aprobado por:**

Activo	Responsable	Amenaza	Consecuencia(s)	Probabilidad
[I] – HCLF	Personal de Admisión	[I.1] Daños por fuego	Divulgación, pérdida o destrucción de sus datos personales.	1
		[N.2] Daños por agua		1
…	…	…	…	…

Tabla 10: Fase 2 – Análisis de activos, amenazas y vulnerabilidad, Proceso 4: Identificación de amenazas
Fuente: Elaboración propia

Proceso 5: Identificación de vulnerabilidades

Seguidamente, se presentará un cuadro de vulnerabilidades, el cual se va a asociar con su respectivo nivel de gravedad para conocer más a fondo las debilidades de la institución, y a su vez las consecuencias de la falla del componente, lo que nos va a permitir tenerlo presente en la elaboración de las medidas de protección. Se tomó en consideración el cuadro de niveles de gravedad, que, de acuerdo con Octave [25] determinan en cuánto tiempo se tiene que tomar la acción inmediata. Se puede solicitar topología o mapas de red que describan la infraestructura actual de la institución y para hallar dónde se encuentran ubicadas esas vulnerabilidades o activos críticos y una lista de los sistemas de información utilizados en el área de Emergencia.

Nivel de gravedad de la vulnerabilidad	**Descripción**
Vulnerabilidades de alta gravedad	Debe arreglarse inmediatamente
Vulnerabilidades de gravedad media	Debe arreglarse pronto (máximo 2 semanas)
Vulnerabilidades de baja gravedad	Debe arreglarse después (máximo 4 semanas)

Tabla 11: Niveles de gravedad de la vulnerabilidad
Fuente: Octave

Revisamos la lista de vulnerabilidades que la NTP ISO-IEC/27005 sugiere (ver Anexo #), o establecemos una nueva vulnerabilidad que se haya detectado durante la entrevista al personal, análisis del área o inspección física, procurando que esté en relación con la amenaza detectada en el proceso anterior. La siguiente plantilla sería la correspondiente a ese proceso.

<table>
<tr><td rowspan="2">F-002</td><td colspan="2">Fase 2: Análisis de activos, amenazas y vulnerabilidades</td><td rowspan="2">Logo de la Institución</td></tr>
<tr><td colspan="2">Proceso 5: Identificación de vulnerabilidades</td></tr>
<tr><td rowspan="2">Objetivos</td><td colspan="2" rowspan="2">Definir los niveles de vulnerabilidad de los activos mencionados en relación con sus amenazas</td><td>Fecha: __ / __ / ____</td></tr>
<tr><td colspan="3">Información Requerida: Lista de los activos críticos con sus respectivas amenazas</td><td>Responsable:
Aprobado por:</td></tr>
<tr><td>Activo</td><td>Amenaza</td><td>Vulnerabilidad</td><td>Nivel de gravedad</td></tr>
<tr><td rowspan="2">[I] – HCLF</td><td>[I.1] Daños por fuego</td><td rowspan="2">Ausencia de capacitación periódica de planes de Contingencia frente a desastres.</td><td rowspan="2">Alta</td></tr>
<tr><td>[N.2] Daños por agua</td></tr>
<tr><td>[SW] - ESSI</td><td>[E.19] Fugas de información</td><td>Ausencia de cultura en seguridad de la información al personal del hospital.</td><td>Alta</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td></tr>
</table>

Tabla 12: Fase 2 – Análisis de activos, amenazas y vulnerabilidad, Proceso 5: Identificación de vulnerabilidades
Fuente: Elaboración propia

Fase 3: Evaluación del Riesgo

Proceso 6: Identificación del Riesgo

Después de un análisis exhaustivo de activos, amenazas y vulnerabilidades, se procederá a identificar el riesgo, para posteriormente tomar un plan de acción necesaria, que vaya en armonía con la normativa de EsSalud. A cada amenaza detectada, se le agregarán las siguientes características para un mayor conocimiento del evento, y así tener resultados más certeros a la hora de hacer el análisis del riesgo. De las amenazas que ya hemos visto, agregaremos al actor, que es quien puede transgredir los requisitos de seguridad (confidencialidad, integridad, disponibilidad) del activo, y el resultado se basa en las consecuencias del riesgo. Como actores se ha definido las siguientes categorías: Acciones premeditadas del personal, Acciones accidentales del personal, Problemas de software y hardware, y Otros problemas relacionados. El resultado se clasificará en 4 tipos de situaciones que se han contextualizado en torno a la seguridad de la información: divulgación, modificación, pérdida/destrucción, interrupción.

Esta información se resumió en el siguiente cuadro:

Actor	Ejemplos	Resultado
Acciones premeditadas del personal	- Personal del área - Personas ajenas al área	- **Divulgación** o visualización de información confidencial. - **Modificación** de información crítica. - **Pérdida / Destrucción** de información, hardware o software. - **Interrupción** de acceso a información crítica, sistemas o servicios como correo electrónico o Web.
Acciones accidentales del personal		
Problemas de software y hardware	- Defectos de hardware y software - No disponibilidad de los sistemas - Códigos maliciosos - Otros	
Problemas a nivel externo o de infraestructura	- Cortes de energía - No disponibilidad del agua y telecomunicaciones - Proveedor de servicios de Internet no disponibles - Inundaciones, temblores, otros	

Tabla 13: Lista de categorías de causantes de amenazas (actores)
Fuente: Elaboración propia

Para ello se dispondrá de la siguiente plantilla:

F-003	**Fase 3: Evaluación del riesgo** **Proceso 6: Identificación del riesgo**		Logo de la Institución
Objetivos	Definir los niveles de gravedad de los activos mencionados.		Fecha: __ / __ / ____
Información Requerida: Lista de vulnerabilidades en relación a sus activos y amenazas.			**Responsable:** **Aprobado por:**
Activo	**Amenaza**	**Actor**	**Resultado (en relación a la información**
[I] – HCLF	[I.1] Daños por fuego [N.2] Daños por agua	Acciones accidentales del personal	Pérdida / Destrucción
…	…	…	…

Tabla 14: Fase 3 – Evaluación del riesgo, Proceso 6: identificación del riesgo
Fuente: Elaboración propia

Proceso 7: Análisis del riesgo

Después de la revisión exhaustiva de las amenazas por activo, vamos a estimar la frecuencia(probabilidad) e impacto de los mismos, para esta ocasión escogeremos los activos que presentan mayor impacto (a partir de la escala 4), activos cuyo resultado es la divulgación o pérdida de la información mayormente, ya que a través de ella se va a determinar el nivel de

riesgo y posteriormente dar su respectiva valoración. A través de ambos datos, vamos a utilizar la siguiente fórmula:

Riesgo = Probabilidad x Impacto

Posteriormente el resultado que arroje determinará los riesgos a priorizar, lo cual se determinó a través de la siguiente escala:

Rango	Riesgo
16 – 25	C: Crítico
11 – 15	I: Importante
6 – 10	B: Bajo
1 – 5	MB: Muy bajo

Tabla 15: Calificación de riesgo
Fuente: Elaboración propia

Para ello se dispondrá de la siguiente plantilla:

F-003	**Fase 3: Evaluación del riesgo** **Proceso 7: Análisis del Riesgo**				Logo de la Institución	
Objetivos	Medir el riesgo para ver al detalle su respectivo nivel de criticidad.				Fecha: __ / __ / ____	
Información Requerida					**Responsable:** **Aprobado por:**	
Nro Riesgo	**Activo**	**Código Amenaza**	**Probabilidad**	**Impacto**	**Resultado (P x I)**	**Tipo de Riesgo**
R-001	[I] – HCLF	[I.1]	1	5	5	Muy Bajo
R-003	[SW] – ESSI	[A.19]	5	4	20	Crítico
…	…	…	…	…	…	…

Tabla 16: Fase 3 – Evaluación del riesgo, Proceso 7: Análisis del riesgo
Fuente: Elaboración propia

Mapa de Riesgos

Luego, creamos una tabla de doble entrada, en donde se tome en cuenta las variables de probabilidad e impacto, y seguidamente ubicamos allí los riesgos que se han analizado en la plantilla anterior.

PROBABILIDAD	Continuo	**5**	5	10	15	20	25
	Recurrente	**4**	4	8	12	16	20
	Probable	**3**	3	6	9	12	15
	Poco Probable	**2**	2	4	6	8	10
	Algo Improbable	**1**	1	2	3	4	5
			1	**2**	**3**	**4**	**5**
			Muy Bajo	Bajo	Regular	Importante	Crítico
			IMPACTO				

Tabla 17: Fase 3 – Mapa de riesgos
Fuente: Magerit

Trasladando el valor de los riesgos obtenidos, el mapa de Riesgos se vería de la siguiente manera:

PROBABILIDAD	Continuo	**5**					
	Recurrente	**4**					R-003
	Probable	**3**					
	Poco Probable	**2**			R-004		
	Algo Improbable	**1**					R-001 R-002
			1	**2**	**3**	**4**	**5**
			Muy Bajo	Bajo	Regular	Importante	Crítico
			IMPACTO				

Proceso 8: Valoración del riesgo

Una vez definida la lista de riesgos, se determina el nivel de tolerancia o límite al mismo, es decir, hasta qué nivel es aceptable o permisible el valor del riesgo, que no contrarreste con los objetivos de la organización.

Nivel Riesgo	Nivel de Tolerancia	Descripción
18-25	Grave	Este riesgo afecta el negocio y los objetivos de la organización
13-17	Intolerable	Riesgos que requieren un tratamiento para reducir la magnitud del mismo
7-12	Poco tolerable	Identificar las mediciones de riesgo que pueden ser aceptables para una posterior gestión que permita reducir el impacto del mismo.
1-6	Aceptada	La empresa está dispuesta a asumir el riesgo para cumplir con sus objetivos

Tabla 18: Niveles de tolerancia al riesgo
Fuente: Elaboración propia

Por cada riesgo se asociará la amenaza y vulnerabilidad correspondiente, luego ubicamos en la plantilla el valor del riesgo junto a su respectiva clasificación, y se finaliza determinando su nivel de criticidad y tolerancia, logrando así gestionar los riesgos y reducir el impacto al mínimo.

F-003	**Fase 3: Evaluación del riesgo** **Proceso 8: Valoración del Riesgo**			Logo de la Institución	
Objetivos	Valorar los riesgos obtenidos y registrar el nivel de tolerancia del mismo.			Fecha: __ / __ / ____	
Información Requerida				**Responsable:** **Aprobado por:**	
Listado de riesgos extraídos del análisis anterior, junto a su respectivo nivel de criticidad					
Cód Riesgo	**Activo**	**Amenaza**	**Resultado Riesgo**	**Clasificación Riesgo**	**Tolerancia**
R-001	[I] – HCLF	[I.1] Daños por fuego	5	Muy Bajo	Aceptada
R – 003	[SW] – ESSI	[E.19] Fugas de información	20	Crítico	Grave
…	…	…	…	…	…

Tabla 19: Fase 3 – Evaluación del riesgo, Proceso 8: Valoración del riesgo
Fuente: Elaboración propia

Fase 4) Tratamiento del riesgo

Proceso 9: Creación de normas de protección

Es importante consolidar la información acumulada de los riesgos, amenazas, vulnerabilidades y sus procesos de Emergencia respectivos, para a partir de ella formular nuevas normas de protección, tanto de las recomendadas por el catálogo de Magerit (ver Anexo X), como las nuevas que podamos disponer a partir de los riesgos expuestos. Hay que buscar estrategias de protección que guarden relación entre el activo, las vulnerabilidades y amenazas encontradas, además que el área de estudio pueda implementar.

Para este nuevo conjunto de normas nos guiaremos de los riesgos que hayan tenido una puntuación de tolerancia a nivel Poco Tolerable, Intolerable y Grave, además de tomarlos como referencia, para los futuros riesgos que guarden relación con la lista sugerida, así mismo considerar las siguientes medidas para contrarrestar los riesgos: Evitar, Compartir y Mitigar el riesgo. Entre las personas encargadas de supervisar las acciones o controles correspondientes para contrarrestar los riesgos, Personal de Admisión, Personal de Triaje, Jefe de TI, Actores externos. Su plantilla sería la siguiente:

F-004	Fase 4: Tratamiento del riesgo	Logo de la Institución
	Proceso 9: Creación de normas de protección	
Objetivos	Generar un catálogo de medidas de protección existentes en la empresa sobre los activos mencionados.	Fecha: __ / __ / ____
Información Requerida		**Responsable:**
		Aprobado por:

Riesgo	**Activo**	**Proceso(s) de Emergencia**	**Amenaza**	**Responsable**	**Tolerancia**	**Respuesta al Riesgo**	**Norma o control recomendado**
R-004	[SW] – ESSI	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia.	[E.19] Fugas de información	Personal de Admisión y Triaje	Intolerable	Mitigar	Promover cultura de concientización de Seguridad de Información al personal del área.
…	…	…	…	…	…	…	…

Tabla 20: Fase 4 – Tratamiento del riesgo, Proceso 9: Creación de normas de protección
Fuente: Elaboración propia

Fase 5) Comunicación y monitoreo

Proceso 10: Plan de Comunicación de Tratamiento de Riesgos

Una vez creadas las normas de protección, corresponde reunir a las partes interesadas para elaborar un informe final del estado del riesgo para formalizar las normas o controles recomendados en la fase anterior, y comunicar su plan de tratamiento o lista de actividades, en la cual involucraremos a todos los participantes para hacerlos partícipes del compromiso y la importancia para contrarrestar el mismo, creando una cultura de responsabilidad entre ellos. Seguidamente, verificar si existe alguna normatividad en relación al riesgo para sumarla a las normas propuestas, para mejorar la calidad de la misma y concientizar su cumplimiento, confirmando el compromiso de los responsables.

F-005	Fase 5: Comunicación y monitoreo Proceso 10: Plan de comunicación de tratamiento de riesgos	Logo de la Institución
Objetivos	Formalizar las normas y a partir de ellas, generar una lista de actividades para ser informadas a la Alta Dirección.	Fecha: __ / __ / ____
Información Requerida		**Responsable:** **Aprobado por:**

Norma Propuesta	**Normas existentes relacionadas**	**Lista de actividades**	**Responsable**	**Destinatarios**	**Periodicidad**
1) Capacitación y concientización sobre seguridad de la información	- Acceso, registro y uso de la información de las prestaciones de salud en el Sistema Informático Servicio de Salud Inteligente. - Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud.	- Diseñar un plan de capacitación formal que incluya capacitaciones sobre sensibilización y formación en materia de seguridad (detección de virus, cortes de red, manejo de información confidencial de pacientes, etc), así como seguridad física.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Cada seis meses
…	…	…		…	…

Tabla 21: Fase 5 – Comunicación y monitoreo, Proceso 10: Plan de comunicación de tratamiento de riesgos
Fuente: Elaboración propia

Proceso 11: Monitoreo de riesgos

Una vez comunicado el plan de tratamiento de riesgos y las partes estén debidamente informadas, se establecerán programas de seguridad, que consiste en materializar las decisiones acordadas para contrarrestar los riesgos, en la cual partimos del listado anterior, y desde allí consideramos los recursos necesarios para el correcto tratamiento del riesgo, se planteará el tiempo a implementar el proyecto, además, estableceremos una serie de indicadores que permitirán ver su evolución a través de determinados periodos de tiempo. Asimismo, estos registros servirán para tener un seguimiento de las anomalías, adicionalmente tomando las medidas correctivas necesarias.

En el programa de seguridad detallaremos lo siguiente:

- La relación de riesgos, activos afectados, tipo de activo, sus amenazas y los niveles de impacto y riesgo.
- La estimación de recursos económicos a utilizar para su realización, se tomará en cuenta:
    - Los costes de adquisición (productos, servicios, programas o instalaciones).
    - Gastos de mantenimiento.
    - Gastos de capacitación.

F-005	Fase 5: Comunicación y monitoreo Proceso 11: Plan de comunicación de riesgos	Logo de la Institución
Objetivos	Describir los programas de seguridad y comunicar el plan de riesgos a las partes correspondientes.	Fecha: __ / __ / ____
Información Requerida: Plan de comunicación de tratamiento de riesgos		**Responsable:** **Aprobado por:**

Programa 01:					
Responsable:			**Tiempo de Implementación:** 2 semanas		
Área:			**Gastos:**		
Indicadores:					
Riesgos relacionados	**Activo(s) asociado(s)**	**Categoría Riesgo**	**Amenaza**	**Lista de actividades**	**Recursos**
- R-004 - R-007	[HW] – PC [HW] - SW	Crítico	[I.8] Fallo de servicio de comunicaciones	- Impulsar que se realice el mantenimiento hacia los equipos y la conectividad eficaz para los equipos dentro del área de Triaje. - Establecimiento de normas que permitan brindar el adecuado uso a los aparatos de red.	- Coordinación con la jefatura del Área de Emergencias y Cuidados Críticos, jefatura de TI y jefe de Unidad de Estadística e Informática
…	…	…	…	…	…

Tabla 22: Fase 5 – Comunicación y monitoreo, Proceso 10: Plan de comunicación de riesgos
Fuente: Elaboración propia

4.3 Resultado para el objetivo específico 03

"Validar el modelo de gestión de riesgos basado en marcos de trabajo estandarizados, mediante juicio de expertos, para valorar el modelo adaptado". Para el cumplimiento de este objetivo se tomaron en cuenta los siguientes ítems: Informes de opinión de expertos y Cuadro de validación del modelo propuesto mediante V. de Aiken.

Informes de opinión de expertos: Se contó con la participación de 3 magíster expertos con experiencia en Gestión de Riesgos de TI, mediante los cuales se logró la aprobación del esquema presentado, en el cual resume las fases y procesos del modelo propuesto (ver Anexo 11).

Cuadro de validación del modelo propuesto mediante V. de Aiken: Con esta herramienta se estimó de forma cuantitativa la validez del modelo, a través de los criterios siguientes: claridad, objetividad, coherencia, suficiencia, relevancia, logrando promediar la calificación de los 3 jueces expertos de la siguiente manera:

V. de Aiken por criterio	**Claridad**	**Objetividad**	**Coherencia**	**Suficiencia**	**Relevancia**
	0,88	0,94	0,95	0,87	0,95

Cuanto el valor esté aproximado a 1, se obtendrá una mayor validez del modelo propuesto, por lo que en el promedio general obtenemos como resultado una aprobación bastante alta por parte de los 3 jueces:

V. de Aiken	**0,92**

4.3 Resultado para el objetivo específico 04

"Implementar de manera parcial el modelo de Gestión de Riesgos para mejorar la Seguridad de la Información en los hospitales del sector Salud Pública de la región". Para este objetivo se consideró iniciar la implementación del modelo propuesto con el uso de las plantillas desarrolladas, logrando obtener un avance de implementación del 90% en el Anexo 15.

Caso de Estudio Hospital "Nuestra Salud"

En el primer proceso de la fase 1, vamos a recopilar la información necesaria para el hospital en estudio, el cual nos permitirá delimitar el alcance del área de Emergencias, para la implementación de la gestión de riesgos. Aquí reuniremos la información respectiva de los diferentes documentos emitidos por parte de Essalud y otras instituciones.

<table>
<tr><td rowspan="2">F-001-1</td><td colspan="2">Fase 1: Establecimiento del contexto</td><td rowspan="2">NUESTRASALUD
Fecha: 30 / 11 / 2023</td></tr>
<tr><td colspan="2">Proceso 1: Alcance de la organización</td></tr>
<tr><td>Objetivos</td><td colspan="2">Conocer el conjunto de normas y directrices que rigen a cada organización, en relación al área de Emergencias y Seguridad de la Información, para poder alinearlas junto a una gestión de riesgos efectiva.</td><td></td></tr>
<tr><td colspan="3">Información requerida: Compendio normativo de EsSalud, Manual de procesos y procedimientos de Emergencias – EsSalud, Política Institucional de Protección de Datos Personales, Política Institucional de Seguridad de la Información u otros documentos relacionados con reglamentaciones del área de Emergencia y la Seguridad de la Información de la institución.</td><td>Responsable:
Analista de riesgo
Aprobado por:
Jefe de TI</td></tr>
<tr><td>Documento</td><td>Secciones</td><td colspan="2">Información</td></tr>
<tr><td>Norma técnica de salud de los servicios de Emergencia.
Fuente: Portal del MINSA</td><td>Lista de normas o disposiciones específicas para los servicios de Emergencia.</td><td colspan="2"><u>De la atención al paciente</u>:
- Del Ingreso y Admisión
- Triaje
- Sala de Reanimación
- Tópico de Atención
- Sala de Observación
- Interconsulta
- Junta Médica
- Información

<u>De los servicios de apoyo</u>:
- Exámenes auxiliares
- Archivo de Historia Clínica

<u>De la transferencia interna de pacientes</u>:
- Sala de Operaciones
- Servicios de Hospitalización

<u>Del alta</u>:
- Constancia de Atención
- Fallecimiento

<u>De la referencia</u>
<u>Del reporte y los registros</u></td></tr>
</table>

Compendio normativo – EsSalud (Normas internas). Fuente: Portal de EsSalud	Lista de normas extraídas desde el portal de EsSalud en torno a Seguridad de la información	- 0003-GCIN-ESSALUD-2001 - Normas para el uso de computadoras personales y periféricos en ESSALUD. - 0005-GG-ESSALUD-2006 - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - 32-GCOI-ESSALUD-2003 - Normas para brindar seguridad a los servidores de las redes de informática. - 0035-GG-ESSALUD-2006 - Norma de soporte informático para la continuidad del negocio frente a eventos de desastre en ESSALUD - 0236-GG-ESSALUD-2005 - Políticas de seguridad informática de ESSALUD. - 0376-GG-ESSALUD-1999 - Normas para el control y la administración de los servicios de Intranet, Internet y Extranet en Essalud. - 0397-GG-ESSALUD-2003 - Normas para la administración y usos del correo electrónico oficial y de los servicios de internet en ESSALUD. - 0607-GG-ESSALUD-2005 - Normas para consolidar y difundir los documentos normativos en el portal intranet de ESSALUD. - 1339-GG-ESSALUD-2023 - Disposiciones para el acceso, registro y uso de la información de las prestaciones de salud en el sistema informático servicio de salud inteligente - ESSI del Seguro Social de Salud – ESSALUD. - 1381-GG-ESSALUD-2015 - Procedimiento para la publicación y actualización de información en el portal institucional, intranet y portal de transparencia del Seguro Social de Salud (ESSALUD). - 1521-GG-ESSALUD-2013 - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD).
Política Institucional de Protección de Datos Personales. Fuente: Portal de EsSalud	Principios para la protección de datos personales	- Legalidad - Consentimiento - Limitaciones al consentimiento para el tratamiento de datos personales - Finalidad - Proporcionalidad - Calidad - Principio de seguridad - Principio de disposición de recurso - Principio de nivel de protección adecuado
Política Institucional de Seguridad de la Información. Fuente: Portal de EsSalud	Objetivos Institucionales de Seguridad de la Información	- Proteger, salvaguardar y mantener la confidencialidad, integridad y disponibilidad de la información. - Incentivar y fortalecer una cultura en seguridad de la información al personal de EsSalud. - Asegurar que la información producida, procesada y almacenada sea de propiedad de EsSalud, estableciendo controles y mecanismos de seguridad de la información. - Proteger los activos de infraestructura tecnológica, sus plataformas tecnológicas y software

		institucional que posee EsSalud para la prestación de sus servicios. - Asegurar plataformas tecnológicas y sistemas de información auditables; y de acuerdo con su criticidad, se registren y documenten los incidentes relacionados a la seguridad de la información. - Garantizar la continuidad y cumplimiento de las acciones que permitan planificar, operar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información. - Establecer mecanismos de control y sanción cuando el dato o información institucional es alterada por cualquier circunstancia.
Salidas		
Lista de normas	Políticas o directrices existentes que refleje el alcance y limitaciones para la implementación de la Gestión de Riesgos de Seguridad de la Información.	

En la sub fase del proceso 1, denominado Sub Proceso 1a: Contexto Externo, conoceremos el alcance a un nivel externo a la institución, para conocer qué otros factores ajenos a ella puedan incidir en la implementación del modelo.

<table>
<tr><td rowspan="2">F-001-1a</td><td>Fase 1: Establecimiento del contexto</td><td rowspan="2"> 
</td></tr>
<tr><td>Sub Proceso 1a: Contexto Externo</td></tr>
<tr><td>Objetivos</td><td>Determinar las limitaciones al más alto nivel de la empresa para comprender en qué ambiente externo se encuentra para lograr sus objetivos.</td><td>Fecha: 30 / 11 / 2023</td></tr>
<tr><td colspan="2">Información Requerida: Información respecto a la situación actual del país en el aspecto económico, social, ambiental y tecnológico en relación a factores que repercutan en el sector Salud.</td><td>Responsable:
Analista de riesgo
Aprobado por:
Jefe de TI</td></tr>
<tr><td>Factor económico</td><td colspan="2">- Tasa de PBI: 230.590 M€, ocupando el puesto 52 de 196 países que publican el PBI.
- PEA: La situación actual del país alcanzó 17 millones 27 mil 200 personas en los tres primeros meses del año 2023.
- Deuda del sector público y privado hacia EsSalud: Sobre la deuda general a cobrar por parte de EsSalud, el 37.1% (S/1,900 millones), está asignado a entidades del sector público, y el 62.9% sobrante (S/3,245 millones) corresponde al sector privado.</td></tr>
<tr><td>Factor social</td><td colspan="2">- Edad registrada en los sistemas estadísticos: De 0 a 85 años.
- Sexo: Masculino y femenino
- Tipo de aseguramiento: Trabajadores dependientes (hijos, cónyuges, concubinos), pensionistas, seguro agrario dependiente, seguro cas, ley de Emergencia, otro tipo de seguro.
- Principales motivos de ingreso: Prioridad I (Resucitación), Prioridad II (Emergencia), Prioridad III (Urgencia), Prioridad IV (Urgencia Menor o Poco Urgente), Prioridad V (Sin Urgencia – No Urgente).</td></tr>
<tr><td>Factor ambiental</td><td colspan="2">- Intensas lluvias, fenómeno del Niño.
- Enfermedades epidemiológicas como: Dengue, Chikungunya, Zika, Malaria, Leishmaniasis (aislamiento de pacientes).
- Variantes del COVID – 19.</td></tr>
<tr><td>Factor tecnológico</td><td colspan="2">- Sistema Operativo: Windows 7 y Windows 10
- Software de oficina: Office 2007, 2010, 2013, 2016, 2019 y Office GLPL
- Antivirus: Sophos
- Computadora: Generalmente viene a ser de la marca Intel Core I7 o AMD Ryzen 5, con RAM de 8 GB y almacenamiento de 1 TB
- Servidor: De la marca Dell, con procesador Intel® o Xeon®, utilizado para soportar servicios como Backup y aplicativos como Asterik y PACS, con sistema operativo Windows Server 2012 R2 y VMware ESXI 6.0.
- Sistemas: ESSI, PACS, Anapat, Acredita, SIAF, SIGA.</td></tr>
<tr><td colspan="3">Salidas</td></tr>
<tr><td>Listado de factores del contexto Externo</td><td colspan="2">Lista de factores que influyan para el uso de una herramienta de Gestión de Riesgos, de acuerdo al contexto externo.</td></tr>
</table>

En la otra sub fase del proceso 1, denominado Sub Proceso 1b: Contexto Interno, conoceremos la institución a un nivel interno, en específico al área de Emergencias, para conocer bajo qué políticas o documentos normativos funciona esta área.

F-001-1B	**Fase 1: Establecimiento del contexto**	NUESTRASALUD
	Sub Proceso 1b: Contexto Interno	
Objetivos	Recolectar información sobre los principales datos organizacionales y sobre los procesos de Emergencia para comprender el funcionamiento del negocio.	Fecha: 30 / 11 / 2023
Información Requerida: Plan Estratégico Institucional de EsSalud, MOPE y otros que describan al hospital en el aspecto del contexto interno.		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Documento	**Secciones**	**Información**
Plan Estratégico Institucional de EsSalud	Misión	Brindar prestaciones de salud, económicas y sociales a nuestros asegurados con una gestión eficiente e innovadora que garantiza la protección financiera de las prestaciones integrales.
	Visión	Ser una institución moderna y en mejora continua, centrada en los asegurados, que garantiza el acceso a la seguridad social con ética, oportunidad y calidad.
	Objetivos Estratégicos	- Proteger financieramente las prestaciones que se brindan a los asegurados garantizando una gestión eficiente de los recursos. - Brindar a los asegurados acceso oportuno a prestaciones integrales y de calidad acorde a sus necesidades. - Impulsar la transformación digital y la gestión para resultados centrada en los asegurados logrando modernizar la institución.
MOPE: Manual de Operaciones del Hospital "Nuestra Salud"	Finalidad de la institución	Brindar prestaciones de salud a la población asegurada del ámbito nacional, referida por los establecimientos de salud de diferentes niveles de atención y capacidad de resolución que conforman la Red Prestadora de EsSalud, a fin de mantener la integralidad y continuidad de la atención a los asegurados.
	Funciones generales de la institución	- Brindar atención integral de salud especializada mediante prestaciones de promoción, prevención de la enfermedad, atención ambulatoria, hospitalización de emergencia y de rehabilitación, así como servicios médicos de apoyo para proporcionar diagnóstico y tratamiento a los pacientes. - Garantizar la continuidad y oportunidad en el otorgamiento de las prestaciones de salud especializada a los asegurados adscritos a las IPRESS de la Red Prestacional Lambayeque y de otras IPRESS de ESSALUD del ámbito nacional, en el marco de las normas vigentes. - Cumplir las políticas, normas, planes, programas, procesos y procedimientos en el ámbito del Hospital Nacional, según corresponda, relacionados a las prestaciones de salud que brinda. - Implementar la cartera de servicios y gestionar la capacidad operativa máxima del Hospital Nacional, de acuerdo a las disposiciones establecidas en el marco normativo vigente.

		- Informar a los pacientes respecto a sus deberes y derechos relacionados a las prestaciones de salud, información institucional, trámites, entre otros.
	Organigrama (ubicar el Servicio de Emergencia)	Ver Anexo 02
	Procesos Estratégicos del área de Emergencias	- Diseño y control de la capacidad operativa. - Gestión de la calidad, seguridad al paciente y riesgos prestacionales.
	Funciones del área de Emergencias	- Monitorear y evaluar la ejecución de técnicas, procedimientos, pruebas y otras acciones en torno a la calidad, seguridad del paciente y gestión de riesgos en los Servicios a su cargo. - Efectuar el monitoreo, seguimiento y evaluación de la atención de los Servicios a su cargo, proponiendo alternativas de mejora en la atención clínica. - Controlar el acceso a la información por parte de los pacientes, en el marco de las normas vigentes, en los Servicios a su cargo. - Proponer la cartera de servicios de salud que correspondan a los Servicios a su cargo, según las prioridades sanitarias, la oferta y demanda y las normas vigentes, así como realizar las acciones para su implementación, control y evaluación respectiva. - Identificar la capacidad operativa máxima de los Servicios a su cargo. - Dirigir y controlar el proceso de planificación y evaluación de los Servicios a su cargo. - Evaluar y presentar a la Gerencia Clínica la productividad de los Servicios a su cargo y de los resultados o beneficios en la salud de los pacientes, así como la calidad y satisfacción lograda.
	Organización	- Servicio de Emergencia Adultos. - Servicio de Emergencia Pediátrica. - Servicio Cuidados Intensivos. - Servicio Cuidados Intermedios
Entrevista	Procesos de Emergencia	- Ingreso y atención de pacientes en triaje. - Admisión de pacientes en Emergencia. - Atención del paciente en la unidad de Shock Trauma Prioridad I. - Atención del paciente en área de Prioridad II de Emergencia. - Ingreso y atención del paciente en sala de observación Estancia Corta / Unidad Cuidados Críticos / Cuidados Intermedios. - Alta médica del Servicio de Emergencia. - Alta Voluntaria. - Transferencia del paciente a otros servicios de hospitalización. - Referencia / Contrarreferencia a otros centros de salud. - Monitoreo Clínico: Evaluación Médica. - Monitoreo Clínico: Atención de Enfermería. - Solicitud de Interconsultas. - Solicitud de exámenes auxiliares. - Emisión de constancia de atención. - Constatación de fallecimiento: Emisión de informe de defunción / Emisión de certificado de defunción.
Salidas		
Fuente	Descripción	
Datos generales de la institución	Información relevante que sea soporte para la implementación de la Gestión de Riesgos de Seguridad de la Información.	

Datos sobre el área de estudio	Información necesaria del área de Emergencias y los procesos de soporte de TI para la misma para poder seguir con la Gestión de Riesgos. Lista de procesos a analizar en el área de Emergencia.

Una vez seleccionados los procesos de Emergencia sobre los que se va a realizar la gestión de riesgos, en este caso Ingreso y atención de pacientes en triaje y Admisión de pacientes en Emergencia, en esta plantilla se añadirá información de los activos informáticos existentes que involucren las áreas de ambos procesos.

F-001-2	**Fase 1: Establecimiento del contexto** **Proceso 2: Análisis del conocimiento del personal**	NUESTRASALUD Fecha: 30 / 11 / 2023___
Objetivos	Recoger toda la información necesaria sobre los activos del área de estudio y relacionarlo con los procesos de Emergencia en el que se involucra.	
Información Requerida: Información extraída del personal sobre los activos que considera importantes para el desempeño que labora, lista de procesos a analizar en el área de Emergencia.		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Nombre del activo	**Categoría**	**Definición**	**Procesos de Emergencia**	**Relación con otros activos**	**Requerimientos de seguridad**		
					CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
Historia clínica física	Información	Documento médico de carácter obligatorio y legal que almacena la información médica del paciente y todos los procesos que realiza el personal que interviene en su salud.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Personal asistencial y médico	*	*	*
ESSI	Software	Servicio de Salud Inteligente: Permite gestionar las historias clínicas, reduciendo de manera considerable el tiempo de atención.	- Ingreso y atención de pacientes según triaje.	- PC de escritorio - Cable de data	*	*	*

PC de escritorio	Hardware	Equipo de cómputo para registrar y visualizar datos del paciente	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Cable de poder			*
Switch para Red	Redes	Dispositivo físico que provee un adecuado servicio de Internet en el área.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Cable de poder			*
Hoja de filiación del asegurado	Información	Documento que genera por primera vez una historia clínica al asegurado.	- Admisión de Pacientes.	- Sistema Acredita	*	*	*
Impresora	Hardware	Dispositivo físico para imprimir documentación.	- Admisión de Pacientes.	- PC de escritorio			*
Máquina de brazaletes	Hardware	Dispositivo físico que imprime un brazalete en el cual se registra los datos principales, historia clínica y hacia dónde es derivado el paciente.	- Admisión de Pacientes.	- Sistema ESSI			*
Tensiómetro digital	Hardware	Aparato médico que observa el nivel de frecuencia cardiaca y pulso del paciente.	- Ingreso y atención de pacientes adultos en triaje.				*
Antivirus Sophos	Software	Programa encargado de proteger y eliminar virus en cada computadora.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- PC de escritorio			*
Password	Información	Mezcla de números, letras y signos que al ser digitados se obtiene acceso al uso del computador, programa, etc.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Personal responsable	*	*	*
Jefe de TI	Personal	Persona encargada del control y administración de los recursos informáticos hacia todas las áreas del hospital.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.				*
Sistema Acredita	Software	Sistema de acreditación del aseguramiento de salud del paciente.	- Admisión de Pacientes.	- Cable de data	*	*	*
Módem	Hardware	Dispositivo físico que hace posible la comunicación entre computadoras.	- Ingreso y atención de pacientes en triaje.	- Cable de data			*

			- Admisión de Pacientes.				
Sistema de Alimentación Ininterrumpida (UPS)	Hardware	Dispositivo físico que permite regular el voltaje en caso sucede una falla o corte de energía eléctrica.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.				*
Servidor Backup	Hardware	Equipo que permite respaldar la información médica del paciente.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Sala de Servidores	*		*
Sala de Servidores	Infraestructura	Espacio donde se resguarda la protección de servidores para su adecuado uso, control y mantenimiento.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Cable de data - Sistema de Alimentación Ininterrumpida (UPS)		*	*
Ticket de Triaje	Información	Documento físico que permite informar al admisionista sobre el área que será destinado el paciente acompañado de la firma del doctor de turno.	- Admisión de Pacientes.	- Personal asistencial y médico - Tensiómetro digital		*	*
Servidor Asterisk	Hardware	Equipo de comunicaciones que brinda funciones de llamadas bajo el protocolo IAX (telefonía IP).	- Ingreso y atención de pacientes en triaje.	- Sala de Servidores	*		*
Formato de Referencia / Contrarreferencia	Información	Formulario digital en la cual el médico registra los síntomas y exámenes realizados con su respectivo diagnóstico, con el fin de asignarlo al centro de salud conveniente.	- Ingreso y atención de pacientes en triaje.	- Sistema ESSI	*	*	*
Emisión de pagaré	Información	Documento que registra el pagaré en caso el paciente no esté asegurado o requiere un servicio de atención extra.	- Admisión de Pacientes.	- Sistema de Registro de Pagaré	*	*	*
Personal asistencial y médico	Personal	Personas capacitadas para brindar atención y servicio médico al paciente.	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.				*
Cable de data	Hardware	Cable por el que viajan los datos de red	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.				*
Sistema de Registro de Pagaré	Software	Sistema que se encarga de emitir el pagaré dirigido a pacientes particulares	- Admisión de Pacientes.	- PC de escritorio	*	*	*

Servicio de Internet	Redes	Sistema descentralizado de redes de computadoras, que permite la conexión a través de una variedad de recursos, servicios e información	- Ingreso y atención de pacientes en triaje. - Admisión de Pacientes.	- Módem			*
Formulario Ley de Emergencia	Información	Formato para gestionar el trámite de atención al paciente en base a su prioridad de atención.	- Admisión de Pacientes.	- Personal asistencial y médico	*	*	*

Una vez listado los activos, se procede a entrevistar a parte del personal que labora en ambas áreas, con el fin de obtener información respecto a la importancia de cada activo en relación a su integridad, disponibilidad y confidencialidad, agregando niveles a partir del 1 (menos importante) al 5 (muy importante). Luego a ello se establecerá una sumatoria por cada activo, y de acuerdo a ello se establece el valor del impacto, establecidos del 1 (Muy bajo) al 5 (Muy alto). Adicional a ello, se buscará información sobre las normas o disposiciones emitidas por organismos como EsSalud o Minsa, que estén en relación con el resguardo de la información de los activos en mención.

F-002 – 3A	**Fase 2: Análisis de activos, amenazas y vulnerabilidades** **Proceso 3: Identificación de Activos**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Valorar los activos clasificados del proceso anterior, teniendo en cuenta la a las dimensiones de la seguridad de la información.	
Información requerida: Lista de activos importantes de los procesos seleccionados de Emergencias.		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Código	**Activo**	**Normas o disposiciones relacionadas con el activo**	**Niveles de valoración del activo**			**Total**	**Impacto**
			Integridad [I]	**Disponibilidad [D]**	**Confidencialidad [C]**		
[I] – HCLF	Historia Clínica Física	- Gestión de la historia clínica en los centros asistenciales del Seguro Social de Salud ESSALUD - Política Institucional de Seguridad de la Información - Política Institucional de Protección de Datos Personales	5	5	5	15	5
[SW] - ESSI	ESSI	- Disposiciones para el acceso, registro y uso de la información de las prestaciones de salud en el sistema informático servicio de salud inteligente - ESSI del Seguro Social de Salud – ESSALUD - Política Institucional de Protección de Datos Personales	5	5	5	15	5
[HW] - PC	PC de Escritorio	- Políticas de Seguridad Informática de EsSalud	3	5	3	11	3

		- Normas para el uso de computadoras personales y periféricos en EsSalud - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD)					
[HW] - SWR	Switch de red	- Políticas de Seguridad Informática – Seguridad Física y del Entorno - Normas para el uso de computadoras personales y periféricos en EsSalud - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD)	2	5	2	9	3
[I] - HFILASG	Hoja de filiación del asegurado	- Política Institucional de Seguridad de la Información - Política Institucional de Protección de Datos Personales	5	5	4	14	4
[HW] – IMP	Impresora	- Políticas de Seguridad Informática de EsSalud - Normas para el uso de computadoras personales y periféricos en EsSalud - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD)	1	5	1	7	2
[HW] – MBRZ	Máquina de brazaletes	- Políticas de Seguridad Informática de EsSalud - Normas para el uso de computadoras personales y periféricos en EsSalud	1	2	5	8	3
[HW] – TENSDG	Tensiómetro digital	- Políticas de Seguridad Informática de EsSalud	1	2	5	8	3
[SW] – SOPH	Antivirus Sophos	- Políticas de Seguridad Informática de EsSalud	3	3	5	11	3
[I] – PWD	Password	- Políticas de Seguridad Informática de EsSalud - Normas para el uso de computadoras personales y periféricos en EsSalud	5	5	5	15	5
[P] – JEFTI	Jefe de TI	- Políticas de Seguridad Informática de EsSalud - Política Institucional de Seguridad de la Información	2	2	4	8	4
[SW] – SISTAC	Sistema Acredita	- Políticas de Seguridad Informática de EsSalud	3	2	5	10	4
[HW] – MODM	Módem	- Normas para el uso de computadoras personales y periféricos en EsSalud	1	2	5	8	3

		- Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD)					
[HW] – UPS	Sistema de Alimentación Ininterrumpida (UPS)	- Políticas de Seguridad Informática de EsSalud - Normas para el uso de computadoras personales y periféricos en EsSalud	1	1	5	7	3
[HW] – SVBCK	Servidor Backup	- Normas para brindar seguridad a los servidores de las redes de Informática - Políticas de Seguridad Informática de EsSalud - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD)	3	4	5	12	4
[L] – SSERV	Sala de Servidores	- Normas para brindar seguridad a los servidores de las redes de Informática - Políticas de Seguridad Informática de EsSalud	4	5	5	14	4
[I] – TCKTR	Ticket de Triaje	- Políticas de Seguridad Informática de EsSalud	4	5	5	14	4
[HW] – SVASK	Servidor Asterisk	- Normas para brindar seguridad a los servidores de las redes de Informática - Criterios de vigencia tecnológica de equipamiento informático y de comunicaciones en el Seguro Social de Salud (ESSALUD) - Políticas de Seguridad Informática de EsSalud	3	4	5	12	3
[I] – FREFCT	Formato de Referencia / Contrarreferencia	- Políticas de Seguridad Informática de EsSalud - Política Institucional de Protección de Datos Personales	5	5	5	15	4
[I] – EMSPAG	Emisión de pagaré	- Política Institucional de Seguridad de la Información - Política Institucional de Protección de Datos Personales	4	5	4	13	3
[HW] – CDTA	Cable de data	- Normas para el uso de computadoras personales y periféricos en EsSalud	1	2	5	8	3
[SW] – SISPAG	Sistema de Registro de Pagaré	- Políticas de Seguridad Informática de EsSalud	3	3	5	11	3
[R] – SINTER	Servicio de Internet	- Normas para una adecuada racionalización y administración de los servicios de internet en EsSalud	1	2	5	8	4

		- Normas para la administración y control de los servicios de internet, intranet y extranet en Essalud					

Posteriormente, se realiza una lista de amenazas por activo, guiándonos del catálogo de amenazas de Magerit, aquí agrupamos los activos que tienen en común las mismas amenazas y consecuencias.

F-002	**Fase 2: Análisis de activos, amenazas y vulnerabilidades** **Proceso 4: Identificación de amenazas**	NUESTRASALUD Fecha: 30/ 11 /2023
Objetivos	Identificar las amenazas correspondientes a los activos críticos, los responsables de ese activo y la probabilidad con que ocurre el determinado evento.	
Información Requerida: Lista de activos principales de los procesos analizados del área de Emergencias.		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Activo	Responsable	Amenaza	Probabilidad	Consecuencia(s)
[I] – HCLF, [I] – HFILASG, [I] – FREFCT	Personal de Admisión y Triaje	[N.1] Fuego	1	- Destrucción de los datos personales del paciente. - Demora en la emisión de informes. - Pacientes insatisfechos. - Aumento de esfuerzo laboral.
		[N.2] Daños por agua	1	
		[I.1] Fuego	1	- Destrucción de los datos personales del paciente. - En caso sea deliberado, se quebranta la Política Institucional de Protección de Datos Personales. - Demora en la emisión de informes. - Pacientes insatisfechos. - Aumento de esfuerzo laboral.
		[I.2] Daños por agua	1	
		[E.15] Alteración accidental de la información	3	- Modificación de datos críticos o sensibles. - Divulgación o destrucción de información confidencial. - Se quebranta la Política Institucional de Protección de Datos Personales.
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	3	
		[A.11] Acceso no autorizado	2	

[I] – TCKTR, [I] – EMSPAG	Personal de Admisión y Triaje	[E.15] Alteración accidental de la información	3	- Modificación de datos críticos o sensibles.
		[E.18] Destrucción de información	2	- Aumento de esfuerzo laboral. - Pacientes insatisfechos.
[I] – PWD	Personal de Admisión y Triaje	[E.19] Fugas de información	1	- Modificación de datos críticos o sensibles. - Divulgación de información confidencial. - Posible sustracción de datos. - Se quebranta la Política Institucional de Protección de Datos Personales.
		[A.11] Acceso no Autorizado	1	
[SW] – ESSI	Personal de Admisión y Triaje	[E.19] Fugas de información	2	- Modificación de datos críticos o sensibles. - Divulgación de información confidencial. - Posible sustracción de datos. - Se quebranta la Política Institucional de Protección de Datos Personales.
		[A.6] Abuso de privilegios de acceso	2	
		[A.11] Acceso no autorizado	3	
		[I.5] Avería de origen físico o lógico	3	- Interrupción de acceso a información crítica o software institucional. - Demora en la emisión de informes de diagnóstico del paciente. - Registro (triaje) de manera manual. - Reclamos por demora de atención. - Aumento de esfuerzo laboral.
		[E.24] Caída del sistema por agotamiento de recursos	1	
[SW] – SISTAC, [SW] – SISPAG	Personal de admisión	[I.5] Avería de origen físico o lógico	2	- Falta de acreditación y autenticación de la identidad del paciente. - Pacientes insatisfechos. - Interrupción de acceso al software. - Aumento de esfuerzo laboral.
		[E.24] Caída del sistema por agotamiento de recursos	3	
[SW] – SOPH	Personal de Admisión y Triaje	[I.5] Avería de origen físico o lógico	2	- Interrupción de acceso al software. - Aumento de esfuerzo laboral - Reclamos por demora de atención.
		[E.24] Caída del sistema por agotamiento de recursos	2	
		[E.8] Difusión de software dañino	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
[HW] – PC, [HW] – SWR, [HW] – IMP, [HW] – UPS	Personal de Admisión y Triaje	[N.1] Fuego	1	- Interrupción de acceso a información crítica o software institucional. - Demora en la emisión de informes de diagnóstico del paciente. - Registro (triaje) de manera manual. - Pacientes insatisfechos. - Aumento de esfuerzo laboral.
		[N.2] Daños por agua	1	
		[I.1] Fuego	1	
		[I.2] Daños por agua	1	
		[I.3] Contaminación mecánica	3	

		[I.6] Corte del suministro eléctrico	2	
		[I.7] Condiciones inadecuadas de temperatura o humedad	4	
		[I.5] Avería de origen físico o lógico	3	
	Personal de TI	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	
[HW] – MODM, [HW] – CDTA	Personal de Admisión y Triaje	[N.1] Fuego	1	- Interrupción de acceso a información crítica o software institucional. - Demora en la emisión de informes de diagnóstico del paciente. - Registro (triaje) de manera manual. - Pacientes insatisfechos. - Aumento de esfuerzo laboral.
		[N.2] Daños por agua	1	
		[I.1] Fuego	1	
		[I.2] Daños por agua	1	
		[I.3] Contaminación mecánica	3	
		[I.6] Corte del suministro eléctrico	2	
[HW] – SVBCK, [HW] – SVASK	Jefe y Técnicos de TI	[I.5] Avería de origen físico o lógico	3	- Interrupción de acceso a información crítica o software institucional. - Destrucción de hardware. - Reubicación temporal del hardware. - Seguridad cuestionada.
		[I.6] Corte del suministro Eléctrico	2	
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	
		[E.2] Errores del administrador	1	
		[E.3] Errores de monitorización (log)	1	
		[E.4] Errores de configuración	1	
[HW] – MBRZ, [HW] – TENSDG	Personal de Admisión y Triaje / Usuarios externos	[I.5] Avería de origen físico o lógico	1	- Posible deterioro de salud del paciente. - Demora en la emisión de informes de diagnóstico del paciente. - Pacientes insatisfechos. - Aumento de esfuerzo laboral.
		[A.23] Manipulación de los equipos	1	
		[I.1] Fuego	1	
		[I.2] Daños por agua	1	
		[E.25] Robo	1	

[L] – SSERV	Jefe y Técnicos de TI	[I.1] Fuego	1	- Demora en la emisión de informes de diagnóstico del paciente. - Aumento de esfuerzo laboral. - Interrupción de acceso a información crítica o software institucional. - Demora en la emisión de informes de diagnóstico del paciente. - Aumento de esfuerzo laboral. - Interrupción de acceso a información crítica o software institucional.
		[I.2] Daños por agua	1	
		[I.10] Degradación de los soportes de almacenamiento de la información	3	
		[I.7] Condiciones inadecuadas de temperatura o humedad	3	
[R] – SINTER	Jefe y Técnicos de TI	[I.8] Fallo de servicios de comunicaciones	3	
		[I.9] Interrupción de otros servicios y suministros esenciales	3	
		[A.24] Denegación de servicio	3	
[P] – JEFTI	Jefe de TI	[E.28] Indisponibilidad del personal	2	- Aumento de esfuerzo laboral. - Demora en atención en cualquier incidencia en el área de Emergencia.
		[E.14] Escapes de información	1	- Divulgación de información confidencial.
		[E.19] Fugas de información	2	
		[A.9] [Re-] encaminamiento de mensajes	1	

Una vez definida las amenazas, se procede a analizar la causa que originan las mismas, y definir su nivel de gravedad (Alta, media, baja) para tenerlo en cuenta en las respectivas medidas de protección.

F-002	**Fase 2: Análisis de activos, amenazas y vulnerabilidades** **Proceso 5: Identificación de vulnerabilidades**		NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Definir los niveles de vulnerabilidad de los activos mencionados en relación con sus amenazas		
Información Requerida: Lista de los activos críticos con sus respectivas amenazas			**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI
Activo	**Amenaza**	**Vulnerabilidad**	**Nivel de gravedad**
[I] – HCLF, [I] – HFASG, [I] – FREFCT	[N.1] Fuego [N.2] Daños por agua	- Falta de capacitación periódica de planes de Contingencia frente a desastres.	Alta
	[I.1] Fuego [I.2] Daños por agua [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [A.11] Acceso no autorizado	- Desconocimiento del personal frente a las normas y prácticas de seguridad de la información en la institución - Falta de responsabilidades de seguridad de la información en descripciones de puestos	Alta
[I] – TCKTR, [I] – EMSPAG	[E.15] Alteración accidental de la información [E.18] Destrucción de información	- Desconocimiento del personal frente a las normas y prácticas de seguridad de la información en la institución	Alta
[I] – PWD	[E.19] Fugas de información		Media

	[A.11] Acceso no Autorizado	- Desconocimiento del personal frente a las normas y prácticas de seguridad de la información en la institución - Manejo pobre de contraseñas	
[SW] – ESSI	[E.19] Fugas de información	- No se cierra la sesión cuando se abandona la estación de trabajo	Alta
	[A.6] Abuso de privilegios de acceso	- Incorrecta asignación de derechos de acceso	Alta
	[A.11] Acceso no autorizado		
	[I.5] Avería de origen físico o lógico	- Falta de procedimientos para reportar debilidades de seguridad - Trabajo no supervisado por personal externo o de limpieza - Uso incorrecto de software	Media
	[E.24] Caída del sistema por agotamiento de recursos	- Pobre conjunto de cableado	Media
[SW] – SISTAC, [SW] – SISPAG	[I.5] Avería de origen físico o lógico	- Falta de procedimientos para reportar debilidades de seguridad - Trabajo no supervisado por personal externo o de limpieza - Uso incorrecto de software	Media
	[E.24] Caída del sistema por agotamiento de recursos	- Pobre conjunto de cableado	Media
[SW] – SOPH	[I.5] Avería de origen físico o lógico	- Uso incorrecto de software - Falta de procedimientos para reportar debilidades de seguridad	Baja
	[E.24] Caída del sistema por agotamiento de recursos		
	[E.20] Vulnerabilidades de los programas (software)		
	[E.8] Difusión de software dañino		
[HW] – PC, [HW] – SWR, [HW] – IMP, [HW] – UPS	[N.1] Fuego	- Falta de protección física del edificio, puertas y ventanas - Uso incorrecto de hardware - Susceptibilidad a humedad, polvo, corrosión - Trabajo no supervisado por personal externo o de limpieza	Media
	[N.2] Daños por agua		
	[I.1] Fuego		
	[I.2] Daños por agua		
	[I.3] Contaminación mecánica		
	[I.7] Condiciones inadecuadas de temperatura o humedad		

	[I.6] Corte del suministro eléctrico	- Pobre conjunto de cableado - Susceptibilidad a variaciones de voltaje	Media
	[I.5] Avería de origen físico o lógico	- Falta de esquemas periódicos de reemplazo - Falta de procedimiento de control de cambio - Falta de planes de continuidad	Media
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)		
[HW] – MODM, [HW] – CDTA	[N.1] Fuego	- Falta de protección física de la institución, puertas y ventanas - Trabajo no supervisado por personal externo o de limpieza	Alta
	[N.2] Daños por agua		
	[I.1] Fuego		
	[I.2] Daños por agua		
	[I.3] Contaminación mecánica		
	[I.6] Corte del suministro eléctrico	- Pobre conjunto de cableado	Alta
[HW] – SVBCK, [HW] – SVASK	[I.5] Avería de origen físico o lógico	- Falta de protección física de la institución, puertas y ventanas - Trabajo no supervisado por personal externo o de limpieza	Alta
	[I.6] Corte del suministro Eléctrico	- Pobre conjunto de cableado	Alta
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	- Falta de procedimiento de seguimiento de instalaciones de procesamiento de la información - Falta de procedimientos para reportar debilidades de seguridad - Falta de esquemas periódicos de reemplazo	Alta
	[E.2] Errores del administrador	- Falta de registros en bitácoras del administrador y operador	Alta
	[E.3] Errores de monitorización (log)		
	[E.4] Errores de configuración	- Falta de procedimientos para reportar debilidades de seguridad	Alta
[HW] – MBRZ, [HW] – TENSDG	[I.5] Avería de origen físico o lógico	- Falta de procedimientos para reportar debilidades de seguridad	Media
	[A.23] Manipulación de los equipos	- Trabajo no supervisado por personal externo o de limpieza	Media
	[I.1] Fuego		
	[I.2] Daños por agua		

	[E.25] Robo	- Almacenamiento no protegido	
[L] – SSERV	[I.1] Fuego	- Uso inadecuado o descuidado de control de acceso físico a edificios y recintos - Falta de protección física del edificio, puertas y ventanas	Media
	[I.2] Daños por agua		
	[I.10] Degradación de los soportes de almacenamiento de la información		
	[I.7] Condiciones inadecuadas de temperatura o humedad	- Trabajo no supervisado por personal externo o de limpieza	Media
[R] – SINTER	[I.8] Fallo de servicios de comunicaciones	- Pobre conjunto de cableado	Alta
	[I.9] Interrupción de otros servicios y suministros esenciales	- Inadecuada gestión de red (Resiliencia de ruteo)	Alta
	[A.24] Denegación de servicio	- Tráfico sensible desprotegido - Red de energía inestable	Alta
[P] – JEFTI	[E.28] Indisponibilidad del personal	- Entrenamiento insuficiente en seguridad - Falta de conciencia de seguridad - Falta de procedimientos de identificación y evaluación de riesgos - Desconocimiento del personal frente a las normas y prácticas de seguridad de la información en la institución	Alta
	[E.14] Escapes de información		
	[E.19] Fugas de información		
	[A.9] [Re]encaminamiento de mensajes	- Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	Media

Se va a analizar de forma más detallada los factores causantes de las amenazas (nombrados como actores) en las cuales se va a agrupar en 4 categorías: Acciones premeditadas del personal, Acciones accidentales del personal, Problemas de software y hardware, Problemas a nivel externo o de infraestructura. Todas las categorías mencionadas engloban distintas situaciones que originan las amenazas. A su costado se presentará el resultado de las amenazas en relación a la seguridad de la información: Divulgación, Modificación, Pérdida / Destrucción, Interrupción.

F-003	**Fase 3: Evaluación del riesgo** **Proceso 6: Identificación del riesgo**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Analizar las amenazas en relación a sus agentes causantes (denominados actores), y describir el resultado que conlleva en caso se materialice dicha amenaza.	
Información Requerida: Lista de vulnerabilidades en relación a sus activos y amenazas.		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Activo	**Amenaza**	**Actor**	**Resultado (en relación a la información)**
[I] – HCLF, [I] – HFASG, [I] – TCKTR, [I] – FREFCT, [I] – EMSPAG	[N.1] Fuego	- Problemas a nivel externo o de infraestructura - Acciones accidentales del personal	- Pérdida / Destrucción
	[N.2] Daños por agua		
	[I.1] Fuego	- Acciones premeditadas del personal	- Pérdida / Destrucción
	[I.2] Daños por agua		
	[E.18] Destrucción de información	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas de software y hardware	- Pérdida / Destrucción
	[E.15] Alteración accidental de la información	- Acciones accidentales del personal - Problemas de software y hardware	- Modificación
	[E.19] Fugas de información	- Acciones premeditadas del personal - Acciones accidentales del personal	- Divulgación
	[A.11] Acceso no autorizado	- Acciones premeditadas del personal - Acciones accidentales del personal	- Divulgación

[I] – TCKTR, [I] – EMSPAG	[E.15] Alteración accidental de la información	- Acciones accidentales del personal	- Modificación
	[E.18] Destrucción de información	- Acciones premeditadas del personal - Acciones accidentales del personal	- Pérdida / Destrucción
[I] – PWD	[E.19] Fugas de información	- Acciones premeditadas del personal - Acciones accidentales del personal	- Modificación - Divulgación
	[A.11] Acceso no autorizado		
[SW] – ESSI, [SW] – SISTAC, [SW] – SISPAG	[E.19] Fugas de información	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas de software y hardware	- Pérdida / Destrucción - Divulgación - Modificación - Interrupción
	[A.6] Abuso de privilegios de acceso		
	[A.11] Acceso no autorizado		
	[I.5] Avería de origen físico o lógico		
	[E.24] Caída del sistema por agotamiento de recursos	- Problemas de software y hardware	- Interrupción
[SW] – SOPH	[I.5] Avería de origen físico o lógico	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas de software y hardware	- Interrupción
	[E.24] Caída del sistema por agotamiento de recursos		
	[E.20] Vulnerabilidades de los programas (software)		
	[E.8] Difusión de software Dañino		
[HW] – PC, [HW] – SWR, [HW] – IMP, [HW] – UPS	[N.1] Fuego	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas a nivel externo o de infraestructura	- Pérdida / Destrucción - Divulgación - Modificación - Interrupción
	[N.2] Daños por agua		
	[I.1] Fuego		
	[I.2] Daños por agua		
	[I.3] Contaminación mecánica	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas de software y hardware - Problemas a nivel externo o de infraestructura	- Pérdida / Destrucción - Divulgación - Modificación - Interrupción
	[I.6] Corte del suministro eléctrico		
	[I.7] Condiciones inadecuadas de temperatura o humedad		
	[I.5] Avería de origen físico o lógico		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)		
[HW] – MODM, [HW] – CDTA	[N.1] Fuego	- Acciones accidentales del personal - Problemas a nivel externo o de infraestructura	- Pérdida / Destrucción
	[N.2] Daños por agua		
	[I.1] Fuego	- Acciones premeditadas del personal - Acciones accidentales del personal	- Pérdida / Destrucción - Interrupción
	[I.2] Daños por agua		
	[I.3] Contaminación mecánica		

	[I.6] Corte del suministro eléctrico		
[HW] – SVBCK, [HW] – SVASK	[I.5] Avería de origen físico o lógico [A.23] Manipulación de los equipos [I.1] Fuego [I.2] Daños por agua [E.25] Robo	- Acciones premeditadas del personal - Acciones accidentales del personal	- Pérdida / Destrucción - Interrupción
[L] – SSERV	[I.1] Fuego [I.2] Daños por agua [I.10] Degradación de los soportes de almacenamiento de la información [I.7] Condiciones inadecuadas de temperatura o humedad	- Acciones premeditadas del personal - Acciones accidentales del personal - Problemas a nivel externo o de infraestructura	- Pérdida / Destrucción - Interrupción
[R] – SINTER	[I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales [A.24] Denegación de servicio	- Acciones accidentales del personal - Problemas de software y hardware - Problemas a nivel externo o de infraestructura	- Interrupción
[P] – JEFTI	[E.28] Indisponibilidad del personal [E.14] Escapes de información [E.19] Fugas de información [A.9] [Re-]encaminamiento de mensajes	- Acciones accidentales del personal - Problemas a nivel externo o de infraestructura	- Pérdida / Destrucción - Divulgación - Interrupción

De acuerdo a la información establecida en el desarrollo de las plantillas, se asociarán los niveles de riesgos a un color establecido, en el cual el color verde es el Más bajo, un verde más encendido calificado como Bajo, el naranja viene a ser Importante y el color rojo viene a ser el que representa el riesgo Crítico

F-003	**Fase 3: Evaluación del riesgo** **Proceso 7: Análisis del Riesgo**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Medir el riesgo para ver al detalle su respectivo nivel de criticidad.	**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI
Información Requerida		

Nro Riesgo	**Activo**	**Código Amenaza**	**Probabilidad**	**Impacto**	**Resultado (P x I)**	**Tipo de Riesgo**
R-001	[I] – HCLF	[N.1]	1	5	5	MB
R-002	[I] – HCLF	[N.2]	1	5	5	MB
R-003	[I] – HCLF	[I.1]	1	5	5	MB
R-004	[I] – HCLF	[I.2]	1	5	5	MB
R-005	[I] – HCLF	[E.15]	3	5	15	I
R-006	[I] – HCLF	[E.18]	2	5	10	B
R-007	[I] – HCLF	[E.19]	3	5	15	I
R-008	[I] – HCLF	[A.11]	2	5	10	B
R-009	[I] - HFILASG	[N.1]	1	4	4	MB
R-010	[I] - HFILASG	[N.2]	1	4	4	MB
R-011	[I] - HFILASG	[I.1]	1	4	4	MB
R-012	[I] - HFILASG	[I.2]	1	4	4	MB
R-013	[I] - HFILASG	[E.15]	3	4	12	I
R-014	[I] - HFILASG	[E.18]	2	4	8	B
R-015	[I] - HFILASG	[E.19]	3	4	12	I
R-016	[I] - HFILASG	[A.11]	2	4	8	B
R-021	[I] – TCKTR	[E.15]	3	4	12	I
R-022	[I] – TCKTR	[E.18]	2	4	8	B
R-025	[I] – FREFCT	[N.1]	1	4	4	MB
R-026	[I] – FREFCT	[N.2]	1	4	4	MB
R-027	[I] – FREFCT	[I.1]	1	4	4	MB
R-028	[I] – FREFCT	[I.2]	1	4	4	MB
R-029	[I] – FREFCT	[E.15]	3	4	12	I
R-030	[I] – FREFCT	[E.18]	2	4	8	B
R-031	[I] – FREFCT	[E.19]	3	4	12	I
R-032	[I] – FREFCT	[A.11]	2	4	8	B
R-037	[I] – EMSPAG	[E.15]	3	3	9	B
R-038	[I] – EMSPAG	[E.18]	2	3	6	B
R-041	[I] – PWD	[E.19]	1	5	5	MB
R-042	[I] – PWD	[A.11]	1	5	5	MB
R-043	[SW] – ESSI	[E.19]	2	5	10	B
R-044	[SW] – ESSI	[A.6]	2	5	10	B
R-045	[SW] – ESSI	[A.11]	3	5	15	I
R-046	[SW] – ESSI	[I.5]	3	5	15	I
R-047	[SW] – ESSI	[E.24]	1	5	5	MB

R-048	[SW] – SISTAC	[I.5]	2	4	8	B
R-049	[SW] – SISTAC	[E.24]	3	4	12	I
R-050	[SW] – SISPAG	[I.5]	2	4	8	B
R-051	[SW] – SISPAG	[E.24]	3	4	12	I
R-052	[SW] – SOPH	[I.5]	2	3	6	B
R-053	[SW] – SOPH	[E.24]	2	3	6	B
R-054	[SW] – SOPH	[E.8]	1	3	3	MB
R-055	[SW] – SOPH	[E.20]	1	3	3	MB
R-056	[HW] – SVBCK	[I.5]	3	4	12	I
R-057	[HW] – SVBCK	[I.6]	2	4	8	B
R-058	[HW] – SVBCK	[E.23]	2	4	8	B
R-059	[HW] – SVBCK	[E.2]	1	4	4	MB
R-060	[HW] – SVBCK	[E.3]	1	4	4	MB
R-061	[HW] – SVBCK	[E.4]	1	4	4	MB
R-062	[HW] – SVASK	[I.5]	3	3	9	B
R-063	[HW] – SVASK	[I.6]	2	3	6	B
R-064	[HW] – SVASK	[E.23]	2	3	6	B
R-065	[HW] – SVASK	[E.2]	1	3	3	MB
R-066	[HW] – SVASK	[E.3]	1	3	3	MB
R-067	[HW] – SVASK	[E.4]	1	3	3	MB
R-068	[L] – SSERV	[I.1]	1	4	4	MB
R-069	[L] – SSERV	[I.2]	1	4	4	MB
R-070	[L] – SSERV	[I.10]	3	4	12	I
R-071	[L] – SSERV	[I.7]	3	4	12	I
R-072	[R] – SINTER	[I.8]	3	4	12	I
R-073	[R] – SINTER	[I.9]	3	4	12	I
R-074	[R] – SINTER	[A.24]	3	4	12	I
R-075	[P] – JEFTI	[E.28]	2	4	8	B
R-076	[P] – JEFTI	[E.14]	1	4	4	MB
R-077	[P] – JEFTI	[E.19]	2	4	8	B
R-078	[P] – JEFTI	[A.9]	1	4	4	MB
R-079	[HW] – PC	[N.1]	1	3	3	MB
R-080	[HW] – PC	[N.2]	1	3	3	MB
R-081	[HW] – PC	[I.1]	1	3	3	MB
R-082	[HW] – PC	[I.2]	1	3	3	MB
R-083	[HW] – PC	[I.3]	3	3	9	B
R-084	[HW] – PC	[I.6]	2	3	6	B
R-085	[HW] – PC	[I.7]	4	3	12	I
R-086	[HW] – PC	[I.5]	3	3	9	B
R-087	[HW] – PC	[E.23]	3	3	9	B
R-088	[HW] – SWR	[N.1]	1	3	3	MB
R-089	[HW] – SWR	[N.2]	1	3	3	MB
R-090	[HW] – SWR	[I.1]	1	3	3	MB
R-091	[HW] – SWR	[I.2]	1	3	3	MB
R-092	[HW] – SWR	[I.3]	3	3	9	B
R-093	[HW] – SWR	[I.6]	2	3	6	B
R-094	[HW] – SWR	[I.7]	4	3	12	I
R-095	[HW] – SWR	[I.5]	3	3	9	B
R-096	[HW] – SWR	[E.23]	3	3	9	B
R-097	[HW] – UPS	[N.1]	1	3	3	MB
R-098	[HW] – UPS	[N.2]	1	3	3	MB
R-099	[HW] – UPS	[I.1]	1	3	3	MB
R-100	[HW] – UPS	[I.2]	1	3	3	MB
R-101	[HW] – UPS	[I.3]	3	3	9	B
R-102	[HW] – UPS	[I.6]	2	3	6	B
R-103	[HW] – UPS	[I.7]	4	3	12	I
R-104	[HW] – UPS	[I.5]	3	3	9	B
R-105	[HW] – UPS	[E.23]	3	3	9	B

R-106	[HW] – MODM	[N.1]	1	3	3	MB
R-107	[HW] – MODM	[N.2]	1	3	3	MB
R-108	[HW] – MODM	[I.1]	1	3	3	MB
R-109	[HW] – MODM	[I.2]	1	3	3	MB
R-110	[HW] – MODM	[I.3]	3	3	9	B
R-111	[HW] – MODM	[I.6]	2	3	6	B
R-112	[HW] – CDTA	[N.1]	1	3	3	MB
R-113	[HW] – CDTA	[N.2]	1	3	3	MB
R-114	[HW] – CDTA	[I.1]	1	3	3	MB
R-115	[HW] – CDTA	[I.2]	1	3	3	MB
R-116	[HW] – CDTA	[I.3]	3	3	9	B
R-117	[HW] – CDTA	[I.6]	2	3	6	B

Una vez definido los riesgos, se procede a ubicarlos en el mapa establecido, y de acuerdo a su ubicación, visualizar la cantidad de riesgos ubicados en los diferentes niveles (Más bajo, Bajo, Importante y Crítico)

PROBABILIDAD	Continuo	**5**					
	Recurrente	**4**		R-016	R-015, R-056, R-070, R-071, R-085, R-094 R-103		
	Probable	**3**		R-102	R-037, R-062, R-083, R-086, R-087, R-092, R-095, R-096, R-101, R-104, R-105, R-110, R-116	R-013, R-021, R-029, R-031, R-049, R-051, R-072, R-073, R-074	R-005, R-007, R-045, R-046
	Poco Probable	**2**			R-038, R-040, R-052 R-053, R-063, R-064 R-084, R-093, R-111 R-117	R-014, R-022, R-030, R-032, R-048, R-050, R-057, R-058, R-075, R-077	R-006, R-008, R-043, R-044
	Algo Improbable	**1**			R-054, R-055, R-065, R-066, R-067, R-079, R-080, R-081, R-082, R-088, R-089, R-090, R-091, R-097, R-098, R-099, R-100, R-106, R-107, R-108, R-109, R-112, R-113, R-114, R-115	R-009, R-010, R-011, R-012, R-025, R-026, R-027, R-028, R-059, R-060, R-061, R-068, R-069, R-076, R-078	R-001, R-002, R-003, R-004, R-041, R-042, R-047
			1	**2**	**3**	**4**	**5**
			Muy Bajo	Bajo	Regular	Importante	Crítico
			IMPACTO				

F-003	Fase 3: Evaluación del riesgo Proceso 8: Valoración del Riesgo	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Valorar los riesgos obtenidos y registrar el nivel de tolerancia del mismo.	
Información Requerida: Listado de riesgos extraídos del análisis anterior, junto a su respectivo nivel de criticidad		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Cod Riesgo	Activo	Amenaza	Resultado Riesgo	Clasificación Riesgo	Tolerancia
R - 001	[I] – HCLF	[N.1] Fuego	5	Muy bajo	Aceptada
R – 002	[I] – HCLF	[N.2] Daños por agua	5	Muy bajo	Aceptada
R – 003	[I] – HCLF	[I.1] Fuego	5	Muy bajo	Aceptada
R – 004	[I] – HCLF	[I.2] Daños por agua	5	Muy bajo	Aceptada
R-005	[I] – HCLF	[E.15] Alteración accidental de la información	15	Importante	Intolerable
R-006	[I] – HCLF	[E.18] Destrucción de información	10	Bajo	Poco tolerable
R-007	[I] – HCLF	[E.19] Fugas de información	15	Importante	Intolerable
R-008	[I] – HCLF	[A.11] Acceso no Autorizado	10	Bajo	Poco tolerable
R-009	[I] – HFASG	[N.1] Fuego	4	Muy bajo	Aceptada
R-010	[I] – HFASG	[N.2] Daños por agua	4	Muy bajo	Aceptada
R-011	[I] – HFASG	[I.1] Fuego	4	Muy bajo	Aceptada
R-012	[I] – HFASG	[I.2] Daños por agua	4	Muy bajo	Aceptada
R-013	[I] – HFASG	[E.15] Alteración accidental de la información	12	Importante	Poco tolerable
R-014	[I] – HFASG	[E.18] Destrucción de información	8	Bajo	Poco tolerable
R-015	[I] – HFASG	[E.19] Fugas de información	12	Importante	Poco tolerable
R-016	[I] – HFASG	[A.11] Acceso no Autorizado	8	Bajo	Poco tolerable
R-021	[I] – TCKTR	[E.15] Alteración accidental de la información	12	Importante	Poco tolerable
R-022	[I] – TCKTR	[E.18] Destrucción de información	8	Bajo	Poco tolerable
R-025	[I] – FREFCT	[N.1] Fuego	4	Muy bajo	Aceptada
R-026	[I] – FREFCT	[N.2] Daños por agua	4	Muy bajo	Aceptada
R-027	[I] – FREFCT	[I.1] Fuego	4	Muy bajo	Aceptada
R-028	[I] – FREFCT	[I.2] Daños por agua	4	Muy bajo	Aceptada
R-029	[I] – FREFCT	[E.15] Alteración accidental de la información	12	Importante	Poco tolerable

R-030	[I] – FREFCT	[E.18] Destrucción de información	8	Bajo	Poco tolerable
R-031	[I] – FREFCT	[E.19] Fugas de información	12	Importante	Poco tolerable
R-032	[I] – FREFCT	[A.11] Acceso no autorizado	8	Bajo	Poco tolerable
R-037	[I] – EMSPAG	[E.15] Alteración accidental de la información	9	Bajo	Poco tolerable
R-038	[I] – EMSPAG	[E.18] Destrucción de información	6	Bajo	Aceptada
R-041	[I] – PWD	[E.19] Fugas de información	5	Muy bajo	Aceptada
R-042	[I] – PWD	[A.11] Acceso no autorizado	5	Muy bajo	Aceptada
R-043	[SW] – ESSI	[E.19] Fugas de información	10	Bajo	Poco tolerable
R-044	[SW] – ESSI	[A.6] Abuso de privilegios de acceso	10	Bajo	Poco tolerable
R-045	[SW] – ESSI	[A.11] Acceso no autorizado	15	Importante	Intolerable
R-046	[SW] – ESSI	[I.5] Avería de origen físico o lógico	15	Importante	Intolerable
R-047	[SW] – ESSI	[E.24] Caída del sistema por agotamiento de recursos	5	Muy bajo	Aceptada
R-048	[SW] – SISTAC	[I.5] Avería de origen físico o lógico	8	Bajo	Poco tolerable
R-049	[SW] – SISTAC	[E.24] Caída del sistema por agotamiento de recursos	12	Importante	Poco tolerable
R-050	[SW] – SISPAG	[I.5] Avería de origen físico o lógico	8	Bajo	Poco tolerable
R-051	[SW] – SISPAG	[E.24] Caída del sistema por agotamiento de recursos	12	Importante	Poco tolerable
R-052	[SW] – SOPH	[I.5] Avería de origen físico o lógico	6	Bajo	Aceptada
R-053	[SW] – SOPH	[E.24] Caída del sistema por agotamiento de recursos	6	Bajo	Aceptada
R-054	[SW] – SOPH	[E.20] Vulnerabilidades de los programas (software)	3	Muy bajo	Aceptada
R-055	[SW] – SOPH	[E.8] Difusión de software dañino	3	Muy bajo	Aceptada
R-056	[HW] – SVBCK	[I.5] Avería de origen físico o lógico	12	Importante	Poco tolerable
R-057	[HW] – SVBCK	[I.6] Corte del suministro eléctrico	8	Bajo	Poco tolerable
R-058	[HW] – SVBCK	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	8	Bajo	Poco tolerable
R-059	[HW] – SVBCK	[E.2] Errores del administrador	4	Muy bajo	Aceptada
R-060	[HW] – SVBCK	[E.3] Errores de monitorización (log)	4	Muy bajo	Aceptada
R-061	[HW] – SVBCK	[E.4] Errores de configuración	4	Muy bajo	Aceptada
R-062	[HW] – SVASK	[I.5] Avería de origen físico o lógico	9	Bajo	Poco tolerable
R-063	[HW] – SVASK	[I.6] Corte del suministro eléctrico	6	Bajo	Aceptada

R-064	[HW] – SVASK	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6	Bajo	Aceptada
R-065	[HW] – SVASK	[E.2] Errores del administrador	3	Muy bajo	Aceptada
R-066	[HW] – SVASK	[E.3] Errores de monitorización (log)	3	Muy bajo	Aceptada
R-067	[HW] – SVASK	[E.4] Errores de configuración	3	Muy bajo	Aceptada
R-068	[L] – SSERV	[I.1] Fuego	4	Muy bajo	Aceptada
R-069	[L] – SSERV	[I.2] Daños por agua	4	Muy bajo	Aceptada
R-070	[L] – SSERV	[I.10] Degradación de los soportes de almacenamiento de la información	12	Importante	Poco tolerable
R-071	[L] – SSERV	[I.7] Condiciones inadecuadas de temperatura o humedad	12	Importante	Poco tolerable
R-072	[R] – SINTER	[I.8] Fallo de servicios de comunicaciones	12	Importante	Poco tolerable
R-073	[R] – SINTER	[I.9] Interrupción de otros servicios y suministros esenciales	12	Importante	Poco tolerable
R-074	[R] – SINTER	[A.24] Denegación de servicio	12	Importante	Poco tolerable
R-075	[P] – JEFTI	[E.28] Indisponibilidad del personal	8	Bajo	Poco tolerable
R-076	[P] – JEFTI	[E.14] Escapes de información	4	Muy bajo	Aceptada
R-077	[P] – JEFTI	[E.19] Fugas de información	8	Bajo	Poco tolerable
R-078	[P] – JEFTI	[A.9] [Re]encaminamiento de mensajes	4	Muy bajo	Aceptada
R-079	[HW] – PC	[N.1] Fuego	3	Muy bajo	Aceptada
R-080	[HW] – PC	[N.2] Daños por agua	3	Muy bajo	Aceptada
R-081	[HW] – PC	[I.1] Fuego	3	Muy bajo	Aceptada
R-082	[HW] – PC	[I.2] Daños por agua	3	Muy bajo	Aceptada
R-083	[HW] – PC	[I.3] Contaminación mecánica	9	Bajo	Poco tolerable
R-084	[HW] – PC	[I.7] Condiciones inadecuadas de temperatura o humedad	6	Bajo	Aceptada
R-085	[HW] – PC	[I.6] Corte del suministro eléctrico	12	Importante	Poco tolerable
R-086	[HW] – PC	[I.5] Avería de origen físico o lógico	9	Bajo	Poco tolerable
R-087	[HW] – PC	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	9	Bajo	Poco tolerable
R-088	[HW] – SWR	[N.1] Fuego	3	Muy bajo	Aceptada

R-089	[HW] – SWR	[N.2] Daños por agua	3	Muy bajo	Aceptada
R-090	[HW] – SWR	[I.1] Fuego	3	Muy bajo	Aceptada
R-091	[HW] – SWR	[I.2] Daños por agua	3	Muy bajo	Aceptada
R-092	[HW] – SWR	[I.3] Contaminación mecánica	9	Bajo	Poco tolerable
R-093	[HW] – SWR	[I.7] Condiciones inadecuadas de temperatura o humedad	6	Bajo	Aceptada
R-094	[HW] – SWR	[I.6] Corte del suministro eléctrico	12	Importante	Poco tolerable
R-095	[HW] – SWR	[I.5] Avería de origen físico o lógico	9	Bajo	Poco tolerable
R-096	[HW] – SWR	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	9	Bajo	Poco tolerable
R-097	[HW] – UPS	[N.1] Fuego	3	Muy bajo	Aceptada
R-098	[HW] – UPS	[N.2] Daños por agua	3	Muy bajo	Aceptada
R-099	[HW] – UPS	[I.1] Fuego	3	Muy bajo	Aceptada
R-100	[HW] – UPS	[I.2] Daños por agua	3	Muy bajo	Aceptada
R-101	[HW] – UPS	[I.3] Contaminación mecánica	9	Bajo	Poco tolerable
R-102	[HW] – UPS	[I.7] Condiciones inadecuadas de temperatura o humedad	6	Bajo	Aceptada
R-103	[HW] – UPS	[I.6] Corte del suministro eléctrico	12	Importante	Poco tolerable
R-104	[HW] – UPS	[I.5] Avería de origen físico o lógico	9	Bajo	Poco tolerable
R-105	[HW] – UPS	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	9	Bajo	Poco tolerable
R-106	[HW] – MODM	[N.1] Fuego	3	Muy bajo	Aceptada
R-107	[HW] – MODM	[N.2] Daños por agua	3	Muy bajo	Aceptada
R-108	[HW] – MODM	[I.1] Fuego	3	Muy bajo	Aceptada
R-109	[HW] – MODM	[I.2] Daños por agua	3	Muy bajo	Aceptada
R-110	[HW] – MODM	[I.3] Contaminación mecánica	9	Bajo	Poco tolerable
R-111	[HW] – MODM	[I.6] Corte del suministro eléctrico	6	Bajo	Aceptada
R-112	[HW] – CDTA	[N.1] Fuego	3	Muy bajo	Aceptada
R-113	[HW] – CDTA	[N.2] Daños por agua	3	Muy bajo	Aceptada
R-114	[HW] – CDTA	[I.1] Fuego	3	Muy bajo	Aceptada

R-115	[HW] – CDTA	[I.2] Daños por agua	3	Muy bajo	Aceptada
R-116	[HW] – CDTA	[I.3] Contaminación mecánica	9	Bajo	Poco tolerable
R-117	[HW] – CDTA	[I.6] Corte del suministro eléctrico	6	Bajo	Aceptada

Una vez establecida la lista de riesgos, se procede con seleccionar los riesgos de mayor nivel crítico a bajo, y enumerar las respectivas normas de protección. Los responsables se dividen en los siguientes grupos: Personal de Admisión, Personal de Triaje, Jefe de TI, Actores externos.

F-004	Fase 4: Tratamiento del riesgo Proceso 9: Creación de normas de protección	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Generar un catálogo de medidas de protección existentes en la empresa sobre los activos mencionados.	
Información Requerida		**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI

Riesgo	Activo	Proceso(s) de Emergencia	Amenaza	Responsable	Tolerancia	Respuesta al Riesgo	Norma o control recomendado
R-005	[I] – HCLF	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[E.15] Alteración accidental de la información	Personal de Admisión y Triaje	Intolerable	Mitigar	1) Capacitación y concientización sobre seguridad de la información 2) Conocimiento del compendio normativo de Essalud y otras normativas institucionales 3) Planificación y supervisión de la seguridad física de las áreas de la institución 4) Administración de sistemas y redes 5) Gestión de controles de acceso 6) Gestión de vulnerabilidades 7) Tratamiento de cifrado de datos 8) Creación de una arquitectura y diseño de seguridad 9) Gestión de incidentes de seguridad
R-006		- Admisión de pacientes a Emergencia	[E.18] Destrucción de información	Personal de Admisión y Triaje	Poco Tolerable	Evitar	
R-007		- Admisión de pacientes a Emergencia	[E.19] Fugas de información	Personal de Admisión y Triaje	Intolerable	Mitigar	
R-008		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[A.11] Acceso no autorizado	Personal de Admisión y Triaje	Poco Tolerable	Evitar	
R-013	[I] – HFASG	- Admisión de pacientes a Emergencia	[E.15] Alteración accidental de la información	Personal de Admisión	Poco Tolerable	Mitigar	
R-014		- Admisión de pacientes a Emergencia	[E.18] Destrucción de información	Personal de Admisión	Poco Tolerable	Evitar	

R-015		- Admisión de pacientes a Emergencia	[E.19] Fugas de información	Personal de Admisión	Poco Tolerable	Mitigar	10) Control de las prácticas de seguridad al personal 11) Plan de contingencia ante desastres
R-016		- Admisión de pacientes a Emergencia	[A.11] Acceso no Autorizado	Personal de Admisión	Poco Tolerable	Evitar	
R-021	[I] – TCKTR	- Ingreso y atención de pacientes en triaje	[E.15] Alteración accidental de la información	Personal de Triaje	Poco Tolerable	Mitigar	
R-022		- Ingreso y atención de pacientes en triaje	[E.18] Destrucción de información	Personal de Triaje	Poco Tolerable	Evitar	
R-029	[I] – FREFCT	- Ingreso y atención de pacientes en triaje	[E.15] Alteración accidental de la información	Personal de Triaje	Poco Tolerable	Evitar	
R-030		- Ingreso y atención de pacientes en triaje	[E.18] Destrucción de información	Personal de Triaje	Poco Tolerable	Evitar	
R-031		- Ingreso y atención de pacientes en triaje	[E.19] Fugas de información	Personal de Triaje	Poco Tolerable	Mitigar	
R-032		- Ingreso y atención de pacientes en triaje	[A.11] Acceso no autorizado	Personal de Triaje	Poco Tolerable	Mitigar	
R-037	[I] – EMSPAG	- Admisión de pacientes a Emergencia	[E.15] Alteración accidental de la información	Personal de Admisión	Poco Tolerable	Evitar	
R-043	[SW] – ESSI	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[E.19] Fugas de información	Personal de Admisión y Triaje	Poco Tolerable	Evitar	
R-044		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[A.6] Abuso de privilegios de acceso	Personal de Admisión y Triaje	Poco Tolerable	Evitar	
R-045		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[A.11] Acceso no autorizado	Personal de Admisión y Triaje	Intolerable	Evitar	
R-046		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	

R-048	[SW] – SISTAC	- Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión	Poco Tolerable	Mitigar	
R-049		- Admisión de pacientes a Emergencia	[E.24] Caída del sistema por agotamiento de recursos	Personal de Admisión	Poco Tolerable	Mitigar	
R-050	[SW] – SISPAG	- Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión	Poco Tolerable	Mitigar	
R-051		- Admisión de pacientes a Emergencia	[E.24] Caída del sistema por agotamiento de recursos	Personal de Admisión	Poco Tolerable	Mitigar	
R-056	[HW] – SVBCK	- Servicio de TI	[I.5] Avería de origen físico o lógico	Jefe de TI	Poco Tolerable	Mitigar	
R-057		- Servicio de TI	[I.6] Corte del suministro eléctrico	Jefe de TI	Poco Tolerable	Mitigar	
R-058		- Servicio de TI	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Jefe de TI	Poco Tolerable	Mitigar	
R-062	[HW] – SVASK	- Servicio de TI	[I.6] Corte del suministro eléctrico	Jefe de TI	Poco Tolerable	Mitigar	
R-070	[L] – SSERV	- Servicio de TI	[I.10] Degradación de los soportes de almacenamiento de la información	Jefe de TI	Poco Tolerable	Mitigar	
R-071		- Servicio de TI	[I.7] Condiciones inadecuadas de temperatura o humedad	Jefe de TI	Poco Tolerable	Mitigar	
R-072	[R] – SINTER	- Servicio de TI	[I.8] Fallo de servicios de comunicaciones	Jefe de TI	Poco Tolerable	Mitigar	
R-073		- Servicio de TI	[I.9] Interrupción de otros servicios y	Jefe de TI	Poco Tolerable	Mitigar	

			suministros esenciales				
R-074		- Servicio de TI	[A.24] Denegación de servicio	Jefe de TI	Poco Tolerable	Mitigar	
R-075	[P] – JEFTI	- Servicio de TI	[E.28] Indisponibilidad del personal	Jefe de TI	Poco Tolerable	Mitigar	
R-077		- Servicio de TI	[E.19] Fugas de información	Jefe de TI	Poco Tolerable	Mitigar	
R-083	[HW] – PC	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.3] Contaminación mecánica	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-085		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.6] Corte del suministro eléctrico	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-086		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-087		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-092	[HW] – SWR	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.3] Contaminación mecánica	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-094		- Servicios externos	[I.6] Corte del suministro eléctrico	Actores externos	Poco Tolerable	Mitigar	
R-095		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-096		- Servicio de TI	[E.23] Errores de mantenimiento /	Jefe de TI	Poco Tolerable	Mitigar	

			actualización de equipos (hardware)				
R-101	[HW] – UPS	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.3] Contaminación mecánica	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-103		- Servicios externos	[I.6] Corte del suministro eléctrico	Actores externos	Poco Tolerable	Mitigar	
R-104		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.5] Avería de origen físico o lógico	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-105		- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Personal de Admisión y Triaje	Poco Tolerable	Mitigar	
R-110	[HW] – MODM	- Servicio de TI	[I.3] Contaminación mecánica	Jefe de TI	Poco Tolerable	Mitigar	
R-116	[HW] – CDTA	- Ingreso y atención de pacientes en triaje - Admisión de pacientes a Emergencia	[I.6] Corte del suministro eléctrico	Jefe de TI	Poco Tolerable	Mitigar	

Seguidamente, se procede a reunir las normas propuestas, revisar las normas con las que cuenta Essalud, relacionar ambas partes, y proponer una serie de actividades que se plantearán a Alta Dirección, con el fin de contar con su aprobación y disponer de las medidas necesarias para su implementación.

F-005	**Fase 5: Comunicación y monitoreo** **Proceso 10: Plan de comunicación de tratamiento de riesgos**				 Fecha: 30 / 11 / 2023
Objetivos	Formalizar las normas y a partir de ellas, generar una lista de actividades para ser informadas a la Alta Dirección.				**Responsable:** Analista de riesgo **Aprobado por:** Jefe de TI
Información Requerida: Normas propuestas y normas existentes relacionadas a la Seguridad de la Información en Essalud.					
Norma Propuesta	**Normas existentes relacionadas**	**Lista de actividades**	**Responsable**	**Destinatarios**	**Periodicidad**
1) Capacitación y concientización sobre seguridad de la información	- Acceso, registro y uso de la información de las prestaciones de salud en el Sistema Informático Servicio de Salud Inteligente. - Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Política Institucional de Protección de Datos Personales. - Política Institucional de Seguridad de la Información - Políticas de seguridad informática de Essalud.	Calendarización sobre las capacitaciones que incluyen sesiones sobre sensibilización y formación en materia de seguridad (detección de virus, cortes de red, manejo de información confidencial de pacientes, etc), así como seguridad física.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Cada seis meses
		Diseñar el plan de capacitación en un material accesible para todos los involucrados.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Cada año
		Preparar una ficha que documente la asistencia de los participantes a los talleres de capacitación.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Cada cuatro meses

2) Difusión del compendio normativo de Essalud.	- Acceso, registro y uso de la información de las prestaciones de salud en el Sistema Informático Servicio de Salud Inteligente. - Gestión de la Historia Clínica en los centros asistenciales del Seguro Social de Salud. - Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Normas para brindar seguridad a los servidores de las redes de informática. - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - Política Institucional de Protección de Datos Personales. - Política Institucional de Seguridad de la Información. - Políticas de seguridad informática de ESSALUD - Plan de Contingencia ante lluvias y eventos asociados de Essalud	- Difundir las diversas normas y/o estatutos al personal de la institución relacionadas con la seguridad de la información.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Por capacitación y cada vez que ingresa nuevo personal
		- Asegurar la comprensión de estas normas y motivar a que se apliquen en la institución, poner en contraste con otras instituciones que sí cumplen con las normas en mención.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Por capacitación y cada vez que ingresa nuevo personal
3) Planificación y supervisión de la seguridad física de las áreas de la institución.	- Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Normas para brindar seguridad a los servidores de las redes de informática. - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - Políticas de seguridad informática de ESSALUD	- Documentar en coordinación con Recursos Humanos sobre los requisitos mínimos para preservar la seguridad física de los aparatos, y qué tipo de acciones, desencadenaría una posterior alerta o baja en la institución.	Personal de TI RRHH	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Una vez por año
		- Documentar informes que analicen la infraestructura y topología de la red en relación a la seguridad de la información, y preparar una lista de verificación para su respectivo cuidado.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Una vez al mes

4) Gestión de controles de acceso	- Acceso, registro y uso de la información de las prestaciones de salud en el Sistema Informático Servicio de Salud Inteligente.	- Documentar los roles, permisos, tiempos de inactividad tolerado y restricciones de los diferentes perfiles de usuario de la institución.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Una vez por año
		- Concientizar sobre el cuidado de las contraseñas de los usuarios.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Por capacitación
		Verificar funcionamiento de las políticas sobre control de acceso.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Una vez al mes
5) Implementación de una arquitectura y diseño de seguridad	- Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Normas para brindar seguridad a los servidores de las redes de informática. - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - Políticas de seguridad informática de ESSALUD - Plan de Contingencia ante lluvias y eventos asociados de Essalud	- Realizar un presupuesto que reúna lo necesario para brindar seguridad física a la institución.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Una vez cada 18 meses
		- Evaluar el cumplimiento de las normas de seguridad.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje	Una vez por año
6) Administración de sistemas y redes	- Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Normas para brindar seguridad a los servidores de las redes de informática. - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - Políticas de seguridad informática de ESSALUD	- Diseñar en base a las normativas de Essalud, una lista de verificación que haga cumplir las respectivas normas interpuestas en el documento.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Una vez al mes
		- Documentar los requerimientos mínimos en relación a seguridad física, que debe cumplir un computador, servidor y otros dispositivos físicos de la instalación, para su respectivo instalación y funcionamiento.	Jefe de TI	Personal de TI	Una vez por año
		- Documentar el diseño actual de la red de la institución, y analizar si hay	Jefe de TI	Personal de TI Alta Dirección	Cada 18 meses

		formas de mejorar la seguridad de ellas, sin que afecte la productividad en los empleados.			
7) Gestión de incidentes de seguridad	- Política Institucional de Protección de Datos Personales. - Política Institucional de Seguridad de la Información. - Políticas de seguridad informática de ESSALUD - Plan de Contingencia ante lluvias y eventos asociados de Essalud	- Desarrollar una lista de verificación u otra(s) herramienta(s) para verificar el cumplimiento de las normas de manera mensual.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Una vez por año
		- Documentar los procedimientos necesarios para la identificación y notificación de incidentes en relación a la Seguridad de la Información.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI Alta Dirección	Una vez por año
8) Control de las prácticas de seguridad al personal	- Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Política Institucional de Protección de Datos Personales. - Política Institucional de Seguridad de la Información. - Políticas de seguridad informática de ESSALUD - Plan de Contingencia ante lluvias y eventos asociados de Essalud - Gestión de la Historia Clínica en los centros asistenciales del Seguro Social de Salud.	- Documentar y difundir las funciones y responsabilidades del personal en relación a la seguridad de la información de la institución.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Alta Direccíón	Por capacitación
		- Difundir las nuevas normas y reiterar el cumplimiento de las mismas a todo el personal.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Por capacitación
		- Crear un documento que valide el cumplimiento de estas normas dentro de las actividades rutinarias del personal.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje Alta Dirección	Una vez por año
		- Inspeccionar la rotación de los registros médicos, sobre todo los que transcurren durante la fase de Admisión y Triaje.	Personal de Admisión y Triaje	Personal de Admisión y Triaje	Diario

9) Gestión de vulnerabilidades	- Acceso, registro y uso de la información de las prestaciones de salud en el Sistema Informático Servicio de Salud Inteligente. - Normas para el correcto uso de equipos informáticos y dispositivos móviles en Essalud. - Normas para brindar seguridad a los servidores de las redes de informática. - Normas para una adecuada racionalización y administración de los servicios de internet en ESSALUD. - Política Institucional de Protección de Datos Personales. - Política Institucional de Seguridad de la Información. - Políticas de seguridad informática de ESSALUD.	- Establecer un comité que permita detectar nuevas vulnerabilidades y a su vez verificar el estado de las anteriores vulnerabilidades detectadas.	Jefe de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Cada 3 meses
11) Plan de contingencia ante desastres	- Plan de Contingencia ante lluvias y eventos asociados de Essalud	- Revisar y actualizar el plan de contingencia, informando a su vez a todo el personal durante las capacitaciones.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Por capacitación
		- Agregar un plan de protección y recuperación de registros físicos del paciente ante posibles desastres.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Por capacitación
12) Reporte de Gestión de Riesgos	Revisión de nuevas y anteriores normas	Implementación de la gestión de riesgos propuesta y comparación del mapa de riesgos de la gestión anterior.	Personal de TI	Personal médico involucrado en las áreas de Admisión y Triaje Personal de TI	Cada 18 meses

F-005	**Fase 5: Comunicación y monitoreo** **Proceso 11: Plan de comunicación de riesgos**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Describir los programas de seguridad y comunicar el plan de riesgos a las partes correspondientes.	
Información Requerida: Plan de comunicación de tratamiento de riesgos		**Responsable:** Analista de riesgo **Aprobado por:** Alta Dirección

Programa 01: Capacitación y concientización sobre seguridad de la información / Difusión del compendio normativo de Essalud

Responsable: Jefe de TI	**Tiempo de Implementación:** 2 semanas
Área: Admisión y Triaje de Emergencia	**Gastos:** Jefatura de Unidad de Estadística e Informática

Indicadores:
- N° de normas y/o políticas difundidas / N° de políticas existentes en relación a Seguridad de la Información
- Porcentaje de asistencia a capacitaciones
- Porcentaje de aprobación de evaluación sobre conocimiento de normas

Riesgos relacionados	**Activo(s) asociado(s)**	**Amenazas relacionadas**	**Insumos**	**Recursos**
R-005, R-006, R-007, R-008, R-013, R-014, R-015, R-016, R-029, R-030, R-031, R-032, R-037	[I] – HCLF, [I] – HFASG, [I] – FREFCT	[E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [A.11] Acceso no autorizado	- Calendarización de capacitaciones - Diseño del plan de capacitación formal - Ficha de asistencia de participantes - Repositorio de normas y/o políticas - Cuestionario sobre conocimiento de normas	- Coordinación con la jefatura del Área de Emergencias y Cuidados Críticos, jefatura de TI y jefe de Unidad de Estadística e Informática.

F-005	**Fase 5: Comunicación y monitoreo** **Proceso 11: Plan de comunicación de riesgos**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Describir los programas de seguridad y comunicar el plan de riesgos a las partes correspondientes.	
Información Requerida: Plan de comunicación de tratamiento de riesgos		**Responsable:** Analista de riesgo **Aprobado por:** Alta Dirección

Programa 02: Planificación y supervisión de la seguridad física de las áreas de la institución / Implementación de una arquitectura y diseño de seguridad / Administración de sistemas y redes / Plan de contingencia ante desastres

Responsable: Jefe de TI	**Tiempo de Implementación:** 2 semanas
Área: Admisión y Triaje de Emergencia	**Gastos:** Jefatura de Unidad de Estadística e Informática

Indicadores:
- Porcentaje de cumplimiento de normas sobre cuidado de los equipos.
- Porcentaje de incidencias presentadas en relación al cuidado de los equipos.
- Porcentaje de cumplimiento de normas sobre cuidado de los servidores.
- Porcentaje de cumplimiento del manejo adecuado de los servicios de Internet.
- Nivel de seguridad en los accesos a las instalaciones a la sala de servidores
- Comprobación de ubicación adecuada de los equipos de usuarios

Riesgos relacionados	Activo(s) asociado(s)	Amenazas relacionadas	Insumos	Recursos
R-043, R-044 R-045, R-046 R-048, R-049 R-050, R-051 R-056, R-057 R-058, R-062 R-070, R-071 R-072, R-073 R-074, R-110 R-116	[SW] – ESSI [SW] – SISTAC [SW] – SISPAG [HW] – SVBCK [HW] – SVASK [L] – SSERV [R] – SINTER	[E.19] Fugas de información [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [I.5] Avería de origen físico o lógico [E.24] Caída del sistema por agotamiento de recursos [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware)	- Lista de verificación - Documento de requisitos para el cuidado de equipos y dispositivos - Topología de red del área institucional - Diseño de la infraestructura de la institución - Propuesta para mejorar la seguridad física de la institución - Plan de contingencia ante desastres	- Coordinación con la jefatura del Área de Emergencias y Cuidados Críticos, jefatura de TI y jefe de Unidad de Estadística e Informática.

		[I.10] Degradación de los soportes de almacenamiento de la información [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales [A.24] Denegación de servicio		

F-005	**Fase 5: Comunicación y monitoreo** **Proceso 11: Plan de comunicación de riesgos**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Describir los programas de seguridad y comunicar el plan de riesgos a las partes correspondientes.	
Información Requerida: Plan de comunicación de tratamiento de riesgos		**Responsable:** Analista de riesgo **Aprobado por:** Alta Dirección

Programa 03: Gestión de controles de acceso

Responsable: Jefe de TI	**Tiempo de Implementación:** 2 semanas
Área: Admisión y Triaje de Emergencia	**Gastos:** Jefatura de Unidad de Estadística e Informática

Indicadores:
- Porcentaje de cumplimiento de normas en relación a los controles de acceso.
- Nivel de administración y mantenimiento a los accesos de los sistemas de información

Riesgos relacionados	**Activo(s) asociado(s)**	**Amenazas relacionadas**	**Insumos**	**Recursos**
R-043, R-044, R-045, R-046, R-048, R-049, R-050, R-051, R-070, R-071	[SW] – ESSI [SW] – SISTAC [SW] – SISPAG [L] – SSERV	[E.19] Fugas de información [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [I.5] Avería de origen físico o lógico [E.24] Caída del sistema por agotamiento de recursos [I.10] Degradación de los soportes de almacenamiento de la información [I.7] Condiciones inadecuadas de temperatura o humedad	- Lista de verificación - Documentación sobre los roles, permisos, tiempos de inactividad tolerado y restricciones de los diferentes perfiles de usuario de la institución.	- Coordinación con la jefatura del Área de Emergencias y Cuidados Críticos, jefatura de TI y jefe de Unidad de Estadística e Informática.

F-005	**Fase 5: Comunicación y monitoreo** **Proceso 11: Plan de comunicación de riesgos**	NUESTRASALUD Fecha: 30 / 11 / 2023
Objetivos	Describir los programas de seguridad y comunicar el plan de riesgos a las partes correspondientes.	
Información Requerida: Plan de comunicación de tratamiento de riesgos		**Responsable:** Analista de riesgo **Aprobado por:** Alta Dirección

Programa 04: Gestión de incidentes de seguridad / Control de las prácticas de seguridad al personal / Gestión de vulnerabilidades / Reporte de Gestión de Riesgos

Responsable: Jefe de TI	**Tiempo de Implementación:** 2 semanas
Área: Admisión y Triaje de Emergencia	**Gastos:** Jefatura de Unidad de Estadística e Informática

Indicadores:
- Nivel de comportamiento activo y participativo del personal.
- Nivel de conocimiento de las funciones y responsabilidades del personal en relación a la seguridad de la información de la institución
- Nivel de cumplimiento de las acciones que permitan mantener la seguridad de la información
- Número de vulnerabilidades sin resolver
- Número de incidentes detectados resueltos / Número de incidentes reportados
- Número de riesgos mitigados o eliminados

Riesgos relacionados	**Activo(s) asociado(s)**	**Amenazas relacionadas**	**Insumos**	**Recursos**
Todos los riesgos con nivel crítico (Proceso 9)	Todos los activos relacionados	Todas las amenazas relacionadas	- Lista de verificación - Mapa de riesgos - Plantillas del modelo de gestión de riesgos. - Test de conocimientos dirigidos al personal	- Coordinación con la jefatura del Área de Emergencias y Cuidados Críticos, jefatura de TI y jefe de Unidad de Estadística e Informática.

4.5 Discusión

Ante la interrogante surgida sobre la manera en que puede impactar una gestión de riesgos en la seguridad de la información sobre los procesos de atención de Emergencia, uno de los procesos más críticos dentro de un hospital, podemos decir que el uso de esta herramienta (modelo de gestión de riesgos), permitió salvaguardar uno de los activos críticos más importantes, que son los datos personales del paciente (fundamentado en la Política Institucional de Protección de Datos Personales de Essalud) el cual si llega a ser vulnerado, constituye una pérdida de imagen reputacional y un daño económico hacia la institución [36].

Cabe resaltar que, el modelo propuesto, a diferencia de otras investigaciones, en especial la de Villegas [20] y Medianero [19], presenta un enfoque que busca mayor conocimiento de las reglamentaciones de Essalud, así mismo el conocimiento técnico-normativo de los procesos de Emergencia, y una identificación con sus políticas en relación a la protección de Datos Personales [37] y de Seguridad de la Información [38], en la cual el analista logra una mayor identificación del entorno normativo de la institución, y busca resaltar el consolidar el conocimiento del personal de TI y personal médico del uso y aplicación que se da a la protección de activos de información, resaltando el conocimiento con el que debe contar todos los integrantes de la institución para que las prácticas internas sobre Seguridad de la Información esté en relación con los lineamientos de la normativa de la misma.

Respecto a las demás investigaciones, la de Ordeñana [12] y la de Carmona [16], se tomó como referencia el hecho de que ambos estudios comparten como punto principal, la implementación de la gestión de riesgos hacia un hospital, pero con la diferencia que en la presente investigación analiza de forma más directa la cercanía con la reglamentación existente de la organización, en el caso de Rovira [13], tomaremos en cuenta la importancia del uso del marco de trabajo COBIT, que a través de su propuesta de una adecuada gestión de riesgos, ayuda al correcto cumplimiento tomando como principal importancia los aspectos de gobierno y gestión de riesgos de TI, en nuestro caso se abocó principal al apartado de gestión de riesgos de TI.

Para la investigación de Brand [14], resalta la importancia de concientizar al personal sobre el tema de Seguridad de la Información, el cual comparte esa misma problemática, el personal del hospital médico de nuestra investigación, en este caso usando como parte de

nuestro modelo, el uso de la norma NTP ISO/IEC 27005, a comparación de ellos que usaron la NTC ISO/IEC 27001, enfocándose más, en lo que respecta a nuestra investigación, a un modelo de Seguridad de la Información enfocado en una gestión de riesgos.

En cuanto al estudio de Mere [15], permitió diferenciar las normativas ISO/IEC 3100 y la ISO 27005, que está presenta en la investigación actual, ya que la 31000 está orientada a una implementación de gestión de riesgos a nivel general, y la 27005, está orientado específicamente para Seguridad de la Información. En lo que respecta al estudio de García [17], y la de Banda [18], se usaron normas y estándares similares, con la diferencia de que la presente propuesta busca que el personal que realiza el análisis de riesgos, tenga en conocimiento hasta qué limitaciones puede proponer el uso de las medidas o controles para contrarrestar los riesgos, ya que hay una existencia de normas y políticas de Essalud, que pueden limitar el alcance de las propuestas.

4.6 Conclusiones

El objetivo general de esta investigación fue desarrollar un modelo de gestión de riesgos para contribuir a la seguridad de la información en los procesos de atención de Emergencias para el Sector Salud Pública, el cual pudo ser realizado, ya que se procedió a construir un modelo contextualizado a ese sector, seleccionando las fases y criterios respectivos que comparten las cuatro normativas, siguiendo diversos objetivos específicos, mencionados a continuación:

Objetivo 1:

"Analizar comparativamente marcos de trabajo y normativas de riesgos de seguridad de la información a través de características que permitan armonizar la propuesta de un modelo de gestión de riesgos adaptado a la realidad del sector Salud Pública". Para el presente objetivo, se procedió con el análisis respectivo de los cuatro documentos: NTP ISO/IEC 27005, Cobit 5 para Riesgos, Magerit y Octave, todos de vital importancia para una exitosa implementación de gestión de riesgos, seguidamente se establecieron las características y criterios necesarios, para luego proceder con la armonización de la información adquirida, que permita la elaboración del modelo. En este caso se cumplió con el siguiente indicador:

Indicador	Total	Porcentaje de cumplimiento
Cantidad de marcos de trabajo y normativas de riesgos de seguridad de la información antes de la implementación parcial del modelo de gestión de riesgos.	0	0%
Cantidad de marcos de trabajo y normativas de riesgos de seguridad de la información después de la implementación parcial del modelo de gestión de riesgos.	4	100%

Objetivo 2:

"Seleccionar las fases alineadas a los procesos de emergencias del sector Salud Pública, que permitan determinar el nuevo modelo de gestión de riesgos de Seguridad de la Información".

Para este objetivo, se procedió a construir el modelo, proponiendo las fases que estén en contextualización con los procesos de Emergencia, cumpliendo con el siguiente indicador: "Cantidad de fases y procesos propuestos", logrando determinar 5 fases y 11 procesos.

Objetivo 3:

"Validar el modelo de gestión de riesgos basado en marcos de trabajo estandarizados, mediante juicio de expertos, para valorar el modelo adaptado".

Se recurrió a la opinión y colaboración de 3 jueces expertos en Gestión de Riesgos de TI, el cual, una vez que se les presentó el esquema del modelo propuesto, procedieron a través de su respectiva valoración, dar por aprobado el modelo propuesto mediante V. de Aiken, con un valor de aprobación del 0.92% respecto al cual, al estar cerca al número 1, se obtiene una aprobación bastante alta, logrando cumplir con el siguiente objetivo "Nivel de validación aprobatoria del modelo propuesto".

Objetivo 4:

Implementar de manera parcial el modelo de Gestión de Riesgos para mejorar la Seguridad de la Información en los hospitales del sector Salud Pública de la región.

Se procedió con la implementación parcial del modelo propuesto, al realizar 9 de los 11 procesos establecidos, teniendo en cuenta que para la puesta en marcha de "Plan de comunicación de riesgos" y "Monitoreo de riesgos", los procesos finales, debe haber una posterior comunicación formal con la jefatura de Emergencias en coordinación con el área de TI, y en Monitoreo de riesgos, se debe proceder a hacer el respectivo análisis de los riesgos posterior a la ejecución de las normas de protección establecidas, para ver en qué nivel se ha mitigado o disminuido, logrando cumplir el indicador "Porcentaje de implementación parcial del modelo de Gestión de Riesgos" con un resultado del 81%.

Respecto a las limitaciones que se tuvieron presente en la actual investigación, cabe resaltar la importancia del disponer de un tiempo y espacio adecuado para una adecuada planificación e implementación de la gestión de riesgos, con la adecuada coordinación entre la

jefatura de Emergencia y el área de TI, junto al personal que analiza el riesgo, el cual, al calendarizar las actividades, estas pueden verse afectadas, al existir una situación de emergencia, ya que la presencia de varios pacientes, y en lugares donde la capacidad de ellos en muchos casos desborda, puede poner limitaciones al momento de querer hacer uso de una adecuada implementación de riesgos, sumado a eso las situaciones imprevistas de cualquier índole que se puedan presentar en el trayecto, al ser un hospital que recibe diariamente una cantidad que excede el límite de pacientes que dispone la institución, es por ello resaltar la importancia de una correcta planificación y organización, y si es posible, replantear cómo avanzar con la adecuada implementación, en caso las situaciones de emergencia se presenten.

Recomendaciones

Es importante que el personal encargado de la implementación de gestión del riesgo, mantenga una constante comunicación con todos los participantes que se involucren en el desarrollo del modelo propuesto, ya que es necesario consolidar la apreciación personal e información por parte de cada uno de ellos sobre los activos que considera críticos, asimismo indagar sobre diversos escenarios de amenazas que ellos puedan detallar, conocer al detalle el flujo de información que ocurre durante los procesos de Atención de Emergencia, y a la vez lograr que ellos se identifiquen más con la institución respecto al uso de las diferentes políticas y normativa que dictamina Essalud para protección de la información.

Es recomendable orientar al personal para que pueda obtener un conocimiento directo de las normativas, políticas y documentos reglamentarios de la institución, necesariamente los que influyen en la seguridad de la información, indicarles en qué fuentes puede indagar para estar actualizado y en constante identificación con la institución.

Bibliografía

[1] E. BLOG, «ehcos.com,» [En línea]. Available: https://www.ehcos.com/ciberseguridad-hospitales-prevenir-como-defensa-ataque/. [Último acceso: 10 01 2020].

[2] A. M. DURÁN, «El Tiempo,» 12 05 2017. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-hospitales-del-reino-unido-87378. [Último acceso: 21 05 2021].

[3] M. Karim Nader Ch., «el Hospital,» 04 2018. [En línea]. Available: https://www.linkedin.com/pulse/riesgos-en-la-seguridad-inform%C3%A1tica-salud-4-casos-c%C3%A1ceres/?originalSubdomain=es. [Último acceso: 23 05 2020].

[4] HIMSS, «Healthcare and Cross-Sector Cybersecurity Report (Vol. 14),» vol. 14, 2017.

[5] L. Tejerina, «El sector salud es el más atractivo para los ciberataques. ¿Estamos preparados para protegerlo?,» 2021. [En línea]. Available: https://blogs.iadb.org/salud/es/el-sector-salud-es-el-mas-atractivo-para-los-ciberataques/. [Último acceso: 21 05 2021].

[6] INFOBAE, «infobae,» 10 08 2017. [En línea]. Available: https://www.infobae.com/america/mundo/2017/08/10/ataques-ciberneticos-la-nueva-amenaza-de-muerte-en-los-hospitales-del-mundo/. [Último acceso: 10 01 2020].

[7] Avast, «WannaCry,» 2019. [En línea]. Available: https://www.avast.com/es-es/c-wannacry. [Último acceso: 20 Julio 2019].

[8] Finanzas.com, «Finanzas.com,» [En línea]. Available: https://www.finanzas.com/empresas-y-directivos/ataques-ciberneticos-la-nueva-amenaza-de-muerte-en-los-hospitales_13670733_102.html. [Último acceso: 15 06 2020].

[9] L. Crónica, «La Crónica de Quindio,» 03 04 2018. [En línea]. Available: https://www.cronicadelquindio.com/noticia-completa-titulo-hospital-san-juan-de-dios-fue-victima-de-un-ataque-informatico-seccion-la_ciudad-nota-119227. [Último acceso: 06 06 2020].

[10] Sindicato Nacional Médico del Seguro Social del Perú, «sinamssop,» 7 Marzo 2019. [En línea]. Available: http://www.sinamssop.org/2019/03/manana-se-reunen-presidenta-de-essalud-y-secretario-general-del-sinamssop-para-atender-problemas-de-funcionamiento-de-sistema-sgss/. [Último acceso: 20 Julio 2019].

[11] M. d. J. y. D. Humanos, «gob.pe: Plataforma Digital Única del Estado Peruano,» [En línea]. Available: https://www.gob.pe/institucion/minjus/noticias/45610-autoridad-nacional-de-proteccion-de-datos-personales-realiza-fiscalizacion-en-clinicas-y-hospitales. [Último acceso: 20 06 2020].

[12] J. N. Ordeñana, «Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistemas de la DGI.,» Managua, Nicaragua, 2019.

[13] S. L. C. Rovira, «Diseño de un Plan Estratégico de Seguridad de la Información en una Organización Pública según COBIT 5,» Buenos Aires, Argentina, 2019.

[14] M. F. B. Pantoja, «Diseño de un sistema de gestión de Seguridad de la Información para los procesos asociados al área de TI de la empresa Axede S.A., aplicando la norma NTC ISO/IEC 27001:2013,» Bogotá, 2023.

[15] M. H. H. MERE, «Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones,» Lima, Perú, 2019.

[16] L. D. Carmona Torres, «Implementación de una Metodología de Gestión de Riesgos alineada a la ISO 27005 y Magerit para el proceso “OSE” de una empresa de facturación electrónica en la ciudad de Lima - 2021,» Lima, 2021.

[17] J. C. H. P. S. C. García Porras, «Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú,» Lima, Perú, 2019.

[18] J. C. B. SANTISTEBAN, «MODELO BASADO EN METODOLOGÍAS DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN EMPRESAS DEL SECTOR AGROINDUSTRIAL DE LA REGIÓN LAMBAYEQUE,» Chiclayo, Perú, 2019.

[19] L. G. N. MEDIANERO, «IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA APOYAR EL PROCESO DE ATENCIÓN AL PACIENTE EN INSTITUCIONES DE SALUD,» Chiclayo, 2019.

[20] C. A. Villegas Rivera, «Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas,» Chiclayo, 2022.

[21] A. -. A. E. d. N. y. Certificación, «UNE 71504 - norma española - Metodología de análisis y gestión de riesgos para los sistemas de información,» AENOR, Madrid, 2008.

[22] W. D. Rowe, «Una anatomía del riesgo,» 1988.

[23] G. d. España, *MAGERIT – versión 3.0: Metodología de Análisis y Gestión,* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[24] I. G. 73:2009, «Risk management,» 2009.

[25] 2. C. M. University, «OCTAVE Method Implementation Guide v2.0,» 2001.

[26] D. d. Pueblo, «Manual de Protección de Datos Personales,» Jasmin Luisa Pablo Falconí, Chiclayo, 2019.

[27] L. G. d. Salud, «EsSalud,» [En línea]. Available: http://www.essalud.gob.pe/transparencia/pdf/publicacion/ley26842.pdf. [Último acceso: 2023 12 04].

[28] MINSA, «Digesa - Ministerio de Salud,» [En línea]. Available: http://www.digesa.minsa.gob.pe/publicaciones/descargas/salud_americas/04--CH4--35-48.pdf. [Último acceso: 2023 12 05].

[29] D. O. EuroInnova, «EuroInnova,» [En línea]. Available: https://www.euroinnova.pe/blog/que-son-las-prestaciones#conoce-con-nosotros-queacute-son-las-prestaciones-y-sus-tipos. [Último acceso: 04 12 2023].

[30] G. D. O. Y. P. -. Essalud, «MANUAL DE PROCESOS Y PROCEDIMIENTOS DEL PROCESO DE ATENCIÓN DE SALUD,» Lima, 2019.

[31] S. S. d. Salud, «EsSalud,» 2020. [En línea]. Available: http://www.essalud.gob.pe/nuestra-institucion/. [Último acceso: 03 12 2023].

[32] C. P. F. G. F. &. P. M. Pardo, «HOMOGENIZATION OF MODELS TO SUPPORT MULTI-MODEL PROCESSES IN IMPROVEMENT ENVIRONMENTS. ICSOFT 2009 - 4th International Conference on Software and Data Technologies,» 2009.

[33] ISACA, *COBIT 5 para Riesgos,* ISACA, 2013.

[34] ESSALUD, «TEXTO ACTUALIZADO Y CONCORDADO DEL MANUAL DE OPERACIONES DEL HOSPITAL NACIONAL ALMANZOR AGUINAGA ASENJO,» 2021.

[35] E. Noticias, «EsSalud,» [En línea]. Available: http://noticias.essalud.gob.pe/?inno-noticia=entidades-publicas-y-privadas-deben-a-essalud-mas-de-s-5-mil-millones-por-aportaciones#:~:text=Anot%C3%B3%20que%20EsSalud%20no%20recibe,los%20empleadores%20p%C3%BAblicos%20y%20privados.. [Último acceso: 7 Noviembre 2023].

[36] D. E. Comercio, «Autoridad Nacional de Protección de Datos Personales multa a Essalud con más de 123 mil soles,» *SUCESOS/NOTICIAS,* 18 07 2022.

[37] N. E. R. Gómez, «CLIMA LABORAL Y SU RELACIÓN CON EL DESEMPEÑO DE LOS SERVIDORES CIVILES DEL HOSPITAL LUIS HEYSEN INCHAUSTEGI-ESSALUD, LAMBAYEQUE-PERÚ, 2019,» Chiclayo, 2021.

[38] latercera.com, «latercera.com,» 10 07 2019. [En línea]. Available: https://www.latercera.com/nacional/noticia/gobierno-alerta-ciberataque-empresa-proveedora-grandes-hospitales/735093/. [Último acceso: 10 06 2020].

[39] S. G. Patiño Rosado, «Propuesta metodológica de Gestión de Riesgos de Tecnología de Información y Comunicación (TIC) para Entidades Públicas conforme normativa NTE INEN ISO/IEC 27005,» Quito, Ecuador, 2018.

[40] P. O. R. M. J. A. Cueva Araujo, «Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014,» 2017.

[41] L. A. Moscoso Anaya, E. E. Peña Núñez y M. d. C. Soto Castrillón, «Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú,» Chiclayo, 2018.

[42] F. B. Vásquez Velásquez, «Modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la región Lambayeque,» Chiclayo, 2018.

[43] S. Seiffe, «Introducción a la Ingeniería,» 15 04 2013. [En línea]. Available: https://introaingenieria.wordpress.com/2013/04/15/modelos/. [Último acceso: 10 05 2021].

[44] Milvus, «milvus,» 03 02 2020. [En línea]. Available: https://milvus.online/blog/gestion-de-ti-guia-completo/. [Último acceso: 10 05 2021].

[45] G. Suite, «¿Qué es ITIL y para que sirve?,» 18 05 2018. [En línea]. Available: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/. [Último acceso: 18 05 2021].

[46] G. &. P. C. Vanegas, «Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT,» *redalyc.org,* vol. 12, nº 30, pp. 35-44, 2014.

[47] U. 71504:2008, «Metodología de análisis y gestión de riesgos para los sistemas de información.,» España, 2008.

[48] E. T. d. l. información., *NTP-ISO/IEC 17799,* R.001-2007/INDECOPI-CRT. .

[49] INACAL, *NTP ISO 27005: Gestión de riesgos de la seguridad de la información,* INACAL 2018.

[50] A. de Jong, A. Kolthof, M. Pieper, R. Tjassing, A. van der Veen, T. Verheijen y J. van Bon, Estrategia del Servicio Basada en ITIL® V3 - Guía de Gestión, Amersfoort: Van Haren Publishing, 2008.

[51] Universidad Tec Virtual del Sistema Tecnológico de Monterrey, *Estrategia de servicio (SS),* Monterrey, 2010.

[52] IT Process Maps GbR, Introducción a ITIL® Versión 3 y al Mapa de Procesos ITIL® V3, Alemania: Miembro itSMF, 2010.

[53] L. L. Ortiz Romero, «Modelo de la gestión de procesos de servicios de tecnologías de información basado en las librerías de infraestructura de tecnologías de información (ITIL) para la administración pública nacional.,» Caracas - Venezuela, 2012.

[54] R. M. Dulanto Ramírez y C. E. Palomino Vidal, «Propuesta de implementación de gestión de servicios de TI en una empresa farinácea.,» Lima, 2014.

[55] T. d. J. Lucio Nieto, «Marco para la definición y adecuación de una service management office en el contexto de los servicios de tecnologías de la información.,» Legenés, 2013.

[56] J. Gomez, Nuevos cambios digitales, México DF: Persa, 2009.

[57] R. Gómez, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *Revista de Ingeniería - Universidad de los Andes, Colombia,* nº 31, pp. 109-118, 2018.

[58] E. Appert, «Los riesgos de la tecnología de la información en los servicios financieros,» Deloitte, Londres, 2016.

[59] F. J. V. Duque, «Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional,» Cali, Colombia, 2016.

[60] Guzmán, «Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega.,» Huancayo, 2015.

[61] J. Y. V. CARAZAS, «MARCO DE TRABAJO RISK IT EN LA GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN LA CAJA RURAL DE AHORRO Y CRÉDITO LOS ANDES S.A.,» Puno, 2015.

[62] M. C. Quincho, «DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA,» Huamanga, 2016.

[63] M. Y. Arangurí García, «Modelo de gestión de riesgos de TI basados en estándares adaptados a las TI que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque,» Chiclayo, 2016.

[64] C. D. d. C. y. E. I. G. Institute, «COBIT MARCO REFERENCIAL,» Governance Institute, USA, 2004.

[65] N. T. Colombiana, «NTC-ISO 31000,» icontec international, Colombia, 2016.

[66] E. N. d. Seguridad, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.,» Gobierno de España, España, 2012.

[67] a. A. P. d. Noticias, «andina,» 04 05 2020. [En línea]. Available: https://andina.pe/agencia/noticia-coronavirus-peru-sufrio-mas-433-millones-intentos-ciberataques-2020-795751.aspx. [Último acceso: 12 05 2020].

[68] L. República, «Diario La República,» 17 05 2020. [En línea]. Available: https://larepublica.pe/sociedad/2020/05/17/coronavirus-en-peru-mujer-denuncia-perdida-de-acta-de-defuncion-de-esposo-victima-de-covid-19/. [Último acceso: 21 5 2020].

[69] V. R. Puyén Santos y B. G. Rivas Palacios, «Modelo de Gestión de Riesgos basados en la norma Iso/Iec 27005 y Metodología Magerit para mejorar la Gestión de Seguridad de la Información en el Hospital Regional de Lambayeque.,» Lambayeque, 2019.

[70] E. A. B. GARAVITO, «DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001- 27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ,» 2016.

[71] J. M. L. J. M. S. y. L. E. G. Carlos A. Guerrero, «ESTUDIO COMPARATIVO DE MARCOS DE TRABAJO PARA EL DESARROLLO SOFTWARE ORIENTADO A ASPECTOS,» 2014. [En línea]. Available: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642014000200008. [Último acceso: 15 06 2020].

[72] G. y. Recaman, 2009.

[73] J. Aguirre, «Cadena de bloques: Diseño de una solución para el control de,» Buenos Aires, Argentina, 2020.

[74] «BBC News,» [En línea]. Available: https://www.bbc.com/mundo/noticias-39929920. [Último acceso: 05 04 2021].

[75] N. L. Actualizadas, *Reglamento de la Ley N° 29733 - Ley de Protección de Datos Personales.*

[76] M. d. Salud, «DIRECTIVA ADMINISTRATIVA QUE ESTABLECE EL TRATAMIENTO DE LOS DATOS PERSONALES RELACIONADOS CON LA SALUD O DATOS PERSONALES EN SALUD,» 08 10 2020. [En línea]. Available: http://bvs.minsa.gob.pe/local/MINSA/5118.pdf. [Último acceso: 12 06 2021].

[77] M. d. Salud, «Fundamentos de Salud Pública - Guía del Participante - Programa de Entrenamiento en Salud Pública dirigido a Personal del Servicio Militar Voluntario,» 2016.

[78] I. 22301, «Sistema de Gestión de Continuidad del Negocio,» 2019.

[79] F. V. D., «emol.Nacional,» 10 07 2019. [En línea]. Available: https://www.emol.com/noticias/Nacional/2019/07/10/954138/Gobierno-investiga-ciberataque-que-sufrio-empresa-que-provee-de-informacion-de-examenes-a-hospitales.html. [Último acceso: 27 08 2022].

[80] E. G. ALEMAN, «SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN BASADO EN METODOLOGÍA DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGO EN LA BIBLIOTECA DE LA UNIVERSIDAD DE LA COSTA,» Barranquilla, 2020.

[81] I. Excellence, «Seguridad de la Información,» [En línea]. Available: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/. [Último acceso: 08 12 2022].

[82] ESSALUD, «Política Institucional de Seguridad de la Información,» Lima, 2022.

[83] ESSALUD, «Política Institucional de Protección de Datos Personales,» 2022.

[84] G. d. O. y. P. S. G. d. P. -. E. Gerencia Central de Planeamiento y Presupuesto, «MAPA DE MACROPROCESOS ESSALUD,» Lima, 2019.

[85] I. 13335:2004, «Tecnologías de la información. Técnicas de seguridad. Gestión de la seguridad de tecnologías de la información y las comunicaciones.,» 2004.

Anexos

Anexo 01

ESSALUD

Misión:

"Brindamos prestaciones de salud económicas y sociales a nuestros asegurados con una gestión eficiente e innovadora que garantiza la protección financiera de las prestaciones integrales".

Visión:

"Ser una institución moderna y en mejora continua, centrada en los asegurados, que garantiza el acceso a la seguridad social en salud con ética, oportunidad y calidad".

Principios:

- Solidaridad: Cada cual debe aportar al sistema según su capacidad y recibir según su necesidad.
- Universalidad: Todas las personas deben participar de los beneficios de la seguridad social, sin distinción ni limitación alguna.
- Igualdad: La seguridad social ampara igualitariamente a todas las personas. Se prohíbe toda forma de discriminación.
- Unidad: Todas las prestaciones deben ser suministradas por una sola entidad o por un sistema de entidades entrelazadas orgánicamente y vinculadas a un sistema único de financiamiento.
- Integralidad: El sistema cubre en forma plena y oportuna las contingencias a las que están expuestas las personas.
- Autonomía: La seguridad social tiene autonomía administrativa, técnica y financiera (sus fondos no provienen del presupuesto público, sino de las contribuciones de sus aportantes).

Los 4 hospitales, pertenecientes a la red asistencial mencionada, y objeto de nuestro estudio, son los siguientes: Hospital III Almanzor Aguinaga Asenjo, Hospital II Luis Enrique Heysen, Hospital I Agustín Arbulú Neyra, Hospital I Naylamp.

Mostraremos una breve referencia de cada uno de ellos

1.- Hospital Nacional Almanzor Aguinaga Asenjo

El Hospital Nacional Almanzor Aguinaga Asenjo (HNAAA), hospital de nivel III y de alta complejidad, es la institución más representativa dentro de las redes asistenciales del departamento de Lambayeque.

El HNAAA tiene como fin otorgar servicios de salud a nivel poblacional que corresponde al sector asegurado, conservando la integralidad y atención continua hacia ellos. A su vez, proporciona líneas políticas, investigaciones y aportes científicos para solucionar problemas en relación al sector asegurado de Essalud.

Entre sus funciones principales relacionadas con el servicio de Emergencia mencionamos a la atención integral de salud, el cual, a través de servicios de promoción, prevención de la enfermedad, servicio de ambulancia, hospitalización. Otra de sus funciones es el cumplimiento de las políticas, normativa, actividad, etc., en relación con los servicios de salud que ofrece. Se organiza en base a un catálogo de servicios, a su vez de tener comunicados a los pacientes sobre sus derechos y obligaciones en relación a los servicios de salud, datos sobre la institución, tramitaciones, etc., ofreciendo vías para la atención de dudas, resolución de reclamos. Entre sus responsabilidades también incluye la programación, ejecución y evaluación de su agenda asistencial, programación de citas, operaciones quirúrgicas, referencias y contrarreferencias en relación con las normas vigentes. Asimismo, también refiere que los sistemas que brindad información de la institución deben estar completamente gestionados y actualizados

2.- Luis Heysen

Es un hospital de nivel II-1, ubicada en Carretera Pimentel Km 3,5, distrito de Pimentel, provincia de Chiclayo, departamento de Lambayeque. Según la investigación presentada por Gómez [37], cuenta con una capacidad instalada para 130 camas, brindando también los siguientes servicios: consulta, hospitalización general, y unidad de vigilancia intensiva, centro quirúrgico, centro obstétrico, emergencia, entre otras.

3.- Arbulú Neyra

Es un hospital de nivel I, atiende a la población asegurada de la provincia de Ferreñafe y de zonas aledañas.

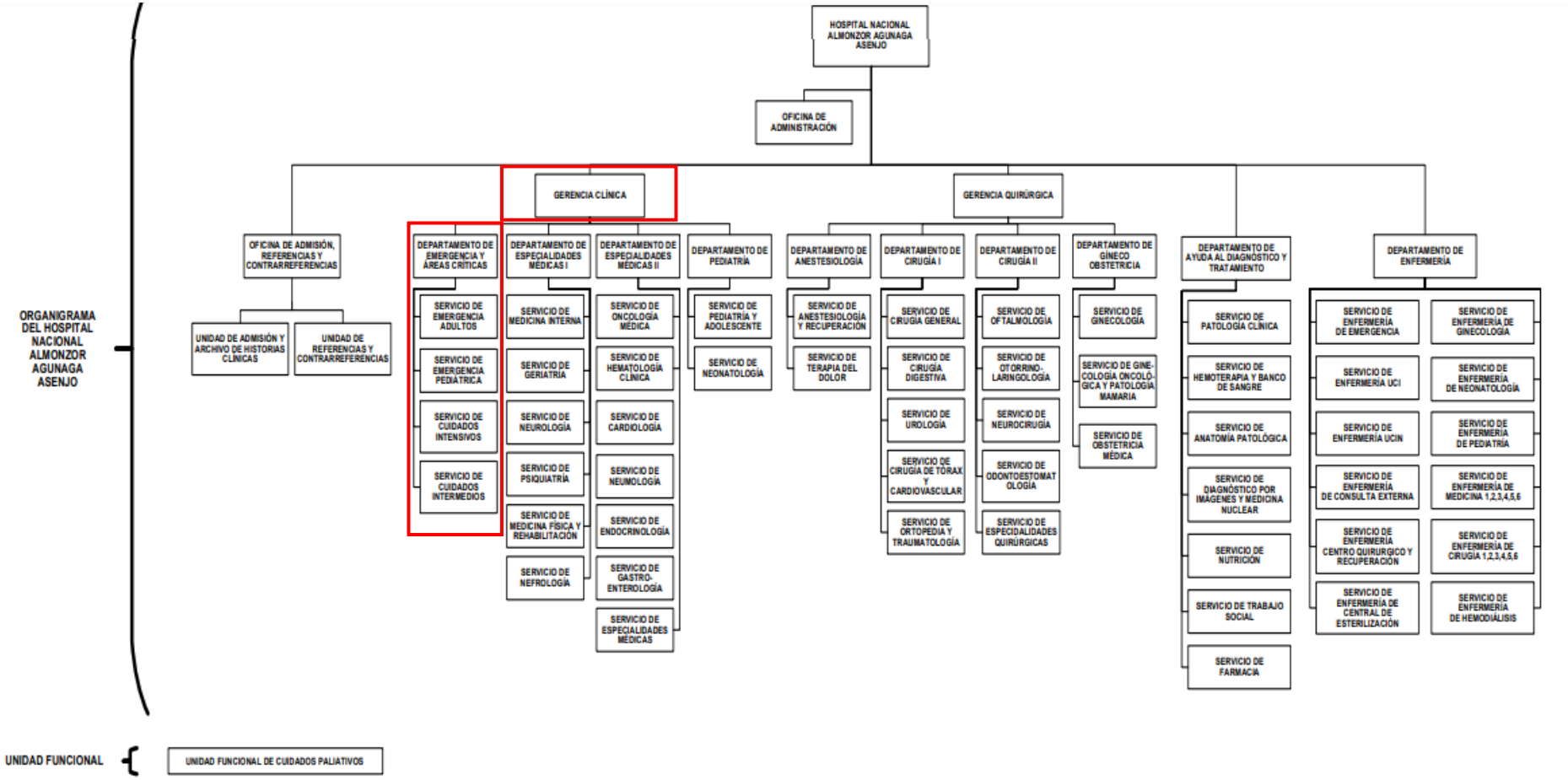
4.- Hospital Naylamp

Hospital correspondiente a nivel I. Se caracteriza por su enorme complejidad estructural y la convivencia entre distintas agrupaciones de trabajo, cuya meta común es la producción de un sistema óptimo que brinde satisfacción a las necesidades de los usuarios y los requerimientos de los mismos.

Anexo 02

Organigrama Hospital Nacional Almanzor Aguinaga Asenjo

Aquí resaltamos la Unidad Orgánica principal que supervisa el área de Emergencias, así como las respectivas sub unidades.



Fuente: Manual de Operaciones del Hospital Almanzor Aguinaga Asenjo (2022)

Anexo 03

ENCUESTA

Objetivo: Recolectar información que aborde las características generales de la organización en estudio, así como los lineamientos considerados en la Gestión de Riesgos de Seguridad de la Información.

Fuente: NTP ISO/IEC 27005, Octave

Seleccione con una X la respuesta que considere pertinente a cada pregunta, en algunos casos complete el detalle la misma.

Objetivo 1: Establecer el contexto

1.1 ¿Tienen definido un modelo de Gestión de Riesgos? Si en caso sea afirmativa, ¿Se llegó a implementar?

Sí ( ) No ( )

_____

_____

1.2 ¿La organización cuenta con una bitácora de incidencias, de hechos que afectan la seguridad de la información en la empresa? Si es afirmativa describa alguna de las más relevantes

Sí ( ) No ( )

_____

_____

_____

1.3 En caso haya bitácora de incidencias, ¿se ha documentado las acciones para gestionar incidencias? En caso sea afirmativo, describa el procedimiento.

Sí ( ) No ( )

_____

_____

_____

1.4 La empresa brinda capacitación o genera algún tipo de esquema de concientización en los miembros de la organización con respecto a la Seguridad de la Información

Sí ( ) No( )

1.5 La organización toma medidas para mitigar los riesgos de seguridad de la información. En caso sea afirmativa cuáles son estas

Sí( ) No( )

_____

_____

_____

1.6 Existen planes o procedimientos de seguridad para poner en resguardo las instalaciones, los edificios y las áreas restringidas

Sí( ) No( )

Organización

1.7 ¿Cuál es el propósito principal de la organización?

_____
_____
_____

1.8 Objetivos de la organización

_____
_____
_____

1.9 ¿Cuáles son los procesos de información críticos de Atención de Emergencia?

_____
_____
_____

1.10 Si se presenta una situación crítica en el negocio, ¿qué servicio(s) complementarios de Emergencia debe seguir operando?

_____
_____
_____

1.11 ¿Con qué áreas interactúa el área de Emergencias generando una transferencia de información?

Área	**Tipo de información**

1.12 ¿Cuándo se comparte información hacia otras entidades existe un previo acuerdo de confidencialidad?
Sí ( ) No ( )

1.13 Existen normas y/o documentación de procesos para regular el acceso físico a las áreas de trabajo y hardware (computadoras, dispositivos de comunicación, etc.) y medios de software.
Sí( ) No ( )

Objetivo 2: Conocer activos

Identificación de procesos

2.1 ¿Cuáles son los procesos más importantes del área de Emergencia y qué información manejan?

Proceso	Información

2.2 ¿Manejan información personal resguardada bajo las leyes nacionales relacionadas con la privacidad? ¿Si es afirmativa qué información es?

Sí ( ) No ( )

_____

_____

2.4 Listado y descripción de los activos del área
Qué activos consideras son de mayor relevancia o criticidad para el área de estudio

i) <u>Información</u>: Información documentada en papel o electrónica

Nombre	Descripción

ii) <u>Sistema:</u> (host, cliente, servidor o red)

Nombre	Descripción

iii) <u>Software:</u> Aplicaciones de software (sistemas operativos, aplicaciones de base de datos, dispositivos de redes, aplicaciones de oficina, aplicaciones personalizadas, etc)

Nombre	Descripción

iv) <u>Hardware</u>: Dispositivos físicos de tecnología de la información (estaciones de trabajo, servidores, etc)

Nombre	Descripción

v) <u>Personas</u>: Personas de la organización (formación, conocimiento y experiencia)

Nombre	Descripción

Nombre:
Cargo:

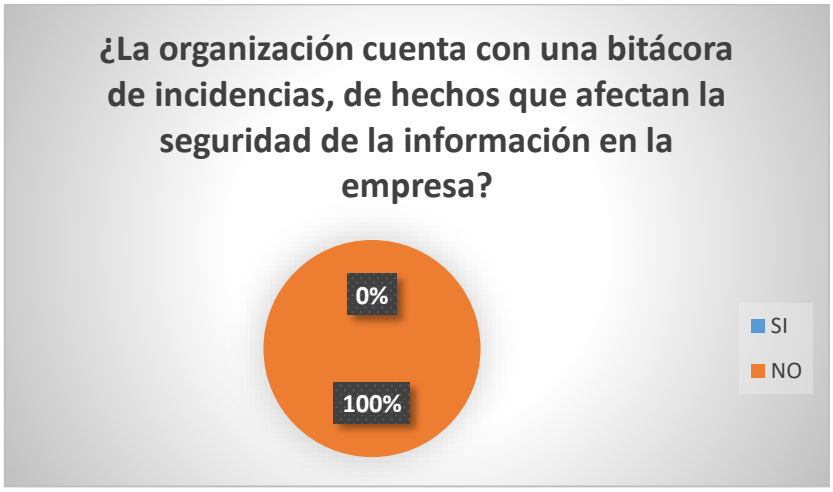
Firma:

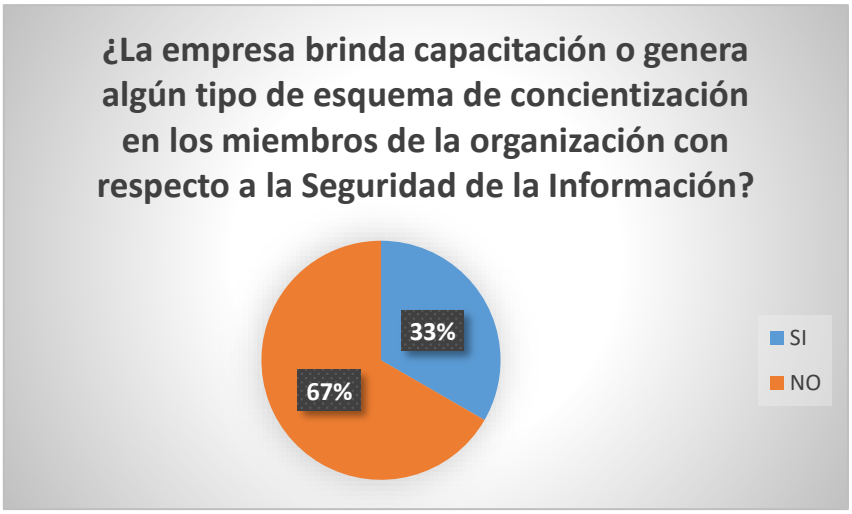
Anexo 04

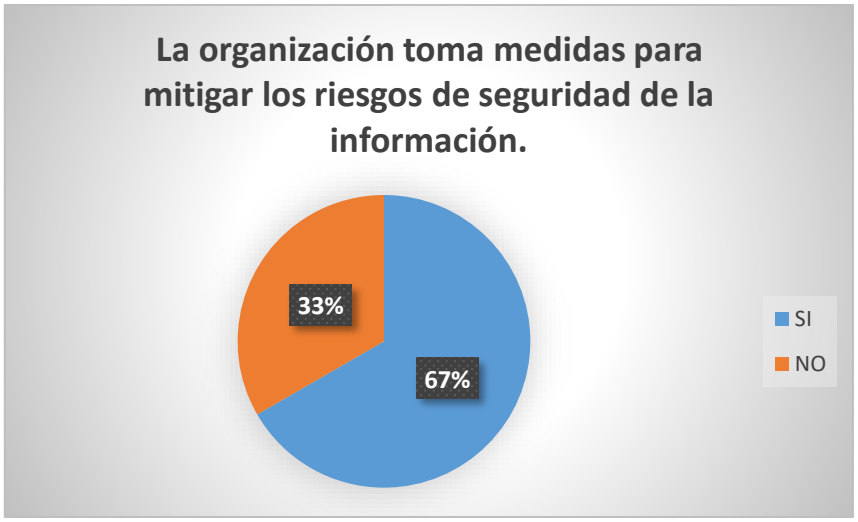
Resultado de la encuesta realizada a los directores de TI de los cuatro hospitales en estudio.

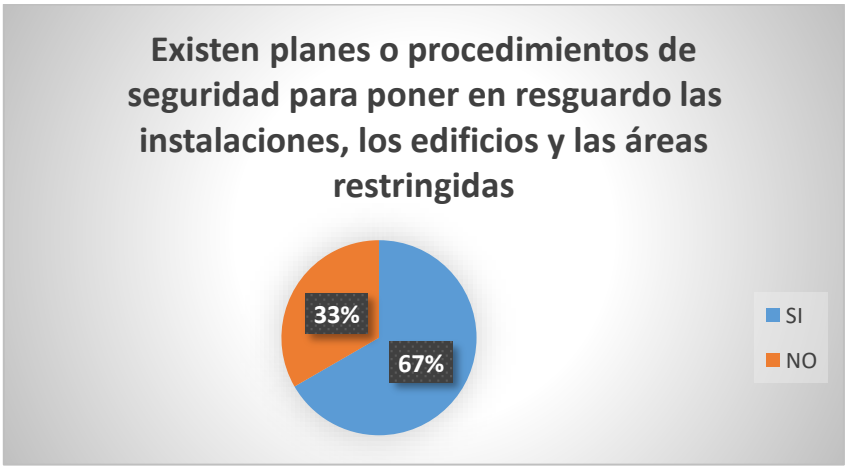
Hospitales:

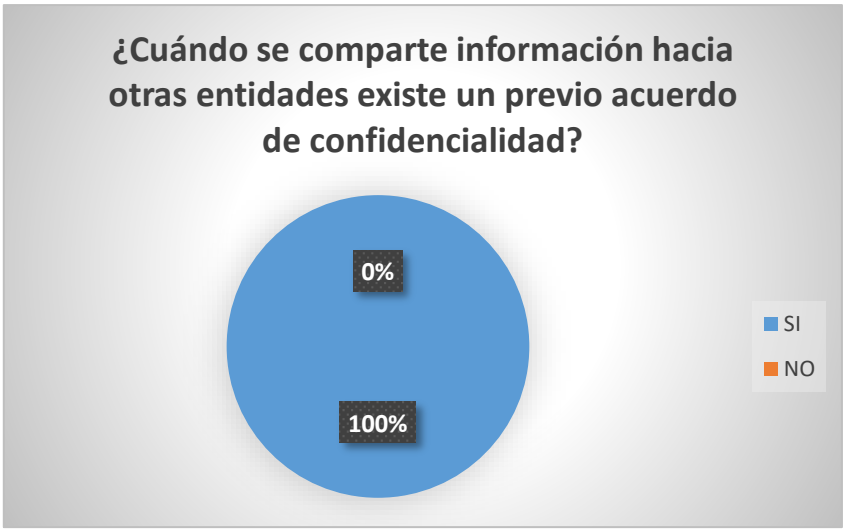
- Hospital Nacional Almanzor Aguinaga Asenjo
- Hospital Luis Heysen
- Hospital Naylamp

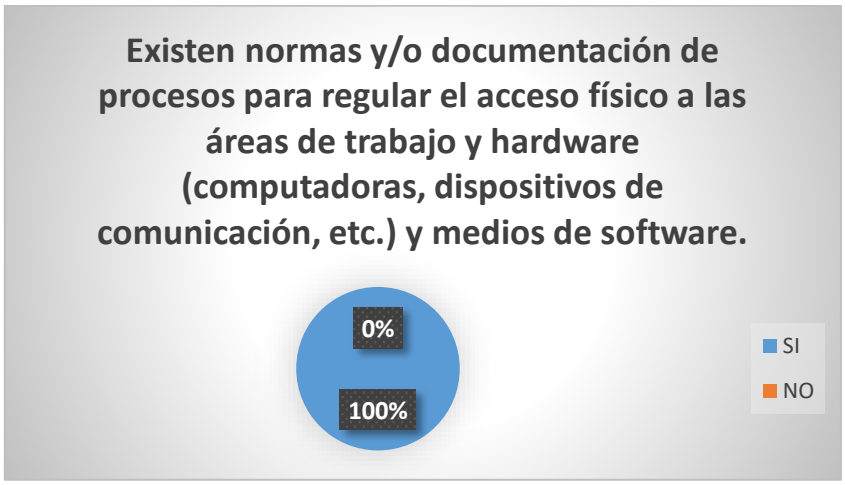


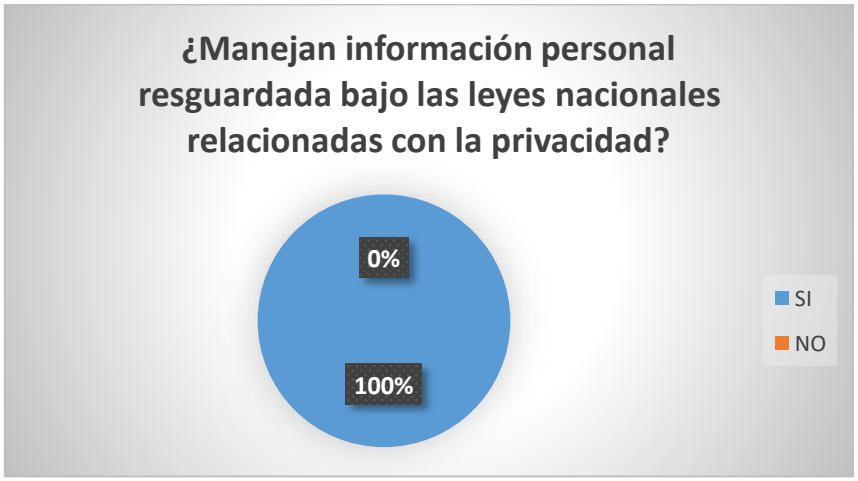

¿La empresa brinda capacitación o genera algún tipo de esquema de concientización en los miembros de la organización con respecto a la Seguridad de la Información?
33%
67%
SI
NO

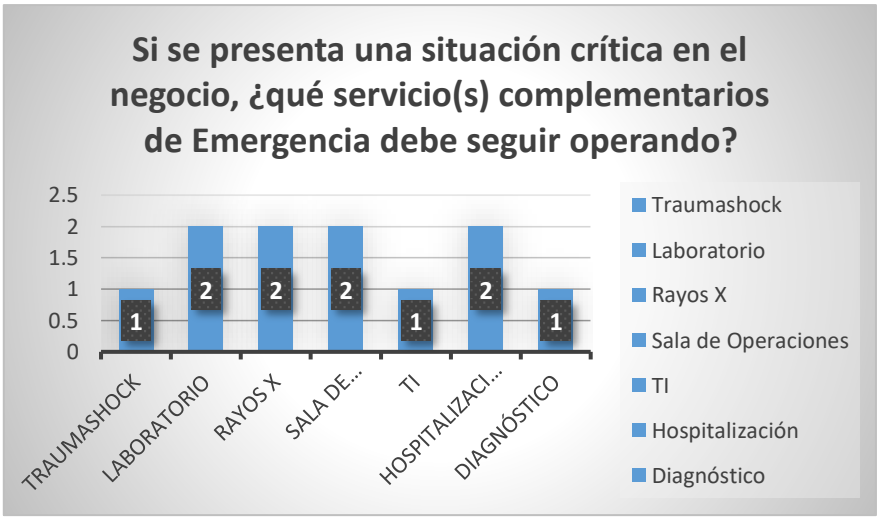

La organización toma medidas para mitigar los riesgos de seguridad de la información.
33%
67%
SI
NO

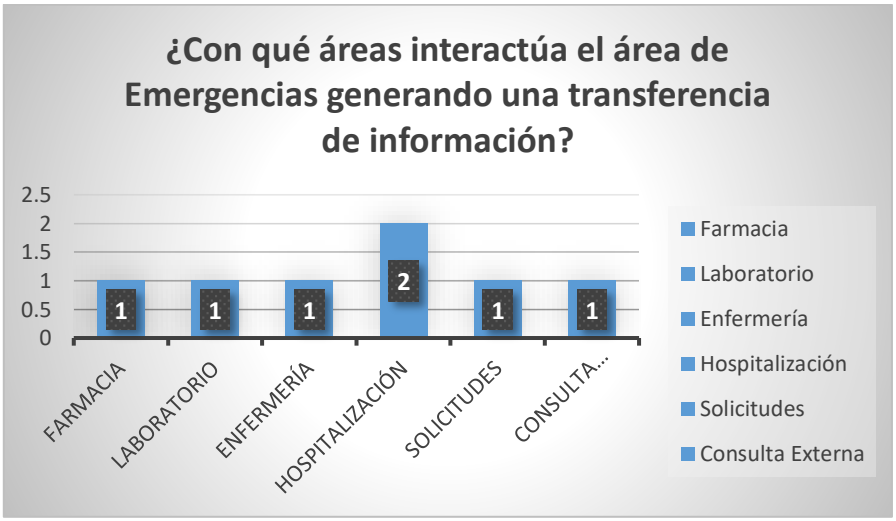

Existen planes o procedimientos de seguridad para poner en resguardo las instalaciones, los edificios y las áreas restringidas
33%
67%
SI
NO

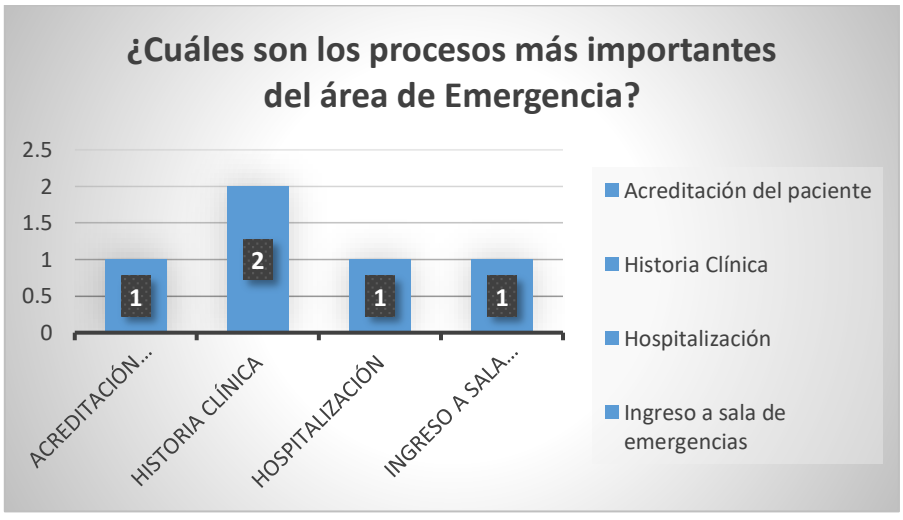

¿Cuándo se comparte información hacia otras entidades existe un previo acuerdo de confidencialidad?
0%
100%
SI
NO


Existen normas y/o documentación de procesos para regular el acceso físico a las áreas de trabajo y hardware (computadoras, dispositivos de comunicación, etc.) y medios de software.
0%
100%
SI
NO


¿Manejan información personal resguardada bajo las leyes nacionales relacionadas con la privacidad?
0%
100%
SI
NO


Si se presenta una situación crítica en el negocio, ¿qué servicio(s) complementarios de Emergencia debe seguir operando?
2.5
2
1.5
1
0.5
0
1
2
2
2
1
2
1
TRAUMASHOCK
LABORATORIO
RAYOS X
SALA DE...
TI
HOSPITALIZACI...
DIAGNÓSTICO
Traumashock
Laboratorio
Rayos X
Sala de Operaciones
TI
Hospitalización
Diagnóstico


¿Con qué áreas interactúa el área de Emergencias generando una transferencia de información?
2.5
2
1.5
1
0.5
0
1
1
1
2
1
1
FARMACIA
LABORATORIO
ENFERMERÍA
HOSPITALIZACIÓN
SOLICITUDES
CONSULTA...
Farmacia
Laboratorio
Enfermería
Hospitalización
Solicitudes
Consulta Externa


¿Cuáles son los procesos más importantes del área de Emergencia?
2.5
2
1.5
1
0.5
0
1
2
1
1
ACREDITACIÓN...
HISTORIA CLÍNICA
HOSPITALIZACIÓN
INGRESO A SALA...
Acreditación del paciente
Historia Clínica
Hospitalización
Ingreso a sala de emergencias

Anexo 05

Usuarios / Procesos	Licenciado(a) de Enfermería	Médico	Vigilante	Familiar y/o acompañante de Paciente	Admisionista	Médico auditor	Enfermero(a)	Técnico de admisión Tec. Enfermería	Trabajador social	Médico especialista	Tecnólogo profesional	Jefe de guardia	Técnica de mortuorio
Ingreso y Atención de Pacientes en Triaje	X	X	X	X									
Admisión de Pacientes en emergencia		X		X	X	X	X						
Atención del paciente en la unidad de Shock Trauma Prioridad I		X						X	X					
Atención médica del paciente en área de Prioridad II de Emergencia	X	X			X								
Atención quirúrgica y/o traumatológica del paciente en área de Prioridad II de Emergencia	X	X			X								
Ingreso y Atención del paciente en Sala de observación en niveles: estancia corta / Unidad Cuidados Críticos / Cuidados Intermedios		X		X	X	X		X						
Alta médica del Servicio de Emergencia		X		X	X	X		X		X				
Alta Voluntaria		X		X				X						
Transferencia de paciente a otros Servicios de Hospitalización		X				X		X		X				
Referencia / Contrarreferencia a Otros Centros de Salud		X			X		X			X	X			
Monitoreo clínico: Evaluación médicas y atención de enfermería		X		X	X			X		X				
Solicitud de interconsultas		X						X				X		
Solicitud de exámenes auxiliares		X						X		X			X	
Emisión de Constancia de atención				X		X								X
Constatación de fallecimiento: emisión de Informe de defunción/emisión de Certificado de defunción		X						X			X			X

Tabla 2: Procesos de Emergencia de ESSALUD
Fuente: Manual de Procesos y Procedimientos de Atención Urgencias/Emergencias Adultos Hospital Nacional Edgardo Rebagliati

Anexo 06

1.- Hospital Nacional Almanzor Aguinaga Asenjo

El Hospital Nacional Almanzor Aguinaga Asenjo (HNAAA), hospital de nivel III y de alta complejidad, brinda servicios de salud al sector poblacional asegurado a nivel nacional, manteniendo una atención continua y de calidad hacia ellos. Tiene a su vez la función de elaborar normativas, técnicas y desarrollar innovaciones científico tecnológicas con el in de brindar soluciones a distintos problemas de salud.

2.- Luis Heysen

Es un hospital de nivel II-1, ubicada en Carretera Pimentel Km 3,5, distrito de Pimentel, provincia de Chiclayo, departamento de Lambayeque. Según la investigación presentada por Gómez [37], cuenta con una capacidad instalada para 130 camas, brindando también los siguientes servicios: consulta, hospitalización general, y unidad de vigilancia intensiva, centro quirúrgico, centro obstétrico, emergencia, entre otras.

3.- Arbulú Neyra

Es un hospital de nivel I, atiende a la población asegurada de la provincia de Ferreñafe y de zonas aledañas.

4.- Hospital Naylamp

Hospital correspondiente a nivel I. Se caracteriza por su enorme complejidad estructural y la convivencia entre distintas agrupaciones de trabajo, cuya meta común es la producción de un sistema óptimo que brinde satisfacción a las necesidades de los usuarios y los requerimientos de los mismos.

Anexo 07

Funciones Principales del Servicio de Emergencias

Departamento de Emergencia y Áreas Críticas

Es la unidad de línea encargada de la atención especializada de emergencia y áreas críticas; depende de la Gerencia Clínica y se mencionarán algunas de sus funciones principales [34]:

- Monitorear y evaluar la ejecución de técnicas, procedimientos, pruebas y otras acciones en torno a la calidad, seguridad del paciente y gestión de riesgos en los Servicios a su cargo.
- Efectuar el monitoreo, seguimiento y evaluación de la atención de los Servicios a su cargo, proponiendo alternativas de mejora en la atención clínica.
- Controlar el acceso a la información por parte de los pacientes, en el marco de las normas vigentes, en los Servicios a su cargo.
- Evaluar y presentar a la Gerencia Clínica la productividad de los Servicios a su cargo y de los resultados o beneficios en la salud de los pacientes, así como la calidad y satisfacción lograda.
- Proponer las necesidades de capacitación del personal de los Servicios a su cargo y controlar su ejecución.
- Monitorear y evaluar la optimización de los procesos a su cargo, para reducir los tiempos de espera para la prestación de los servicios.
- Consolidar y evaluar los indicadores contenidos en los Acuerdos de Gestión, según corresponda.
- Velar por la articulación de los servicios y unidades prestadoras de servicios al interior del Departamento, así como con los demás Departamentos de la Gerencia Clínica.
- Supervisar y controlar la aplicación de las normas del Sistema de Referencia y Contrarreferencia en los Servicios que conforman el Departamento, a fin de garantizar la continuidad de la atención de salud a los pacientes.
- Monitorear y evaluar la disponibilidad de la información en los registros, formatos y sistemas de información institucionales con relación a la atención de salud que se brinda en los Servicios a su cargo, así como, supervisar la implementación de las medidas correctivas.

- Evaluar los informes, reportes y demás documentos emitidos por los Servicios a su cargo sobre la gestión, resultados, incapacidad temporal, reclamos y quejas de los pacientes y otros que sean requeridos por la Gerencia del Hospital Nacional Almanzor Aguinaga Asenjo.
- Supervisar y efectuar el seguimiento de la implementación de las recomendaciones de las acciones de control, supervisión u otras medidas para la mejora de los Servicios a su cargo.
- Cumplir con las normas del Código de Ética institucional, de transparencia y **acceso a la información** y de los sistemas de control interno, gestión de la calidad, seguridad y salud en el trabajo, en el ámbito de su competencia.

El departamento mencionado está conformado por las siguientes sub unidades de servicio:

- Servicio de Emergencia Adultos
- Servicio de Emergencia Pediátrica
- Servicio Cuidados Intensivos
- Servicio Cuidados Intermedios

Anexo 08

Diferentes servicios que ofrece Emergencias

Criterios	Hosp. Almanzor Aguinaga A.	Hosp. Naylamp	Hosp. Heysen
Nivel	Nivel III - 1	Nivel I	Nivel II
Tópicos	- Medicina General - Cirugía - Traumatología - Ginecoobstetricia - Pediatría - Cirugía Pediátrica - Oftalmología - Otorrinolaringología - Urología - Neurocirugía - Neonatología	- Medicina General - Ginecoobstetricia - Pediatría - Oftalmología - Otorrinolaringología - Urología - Neonatología	- Medicina General - Ginecoobstetricia - Pediatría - Oftalmología - Otorrinolaringología - Urología - Neonatología
Procesos	- Ingreso y atención de pacientes en triaje - Admisión de pacientes en Emergencia - Atención del paciente en la unidad de Shock Trauma Prioridad I - Atención del paciente en área de Prioridad II de Emergencia - Ingreso y atención del paciente en sala de observación Estancia Corta / Unidad Cuidados Críticos / Cuidados Intermedios - Alta médica del Servicio de Emergencia - Alta Voluntaria - Transferencia del paciente a otros servicios de hospitalización - Referencia / Contrarreferencia a otros centros de salud - Monitoreo Clínico: Evaluación Médica - Monitoreo Clínico: Atención de Enfermería - Solicitud de Interconsultas - Solicitud de exámenes auxiliares - Emisión de constancia de atención - Constatación de fallecimiento: Emisión de informe de defunción /	- Ingreso y atención de pacientes en triaje - Admisión de pacientes en Emergencia - Atención del paciente en área de Prioridad II,III, IV y V de Emergencia - Ingreso y atención del paciente en sala de observación Estancia Corta / Unidad de Vigilancia Intensiva / Cuidados Intermedios - Alta médica del Servicio de Emergencia - Alta Voluntaria - Transferencia del paciente a otros servicios de hospitalización - Referencia / Contrarreferencia a otros centros de salud - Monitoreo Clínico: Evaluación Médica - Monitoreo Clínico: Atención de Enfermería - Solicitud de Interconsultas - Solicitud de exámenes auxiliares - Emisión de constancia de atención - Constatación de fallecimiento: Emisión de informe de defunción / Emisión de certificado de defunción	

	Emisión de certificado de defunción		
Personal de TI	9	2	2
Sofware	- Sistema PACS: Se encarga de almacenar y distribuir imágenes médicas del paciente. Es utilizado por el médico para exámenes auxiliares. - Sistema Anapat: Sistema de Anatomía Patológica del Estado Peruano. - Essi: Se encarga de digitalizar las historias clínicas, en la cual el médico accede a toda la información completa del paciente. Se utiliza al momenta de registrar la prioridad del paciente en Emergencia, seguidamente pasando por el proceso de Admisión en la cual hace constancia de la cita en la Historia Clínica, luego se registra su atención por parte del médico, sea para Cirugía o Sala de Observación, orden de Interconsulta y finalmente su Alta médica, con su respectiva constancia de Atención. - Acredita: Verifica la condición de asegurado del paciente. Es utilizado al momento de ingresar al área de Admisión, para consultar al empleador y la vigencia del Seguro.		
Red	Cableado / Wifi	Cableado	Cableado

Anexo 09

Cuadro resumen de análisis de estándares, marcos de trabajo y metodologías

FASES	NTP ISO/IEC 27005	COBIT 5 PARA RIESGOS	MAGERIT	OCTAVE
Seleccionar equipo de análisis	- Establecer roles y responsabilidades a cada integrante. - Establecer una organización para la gestión del riesgo de seguridad de la información (partes interesadas).	- Aquí se tomará en cuenta al catalizador *Personas*, que reúne a las personas con roles y niveles con habilidades. - Tomará en cuenta al catalizador *Estructuras Organizativas*, que nos brinda recomendaciones para definir los niveles de autoridad, hablando de dos funciones importantes: Función de riesgos y Gestor de Riesgos.	- Aquí los roles y funciones se define por lo siguiente: Órganos de gobierno, dirección ejecutiva, dirección operacional. - Emplea la matriz RACI.	- Seleccionar miembros del equipo de análisis y establecer sus roles, funciones y responsabilidades en la evaluación. - Buscar el patrocinio de la alta Dirección a través de reuniones informativas. - Evaluar personal general y de TI, a través de habilidades requeridas como buena capacidad de comunicación, comprensión del entorno empresarial y de la organización, capacidad para trabajar en equipo.
Contexto	- Definir el alcance y los límites del proceso de gestión de riesgo de seguridad de la información, además de los criterios de valoración del riesgo. - Se establecen criterios como: valoración de riesgos, evaluación	- *EDM03*: Habla sobre el apetito del riesgo y la tolerancia de la organización. - *APO12:* Identifica, evalúa y reduce los riesgos dentro de niveles de tolerancia establecidos.	- Está enmarcado en el ambiente cultural, social y político. - Leyes reglamentarias y contractuales de la organización y restricciones de distinta índole. - Determina los activos esenciales, los puntos de interconexión con	- Alcance: Áreas operativas seleccionadas para la gestión del riesgo. - Evaluar el soporte logístico, como la coordinación de reuniones. - Se debe contar con documento e información de respaldo, tales como:

	del impacto, aceptación del riesgo, dentro de ellos está el contexto interno y externo. - Evaluar si existen los recursos necesarios y las restricciones para la implementación del Sistema de Gestión de Riesgos.	- *Estructuras Organizativas:* responsabilidades y funciones relacionadas a la gestión del riesgo. - *Información*: dentro de ella el factor de Riesgo (Perfil de Riesgo) incluye al contexto interno y externo como parte de los factores de riesgo.	otros sistemas y proveedores externos para determinar el alcance y objetivos del proyecto, informe de abastecimiento necesario de recursos. - Establece criterios de valoración de riesgos y de aceptación de riesgos.	organigrama, lista de terminales informáticas, topología de red, documentación actual de la infraestructura informática, etc. - Los criterios de evaluación vienen a ser definidos como los impactos descritos desde una fase anterior utilizado en el perfil de riesgo de cada activo (Bajo, Medio, Alto).
Evaluación del riesgo de seguridad de la información **- Identificación del riesgo** **- Análisis del riesgo** **- Valoración del riesgo**	**<u>Identificación de riesgos</u>:** - Alcance y límites de la evaluación del riesgo, lista de activos y procesos de negocio identificados. - Se identifican las amenazas, hay una revisión de controles existentes e identificación de vulnerabilidades y consecuencias, y por último se determina el nivel de riesgo. **<u>Análisis de riesgos</u>**: - Tiene dos metodologías: cualitativa y cuantitativa. - Cuenta con evaluar las consecuencias y evaluar la probabilidad de incidentes.	Se enfoca en los siguientes procesos de soporte de riesgos (EDM03 *Asegurar la optimización del riesgo*) y APO12 (*Gestionar el riesgo*). **<u>Identificación del riesgo</u>**: Toma en cuenta al catalizador *Información* en donde trata al perfil de riesgo, en el cual se encuentra el escenario de riesgos y el análisis de riesgos. **<u>Análisis del riesgo</u>**: Primero considera a los Escenarios de riesgos, que pueden conducir a un impacto en la empresa, luego, presenta una técnica para hacer el riesgo más comprensible y permitir la análisis y evaluación apropiada de	**<u>Análisis de riesgos</u>:** - Considera: activos, dependencias de activos, amenazas y salvaguardas. - Estima: El impacto y riesgo. - Mientras más valioso es un activo, más dimensiones de seguridad requiere, la valoración de los activos puede ser cualitativa o cuantitativa. - Requiere estimar las amenazas que pueden afectar a cada activo, se utiliza la probabilidad de ocurrencia. - Impacto: degradación y amenaza a los activos, su estimación se puede hacer mediante tablas.	**<u>Identificación de riesgos</u>:** Se recopila, consolida y analiza la información de activos desde varios niveles de la organización. - Busca la opinión de los altos directivos sobre los activos más críticos de la empresa. - Se abordan los siguientes conceptos: a) Activos de información b) Áreas de preocupación **<u>Análisis del riesgo</u>:** Aquí se toma en cuenta los siguientes criterios: - Requerimientos de seguridad (Confidencialidad, disponibilidad e integridad). En algunos casos autenticidad y no repudio.

	<u>Valoración de riesgos</u>: - Los riesgos pueden ser cualitativos y cuantitativos - Se van a usar matrices para la medición de riesgos. - Debe haber consistencia con el contexto interno y externo de gestión de riesgo de seguridad de la información. - Los riesgos deben ser priorizados.	los riesgos. Todo ello dentro del Perfil de Riesgo. **<u>Valoración de riesgos</u>:** - Se usa el mapa de riesgos (frecuencia e impacto). Ofrece una vista completa de los riesgos y sus áreas para su respectiva acción. Se utilizan zonas de color para indicar el apetito en modo gráfico. - El mapa de riesgos se debe vincular a los objetivos de la empresa.	- Los activos deben caracterizarse por código, responsable, ubicación, etc. - Se resume en cuadro de tipo de activos, dimensiones de valoración, cuadro de amenazas y salvaguardas. **<u>Valoración de riesgos</u>:** - Modelo de valor: valor que representan los activos y sus dependencias. - Toma en cuenta las dimensiones de la seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad. - Para cada amenaza se registra la frecuencia, el daño (degradación). - Mapa de riesgos: La estimación del riesgo se puede hacer por medio de escalas cualitativas.	- Para los activos críticos seleccionados se crean perfiles de amenazas, estos se deben proteger por ley o reglamento. Pueden ser actores humanos con acceso a a la red, los que utilizan el acceso físico, problemas del sistema, etc. - Analiza las vulnerabilidades tecnológicas de la infraestructura de la organización sobre los activos críticos. Se solicita la topología o mapa de red para revisar dónde viven los activos críticos. - Componentes: Sistemas de interés para cada activo crítico (dependencia), finalmente, estos pasan por una evaluación de vulnerabilidad. **<u>Valoración de riesgos</u>**: - Se crea perfiles de riesgo para cada activo crítico (los cuales agregan una medida cualitativa del impacto en la organización). - La combinación de una amenaza y el impacto resultante define el riesgo para la organización. El impacto se añade a los perfiles de amenaza.

Tratamiento del riesgo	- Indica usar controles para reducir, evitar, retener o transferir los riesgos. - Menciona aplicar un Plan de tratamiento de riesgos y riesgos residuales. - Las opciones del tratamiento del riesgo son las siguientes: • Modificación del riesgo • Retención del riesgo • Evitar el riesgo • Intercambio del riesgo	- La empresa responde al riesgo (APO12.06). Vincula los escenarios de riesgo y la respuesta adecuada. - Se encuentra vinculado con APO13: *Gestionar la seguridad* y DSS05: *Gestionar los servicios de seguridad.* - Catalizador *Información*, en lo que respecta al Plan de Acción de riesgos, mencionando entre ellos a la Matriz de Actividad de Control y Riesgo. - Ofrece una respuesta al riesgo: Evitar, Mitigar, Compartir, Aceptar.	- Uso de despliegue de medidas de seguridad: toma de conciencia sobre la consecuencia de los riesgos. - Uso de salvaguardas y plan de seguridad, tomando en cuenta las de mayor relevancia. - Participación de la dirección. - Monitorización continua. - Como opciones tiene: evitar, prevenir, mitigar, compartir y aceptar el riesgo.	- Desarrollar planes y estrategias de seguridad: Menciona talleres para analizar información sobre activos, amenazas y vulnerabilidades e identificar los riesgos para la organización. - Menciona los requisitos de seguridad de activos que es importante proteger (confidencialidad, integridad, disponibilidad). - Se realizan los cambios deseados con los pasos necesarios para comenzar a implementar la estrategia y los planes.
Comunicación y consulta del riesgo	- La gestión de riesgos será comunicado al directivo apropiado, personal de operaciones y stakeholders.	Plan de Comunicación de riesgos, para definir la frecuencia, los tipos y destinatarios sobre el riesgo.	- Elabora un informe del estado de riesgo: estimación de impacto y riesgo y un informe de insuficiencias a los stakeholders: debilidades en las salvaguardas. - Resalta destacar en forma gráfica distintos niveles de escenarios: impacto, riesgo, etc.	Informar a todos los participantes (Informe de resultados)
Monitorización y seguimiento	- Verificación regular de los criterios que se usaron para medir el riesgo junto a sus elementos válidos.		- Se define sectores a monitorizar y se realiza un periodo de revisión del análisis y las decisiones del tratamiento.	

Anexo 10

ANÁLISIS DE MARCOS DE TRABAJO, METODOLOGÍAS Y ESTÁNDARES RELACIONADOS

MODELO ARMÓNICO

FASES	PROCESOS	SUBPROCESOS	NTP ISO/IEC 27005	COBIT 5 PARA RIESGOS	MAGERIT	OCTAVE	METODOLOGÍA SELECCIONADA	JUSTIFICACIÓN
Fase 1.- Contexto de la organización	-Alcance de la Organización	- Contexto Externo - Contexto Interno	**X**	**X**		**X**	**NTP ISO/IEC 27005 / COBIT 5 PARA RIESGOS / OCTAVE**	Considera al contexto externo y al contexto interno, por ejemplo, las metas, objetivos, estrategia, y todo tipo de factores en general que puedan influir en factores causales de riesgo hacia la organización.
	-Análisis del conocimiento del personal					**X**	**OCTAVE**	Requiere reunir información en lo que respecta a sus **activos de información**. Todo ello desde el área directiva hasta el personal que labora en la misma, incluyendo al de TI. De la lista reunida, analizar si cuenta con las herramientas de protección respectiva. También deben conocer las debilidades o vulnerabilidades que recaen sobre ellos.
Fase 2.- Análisis de activos, amenazas y vulnerabilidades	-Identificación y Valoración de activos -Identificación de Vulnerabilidades -Identificación de Amenazas	**X**			**X**		**NTP ISO/IEC 27005 / MAGERIT**	Se utilizarán catálogos de elementos para reconocer cada uno de los procesos definidos en esta fase, lo que nos ayudará en la identificación rápida de activos, amenazas y vulnerabilidades durante la gestión del riesgo.

Fase 3.- Evaluación del Riesgo	-Identificación del Riesgo	Uso de escenarios de riesgo		**X**		**X**	**NTP ISO/IEC 27005 / OCTAVE**	Se lista los activos críticos de mayor relevancia en la organización, con ella, se plantea posibles escenarios o accidentes de riesgo y las probables consecuencias para los objetivos de la organización.
		Identificación de consecuencias	**X**			**X**	**NTP ISO/IEC 27005 / OCTAVE**	Aplicamos una descripción de las consecuencias en caso se materializara el riesgo, es decir, una breve descripción del daño para el área en estudio, y qué activos pueden verse afectados.
	-Análisis del Riesgo	Estimación de riesgo	**X**		**X**		**NTP ISO/IEC 27005 / MAGERIT**	Para estimar el riesgo se utilizará una tabla de doble entrada (impacto y probabilidad), en el cual, de acuerdo a una escala cualitativa o cuantitativa, nos devolverá como resultado los riesgos con un nivel de priorización.
	-Valoración del Riesgo		**X**		**X**		**NTP ISO/IEC 27005 / MAGERIT**	Se va a aplicar una lista resultante de priorización de riesgos con los niveles estimados de los mismos, determinar su nivel de tolerancia, y en la cual se decidirá tomar acción inmediata sobre los riesgos críticos para el área de estudio.
Fase 4.- Tratamiento del riesgo	- Lista de normas de protección (existentes y propuestas)			**X**	**X**		**COBIT 5 PARA RIESGOS / MAGERIT**	Se aplicarán normas de protección que vaya en correlación con la información de la organización y de los sistemas e infraestructuras asociadas, junto con las normas ya existentes de política de gobierno de TI de la organización. Entre las

								medidas para contrarrestar los riesgos se encuentran: Aceptar, Mitigar, Compartir y Transferir.
Fase 5.- Comunicación y Monitoreo	- Plan de Comunicación de Riesgos			**X**			**COBIT 5 PARA RIESGOS**	Mantener información que abarque la política de riesgos enfocados en la seguridad de la información y compartirla con la parte directiva. Reducir el exceso de información no relevante, logrando una comprensión adecuada sobre el panorama actual de los riesgos que afecten las operaciones estratégicas y objetivos del negocio, logrando asignar los recursos adecuados que permitan contrarrestar estos riesgos, teniendo en cuenta su apetito y tolerancia.
	-Monitoreo de Riesgos				**X**		**MAGERIT**	Aquí se va a dar control y seguimiento al Plan de Tratamiento de Riesgos planteado, si ésta ya fue completada en el período propuesto o aún no.

Anexo 11

Modelo de Gestión de riesgos para mejorar la Seguridad de la Información en los procesos de emergencia en el sector salud pública de la región Lambayeque

Autor: Miluska Natalia Nicho Gómez

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es poner a evaluación o juicio el modelo de gestión de Riesgos de Seguridad de la Información presentado. El esquema presentado es resultado de la armonización de las normas, marcos de trabajo y metodologías mencionadas anteriormente (NTP/ISO 27005 prioritariamente, Magerit, COBIT 5 para Riesgos y Octave). El modelo está dirigido para el área de Emergencias del sector Público.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Grado académico y profesión
Áreas de experiencia profesional
Institución donde labora
Tiempo de experiencia

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación delmodelo.

Indicador	**Criterio**	**Valoración**				
		Muy malo	Malo	Regular	Bueno	Muy bueno
CLARIDAD	El contenido se presenta utilizando un lenguaje apropiado que facilita su comprensión.	1	2	3	4	5
OBJETIVIDAD	El contenido presentado es objetivo y concreto, y está expresado en conductas observables o medibles.	1	2	3	4	5
COHERENCIA	Existe una correspondencia lógica entre el contenido presentado y la teoría.	1	2	3	4	5
SUFICIENCIA	La cantidad y calidad de los elementos presentados en el contenido son suficientes.	1	2	3	4	5
RELEVANCIA	El contenido presentado es importante y determinante para lograr el entendimiento deltema.	1	2	3	4	5

III. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.							
FASE	Actividad	Criterios					Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Suficiencia	Relevancia	
Fase I. Contexto de la organización	Alcance de la organización						
	Análisis del conocimiento del personal						
FASE II. Análisis de activos, amenazas y vulnerabilidades	Identificación de activos						
	Identificación de amenazas						
	Identificación de vulnerabilidades						
FASE III. Evaluación del riesgo	Identificación del Riesgo						
	Análisis del Riesgo						
	Valoración del Riesgo						

FASE IV. Tratamiento del riesgo	Creación de normas de protección						
	Plan de Tratamiento de Riesgos						
FASE V. Comunicación y Monitoreo	Plan de Comunicación de Riesgos						
	Monitoreo de Riesgos						
	TOTAL						

RESULTADOS

Opinión:

	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma Experto

Modelo de Gestión de riesgos para mejorar la Seguridad de la Información en los procesos de emergencia en el sector salud pública de la región Lambayeque

Autor: Miluska Natalia Nicho Gómez

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es poner a evaluación o juicio el modelo de gestión de Riesgos de Seguridad de la Información presentado. El esquema presentado es resultado de la armonización de las normas, marcos de trabajo y metodologías mencionadas anteriormente (NTP/ISO 27005 prioritariamente, Magerit, COBIT 5 para Riesgos y Octave). El modelo está dirigido para el área de Emergencias del sector Público.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Rómulo Fernando, Lomparte Alvarado
Grado académico y profesión
MBA / Licenciado en Computación
Áreas de experiencia profesional
Gobierno de TI, Seguridad de la Información, Ciberseguridad, Auditoría de Sistemas, Riesgo de TI, Gestión de la Calidad, Gerencia de Proyectos, etc.
Institución donde labora
UNMSM, USAT, UPN, UTP, U. Continental, UPAO, etc. / Telefónica Tech
Tiempo de experiencia
30 años

II. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.							
FASE	Actividad	Criterios					Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Suficiencia	Relevancia	
Fase I. Contexto de la organización	Alcance de la organización	5	5	5	5	5	
	Análisis del conocimiento del personal	5	5	5	5	5	
FASE II. Análisis de activos, amenazas y vulnerabilidades	Identificación de activos	5	5	5	5	5	
	Identificación de amenazas	5	5	5	5	5	
	Identificación de vulnerabilidades	5	5	5	5	5	
FASE III. Evaluación del riesgo	Identificación del Riesgo	5	5	5	5	5	
	Análisis del Riesgo	5	5	5	5	5	
	Valoración del Riesgo	5	5	5	5	5	

FASE IV. Tratamiento del riesgo	Creación de normas de protección	5	5	5	5	5	
	Plan de Tratamiento de Riesgos	5	5	5	5	5	
FASE V. Comunicación y Monitoreo	Plan de Comunicación de Riesgos	5	5	5	5	5	
	Monitoreo de Riesgos	5	5	5	5	5	
	TOTAL	60	60	60	60	60	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma Experto

FIRMA DIGITAL

Firmado digitalmente por: LOMPARTE ALVARADO ROMULO FERNANDO FIR 32100189 hard
Motivo: Doy V° B°
Fecha: 29/09/2023 03:15:23-0500

Modelo de Gestión de riesgos para mejorar la Seguridad de la Información en los procesos de emergencia en el sector salud pública de la región Lambayeque

Autor: Miluska Natalia Nicho Gómez

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es poner a evaluación o juicio el modelo de gestión de Riesgos de Seguridad de la Información presentado. El esquema presentado es resultado de la armonización de las normas, marcos de trabajo y metodologías mencionadas anteriormente (NTP/ISO 27005 prioritariamente, Magerit, COBIT 5 para Riesgos y Octave). El modelo está dirigido para el área de Emergencias del sector Público.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Róger Gustavo Abanto Ortiz
Grado académico y profesión
Maestro en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de Tecnologías de información.
Áreas de experiencia profesional
Auditoría Área de Tecnologías de la información (analista, especialista en redes, responsable de área y Jefe)
Institución donde labora
Contraloría General de la República
Tiempo de experiencia
18 años y 9 meses de experiencia en general

II. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.							
FASE	Actividad	Criterios					Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Suficiencia	Relevancia	
Fase I. Contexto de la organización	Alcance de la organización	4	5	5	4	5	
	Análisis del conocimiento del personal	4	5	5	4	5	
FASE II. Análisis de activos, amenazas y vulnerabilidades	Identificación de activos	4	5	5	4	5	
	Identificación de amenazas	4	5	5	4	5	
	Identificación de vulnerabilidades	4	5	5	4	5	
FASE III. Evaluación del riesgo	Identificación del Riesgo	4	5	5	4	5	
	Análisis del Riesgo	4	5	5	4	5	
	Valoración del Riesgo	4	5	5	4	5	

FASE IV. Tratamiento del riesgo	Creación de normas de protección	4	5	5	4	5	
	Plan de Tratamiento de Riesgos	4	5	5	4	5	
FASE V. Comunicación y Monitoreo	Plan de Comunicación de Riesgos	4	5	5	4	5	
	Monitoreo de Riesgos	4	5	5	4	5	
	TOTAL	48	60	60	48	60	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma Experto

Modelo de Gestión de riesgos para mejorar la Seguridad de la Información en los procesos de emergencia en el sector salud pública de la región Lambayeque

Autor: Miluska Natalia Nicho Gómez

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es poner a evaluación o juicio el modelo de gestión de Riesgos de Seguridad de la Información presentado. El esquema presentado es resultado de la armonización de las normas, marcos de trabajo y metodologías mencionadas anteriormente (NTP/ISO 27005 prioritariamente, Magerit, COBIT 5 para Riesgos y Octave). El modelo está dirigido para el área de Emergencias del sector Público.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Róger Gustavo Abanto Ortiz
Grado académico y profesión
Maestro en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de Tecnologías de información.
Áreas de experiencia profesional
Auditoría Área de Tecnologías de la información (analista, especialista en redes, responsable de área y Jefe)
Institución donde labora
Contraloría General de la República
Tiempo de experiencia
18 años y 9 meses de experiencia en general

II. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.							
FASE	Actividad	Criterios					Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Suficiencia	Relevancia	
Fase I. Contexto de la organización	Alcance de la organización	4	5	5	4	5	
	Análisis del conocimiento del personal	4	5	5	4	5	
FASE II. Análisis de activos, amenazas y vulnerabilidades	Identificación de activos	4	5	5	4	5	
	Identificación de amenazas	4	5	5	4	5	
	Identificación de vulnerabilidades	4	5	5	4	5	
FASE III. Evaluación del riesgo	Identificación del Riesgo	4	5	5	4	5	
	Análisis del Riesgo	4	5	5	4	5	
	Valoración del Riesgo	4	5	5	4	5	

FASE IV. Tratamiento del riesgo	Creación de normas de protección	4	5	5	4	5	
	Plan de Tratamiento de Riesgos	4	5	5	4	5	
FASE V. Comunicación y Monitoreo	Plan de Comunicación de Riesgos	4	5	5	4	5	
	Monitoreo de Riesgos	4	5	5	4	5	
	TOTAL	48	60	60	48	60	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma Experto

Modelo de Gestión de riesgos para mejorar la Seguridad de la Información en los procesos de emergencia en el sector salud pública de la región Lambayeque

Autor: Miluska Natalia Nicho Gómez

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es poner a evaluación o juicio el modelo de gestión de Riesgos de Seguridad de la Información presentado. El esquema presentado es resultado de la armonización de las normas, marcos de trabajo y metodologías mencionadas anteriormente (NTP/ISO 27005 prioritariamente, Magerit, COBIT 5 para Riesgos y Octave). El modelo está dirigido para el área de Emergencias del sector Público.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Gilberto Carrión Barco
Grado académico y profesión
Doctor en Ciencias de la Computación y Sistemas, Maestro en Ingeniería de Sistemas, Magíster en Docencia Universitaria, Ingeniero en Computación e Informática.
Áreas de experiencia profesional
Con más de 18 años de experiencia en docencia universitaria en UNPRG, USS, UTP, USMP, USAT e Investigador en la línea de Ciencia de Datos, Transformación Digital, Informática Educativa, Modernización del Estado e Innovación y Gestión por Procesos.
Institución donde labora
Docente de Investigación del Doctorado en Educación y Gestión Pública Escuela de Posgrado UCV.
Tiempo de experiencia
18 años.

II. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.							
FASE	Actividad	Criterios					Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Suficiencia	Relevancia	
Fase I. Contexto de la organización	Alcance de la organización	4	4	5	4	4	
	Análisis del conocimiento del personal	5	4	4	4	5	
FASE II. Análisis de activos, amenazas y vulnerabilidades	Identificación de activos	5	4	4	4	4	
	Identificación de amenazas	5	4	5	5	4	
	Identificación de vulnerabilidades	4	5	5	5	4	
FASE III. Evaluación del riesgo	Identificación del Riesgo	5	4	4	5	5	
	Análisis del Riesgo	4	5	5	4	4	
	Valoración del Riesgo	4	4	4	5	5	

FASE IV. Tratamiento del riesgo	Creación de normas de protección	4	4	4	4	4	
	Plan de Tratamiento de Riesgos	4	5	5	4	4	
FASE V. Comunicación y Monitoreo	Plan de Comunicación de Riesgos	4	4	4	5	5	
	Monitoreo de Riesgos	5	5	4	4	5	
	TOTAL	53	52	53	53	53	

RESULTADOS

Opinión: El modelo propuesto contiene las fases y actividades suficientes y necesarias para ser consideradas validas, por lo tanto, aptas para ser aplicadas en el logro de los objetivos que se plantean en la investigación.

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Gilberto Carrión Barco
Investigador RENACYT
Código P0070731

Anexo 13

Cuadro de amenazas según Magerit (Marca a la dimensión de seguridad de la información más afectada o más relevante)

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
Natural	[N.1] Fuego	X		
	[N.2] Daños por agua	X		
	[N.*] Desastres naturales	X		
Industrial	[I.1] Fuego	X		
	[I.2] Daños por agua	X		
	[I.*] Desastres industriales	X		
	[I.3] Contaminación mecánica	X		
	[I.4] Contaminación electromagnética	X		
	[I.5] Avería de origen físico o lógico	X		
	[I.6] Corte del suministro eléctrico	X		
	[I.7] Condiciones inadecuadas de temperatura o humedad	X		
	[I.8] Fallo de servicios de comunicaciones	X		
	[I.9] Interrupción de otros servicios y suministros esenciales	X		
	[I.10] Degradación de los soportes de almacenamiento de la información	X		
	[I.11] Emanaciones electromagnéticas		X	
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	X	X	X
	[E.2] Errores del administrador	X	X	X
	[E.3] Errores de monitorización (log)		X	
	[E.4] Errores de configuración		X	
	[E.7] Deficiencias en la organización			X
	[E.8] Difusión de software dañino	X	X	X
	[E.9] Errores de [re-]encaminamiento	X		
	[E.10] Errores de secuencia			X
	[E.14] Escapes de información	X		

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
	[E.15] Alteración accidental de la información			X
	[E.18] Destrucción de información	X		
	[E.19] Fugas de información	X		
	[E.20] Vulnerabilidades de los programas (software)	X	X	X
	[E.21] Errores de mantenimiento / actualización de programas (software)		X	X
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)		X	
	[E.24] Caída del sistema por agotamiento de recursos		X	
	[E.25] Pérdida de equipos	X	X	
	[E.28] Indisponibilidad del personal		X	
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)		X	
	[A.4] Manipulación de la configuración	X	X	X
	[A.5] Suplantación de la identidad del usuario	X	X	X
	[A.6] Abuso de privilegios de acceso	X	X	X
	[A.7] Uso no previsto	X	X	X
	[A.8] Difusión de software dañino	X	X	X
	[A.9] [Re]encaminamiento de mensajes	X		
	[A.10] Alteración de secuencia		X	
	[A.11] Acceso no autorizado		X	X
	[A.12] Análisis de tráfico		X	
	[A.13] Repudio			X
	[A.14] Interceptación de información (escucha)		X	

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
	[A.15] Modificación deliberada de la información			X
	[A.18] Destrucción de información	X		
	[A.19] Divulgación de información		X	
	[A.22] Manipulación de programas	X	X	X
	[A.23] Manipulación de los equipos	X	X	
	[A.24] Denegación de servicio	X		
	[A.25] Robo	X	X	
	[A.26] Ataque destructivo	X		
	[A.27] Ocupación enemiga	X	X	
	[A.28] Indisponibilidad del personal	X		
	[A.29] Extorsión	X	X	X
	[A.30] Ingeniería social (picaresca)	X	X	X

Anexo 14: Cuadro de amenazas según Magerit

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
Natural	[N.1] Fuego	X		
	[N.2] Daños por agua	X		
	[N.*] Desastres naturales	X		
Industrial	[I.1] Fuego	X		
	[I.2] Daños por agua	X		
	[I.*] Desastres industriales	X		
	[I.3] Contaminación mecánica	X		
	[I.4] Contaminación electromagnética	X		
	[I.5] Avería de origen físico o lógico	X		
	[I.6] Corte del suministro eléctrico	X		
	[I.7] Condiciones inadecuadas de temperatura o humedad	X		
	[I.8] Fallo de servicios de comunicaciones	X		
	[I.9] Interrupción de otros servicios y suministros esenciales	X		
	[I.10] Degradación de los soportes de almacenamiento de la información	X		
	[I.11] Emanaciones electromagnéticas		X	
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	X	X	X
	[E.2] Errores del administrador	X	X	X
	[E.3] Errores de monitorización (log)		X	
	[E.4] Errores de configuración		X	
	[E.7] Deficiencias en la organización			X
	[E.8] Difusión de software dañino	X	X	X
	[E.9] Errores de [re-]encaminamiento	X		
	[E.10] Errores de secuencia			X
	[E.14] Escapes de información	X		

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
	[E.15] Alteración accidental de la información			X
	[E.18] Destrucción de información	X		
	[E.19] Fugas de información	X		
	[E.20] Vulnerabilidades de los programas (software)	X	X	X
	[E.21] Errores de mantenimiento / actualización de programas (software)		X	X
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)		X	
	[E.24] Caída del sistema por agotamiento de recursos		X	
	[E.25] Pérdida de equipos	X	X	
	[E.28] Indisponibilidad del personal		X	
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)		X	
	[A.4] Manipulación de la configuración	X	X	X
	[A.5] Suplantación de la identidad del usuario	X	X	X
	[A.6] Abuso de privilegios de acceso	X	X	X
	[A.7] Uso no previsto	X	X	X
	[A.8] Difusión de software dañino	X	X	X
	[A.9] [Re]encaminamiento de mensajes	X		
	[A.10] Alteración de secuencia		X	
	[A.11] Acceso no autorizado		X	X
	[A.12] Análisis de tráfico		X	
	[A.13] Repudio			X
	[A.14] Interceptación de información (escucha)		X	

Origen	Descripción	[D] Disponibilidad	[C] Confidencialidad	[I] Integridad
	[A.15] Modificación deliberada de la información			X
	[A.18] Destrucción de información	X		
	[A.19] Divulgación de información		X	
	[A.22] Manipulación de programas	X	X	X
	[A.23] Manipulación de los equipos	X	X	
	[A.24] Denegación de servicio	X		
	[A.25] Robo	X	X	
	[A.26] Ataque destructivo	X		
	[A.27] Ocupación enemiga	X	X	
	[A.28] Indisponibilidad del personal	X		
	[A.29] Extorsión	X	X	X
	[A.30] Ingeniería social (picaresca)	X	X	X

ANEXO 15

Cuestionarios realizados a los 3 hospitales

Hospital Naylamp

ENCUESTA

Objetivo: Recolectar información que aborde las características generales de la organización en estudio, así como los lineamientos considerados en la Gestión de Riesgos de Seguridad de la Información.

Fuente: NTP ISO/IEC 27005, Octave

Seleccione con una X la respuesta que considere pertinente a cada pregunta, en algunos casos complete el detalle la misma.

Objetivo 1: Establecer el contexto

1.1 ¿Tienen definido un modelo de Gestión de Riesgos? Si en caso sea afirmativa, ¿Se llegó a implementar?
Si ( ) No (X)
Normativa Essalud

1.2 ¿La organización cuenta con una bitácora de incidencias, de hechos que afectan la seguridad de la información en la empresa? Si es afirmativa describa alguna de las más relevantes
Si ( ) No (X)
Uso de Ayuda por correo, problemas de seg inf. no ha tenido problemas

1.3 En caso haya bitácora de incidencias, ¿se ha documentado las acciones para gestionar incidencias? En caso sea afirmativo, describa el procedimiento.
Si ( ) No (X)

1.4 La empresa brinda capacitación o genera algún tipo de esquema de concientización en los miembros de la organización con respecto a la Seguridad de la Información
Si ( ) No(X)

1.5 La organización toma medidas para mitigar los riesgos de seguridad de la información. En caso sea afirmativa cuáles son estas
Si( ) No(X)

1.6 Existen planes o procedimientos de seguridad para poner en resguardo las instalaciones, los edificios y las áreas restringidas
Si( ) No(X) El local desde Agosto

Organización

1.7 ¿Cuál es el propósito principal de la organización?

1.8 Objetivos de la organización

1.9 ¿Cuáles son los procesos de información críticos de Atención de Emergencia?
Triaje, actos médicos y derivación a Med. (cirugía) General y pediatría (Bicaños), análisis solicitud Lab. (rayos X) ecografía) rec. Medicas

Naylamp: No hay sede de operaciones, solo cons. ext. y pm aux.

1.10Si se presenta una situación crítica en el negocio, ¿qué servicio(s) complementarios de Emergencia debe seguir operando?
~~Solo~~ Traumashock

1.11¿Con qué áreas interactúa el área de Emergencias generando una transferencia de información?

Área	Tipo de información
Farmacia	Receta
Laboratorio	Análisis (solicitud)
Enfermería	Observación

1.12¿Cuándo se comparte información hacia otras entidades existe un previo acuerdo de confidencialidad?
Si (X) No ( )

1.13 Existen normas y/o documentación de procesos para regular el acceso físico a las áreas de trabajo y hardware (computadoras, dispositivos de comunicación, etc.) y medios de software.
Si(X) No ( )

Objetivo 2: Conocer activos

Identificación de procesos

2.1 ¿Cuáles son los procesos más importantes del área de Emergencia y qué información manejan?

Proceso	Información
Ver acreditación del pac.	Ver si está asegurado

2.3 ¿Manejan información personal resguardada bajo las leyes nacionales relacionadas con la privacidad? ¿Si es afirmativa qué información es?
Si (X) No ( )
Durante el covid hubo fuga de inf para ver historias clínicas Hist. Clínica del paciente, pero ya dieron normas establecidas

2.4 Listado y descripción de los activos del área

Qué activos consideras son de mayor relevancia o criticidad para el área de estudio

i) Información: Información documentada en papel o electrónica

Nombre	Descripción
97% inf digital	
Papel	ticket de atención, recetas, lab, análisis

ii) Sistema: (host, cliente, servidor o red)

Nombre	Descripción
	Windows 10
Red	Cable UTP-6, sin cable, fibra óptica
Servidor	Casa Comunal de la Juv. (inf pasa por antenas) (rayos X)

iii) Software: Aplicaciones de software (sistemas operativos, aplicaciones de base de datos, sw de redes, aplicaciones de oficina, aplicaciones personalizadas, etc)

Nombre	Descripción
ESSI	
Office	
	Paus, SAP, SIAD (Dcam), Anexpad
Correo	Outlook 365

iv) Hardware: Dispositivos físicos de tecnología de la información (estaciones de trabajo, servidores, etc)

Nombre	Descripción
Est de trabajo	10 (Lenovo y Dell)

v) Personas: Personas de la organización (formación, conocimiento y experiencia)

Nombre	Descripción
Med, enf, tec	Prom de 20
TI	2 oper. red, ing electrónico

Nombre: Dante Sono Rodriguez

Cargo: Operador de Red - Hosp. Naylamp

Firma:

Hospital Luis Heysen Incháustegui

ENCUESTA

Objetivo: Recolectar información que aborde las características generales de la organización en estudio, así como los lineamientos considerados en la Gestión de Riesgos de Seguridad de la Información.

Fuente: NTP ISO/IEC 27005, Octave

Seleccione con una X la respuesta que considere pertinente a cada pregunta, en algunos casos complete el detalle la misma.

Objetivo 1: Establecer el contexto

1.1 ¿Tienen definido un modelo de Gestión de Riesgos? Si en caso sea afirmativa, ¿Se llegó a implementar?
Si ( ) No (X)
Todo es Normatividad

1.2 ¿La organización cuenta con una bitácora de incidencias, de hechos que afectan la seguridad de la información en la empresa? Si es afirmativa describa alguna de las más relevantes
Si ( ) No (X)

1.3 En caso haya bitácora de incidencias, ¿se ha documentado las acciones para gestionar incidencias? En caso sea afirmativo, describa el procedimiento.
Si ( ) No (X)

1.4 La empresa brinda capacitación o genera algún tipo de esquema de concientización en los miembros de la organización con respecto a la Seguridad de la Información
Si ( ) No(X)

1.5 La organización toma medidas para mitigar los riesgos de seguridad de la información. En caso sea afirmativa cuáles son estas
Si(X) No( )
De acuerdo a las normas emitidas por la OTIC

1.6 Existen planes o procedimientos de seguridad para poner en resguardo las instalaciones, los edificios y las áreas restringidas
Si(X) No( )

Organización

1.7 ¿Cuál es el propósito principal de la organización?

1.8 Objetivos de la organización

1.9 ¿Cuáles son los procesos de información críticos de Atención de Emergencia?
Los derivaciones del paciente que ingresó al area en Historia Clínica (ESSI)

Proceso	Información
Todos los procesos	Historia Clínica del paciente

1.10Si se presenta una situación crítica en el negocio, ¿qué servicio(s) complementarios de Emergencia debe seguir operando?
Todos los servicios, en especial Centro Quirúrgico, Diagnostico, Labor Rayos X, Hospitalización

1.11¿Con qué áreas interactúa el área de Emergencias generando una transferencia de información?

Área	Tipo de información
Hospitalización	Interconsultas
Exámenes	Análisis Clínicos
Consulta Externa	Derivación a Especialidad

1.12¿Cuando se comparte información hacia otras entidades existe un previo acuerdo de confidencialidad?
Si (X) No ( )

1.13 Existen normas y/o documentación de procesos para regular el acceso físico a las áreas de trabajo y hardware (computadoras, dispositivos de comunicación, etc.) y medios de software.
Si(X) No ( )

Objetivo 2: Conocer activos

Identificación de procesos

2.1 ¿Cuáles son los procesos más importantes del área de Emergencia y qué información manejan?

2.3 ¿Manejan información personal resguardada bajo las leyes nacionales relacionadas con la privacidad? ¿Si es afirmativa qué información es?
Si (X) No ( )
Historia Clínica

2.4 Listado y descripción de los activos del área

Qué activos consideras son de mayor relevancia o criticidad para el área de estudio

i) Información: Información documentada en papel o electrónica

Nombre	Descripción
Electrónico (BOT.)	Toda la inf. del paciente se rag. en el sistema

ii) Sistema: (host, cliente, servidor o red)

Nombre	Descripción
Red	Cableado Cat-6 Sin Wifi Ethernet
S Operativo	Windows 10
Servidor	Windows Server

iii) Software: Aplicaciones de software (sistemas operativos, aplicaciones de base de datos, sw de redes, aplicaciones de oficina, aplicaciones personalizadas, etc)

Serv. Backup Respaldo PACS

Nombre	Descripción
ESSI	
Office 2016	
Outlook	
Sophos (Antivirus)	

PACS, SAP

iv) Hardware: Dispositivos físicos de tecnología de la información (estaciones de trabajo, servidores, etc)

Nombre	Descripción
	Dell y Lenovo
	Core I5, Core I7
	General (160), Emergencia (20)
	Ram 8

v) Personas: Personas de la organización (formación, conocimiento y experiencia)

Nombre	Descripción
TI	Enc. ~~Soporte~~ (Oficina Informática)
Personal	Jefe de Emerg, Jefe de Guardia, Técnica Enfer, Enf, Médico

Hospital Luis Heysen Incháustegui
Nombre: Sa. th Alca Romero
Cargo: Encargado OS. Informática

Hospital Almanzor Aguinaga Asenjo

ENCUESTA

Objetivo: Recolectar información que aborde las características generales de la organización en estudio, así como los lineamientos considerados en la Gestión de Riesgos de Seguridad de la Información.

Fuente: NTP ISO/IEC 27005, Octave

Seleccione con una X la respuesta que considere pertinente a cada pregunta, en algunos casos complete el detalle la misma.

Objetivo 1: Establecer el contexto

1.1 ¿Tienen definido un modelo de Gestión de Riesgos? Si en caso sea afirmativa, ¿Se llegó a implementar?
Sí ( ) No (X)
Normatividad de Essalud para el manejo de datos

1.2 ¿La organización cuenta con una bitácora de incidencias, de hechos que afectan la seguridad de la información en la empresa? Si es afirmativa describa alguna de las más relevantes
Sí ( ) No (X)

1.3 En caso haya bitácora de incidencias, ¿se ha documentado las acciones para gestionar incidencias? En caso sea afirmativo, describa el procedimiento.
Sí ( ) No (X)

1.4 La empresa brinda capacitación o genera algún tipo de esquema de concientización en los miembros de la organización con respecto a la Seguridad de la Información
Sí (X) No ( )

1.5 La organización toma medidas para mitigar los riesgos de seguridad de la información. En caso sea afirmativa cuáles son estas
Sí ( ) No(X)
De acuerdo a las normas de Essalud

1.6 Existen planes o procedimientos de seguridad para poner en resguardo las instalaciones, los edificios y las áreas restringidas
Sí(X) No( )

Organización

1.7 ¿Cuál es el propósito principal de la organización?
Brindar prestaciones de salud y económicas a los ciudadanos

1.8 Objetivos de la organización
Velar por la salud de los ciudadanos y derechos a pianes

1.9 ¿Cuáles son los procesos de información críticos de Atención de Emergencia?
La información del paciente, que llegue a personas ajenas a los familiares

1.10Si se presenta una situación crítica en el negocio, ¿qué servicio(s) complementarios de Emergencia debe seguir operando?
Laboratorios, Rayos X, Salas de Operaciones, TI, Hospitalización, luz - agua

1.11¿Con qué áreas interactúa el área de Emergencias generando una transferencia de información?

Área	Tipo de información
Hospitalización (Internam. del pac)	Diagnósticos del paciente

1.12¿Cuándo se comparte información hacia otras entidades existe un previo acuerdo de confidencialidad?
Sí (X) No ( )

1.13 Existen normas y/o documentación de procesos para regular el acceso físico a las áreas de trabajo y hardware (computadoras, dispositivos de comunicación, etc.) y medios de software.
Sí(X) No ( )

Objetivo 2: Conocer activos

Identificación de procesos

2.1 ¿Cuáles son los procesos más importantes del área de Emergencia y qué información manejan?

Proceso	Información
Registro de información	H.C. del paciente
Hospitalización	"
Sala de emergencias (ingreso)	"

2.3 ¿Manejan información personal resguardada bajo las leyes nacionales relacionadas con la privacidad? ¿Si es afirmativa qué información es?
Sí (X) No ( )
H.C. del paciente

2.4 Listado y descripción de los activos del área

Qué activos consideras son de mayor relevancia o criticidad para el área de estudio

i) Información: Información documentada en papel o electrónica

Nombre	Descripción
ESSI	
Doc en papel	Recetas, ordenes de exámenes auxiliares

ii) Sistema: (host, cliente, servidor o red)

Nombre	Descripción
Red (Cableado-Wifi)	Categoría 6 - Ethernet (interadiar con fibra óptica) 99%
Sist. Operativo	Windows 10 - Linux (RedHat) para imágenes

iii) Software: Aplicaciones de software (sistemas operativos, aplicaciones de base de datos, sw de redes, aplicaciones de oficina, aplicaciones personalizadas, etc)

Nombre	Descripción
Antivirus	Sophos
Office	
Outlook	
	SAP, Personal, Estadística, PACS

iv) Hardware: Dispositivos físicos de tecnología de la información (estaciones de trabajo, servidores, etc)

Nombre	Descripción
Computadoras	20
Servidor	En Linux para imágenes, Windows Server

v) Personas: Personas de la organización (formación, conocimiento y experiencia)

Nombre	Descripción
Admisión	6

Nombre: Luis Canales López
Cargo: Soporte de Sistemas

Firma:

Hospital Almanzor Aguinaga Asenjo