UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

Modelo de seguridad de la información para contribuir en la gestión de entidades de servicios de saneamiento del norte peruano

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

AUTOR

Alejandro Javier Navarro Reyes

ASESOR

Ricardo David Iman Espinoza

https://orcid.org/0000-0003-0409-8773

Chiclayo, 2024

Modelo de seguridad de la información para contribuir en la gestión de entidades de servicios de saneamiento del norte peruano

PRESENTADA POR

Alejandro Javier Navarro Reyes

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

Jury Yesenia Aquino Trujillo
PRESIDENTE

Gregorio Manuel León Tenorio
SECRETARIO

Ricardo David Iman Espinoza
VOCAL

INFORME DE ORIGINALIDAD

12%	11%	4%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	tesis.usat.edu.pe Fuente de Internet	4%
2	hdl.handle.net Fuente de Internet	3%
3	bibliotecadigital.univalle.edu.co Fuente de Internet	2%
4	sedici.unlp.edu.ar Fuente de Internet	1%
5	Submitted to Universidad Católica de Santa María Trabajo del estudiante	1%
6	www.repositorio.usanpedro.edu.pe Fuente de Internet	<1%
7	www.esdegrepositorio.edu.co Fuente de Internet	<1%
8	news.dniproavia.com Fuente de Internet	<1%
9	ri.ues.edu.sv Fuente de Internet	<1%
10	Submitted to Corporación Universitaria Iberoamericana Trabajo del estudiante	<1%
11	Submitted to Universidad TecMilenio Trabajo del estudiante	<1%
12	andina.pe Fuente de Internet	<1%
13	www.informatica-juridica.com Fuente de Internet	<1%

Índice

Lista de Figuras

Lista de Tablas

Resumen

El trabajo de investigación realizado, se focaliza en la exigencia de gestionar adecuadamente la Seguridad de la Información (en adelante SI) en las Entidades Prestadoras de Servicios de Saneamiento (EPS) del norte peruano, detectada luego del diagnóstico aplicado a una muestra de cuatro entidades del sector, donde se demostró que carecen de instrumentos para su gestión con el fin de asegurar la disponibilidad, integridad y confidencialidad de sus activos de información, además de no contar con estructuras (roles y áreas) que den soporte a la gestión de la SI. El objetivo general planteado fue proponer un modelo de SI basado en marcos de trabajo y estándares relacionados con la SI, para contribuir en la gestión de las EPS del norte peruano. El trabajo de investigación realizado es de tipo propositiva y descriptiva, de diseño no experimental. El contenido del modelo de SI propuesto se validó por juicio de expertos, logrando su aceptación, lo cual le permite ser aplicado en otras EPS del norte peruano. Asimismo, se comprobó la validez de la pertinencia del modelo de SI propuesto al aplicarse como caso de estudio en la Entidad Prestadora de Servicios de Saneamiento de Lambayeque (EPSEL S.A.), logrando identificar 165 riesgos, de los cuales se observó que existen 31 riesgos de magnitud extrema y 30 riesgos de magnitud alta, a los que se aplicaron 15 controles de seguridad, que fueron monitoreados para estimar su grado de cumplimiento, estableciéndose un plan de mejora continua con los 10 controles que cumplen parcialmente su desempeño.

Palabras clave: Seguridad de la Información, Entidad Prestadora de Servicios de Saneamiento, controles de seguridad.

Abstract

The research work carried out focuses on the requirement to adequately manage Information Security (hereinafter SI) in the Sanitation Service Providing Entities (EPS) in northern Peru, detected after the diagnosis applied to a sample of four entities. of the sector, where it was demonstrated that they lack instruments for their management in order to ensure the availability, integrity and confidentiality of their information assets, in addition to not having structures (roles and areas) that support the management of the IS. . The general objective set was to propose an IS model based on frameworks and standards related to the IS, to contribute to the management of the EPS in northern Peru. The research work carried out is of a purposeful and descriptive type, with a non-experimental design. The content of the proposed IS model was validated by expert judgment, achieving its acceptance, which allows it to be applied in other EPSs in northern Peru. Likewise, the validity of the relevance of the proposed IS model was verified when applied as a case study in the Lambayeque Sanitation Services Provider Entity (EPSEL S.A.), managing to identify 165 risks, of which it was observed that there are 31 risks of extreme magnitude and 30 high magnitude risks, to which 15 security controls were applied, which were monitored to estimate their degree of compliance, establishing a continuous improvement plan with the 10 controls that partially comply with their performance.

Keywords: Information Security, Sanitation Service Provider Entity, security controls.

Introducción

La importancia de la información en instituciones privadas o públicas, independientemente de su formato, va tomando más fuerza cada día. No se trata tan solo de información registrada, tampoco precisamente la que las personas producen por sí misma, también se refiere a la generada en los diferentes dispositivos y medios digitales. Esta información se considera un activo muy valioso para dichas entidades, por lo que requiere ser preservada convenientemente frente a las amenazas que hagan peligrar su disponibilidad, integridad y confidencialidad, esenciales para cumplir los objetivos estratégicos de las entidades.

En el ámbito internacional, según Torres [1], la evolución de nuevas corrientes tecnológicas ha dado un vuelco importante en la forma de hacer negocios, dado que ha significado el aumento de los riesgos para las organizaciones, puesto que han quedado expuestas a amenazas inesperadas. Lamentablemente hoy en día es bastante accesible agenciarse de diversos recursos y herramientas que permiten a individuos no autorizados alcanzar, con poco esfuerzo y conocimiento, hasta la información protegida, ocasionando graves pérdidas para las organizaciones. La mayor cantidad de información en las organizaciones, se encuentra en los equipos computacionales, dispositivos de almacenamiento y hasta en la misma red de datos, contenidos dentro de lo que se conoce como Tecnologías de la Información (TI), siendo estos los que están sometidos a potenciales amenazas de SI, originadas tanto desde adentro de la propia organización, como desde afuera, procedentes de una amplia variedad de fuentes.

Una situación que ejemplifica lo mencionado según nos comenta Crespo [2], es lo ocurrido a BitGo, una empresa con origen norteamericano, que brinda una plataforma Web líder en el campo de la custodia y almacenamiento de criptomonedas, se puede decir que es la más rápida y segura, una de las más poderosas, pero que en 2016 sufrió un ataque DDoS prolongado que sacudió al sector, pues los servicios de la firma fueron atacados, el hackeo provocó la filtración de información de los clientes y para muchos de ellos implicó vaciar sus cuentas. El ataque a servicios no sólo afectó a esta billetera virtual, sino también a servicios de otros negocios que utilizan su API. Como resultado, se obtuvo un número considerable de horas sin servicio.

De forma similar, nos dice Turton [3], en 2016 los piratas informáticos patrocinados por gobiernos de países importantes utilizaron una artimaña inteligente con la finalidad de arremeter contra infraestructura crítica, como instalaciones de energía nuclear, refinerías de petróleo represas, etc. Según Knapp, especialista de ciberseguridad en Honeywell, la tercera parte del malware hallado en distintas instalaciones y sistemas críticos, se originó en dispositivos USB conectados por el usuario. El malware especialmente diseñado se transmite a dichos

dispositivos y luego se infiltra en los servidores de control de dichas instalaciones críticas. Por ejemplo, el caso del malware Stuxnet, desarrollado por Estados Unidos e Israel específicamente para atacar la planta nuclear de Irán; en el cual el virus simulaba ser un aplicativo convencional para los operadores de la planta nuclear, sin embargo, fue debilitándola gradualmente, dejando sin otra opción a los iraníes, que la de cerrar la planta.

Nuestro país, no es exento de estas situaciones, Acosta [4] nos comunicó lo ocurrido en 2012, cuando en el Organismo Superior de Contrataciones del Estado (OCSE), el 4 de noviembre en la madrugada, una falla en el servidor de datos desencadenó el colapso del Sistema de Adquisiciones y Contrataciones del Estado. Perdiéndose información sustancial de la totalidad de entidades del país, registrada entre los años 2009 y 2012, sobre los procesos de contratación con el estado y desapareciendo casi 800.000 archivos digitales que contenían documentos de procesos, licitaciones, contratos, cartas de garantía, entre otros, los cuales se encontraban almacenadas en los servidores de datos del OSCE. El siniestro afectó a cerca de dos mil entidades públicas.

América Noticias [5], publicó otro ejemplo claro de que cualquier empresa o entidad está expuesta a cualquier ataque, el cual aconteció en noviembre de 2015, cuando el sitio web de la presidencia del Perú fue blanco de piratas informáticos. Dicho sitio web fue hackeado y en lugar de la página web inicial acostumbrada, se publicó una foto que se relacionaba con los enfrentamientos ocurridos en esos días, ocasionados por el conflicto social contra el proyecto minero Tía María en Arequipa.

A nivel local también se han suscitado eventos similares, tal como publicó el Diario Uno [6] en 2016, cuando varios clientes de instituciones financieras, incluido el Banco de la Nación de Chiclayo, fueron víctimas de un importante robo cibernético. Se conoce que el delito fue cometido por "hackers" experimentados en irrumpir en los sistemas informáticos de instituciones financieras, quienes accedieron desde otro país a la red de datos de distintas instituciones bancarias en el Perú, para sustraer dinero de varias cuentas de ahorros y efectuar compras internacionales mediante las tarjetas bancarias de los clientes.

Según el diagnóstico del sector saneamiento en el norte peruano, realizado en las cuatro EPS seleccionadas, específicamente en la EPS del caso de estudio, se identificó algunos problemas coincidentes, de lo cual se puede concluir que no se tiene un Sistema de Gestión de Seguridad de la Información (SGSI), tampoco se cuenta con una política y mucho menos con objetivos de SI que permitan asegurar la disponibilidad, la integridad y la confidencialidad de la información, por lo que, de no solucionarse la situación anteriormente expuesta, se puede incrementar el nivel de riesgo de ocurrencia de incidentes relacionados a la SI, como son la

indisponibilidad, la inutilización o la pérdida de información; haciendo inviable mantener las funciones misionales de la EPS, lo que implicaría pérdidas económicas, desconfianza, así como el daño en la imagen de la entidad.

Esta investigación se formula, de acuerdo mencionado anteriormente, la siguiente interrogante, *¿De qué forma se podría contribuir en gestión de la SI de las EPS del norte peruano?*; a la que se proyectaría la siguiente respuesta: Mediante la propuesta de un modelo de SI basado en marcos de trabajo y estándares relacionados con la SI.

La presente investigación tiene el propósito de contribuir con la gestión de la SI en las EPS del norte peruano, mediante la aplicación en las EPS del modelo de SI propuesto. Para lograr dicho objetivo, fue necesario la consecución de objetivos específicos como: Analizar marcos de trabajo y estándares relacionados con la SI, que sirvan de referencia para el desarrollo de un modelo que se adapte a la realidad de las EPS del norte peruano; armonizar los marcos de trabajo y estándares relacionados con la SI, comparándolos, para determinar fases coincidentes y definir los procesos y actividades relevantes que sirvan de estructura para el modelo de SI propuesto; validar mediante juicio de expertos el contenido del modelo de SI propuesto, que permita su aplicación en una EPS; validar la pertinencia del modelo de SI propuesto a través de un caso de estudio aplicado en una EPS e interpretar sus resultados y conclusiones.

La importancia de la investigación se justifica, en materia económica, entendiendo que se podrán eliminar los sobrecostos generados por una mala gestión en el aseguramiento de las TI, reduciendo los gastos derivados de la racionalización de los recursos tecnológicos; así mismo, permitirá aumentar la recaudación de los servicios prestados a los ciudadanos, permitiendo que se cumplan los objetivos estratégicos económicos y financieros de la entidad. La presente investigación también es de alto interés tecnológico, ya que se aplican los conocimientos que están siendo desarrollados en el mundo sobre gestión de SI. En el aspecto social, existe la necesidad en todo tipo de instituciones, principalmente en las de servicio público, de mejorar la situación problemática, proporcionando continuidad a los procesos misionales, que les permitan brindar mejores y nuevos servicios a los ciudadanos.

La investigación llevada a cabo propone un modelo de SI que pueda aplicarse en las EPS del norte peruano. Aun cuando existe una variedad de estándares de SGSI que determinan marcos de trabajo, éstos difieren con los procesos que se gestionan en el contexto de las EPS. Es por esto el planteamiento de este modelo, basado en estándares reconocidos, es importante porque permite contribuir en la gestión de la SI en las EPS del norte peruano.

CAPÍTULO I: Revisión de literatura

1.1 Antecedentes

En años recientes, se han realizado diferentes investigaciones relacionadas al campo de estudio y/o sector, revelando diferentes posiciones y avances desde una perspectiva científica. Para sustentar la presente investigación, se ha escogido los antecedentes afines y relevantes que sirven de referencia para su desarrollo.

A nivel internacional, Parra [7] propone para el estado colombiano, una estrategia para implementar el modelo de SI en las instituciones públicas, con la implementación de un SGSI sostenible apoyado en el ciclo PDCA. Por ello, se desarrollaron los pasos imprescindibles que se deben considerar al momento de implementar un SGSI. Su objetivo principal es cumplir con las exigencias del gobierno colombiano, que es fortalecer la infraestructura crítica del estado con la implementación de un SGSI, que proporcione una protección eficaz a los recursos de información más valiosos que manejan las instituciones. Para realizar la evaluación del estado actual de SI, se realizó un análisis de brechas, cuyo resultado permitió conseguir una perspectiva general de la situación de los requerimientos de seguridad en la institución. En cuanto a su relación con la presente investigación, su aporte está en relación al conjunto de metodologías y normas que se tomaron en cuenta, así como su análisis para tomar lo que se requiere de cada una al momento de diseñar un modelo, aportando valor en el conocimiento de dichas normas y metodologías. Además, la empresa donde se lleva a cabo la investigación también pertenece al sector de servicios públicos, específicamente de saneamiento, lo cual nos brinda otra óptica de cómo se desarrollan los procesos en una entidad similar.

Vanegas y Pardo [8] en su tesis, nos expone que los proyectos de creación de software no consiguen prosperar debido a varias causas. En tal sentido, tanto administrar proyectos, que traza el camino a seguir, como analizar los riesgos, se han vuelto imprescindibles con el tiempo. El documento muestra la armonización de los estándares reconocidos de riesgos de TI y algunos otros centrados en brindar apoyo a los riesgos, realizando un análisis comparativo a todo nivel para identificar las características afines y relevantes de cada uno de ellos. Los resultados obtenidos revelan las ventajas y la forma en que los estándares contrastados y su implementación pueden armonizarse y así apoyar las tareas desarrollo software de las empresas. Al respecto, el artículo proporciona una vista más precisa sobre las diferencias, similitudes e integraciones viables de los estándares reconocidos de riesgos de TI. Su relación con la presente investigación está basada en el aporte de metodológico utilizado, que sirve de estrategia para para comparar y luego armonizar los estándares identificados. Las recomendaciones

metodológicas de este trabajo derivan de la investigación realizada para cada estándar adaptado, en la que se adoptaron las fases y procesos existentes de cada uno, logrando una combinación de todas las cualidades y preceptos comunes en un nuevo modelo.

En el ámbito nacional, Tarrillo [9], en su investigación afirma que uno de los problemas que provocan las crisis empresariales es la falta de mecanismos de control de incidencias de tipo operativo que surgen durante la marcha de los procesos misionales de negocio. El desarrollo de la propuesta empieza al seleccionar las incidencias más frecuentes y representativas a partir de dos casos de estudio, con base en ello se establecieron los procesos de ITIL que intervienen en la construcción de la metodología, los cuales se alinearon con las perspectivas de CMI, basándose en el plan maestro y estratégico de la entidad, resultando el mapa estratégico de CMI, con sus criterios de cumplimiento correspondientes. Además, se definieron roles, responsabilidades, formatos, reglas y procesos, que constituyen los entregables de la propuesta metodológica. Finalmente, se desarrolló un plan en tres etapas para la implementación de dicha metodología en dicha entidad. Como se puede evidenciar, existe una conexión estrecha con la presente investigación, dado que las entidades objeto de estudio poseen una estructura orgánica similar. Su aporte está en relación al modelo de negocio de ambas entidades, lo que nos dará un mejor criterio en la determinación de los riesgos de SI que se registran en este tipo de entidades. Así mismo, entender mejor cómo se alinean los objetivos de TI a los estratégicos de la entidad, con el propósito de generar valor a la EPS.

En el entorno local, Soto, Peña y Moscoso [10], centran su trabajo en la necesidad de incorporar la gestión de riesgos de TI a las entidades del sector, detectando, después de la evaluación realizada, que estas no desarrollan la gestión de los riesgos o, en su defecto, no la efectúan de manera adecuada. Además, los autores concluyeron que los temas de gestión de riesgos de TI son desconocidos para el personal de TI, por lo que reaccionan instintivamente ante la ocurrencia de incidentes en sus servicios esenciales que son soportados por TI, con la eventualidad de generar perjuicios económicos y daño reputacional ante la sociedad. El antecedente citado resulta de especial interés para el investigador, porque también se desarrolla en el sector saneamiento y su modelo igualmente fue aplicado como caso de estudio en la misma entidad, lo cual hace posible un mejor entendimiento del contexto, así como de las causas que generan riesgos de TI; sirviendo como referencia para la preparación del modelo de SI propuesto.

1.2 Base Teórico Conceptual

Esta sección hace referencia a cada uno de los conceptos estudiados que están relacionados con el tema de investigación, los cuales proporcionan el sustento teórico pertinente al modelo de SI propuesto.

1.2.1 Seguridad de la Información (SI)

Es la preservación de los principios elementales de la disponibilidad, integridad y confidencialidad de la información y los sistemas involucrados en su tratamiento.

La SI, no solo abarca los aspectos referidos a la tecnología, sino también los espacios físicos, los procesos y esencialmente las personas.

1.2.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Es una colección de medidas proactivas y reactivas, con el propósito de proteger y asegurar la información de las amenazas, así como de accesos no autorizados, errores en las operaciones, ciberataques, entre otros.

Un SGSI tiene un enfoque sistémico que permite establecer, planificar, operar, monitorear, revisar y mejorar la SI en una entidad, con la única intención de conseguir los objetivos y metas del negocio.

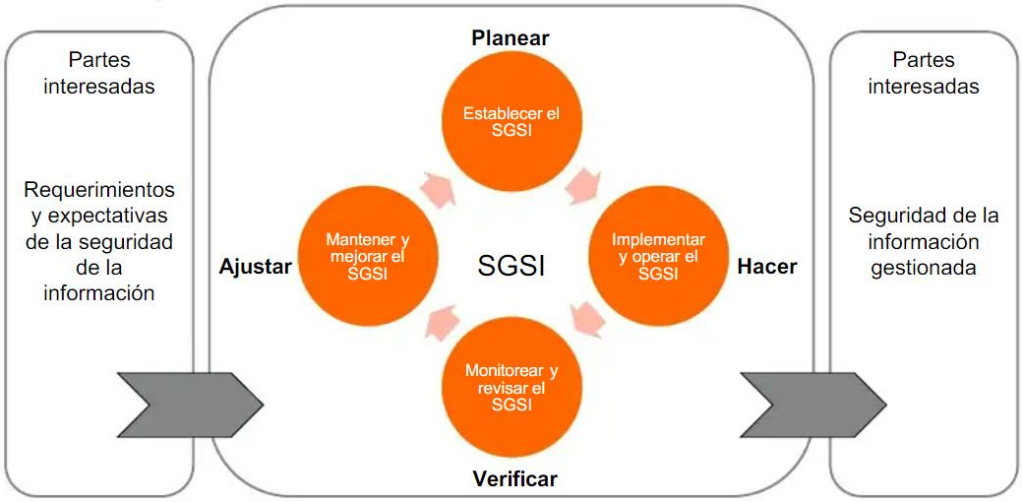
El SGSI es una herramienta que permite a la entidad poner en marcha la implantación de políticas y objetivos de seguridad, dispuestos por los órganos de dirección de la organización.

1.2.3 NTP ISO/IEC 27001:2022

La mencionada norma, especifica los requisitos que permiten el establecimiento, implementación, operación y mejoramiento continuo de un SGSI dentro del ambiente de la entidad. Esta norma incluye también los requerimientos para la evaluación y el tratamiento de riesgos de SI adecuados a las exigencias de la organización. [11]

La norma sigue el ciclo o modelo Plan, Do, Check, Act (PDCA o PHVA por las siglas en español), que estructura los procesos del SGSI, tal como se explica en la Figura 1.

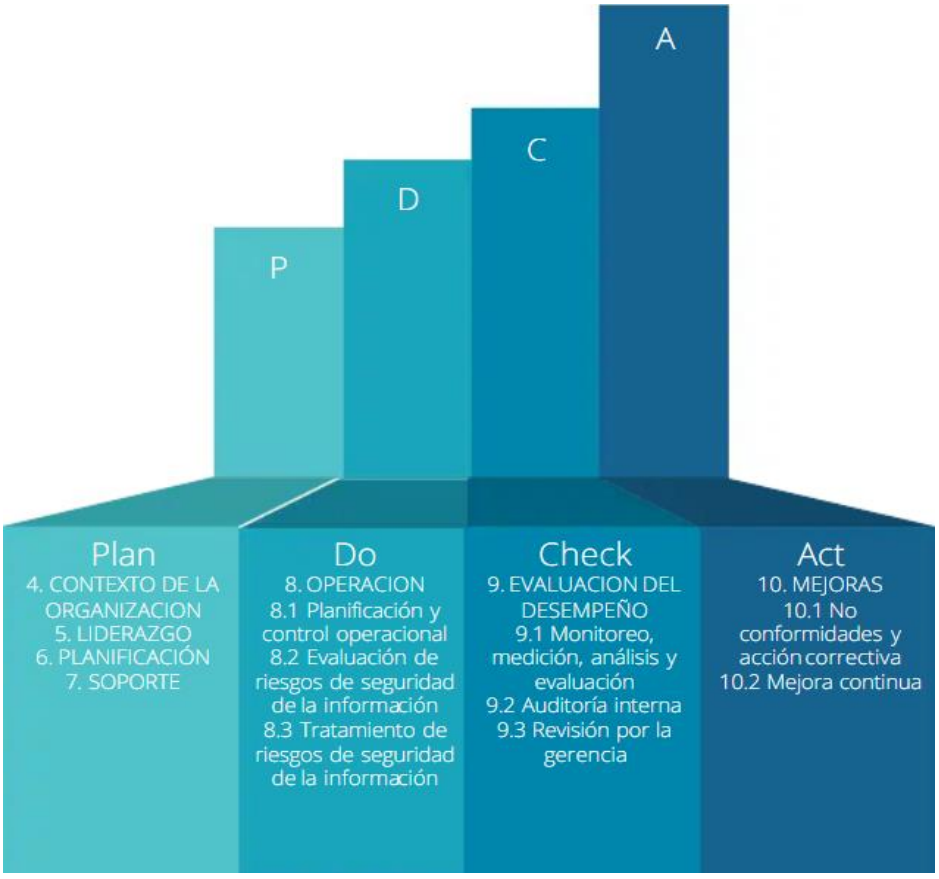
Figura 1: Ciclo PDCA aplicado a procesos del SGSI



Fuente: COBIT 5 para SI

La NTP ISO/IEC 27001:2022 detalla un conjunto de requerimientos que permiten implementar un SGSI (Clausula 4 a 10), los cuales se enumeran y clasifican según el ciclo PDCA. (Figura 2)

Figura 2: Requerimientos del SGSI



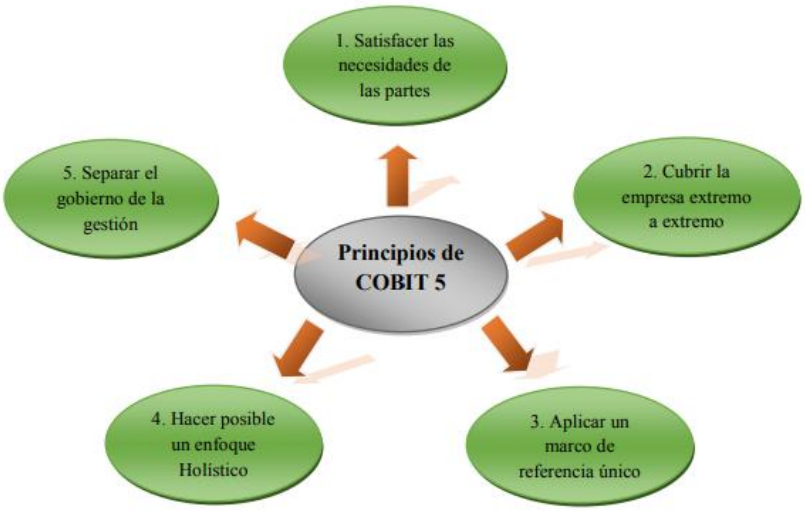
Fuente: NTP ISO/IEC 27001:2022

1.2.4 COBIT 5 (para SI)

Se refiere de un marco de trabajo contiene las prácticas más desarrolladas en lo que es la administración de los sistemas de información y brinda un enfoque holístico en cuanto al manejo de la seguridad y gobierno de TI, complementándose con publicaciones y guías especializadas en gestión de riesgos, seguridad, cumplimiento, gobierno de TI, etc. Su aplicación está abierta a integrarse con otros marcos de trabajo adoptados en las organizaciones, lo cual ayudaría a crear valor añadido en los procesos de TI.

COBIT 5 para SI está soportado por cinco principios que proporcionan un manejo integrado en las organizaciones, dejando claro que el gobierno corporativo de la empresa no debe estar separado de los recursos de TI, tal como muestra la Figura 3.

Figura 3: Principios COBIT 5

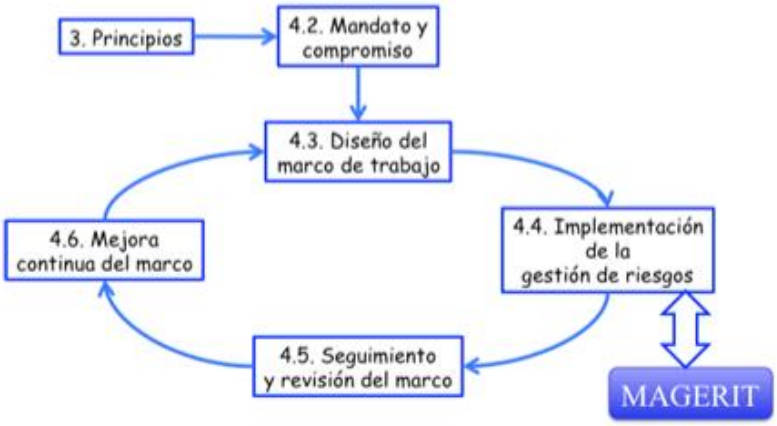


Fuente: COBIT 5

1.2.5 MAGERIT

Esta metodología ejecuta el procedimiento de gestión de riesgos, de manera ordenada, dentro de un marco de trabajo (Figura 4); el cual sirve para investigar los riesgos que han surgido del uso generalizado de las TIC, con el fin de que los organismos de dirección puedan tomar decisiones recomendando medidas eficaces que deberían adoptarse para mitigar dichos riesgos. [12]

Figura 4: Marco de trabajo para gestión de riesgos

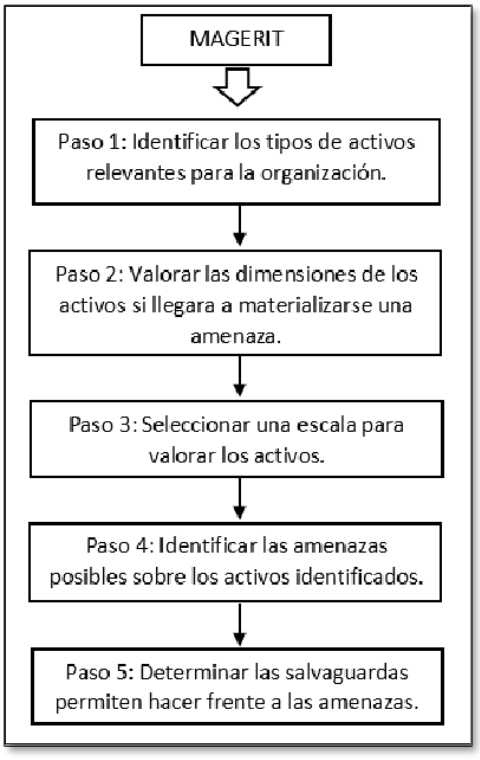


Fuente: ISO 31000

MAGERIT busca concienciar a los representantes de las empresas acerca la presencia de diferentes tipos de riesgos y la exigencia de mitigarlos oportunamente, así como brindar un método ordenado para evaluar dichos riesgos y contribuir a establecer y planear acciones eficaces para controlarlos. Además de preparar a la institución hacia auditorías o procesos de acreditación o certificación.

A continuación, la Figura 5 muestra los pasos para analizar y gestionar el riesgo de acuerdo a MAGERIT.

Figura 5: Proceso de análisis y gestión del riesgo



Fuente: MAGERIT (versión 3.0)

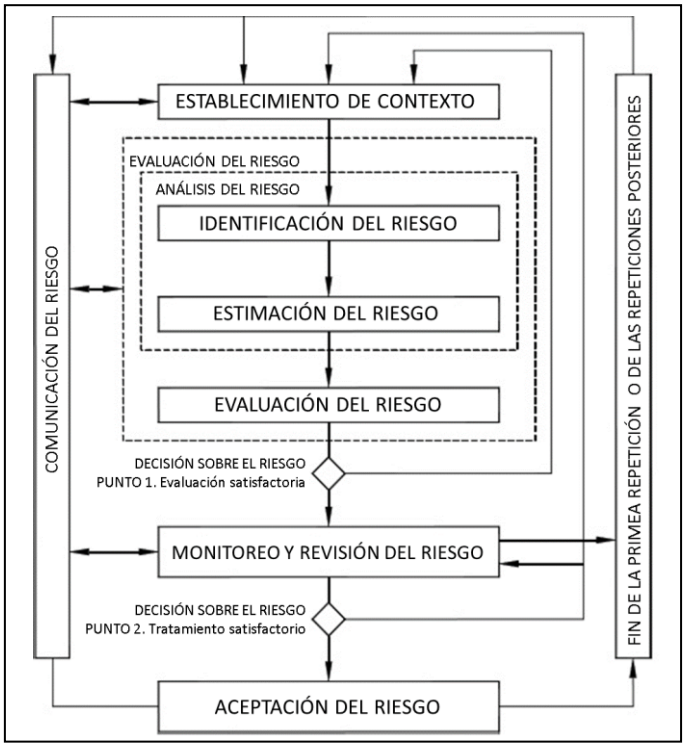
1.2.6 ISO/IEC 27005

ISO/IEC 27005 [13], se refiere a un estándar cuyo propósito se destina a la administración de riesgos de SI. La norma facilita pautas con el propósito de gestionar los riesgos de SI de la empresa y respalda los requerimientos del SGSI puntualizados en ISO 27001.

Ésta norma es apropiada para instituciones de cualquier índole, que pretendan administrar los riesgos que puedan afectar la SI de su organización. No sugiere un método específico, sino que depende de diferentes variables, como el alcance existente del SGSI o como el sector económico al que pertenece la propia industria.

La Figura 6, a continuación, muestra a detalle la secuencia ordenada de la gestión de los riesgos de SI.

Figura 6: Proceso de gestión de riesgos en SI – ISO/IEC 27005



Fuente: ISO/IEC 27005:2011

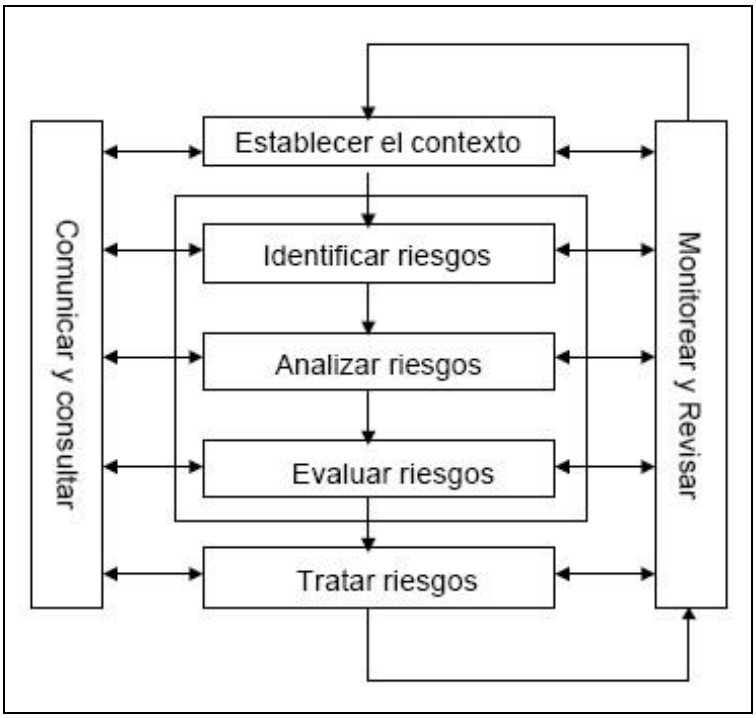
1.2.7 ISO/IEC 31000

Gestión de Riesgos. Principios y Directrices - ISO/IEC 31000 [14], es un cúmulo de directrices y principios que brindan un enfoque sistémico y estructurado para identificar, evaluar, tratar y monitorear los riesgos en cualquier tipo de organización.

Esta norma facilita un itinerario de cómo planificar tanto una auditoría interna, como externa; no impone pautas específicas para gestionar los riesgos, en cambio provee indicaciones para el establecimiento de un sistema de gestión del riesgo.

La Figura 7, a continuación, muestra el proceso de gestión del riesgo.

Figura 7: Proceso de gestión del riesgo – ISO 31000



Fuente: ISO 31000:2016

1.2.8 Metodología para Comparar y Armonizar Modelos

Metodología que sirve de estrategia para comparar y luego armonizar estándares adaptados que respalden la gestión de la SI. [15]

Esta metodología consta de cuatro etapas, tal como se explica en la Figura 8 y se describe subsiguientemente:

- Etapa 1. Identificar los diferentes marcos de trabajo y estándares concernientes a la gestión de la SI.
- Etapa 2. Comparar los modelos identificados, analizando detalladamente sus particularidades, ventajas y desventajas, reconociendo los elementos comunes y clasificándolos según su enfoque.
- Etapa 3. Clasificar los atributos generales del proceso de gestión de SI de forma que queden clasificadas por fases, donde cada una de éstas describan los puntos comunes del manejo de SI.

- Etapa 4. Elaborar un resumen ejecutivo presentando las conclusiones del análisis de las dos fases anteriores para proporcionar recomendaciones y conclusiones sobre el manejo de la SI.

Figura 8: Etapas para comparar y armonizar modelos

Fuente: Tesis doctoral [15]

CAPÍTULO II: Materiales y Métodos

2.1 Diseño de investigación

Se trata de una investigación del tipo propositiva y descriptiva.

Asimismo, esta investigación es de diseño no experimental.

2.2 Definición de variables

Independiente: Modelo de SI basado en marcos de trabajo y estándares relacionados con la SI.

El modelo de SI es un SGSI desarrollado a medida, en el cual se integran diferentes marcos de trabajo y estándares armonizados de acuerdo a la realidad de las EPS del norte peruano. El desarrollo de un modelo de SI nos va a permitir contribuir en su gestión.

Dependiente: Gestión de la SI de las EPS del norte peruano.

Se refiere al manejo apropiado de los diversos activos de información, con el propósito de asegurar la disponibilidad, integridad y confidencialidad de la información en las EPS del norte peruano. Va a depender de la implementación de controles indispensables para impedir la pérdida de datos, inutilización o indisponibilidad de información relevante.

2.3 Población, muestra y muestreo

Para la investigación, la población se extendió a todas las EPS del norte peruano.

De acuerdo a la población accesible, se seleccionaron cuatro EPS del norte peruano, las cuales se describen en el Anexo 1.

2.4 Criterios de selección

El criterio que cumplen las entidades que son parte de la población para la investigación, es el de desarrollar actividades vinculadas al sector saneamiento, las cuales se encuentran bajo el ámbito de regulación de la SUNASS como EPSs, con el propósito primordial de brindar servicios de saneamiento, conforme a lo dispuesto en Ley General de Servicios de Saneamiento.

2.5 Técnicas Instrumentos de recolección de datos

Se emplearon diferentes técnicas con sus respectivos instrumentos para la recolección información, detallados a continuación:

- Observación: Se realizó una observación no estructurada, donde se analizaron los procesos comerciales y administrativos de las EPS seleccionadas, nos permitió comprender cómo se procesa la información para identificar puntos críticos y determinar cuáles son riesgos de información latentes.
- Encuesta: Se aplicó un cuestionario (Anexo 2) para diagnosticar la SI en las EPS seleccionadas, a los gerentes y responsables de Informática de las EPS seleccionadas, el cual ha sido validado de acuerdo a los requerimientos de la NTP ISO/IEC 27001:2022 como puede verse en el Anexo 3.
- Análisis documental: Se estudió ampliamente la literatura relacionada con la SI; Así mismo, se revisaron los siguientes documentos de gestión de las cuatro EPS seleccionadas (Anexo 1):
  - ✓ Directivas y políticas de la EPS.
  - ✓ MOF y ROF.
  - ✓ Visión, misión, valores, objetivos estratégicos, ámbito y organigrama.
  - ✓ Plan estratégico.
  - ✓ TI.
- Validez del contenido: El modelo de SI propuesto, se sometió a juicio de expertos para evaluar su contenido, siendo validado por medio del coeficiente de concordancia de Kendall.

2.6 Técnicas de procesamiento de datos

Después de aplicar el cuestionario para diagnosticar la SI en las EPS seleccionadas, se analizaron y procesaron los resultados empleando hojas del cálculo.

De esta forma, con dichos resultados, conjuntamente con la información recolectada mediante la observación y análisis documental, y luego del estudio de literatura relacionada con la SI y gestión de EPS, se comenzó con el diseño de la propuesta de un modelo de SI a medida para las EPS del norte peruano.

CAPÍTULO III: Resultados y Discusión

3.1 Diagnóstico del Sector

Después de recabar información acerca de las EPS, se puede resumir que, son empresas que operan en zonas urbanas; las cuales fueron instituidas con objeto específico de suministrar servicios de saneamiento, acorde a lo establecido en la Ley General de Servicios de Saneamiento del Perú. Según la normativa vigente, se reconoce como EPS a una entidad pública, privada, municipal o mixta que ofrece, total o parcialmente, uno o más servicios de saneamiento en dichas zonas urbanas.

La responsabilidad de la prestación del servicio recae en los gobiernos locales provinciales, que son responsables de celebrar los contratos de explotación con las EPS, con el propósito de mejorar la calidad y eficiencia en la administración de los servicios suministrados.

Perú cuenta con 50 EPS, 48 son municipales, una EPS concesionada (ATUSA) y una gestionada por el estado (FONAFE), las cuales se encuentran distribuidas en todo el país, gestionando un total aproximado de 3.7 millones de conexiones de agua potable y desagüe. Estas EPS no solo están dentro del alcance regulatorio de la Superintendencia Nacional de Servicios de Saneamiento (SUNASS), sino que también se encuentran vinculadas con diversas entidades del gobierno central, regional o local, con el fin de coordinar y gestionar cuestiones referidas a la inversión, calidad del agua potable, drenaje de aguas servidas, aprovechamiento de aguas subterráneas, gobierno administrativo, entre otros. También deben cumplir con diversas responsabilidades y exigencias, así como requisitos regulatorios y normativos específicos del sector.

Las EPS deben cumplir con los requerimientos de las diferentes entidades gubernamentales, en su condición de proveedoras de servicios esenciales. Estas demandas van desde disponer de un presupuesto certificado por el Ministerio de Economía y Finanzas, hasta el cumplimiento de normas de calidad del agua potable, estándares ambientales para tratamiento de aguas servidas,

así como el cumplimiento de requisitos sectoriales del Ministerio de Vivienda, Construcción y Saneamiento, Organismo Técnico de Administración de los Servicios de Saneamiento y de los niveles de calidad para la prestación de servicios de saneamiento establecidos por SUNASS.

Adicionalmente, las EPS deben cumplir con la fiscalización por parte de la Contraloría General de la República y con las obligaciones laborales de toda entidad estatal, así como con el pago de impuestos a la Superintendencia Nacional de Administración Tributaria; al mismo tiempo, gran parte de las EPS se encuentran endeudadas con el Fondo Nacional de Vivienda.

Al brindar servicios públicos, las EPS son responsables ante los gobiernos locales y los ciudadanos por sus acciones, por lo que deben dar a conocer los actos de su gestión utilizando mecanismos de buen gobierno corporativo, incluidas consultas públicas y otras actividades que contribuyan a la transparencia de la administración pública.

De todo lo anterior se desprende que la prestación de servicios de saneamiento debe cumplir con disposiciones reglamentarias, que incluyen una serie de responsabilidades asumidas con diferentes organismos públicos.

Respecto a la SI, según el análisis realizado en las cuatro EPS seleccionadas, específicamente en la EPS del caso de estudio, se identificó algunos problemas, de los cuales se puede concluir que no se tiene un SGSI, tampoco se cuenta con una política y mucho menos con objetivos de SI que permitan asegurar la disponibilidad, integridad y confidencialidad de la información, de manera que, al no solucionarse la situación anteriormente expuesta, se puede incrementar el nivel de riesgo de ocurrencia de incidentes relacionados a la SI, como son la indisponibilidad, la inutilización o la pérdida de información; haciendo inviable mantener las funciones misionales de la EPS, lo que implicaría pérdidas económicas, desconfianza, así como el daño en la imagen de la entidad.

3.2 Análisis de marcos de trabajo y estándares relacionados con SI

Para el desarrollo del modelo de SI propuesto, se estudiaron diferentes marcos de trabajo y estándares que estuvieron relacionados al tema de investigación, los cuales se analizaron, compararon y armonizaron tal como se muestra en la Tabla 1.

- NTP ISO/IEC 27001:2022
- COBIT 5 para SI
- MAGERIT 3.0.
- NTP ISO 27005:2008
- NTP ISO/IEC 31000:2011

Tabla 1: Análisis comparativo y armonización de marcos de trabajo y estándares de SI

ISO/IEC 27001:2022	COBIT 5 para SI	MAGERIT	ISO 27005	ARMONIZACIÓN
Cláusula 4 - Contexto de la organización	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 01 - Contexto de la EPS** Ref.: "Establecimiento del contexto" - Norma ISO 31000
4.1 Entender la organización y su contexto	APO01.01 Definir la estructura organizacional	1.2 Determinación del alcance del proyecto	1.1 Definir el alcance y los límites	1.1 Conocimiento de la EPS y de su contexto
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	EDM02 Asegurar la entrega beneficios EDM05 Asegurar la transparencia hacia las partes interesadas APO02.01 Entender la dirección de la empresa APO04.2 Mantener un entendimiento del ambiente de la empresa APO08.01 Entender las expectativas del negocio APO10.01 Identificar y evaluar las relaciones y contratos con el proveedor	1.1 Estudio de la oportunidad 1.4 Lanzamiento del proyecto	1.1 Definir el alcance y los límites	1.2 Comprensión de las necesidades y expectativas de las partes interesadas
4.3 Determinación del alcance del SGSI	APO13.01 Establecer y mantener un SGSI	1.2 Determinación del alcance del proyecto	1.1 Definir el alcance y los límites	1.3 Determinación del alcance
Cláusula 5 - Liderazgo	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 02 - Liderazgo**
5.1 Liderazgo y compromiso	APO01.04 Comunicar objetivos y dirección de administración APO02.05 Definir el plan estratégico y el plan de proyectos y objetivos a seguir APO11.06 Gestionar la mejora continua			2.1 Liderazgo y compromiso
5.2 Política	APO01.08 Mantener la conformidad con políticas y procedimientos			2.2 Política
5.3 Roles organizacionales, responsabilidades y autoridades	APO01.02 Establecer roles y responsabilidades APO02.02 Evaluar el entorno actual, las capacidades y el rendimiento	1.3 Planificación del proyecto	1.3 Establecer y mantener las responsabilidades en la organización	2.3 Roles y responsabilidades
Cláusula 6 - Planificación	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 03 - Planificación**

6.1 Acciones para dirigir los riesgos y oportunidades	APO02.03 Definir las capacidades de TI y sus objetivos	1.4 Lanzamiento del proyecto 2.1 Caracterización de los activos 2.2 Caracterización de las amenazas 2.3 Caracterización de las salvaguardas 2.4 Estimación del estado de riesgo	1.2 Desarrollar criterios de evaluación de riesgo, criterios de impacto, criterios de la aceptación del riesgo	3.1 Identificación del riesgo 3.2 Análisis del riesgo 3.3 Valoración del riesgo 3.4 Tratamiento del riesgo
6.2 Objetivos de SI y planes para lograrlos	APO01.04 Comunicar objetivos y dirección de administración	1.3 Planificación del proyecto		
6.3 Planificación de los cambios	APO13.03 Supervisar y revisar el SGSI	3.1 Toma de decisiones 1.3 Planificación del proyecto		
Cláusula 7 - Soporte	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 04 - Soporte**
7.1 Recursos	APO05 Gestionar el portafolio APO06 Gestionar el presupuesto y los costes APO07 Gestionar los recursos humanos EDM04 Asegurar la optimización de recursos	1.4 Lanzamiento del proyecto		4.1 Recursos
7.2 Competencia	APO07 Gestionar los recursos humanos EDM04 Asegurar la optimización de recursos	1.4 Lanzamiento del proyecto		
7.3 Concienciación	EDM04 Asegurar la optimización de recursos APO07 Gestionar los recursos humanos EDM04 Asegurar la optimización de recursos	1.4 Lanzamiento del proyecto		4.2 Comunicación y Concienciación
7.4 Comunicación	APO01.04 Comunicar objetivos y dirección de administración APO02.06 Comunicar la estrategia y la dirección de TI APO08.04 Coordinar y comunicar	1.4 Lanzamiento del proyecto	Cláusula 11 - Comunicación del riesgo	
7.5 Información documentada	APO01.06 Definir información y propietarios del sistema APO09.02 Catálogo de servicios permitidos por IT			
Cláusula 8 - Operación	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 05 - Operación**

8.1 Planificación y control operacional	EDM03 Asegurar la optimización del riesgo APO12 Gestionar el riesgo	3.1 Toma de decisiones 3.2 Plan de seguridad 3.3 Ejecución del plan		5.1 Planificación y control operacional
8.2 Evaluación de riesgos de SI	APO12.02 Analizar el riesgo	3.3 Ejecución del plan	2.1 Análisis del riesgo 2.2 Estimación del riesgo 2.3 Evaluación del riesgo	
8.3 Tratamiento de los riesgos de SI	APO12.06 Respuesta al riesgo	3.3 Ejecución del plan	3.1 Reducción del riesgo 3.2 Retención del riesgo 3.3 Evitación del riesgo 3.4 Transferencia del riesgo Cláusula 10 - Aceptación del riesgo	
Cláusula 9 - Evaluación del desempeño	APO13 Gestionar la Seguridad DSS05 Gestionar servicios de seguridad			**FASE 06 - Evaluación del Desempeño**
9.1 Seguimiento, medición, análisis y evaluación	APO04.3 Monitorear y observar el ambiente tecnológico APO04.6 Monitorear la implementación y el uso de la innovación	3.1 Toma de decisiones	5.1 Monitoreo y revisión de los factores de riesgo	6.1 Monitoreo, análisis y evaluación
9.2 Auditoría interna	APO07.04 Evaluar el desempeño laboral del personal APO07.05 Planear y hacer seguimiento del uso de recursos humanos de TI y de negocio			
9.3 Revisión por la dirección	APO05.06 Gestión de beneficios logrados APO12.04 Articular el riesgo			
Cláusula 10 - Mejoras	APO13 Gestionar la seguridad DSS05 Gestionar servicios de seguridad			**FASE 07 - Mejora**
10.1 No conformidades y acciones correctivas	APO05.06 Gestión de beneficios logrados			
10.2 Mejora continua	APO01.07 Administrar la mejora continua de procesos APO04.5 Recomendar más iniciativas apropiadas APO08.05 Aportaciones a la mejora continua de los servicios APO11.06 Gestionar la mejora continua	3.1 Toma de decisiones	5.2 Monitoreo, revisión y mejora de la gestión del riesgo	7.1 Mejora continua

Posteriormente al análisis de los diferentes marcos de trabajo y estándares relacionados con la SI, se concluye lo siguiente:

COBIT 5 para SI proporciona un marco de gobierno de SI compatible con la NTP ISO/IEC 27001:2022, para garantizar que la información dentro de una organización esté protegida contra la divulgación por parte de usuarios no autorizados (confidencialidad), modificaciones inapropiadas (integridad) y diseñado para asegurar el acceso requerido (disponibilidad).

Por su parte, para ISO/IEC 27001:2022 el SGSI está encaminado a salvaguardar la disponibilidad, integridad y confidencialidad de la información a través de procedimientos para la gestión de riesgos, lo cual ofrece a todas las partes interesadas, la confianza de que el riesgo está debidamente controlado.

Ambos estándares coinciden en el mismo enfoque sobre disponibilidad, integridad y confidencialidad de la información; y establecen como requisitos esenciales para la SI los siguientes:

- Entendimiento de la EPS.
- Necesidades y expectativas de los interesados.
- Compromiso de la alta dirección.
- Roles y responsabilidades.
- Planeación.
- Evaluación y tratamiento de los riesgos.
- Documentación.
- Medición de resultados.
- Mejora continua.

Por otro lado, el método MAGERIT cubre las fases relacionadas a analizar y gestionar los riesgos, estableciéndose un punto de partida para las medidas a tomar durante la disposición y la ejecución. Para implementar el SGSI apoyado en la norma ISO 27001, MAGERIT termina siendo el foco de todas las actividades organizadas en dicho campo.

Además, la relación entre ISO 31000 e ISO/IEC 27001:2022 se establece exactamente en la Cláusula 4.1 de la ISO/IEC 27001:2022 que dice: “La organización puede considerar los contextos externos e internos de acuerdo con la cláusula 5.3 de la norma ISO 31000:2009”. Al mismo tiempo, si se lee detalladamente las cláusulas 5.3.2 y 5.3.3 de ISO 31000:2009 se distingue que son aprovechables, ya que proveen información invaluable sobre el contexto interno y externo en una organización.

Finalmente, como resultado del análisis realizado se identificaron fases coincidentes que se adaptaron al contexto de las EPS del norte peruano, tomando los procesos y actividades

relevantes de cada una de ellas, los cuales estructuraron el modelo propuesto, como se observa en la Tabla 1. Complementariamente, se especificaron los ítems de cada marco de trabajo y estándar que respaldaron el diseño de la estructura, así como el desarrollo de las fases del modelo de SI propuesto, lo cual se ha esquematizado en el la Tabla 2.

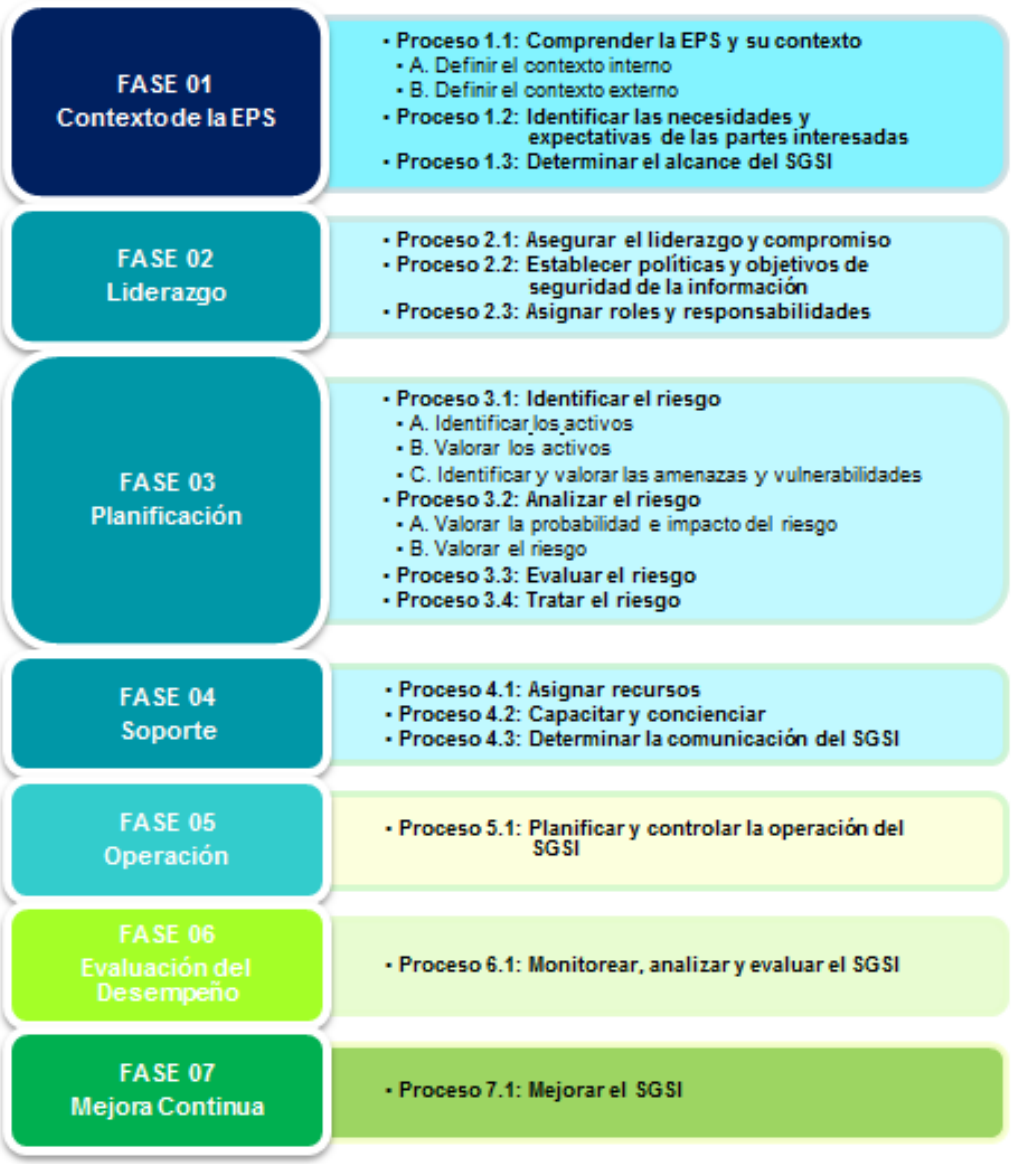
Tabla 2: Especificación de ítems de cada marco de trabajo y estándar que apoyaron el desarrollo del modelo de SI propuesto

PROPUESTA	MARCO DE TRABAJO O ESTÁNDAR DE REFERENCIA
FASE 01 - Contexto de la Organización	
1.1 Conocimiento de la organización y de su contexto	ISO 31000, cláusula 5.3
1.2 Comprensión de las necesidades y expectativas de las partes interesadas	COBIT 5 para SI, Apéndice E.1
1.3 Determinación del alcance	ISO/IEC 27001:2022, numeral 4.1 y 4.2
FASE 02 - Liderazgo	
2.1 Liderazgo y compromiso	ISO/IEC 27001:2022, numeral 5.1
2.2 Política	ISO 27001 - Anexo A.5, numeral 5.2 COBIT 5 para SI, Apéndice A
2.3 Roles y responsabilidades	COBIT 5 para SI, Apéndice C
FASE 03 - Planificación	
3.1 Identificar el riesgo	ISO/IEC 27001:2022, cláusula 6 ISO 27005:2011, numeral 8.2, 8.3 y 9.0 MAGERIT, capítulo 5
3.2 Análisis del riesgo	
3.3 Valoración del riesgo	
3.4 Tratamiento del riesgo	
FASE 04 - Soporte	
4.1 Recursos	COBIT 5 para SI, Apéndice F y G
4.2 Comunicación y Concienciación	
FASE 05 - Operación	
5.1 Planificación y control operacional	ISO/IEC 27001:2022, numeral 8.1
FASE 06 - Evaluación del Desempeño	
6.1 Monitoreo, análisis y evaluación	ISO/IEC 27001:2022, numeral 9.2. ISO 27005:2011, numeral 12.1 y 12.2
FASE 07 - Mejora	
7.1 Mejora continua	ISO/IEC 27001:2022, cláusula 10 COBIT 5 para SI

3.3 Desarrollo del modelo de SI propuesto

Con el propósito de poder definir un modelo adaptado a la realidad del sector y que sirva como referencia para las EPS del norte peruano, se propone un modelo de SI que aborde las principales necesidades de este tipo de organizaciones, el cual se ha desarrollado analizando, comparando y armonizando los marcos de trabajo y estándares reconocidos, relacionados con la SI cuya estructura del modelo de SI propuesto se muestra en la Figura 9, indicando los procesos y actividades que configuran cada fase.

Figura 9: Estructura del Modelo Propuesto



En el Anexo 4 se describe cada una de las fases, así como las entradas, salidas, procedimientos y herramientas a usar en cada uno de los procesos / actividades del modelo de SI propuesto.

3.4 Evaluación del modelo propuesto

3.4.1 Validez del modelo propuesto

Para demostrar el logro del objetivo general trazado para la presente investigación, el cual fue la propuesta de un modelo de SI basado en marcos de trabajo y estándares relacionados con la SI, para contribuir en la gestión de las EPS del norte peruano; se sometió dicha propuesta a juicio de expertos con el apoyo de tres profesionales especializados en el tema, quienes evaluaron el modelo de SI propuesto (Anexo 5), con el fin de valorar su nivel de confiabilidad, calificando los procesos / actividades del modelo de SI propuesto de acuerdo con los indicadores definidos en la Tabla 3.

Tabla 3:Indicadores de calificación para el juicio de expertos

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

Fuente: Adaptado de Escobar y Cuervo [16]

Obtenidas las evaluaciones de los tres expertos después de calificar cada uno de los procesos / actividades del modelo de SI propuesto con relación a suficiencia (SU), coherencia (CO), claridad (CL) y relevancia (RE); se procedió a consolidar los datos de las fichas de validación de expertos en la tabla 4.

Se analizaron los datos de las fichas de evaluación de los expertos mediante el coeficiente de concordancia de Kendall, que sirve para validar el contenido del modelo de SI propuesto, del cual se obtuvo que SI existe concordancia entre las valoraciones de los expertos quienes evaluaron en relación a su coherencia, suficiencia, claridad y relevancia.

Tabla 4: Consolidado de la evaluación de juicio de expertos

FASES	PROCESOS / ACTIVIDADES	EXPERTO 1				EXPERTO 2				EXPERTO 3			
		SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE
FASE 1 Contexto de la EPS	**Proceso 1.1: Comprender la EPS y su contexto**												
	A. Definir el contexto interno	4	4	4	4	4	4	4	4	3	4	3	3
	B. Definir el contexto externo	4	4	4	4	4	4	4	4	3	4	3	3
	Proceso 1.2: Identificar las necesidades y expectativas de las PI	3	4	4	4	4	4	4	4	3	4	3	3
	Proceso 1.3: Determinar el alcance del SGSI	4	4	4	4	4	4	4	4	3		3	3
FASE 2 Liderazgo	**Proceso 2.1: Asegurar el liderazgo y compromiso**	3	4	4	4	4	4	4	3	4	3	3	3
	Proceso 2.2: Establecer políticas y objetivos de SI	4	4	4	4	3	3	4	3	4	3	3	3
	Proceso 2.3: Asignar roles y responsabilidades	3	4	4	4	3	3	4	3	4	3	3	3
FASE 3 Planificación	**Proceso 3.1: Identificar el riesgo**												
	A. Identificar los activos	4	4	4	4	4	4	4	4	4	4	3	3
	B. Valorar los activos	4	4	4	4	4	4	4	4	4	4	3	3
	C. Identificar y valorar las amenazas y vulnerabilidades	4	4	4	4	4	4	4	4	4	4	3	3
	Proceso 3.2: Analizar el riesgo												
	A. Valorar la probabilidad e impacto del riesgo	4	4	4	4	4	4	4	4	3	3	3	4
	B. Valorar el riesgo	4	4	4	4	4	4	4	4	3	4	3	4
	Proceso 3.3: Evaluar el riesgo	4	4	4	4	4	4	4	4	3	4	3	3
	Proceso 3.4: Tratar el riesgo	4	4	4	4	4	4	4	4	3	4	3	3
FASE 4 Soporte	**Proceso 4.1: Asignar recursos**	4	4	4	4	3	3	3	3	3	3	3	4
	Proceso 4.2: Capacitar y concienciar	3	4	4	4	3	3	3	3	3	3	4	4
	Proceso 4.3: Determinar la comunicación del SGSI	4	4	4	3	3	4	4	4	3	3	3	4
FASE 5 Operación	**Proceso 5.1: Planificar y controlar la operación del SGSI**	3	4	4	4	3	3	4	4	3	3	3	4
FASE 6 Evaluación del Desempeño	**Proceso 6.1: Monitorear, analizar y evaluar el SGSI**	4	4	4	4	4	4	4	4	3	3	4	3
FASE 7 Mejora Contínua	**Proceso 7.1: Mejorar el SGSI**	4	4	4	4	4	4	4	4	3	3	3	4

3.4.2 Aplicación del modelo de SI propuesto como caso de estudio

Luego del diagnóstico realizado y después de analizar la situación problemática de las EPS en materia de SI, se identificaron algunos problemas coincidentes, como la falta de políticas y controles de SI implantados, por lo que ante una amenaza, responden por reacción.

Es por esto que se aplicó el modelo de SI propuesto y también validado por juicio de expertos como caso de estudio en EPSEL S.A. (Anexo 6), producto del cual se obtuvieron resultados positivos, mencionando entre otros, los más relevantes:

Se consideraron cuatro políticas de seguridad planteadas por COBIT 5 para SI. Además, se lograron identificar 165 riesgos, de los cuales se observa que existen 31 riesgos de magnitud extrema, asimismo se observan 30 riesgos de magnitud alta, para los cuales se aplicaron 15 controles de seguridad, que fueron monitoreados para medir el nivel de cumplimiento y de ellos sólo 10 controles para planear su mejora continua. Por otro lado, se elaboró el plan de acciones a desarrollar para capacitar y concientizar al personal de la EPS, entre otros; los cuales se detallan en el caso de estudio presentado en el Anexo 6.

Conclusiones

- Resultado de la investigación, se confirmó que las EPS, específicamente la del caso de estudio, no cuentan con procedimientos, medidas y controles de SI para conservar la disponibilidad, integridad y confidencialidad de la información, para lo cual se ha propuesto un modelo de SI, adaptado a la realidad del sector y que aborde sus principales necesidades, para contribuir en la gestión de la SI en las EPS del norte peruano.
- Luego de identificar los marcos de trabajo y estándares relacionados con la SI, se analizaron sus elementos en común y diferencias de acuerdo a las necesidades y prioridades dentro del contexto de las EPS del norte peruano, lo cual sirvió de referencia para desarrollar el modelo de SI propuesto.
- Se logró armonizar los marcos de trabajo y estándares identificados eliminando redundancias y tomando las actividades y procesos relevantes de cada uno de ellos, lo que permitió determinar las fases que estructuraron el modelo propuesto; asimismo se especificaron los ítems de cada estándar y marco de trabajo que favorecieron al desarrollo de las fases del modelo propuesto.
- Mediante juicio de expertos, tres profesionales especializados en el tema han validado la confiabilidad del contenido del modelo de SI propuesto, logrando su aceptación, lo cual permite que sea aplicado a otras EPS del norte peruano.
- El modelo de SI propuesto se aplicó como caso de estudio en EPSEL S.A., para validar su pertinencia, logrando identificar 165 riesgos, de los cuales se observa que existen 31 riesgos de magnitud extrema y 30 riesgos de magnitud alta, para los cuales se aplicaron 15 controles de seguridad, que fueron monitoreados para medir su nivel de cumplimiento, estableciéndose un plan de mejora continua solo con los 10 controles que cumplen parcialmente su desempeño.

Recomendaciones

- ✓ Según los resultados tanto del diagnóstico efectuado como de la aplicación del modelo propuesto, se estima conveniente la creación de los roles de oficial de SI, así como del comité de SI, que dependan de la alta dirección, para así asegurar el compromiso y liderazgo de la gerencia general y del directorio de la EPS.
- ✓ De esta forma, se sugiere conformar un comité de SI, que pueda comenzar sus funciones y asignar responsabilidades, las cuales tendrán como finalidad la implementación de la propuesta del SGSI planteado.
- ✓ Asimismo, se considera primordial la creación de un área de SI, debiendo disponer de personal especializado en SI, dedicado inicialmente a la implementación del modelo de SI propuesto y posteriormente al control y mantenimiento de dicho SGSI, el cual estaría a cargo del oficial de SI.
- ✓ Es conveniente la reorganización de la oficina de informática o su equivalente, posicionándolas a nivel de gerencia de TI, cuyas funciones deberán ser disgregadas a cada área de las EPS, para lograr una mejor funcionalidad por considerarse una pieza clave la implementación del SGSI.
- ✓ Urge en primera instancia, realizar actividades de capacitación y concienciación a todo el personal de la EPS, acerca de la importancia de la información que utilizan en el ejercicio de sus funciones, así como el compromiso de salvaguardarla.

Referencias

[1] Jaime Torres, “Sistema de Gestión de Seguridad de la Información”. [En línea]. Disponible: http://jaimetorresy.blogspot.com/p/sistema-de-gestion-de-seguridad-de-la.html. [Consultado: 04 de Agosto 2018].

[2] Adrián Crespo, “Monedero BitGo sufre ataque DDoS prolongado que hace que la industria se tambalee”, 7 de Junio 2016. [En línea]. Disponible: https://www.redeszone.net/2016/06/07/monedero-bitgo-sufre-ataque-ddos-prolongado-hace-la-industria-se-tambalee/

[3] William Turton, “Los hackers están utilizando unidades USB infectadas para atacar la infraestructura crítica”, 25 de Junio 2017. [En línea]. Disponible: https://es.upost.info/31373830333034373735

[4] Christopher Acosta - El Comercio, “OSCE: se perdieron 800 mil archivos de compras del Estado”, en elcomercio.pe, 19 Agosto 2015. [En línea]. Disponible: https://elcomercio.pe/politica/gobierno/osce-perdieron-800-mil-archivos-compras-197921

[5] América Noticias, “Hackearon sitio web de Palacio de Gobierno”, en www.americatv.com.pe, 13 de Mayo 2015. [En línea]. Disponible: https://www.americatv.com.pe/noticias/actualidad/piratas-informaticos-hackearon-sitio-web-palacio-gobierno-n181354

[6] Diario Uno, “Hacker roba al Banco de la Nación”, en diariouno.pe, 26 de Diciembre 2016. [En línea]. Disponible: http://diariouno.pe/hacker-roba-el-banco-de-la-nacion/

[7] Julieth Parra Casallas, “Elaboración de un plan de implementación de la Norma ISO/IEC 27001:2013 en una empresa prestadora de servicios de acueducto y alcantarillado”, Colombia, Mayo de 2015. [En línea]. Disponible: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43114/6/jparracasaTFM0715memoria.pdf

[8] Gonzalo Vanegas, César Pardo, “Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT”, Colombia, Agosto 2014. Revista S&T, 12(30), 35-48. [En línea]. Disponible: http://www.redalyc.org/articulo.oa?id=411534000003

[9] Omar Tarrillo, “Propuesta de una metodología para el control de incidencias de los procesos en la empresa prestadora de servicios de saneamiento basado en la biblioteca de infraestructura de Tecnologías de Información (ITIL) v3 y el cuadro de mando integral (CMI), Moquegua - 2015”, Moquegua, 2015. [En línea]. Disponible:

http://repositorio.unjbg.edu.pe/bitstream/handle/UNJBG/2504/1217_2017_tarrillo_vargas_od_fain_ingenieria_en_informatica_y_sistemas.pdf?sequence=1&isAllowed=y

[10] María del Carmen Soto, Lissete Moscoso, Edgard Peña, “Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de empresas del sector saneamiento del norte del Perú”, USAT. [Tesis maestría]. 2018.

[11] El Peruano - PCM, Resolución Ministerial Nº 004-2016-PCM - “NTP ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. 2a. Edición", en Normas Legales, p. 2, 14 de Enero 2016.

[12] Javier Candau, José Mañas, Miguel Amutio, “MAGERIT 3.0. Metodología de Análisis y Gestión de Riesgos de Sistemas de Información”, Madrid, España: Ministerio de Hacienda y Administración Pública, pp. 7-70. 2012.

[13] INDECOPI. 2008. ISO/IEC 27005. Gestión de riesgos de Seguridad de Información.

[14] INACAL. 2011. NTP-ISO/IEC 31000. “Gestión del riesgo. Principios y directrices”. Lima.

[15] Carlos Montenegro, Andrés Larco, Efraín Fonseca, “Enfoque Ágil de Armonización de Modelos para Mejora de los Procesos de TI”, Universidad Castilla, La Mancha: Ciudad Real, España. [Tesis doctoral]. Diciembre 2017.

[16] Jazmine Escobar, Ángela Cuervo, “Validez de contenido y juicio de expertos: una aproximación a su utilización”, Revista Avances en Medición, vol. 6, núm. 1, pp. 27-36. 2008

Anexos

ANEXO 1

Descripción de las EPS seleccionadas

Criterio	EPS SEDALORETO S.A.	EPS GRAU S.A.	EPS SEDALIB S.A.	EPSEL S.A.
Razón Social:	Entidad prestadora de servicios de saneamiento de agua potable y alcantarillado de Loreto S.A.	Entidad prestadora de servicios de saneamiento Grau S.A.	Empresa de servicios de agua potable y alcantarillado la Libertad S.A.	Entidad prestadora de servicios de saneamiento de Lambayeque S.A.
Fecha de Creación:	1945	1930	1976	1930
Dirección:	Av. Guardia Civil 1260, Pampa Chica, Iquitos, Loreto	Urb. Santa Ana, Jr. Zelaya la Arena s/n, Piura, Piura	Av. Federico Villarreal No. 1300, Semirústica El Bosque, Los Sapitos, Trujillo, La Libertad	Av. Miguel Grau N° 451 - Chiclayo
Representante Legal:	Ever García Rodríguez	Roberto Sandoval Maza	Oscar Delgado Vásquez	Arturo Colchado Bolívar
Teléfonos de Contacto:	(065) 264343	(073) 306114	(044) 48234 (044) 482364	(074) 238363
Misión:	Brindar servicios de alta calidad y rendimiento, en los aspectos de agua potable y alcantarillado; contribuyendo a mejorar la calidad de vida de la población, mediante una gestión eficiente en el uso de sus recursos y la preservación del medio ambiente.	Contribuir a mejorar la calidad de vida de la población piurana, en el ámbito de nuestra atención, brindando el servicio indispensable de agua potable y saneamiento en condiciones de calidad.	Brindamos con calidad los servicios de abastecimiento de agua apta para el consumo humano y disposición final de aguas residuales; contribuyendo al desarrollo sostenible de la región.	Contribuir a mejorar la calidad de vida de la población de Lambayeque, brindando servicios de saneamiento eficientes y de calidad que ayuden a preservar el medio ambiente obteniendo niveles de rentabilidad que permitan su desarrollo empresarial y de su personal.
Visión:	Ser una empresa de alto nivel y competitividad, liderando los servicios de agua potable y alcantarillado, a nivel nacional.	Ser una empresa respetada y reconocida, con trabajadores orgullosos de pertenecer a una entidad referente del Norte del País.	Al 2021 seremos una empresa reconocida a nivel nacional por su excelencia operativa en el sector saneamiento.	Ser una organización eficiente, rentable, sólida, entre las más importantes del sector, con recursos humanos altamente capacitados que trabajen en equipo, actuando con permanente esfuerzo para lograr un crecimiento sostenible y brindar servicios de calidad orientados a la satisfacción del cliente.
Valores:	- Atención al Cliente: La satisfacción de sus demandas con equidad y su atención con calidad superior en nuestros servicios, es el objetivo primordial y compromiso de la institución. - Eficiencia, Eficacia: Mantener la eficiencia y la eficacia de los servicios, innovando de manera permanente los procesos administrativos y técnicos y en favor de la gestión, afirmándose la confianza de los clientes del servicio. - Trabajador: Es el capital más importante de la empresa. Se prioriza su justa remuneración, su capacitación permanente, su desarrollo y realización personal. - Ética Empresarial: Es práctica permanente en todos los actos y procesos; base principal de la imagen empresarial y de pertenencia al patrimonio de la entidad; y compromiso de todo el equipo de trabajo.	- Servicio: Nosotros asumimos una actitud proactiva de colaboración hacia los demás, desarrollando un esfuerzo permanente en contribución a la mejora de la calidad de vida de la población. - Integridad: Cultivamos las relaciones humanas en base al respeto, honestidad, lealtad, confianza y transparencia, siendo responsables de nuestras acciones frente a la comunidad. - Responsabilidad: Valoramos la salud, la seguridad y el bienestar de nuestros colaboradores, así como de la comunidad, cuidando el medio ambiente y gestionando los recursos esmeradamente. - Trabajo en equipo: Desarrollamos actividades en un entorno flexible y participativo, compartiendo nuestras ideas, conocimientos y experiencias, orientados a la mejora continua.	- Valoramos y respetamos a las personas - Actuamos con honestidad - Fomentamos el liderazgo - Trabajamos en equipo - Logramos metas - Actuamos con responsabilidad - Cuidamos el medio ambiente	- Trabajo en equipo: Unamos capacidades para alcanzar nuestros objetivos. - Honestidad: Seamos honestos con nosotros mismos y con los demás. - Protección del medio ambiente: Respeto a las leyes sobre salud pública y protección del medio Ambiente. - Servicio de calidad a Los clientes: Porque sabemos que desean nuestros clientes, trabajamos para ellos. - Responsabilidad: Asumamos los retos diarios y preparémonos para el futuro. - Respeto por la persona y dignidad humana: Es nuestro compromiso social y responsabilidad de la Empresa.

Criterio	EPS SEDALORETO S.A.	EPS GRAU S.A.	EPS SEDALIB S.A.	EPSEL S.A.
Objetivos Estratégicos:	- Reducir el índice de Agua No Facturada. - Mejorar lo imagen institucional y desarrollar una cultura sanitaria basada en el "valor" y "calidad" de los servicios de saneamiento. - Asegurar la sostenibilidad y autosuficiencia económica y financiera de la empresa. - Incrementar la cobertura y mejorar la calidad de los servicios de agua potable y alcantarillado.	- Mejorar la eficiencia empresarial. - Asegurar la sostenibilidad económica-financiera. - Garantizar la satisfacción de los clientes y la calidad de la vida de la población servida. - Comprometer nuestra gestión con la preservación y cuidado del ambiente.	- Generar una cultura de ejecución d la estrategia institucional. - Alinear la organización a la estrategia. - Gestionar el conocimiento y las mejores prácticas en agua y saneamiento. - Fortalecer las competencias del personal. - Modernizar e integrar las tecnologías de información y comunicaciones. - Asegurar la calidad de los servicios, a través de la gestión de procesos críticos. - Modernizar los procesos operativos claves con tecnología adecuada. - Reducir la brecha de acceso a los servicios. - Mejorar los resultados económicos-financieros buscando un crecimiento sostenido. - Gestionar nuevas fuentes de financiamiento. - Lograr a satisfacción de clientes y grupos de interés. - Posicionar a SEDALIB S.A. como empresa socialmente responsable	- . Suministrar, mejorar y ampliar la cobertura de los servicios de agua potable y alcantarillado. - Gestionar la calidad de los servicios de agua potable y alcantarillado. - Lograr óptimos resultados económicos financieros. - Lograr una óptima gestión empresarial. - Fortalecer las competencias del talento humano.
Descripción del área de TI:	- Le compete brindar el soporte informático para el procesamiento de información general y clasificada, y generar, a pedido de los usuarios, sistemas de información que ayuden a perfeccionar el proceso de toma de decisiones. Adicional a lo expuesto, se le asigna la responsabilidad de adecuar la organización a una que sea inteligente en su accionar, planteando las veces que sea necesario el uso de nuevos sistemas que permitan estar a la vanguardia de la tecnología. - La Oficina de Informática depende jerárquicamente de la Gerencia General y está a cargo de un funcionario con nivel de jefe de departamento, quien supervisa al siguiente personal a su cargo: profesional en desarrollo de software, profesional en redes, servidores y servicios web, técnico en soporte hardware y software y técnico en soporte usuario en sistemas, cuyas funciones se describen a continuación: - Jefe de oficina de informática: Formula, desarrolla, implementa y controla los planes de sistemas y de tecnologías de información, de acuerdo a los objetivos y metas de EPS SEDALORETO S.A. Además, administra y gestiona los recursos informáticos con el fin de garantizar un servicio de calidad a las áreas usuarias.	Es la oficina encargada de programar, diseñar y desarrollar los sistemas informáticos centrales y periféricos según requerimientos de la gestión de la EPS GRAU S.A. Asume la administración del procesamiento del sistema de información centralizada, apoya y evalúa la producción informática en los órganos de la EPS GRAU S.A. La oficina de informática es el órgano de apoyo que depende de la gerencia general y es la encargada de programar, coordinar, controlar y evaluar el diseño, desarrollo e implementación del Sistema de Gestión Comercial de la EPS GRAU S.A., con la finalidad de efectuar todos los procesos mecanizados de la gestión comercial y de esta manera obtener los estadísticos correspondientes. Como soporte a la gestión comercial se emplea el Sistema Comercial Integrado (SICI), sistema de información para empresas de servicios que integra todos los procesos y funciones implicadas en la gestión comercial en un único sistema. Utiliza como plataforma FoxPro, sus datos de encuentran almacenados en Base datos Fox, teniendo dos ambientes de aplicación; el acceso en línea (tiempo real), a través de toda la infraestructura de red de la empresa, desarrollado en lenguaje de programación FoxPro que se ejecuta diariamente, y mediante el	La sub subgerencia de informática e información depende jerárquicamente de la gerencia general, a quien reporta los resultados de su gestión. Esta área es responsable de los diferentes proyectos informáticos que hubiere. Está conformada por el subgerente de informática e información quien a su vez cuenta con cuenta con personal a su cargo especialistas en desarrollo de software, base de datos y comunicaciones, cuyas funciones se detallan a continuación: Subgerente de informática e información: Planifica el desarrollo tecnológico de la empresa, alineando la estrategia empresarial con bondades que provee las Tecnologías de la Información. Administrar el sistema de información, a fin de mantener un alto nivel de servicio en el soporte informático a la empresa, asesorando y utilizando las más modernas Tecnologías de la Información al servicio de la institución. Ingeniero de software: Planifica e implanta sistemas de información a nivel empresarial. Administra los proyectos informáticos nuevos, brinda soporte y mantenimiento a sistemas informáticos en producción, administra proyectos especiales, así como proyectos web cumpliendo la metodología y las normas estándares a usarse en el desarrollo de los sistemas. Así mismo, coordina y supervisa la	La Oficina de Informática, es el órgano responsable de administrar el sistema de información integral de la Empresa, proporcionando oportunamente los servicios de informática a las demás áreas y dependencias que la requieran, de tal forma que permitan alcanzar las metas empresariales y faciliten una adecuada y oportuna toma de decisiones de la alta dirección. Depende jerárquicamente de la gerencia general. Las funciones de los cargos dentro de la estructura orgánica de la oficina de informática son: Jefe de oficina de informática: Administra la oficina de informática de acuerdo a los planes de trabajo y normas de la empresa, velando que el personal a su cargo cumpla sus responsabilidades brindando soporte técnico a todas las áreas de la empresa. También participa directa e indirectamente en la elaboración y garantizar su cumplimiento de los planes estratégicos informáticos a fin de que estos permitan el logro de los objetivos institucionales y estratégicos de la empresa. Además, elabora y garantiza la ejecución de los planes operativos informáticos que contribuyan al logro de los objetivos estratégicos e institucionales. Es el encargado de administrar eficientemente los recursos informáticos de la empresa, así como proponer la

Criterio	EPS SEDALORETO S.A.	EPS GRAU S.A.	EPS SEDALIB S.A.	EPSEL S.A.
	- Profesional en desarrollo de software: Asegura el funcionamiento de los sistemas informáticos de la institución, realizando el mantenimiento y actualización de los mismos. Además de desarrollar nuevas aplicaciones requeridas por las áreas usuarias. - Profesional en redes, servidores y servicios web: Configura, opera y administra los servicios de red, estableciendo los lineamientos necesarios que garanticen el funcionamiento de los Sistemas de Información y la Seguridad de la Información. Además de administrar el Portal Web. - Técnico en soporte de hardware y software: Soluciona los problemas de hardware y software que se presentan en la Institución, así como dar asistencia técnica a los usuarios que lo requieran. Además de realizar periódicamente el mantenimiento preventivo. - Técnico en Soporte a usuarios en sistemas: Dar soporte a los usuarios en el manejo de los sistemas informáticos con que cuenta la EPS SEDALORETO S. A.	cual se permite la ejecución de procesos como la facturación. El SICI no es considerado un Sistema de Información Gerencial, básicamente por no contar con reportes estadísticos, cuadros comparativos, proyecciones, o indicadores, ayudas que faciliten la visualización de la información. Durante la Implantación del SICI en Zonales, se presentaron problemas que han sido solucionados progresivamente por ajustes en la implantación, presentándose esta situación por efecto del impacto en la implantación de sistemas informáticos de esta envergadura, y por demanda permanente de cambio y mejoras. Existen problemas en el funcionamiento normal de los procesos comerciales en el SICI que son producto de la implantación y nuevos requerimientos, que conjuntamente con los problemas, se vienen coordinando entre las zonales de la Empresa, Equipo de Gestión Comercial y el Equipo de Informática, los cuales se vienen solucionando e incorporando con la puesta a producción de las nuevas versiones del Sistema de Gestión Comercial. El Personal Informático del Sistema comercial, así como la Oficina de Informática (OFIN) proporcionan apoyo informático en la búsqueda de la optimización de los trabajos repetitivos que día a día se realizan, utilizando diversos aplicativos y software para el control comercial de nuestros clientes. OFIN es el órgano directriz sobre informática, entre las Zonales para la solución de los problemas que se presentan con el SICI, tratando de ser el medio más adecuado de solución en la búsqueda de información. El Sistema de información Catastral (AGUASIG), tiene la finalidad de gestionar la actividad de actualización catastral y mantener actualizada la información de la planimetría digital y las conexiones domiciliarías, en un ambiente GIS (Sistema de Información Geográfica), donde la información de las bases de datos del sistema comercial se encuentra asociada a la cartografía digital.	operatividad de los sistemas de informática y de información a su cargo. Además, elabora y mantiene actualizado la documentación técnica de los sistemas, especialmente manuales de diseño y funcionamiento de los sistemas; así como también se encarga de la capacitación de los usuarios de los sistemas. Asistente de base de datos y comunicaciones: Analiza, diseña, controla la integridad y seguridad de la red de comunicaciones de la empresa. Además, analiza, diseña, controla la integridad y seguridad de la base de datos empresarial, estableciendo los mecanismos de control adecuados. Es el encargado de establecer los lineamientos de los estándares y control d calidad de los sistemas de información. También es el responsable de dar soporte informático a todos los niveles de la organización. Apoya en el establecimiento de políticas y estrategias en materia de comunicaciones, hardware, software y aplicaciones informáticas.	automatización de los procesos de información, que contribuyan al logro de eficiencia de la empresa. Analista informático en producción e integración: Proporciona los servicios informáticos para el procesamiento de datos. Es el responsable de realizar las copias de respaldo de información de las bases de datos, información de los servidores, así como la de las diferentes áreas de la empresa de acuerdo a los procedimientos establecidos, así como de la custodia de todos los programas fuentes y ejecutables, estableciendo para ello políticas de resguardo de la información, de tal manera que garantice la integridad de los mismos hasta en caso de algún desastre. Es el encargado de desarrollar capacitaciones y adiestramiento al personal de las áreas usuarias. Propone políticas de operación de los equipos de cómputo en las diferentes oficinas de la empresa, asegurando el cumplimiento del cronograma de trabajo. Analista informático en desarrollo: Desarrolla en coordinación con las áreas de la empresa la implementación del sistema de información gerencial. Analiza y evalúa los requerimientos de automatización solicitados por los usuarios en las diferentes áreas, para determinar su factibilidad y/o ejecución. Es el encargado de desarrollar y actualizar los sistemas de información. También identifica, evalúa y propone nuevos software y técnicas para el incremento de la productividad en el desarrollo de operaciones diarias. Técnico en soporte informático: Mantiene operativa física y lógicamente la red informática, brindando el soporte técnico que requieran los usuarios de acuerdo a sus necesidades de hardware y software; así como mantener la plena operatividad de los equipos de cómputo con los que cuenta la empresa. Se encarga de ejecutar el plan anual de mantenimiento preventivo. Además, efectúa el mantenimiento correctivo de los equipos de cómputo. Es el responsable de salvaguardar los accesorios y/o equipos informáticos que se encuentren como stock en el área de soporte técnico, así mismo registra y controla los ingresos y salidas de estos. Es el encargado de llevar un control del inventario de hardware y software, así como de las licencias de software con que cuenta la empresa.

ANEXO 2

Cuestionario

Objetivo: Mediante este instrumento se busca recoger información para conocer el estado situacional de la Seguridad de Información en Entidades Prestadoras de Servicios de Saneamiento del norte peruano.

DATOS GENERALES	
Entidad:	
Cargo:	
Nombre:	
Fecha:	

Marcar con "X" la casilla que usted crea conveniente:
- SI: Si se cumple con la pregunta señalada.
- PARCIAL: La actividad de la pregunta señalada está incompleta.
- NO: No se cumple con la pregunta señalada.

PREGUNTAS	SI	PARCIAL	NO
1. ¿La entidad ha determinado las cuestiones internas y externas que son relevantes para establecer el contexto organizacional?			
2. ¿La entidad ha identificado las partes interesadas y los requisitos más importantes para la Seguridad de la Información?			
3. ¿Han implementado un sistema de gestión de seguridad de información en la entidad?			
4. ¿El directorio garantiza los recursos necesarios para la implementación, supervisión y mejora continua de un SGSI cuando sea necesario?			
5. ¿El directorio asegura la mejora de la Seguridad de la Información?			
6. ¿Existe una política de Seguridad de la Información con objetivos definidos o un marco para el establecimiento de objetivos?			
7. ¿Están asignados y comunicados los roles, responsabilidades y autoridades para la Seguridad de la Información?			
8. ¿Hay un proceso documentado para identificar los riesgos de Seguridad de la Información, incluyendo los criterios de aceptación del riesgo y criterios de evaluación del riesgo?			
9. ¿Está documentado el proceso de tratamiento del riesgo, incluyendo las opciones de tratamiento del riesgo?			
10. ¿Existe un plan para lograr los objetivos de Seguridad de la Información incluyendo responsabilidades, método de evaluación y tiempos para el plan?			
11. ¿Se cuenta con los recursos adecuados para todos los elementos de un SGSI?			
12. ¿Es evaluada la competencia, y la capacitación donde sea necesario, para el personal que realiza tareas que puedan afectar a la Seguridad de la Información?			
13. ¿La entidad ha promovido la concientización de la Seguridad de la Información, de manera que el personal sea consciente de su papel y las consecuencias de no cumplir con las normas?			
14. ¿Hay un proceso de comunicación relacionado con la Seguridad de la Información, incluyendo las responsabilidades, ¿qué se comunica, a quién y cuándo?			
15. ¿Se asegura que existe un manejo de documentos y registros, incluyendo quién revisa y aprueba los documentos, ¿cómo y dónde se publican, almacenan y protegen?			

16. ¿La entidad tiene la información documentada necesaria para estar segura de que sus procesos se llevan a cabo según lo planeado?			
17. ¿Los riesgos, sus propietarios, la probabilidad, las consecuencias y el nivel de riesgo son identificados y estos resultados se encuentran documentados?			
18. ¿Existe un plan de tratamiento del riesgo, aprobado por los propietarios de riesgo?			
19. ¿Está definido qué tiene que ser medido, a través de qué método, quien es responsable, y quien analizará y evaluará los resultados?			
20. ¿Existe un programa de auditoría interna que define las fechas, responsabilidades, reportes, criterios de auditoría y alcance?			
21. ¿La revisión por el directorio se realiza regularmente, y se documentan los resultados en actas de reunión?			
22. ¿La entidad reacciona eficazmente a cada no conformidad?			
23. ¿Se registran todas las no conformidades, junto con las acciones correctivas?			

NOTA: La encuesta se ha validado de acuerdo a los requerimientos de la Norma ISO/IEC 27001:2022, como se puede ver en el ANEXO 3

ANEXO 3

Alineamiento del cuestionario de acuerdo a los requerimientos de ISO/IEC 27001:2022

Requisitos de la norma ISO/IEC 27001:2022	Preguntas
4.0 Contexto de la organización	
4.1 Conocimiento de la organización y su contexto	**1.** ¿La entidad ha determinado las cuestiones internas y externas que son relevantes para establecer el contexto organizacional?
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	**2.** ¿La entidad ha identificado las partes interesadas y los requisitos más importantes para la Seguridad de la Información?
4.3 Determinar el alcance del SGSI	
4.4 SGSI	**3.** ¿Han implementado un sistema de gestión de seguridad de información en la entidad?
5.0 Liderazgo	
5.1 Liderazgo y compromiso	**4.** ¿El directorio garantiza los recursos necesarios para la implementación, supervisión y mejora continua de un SGSI cuando sea necesario?
	5. ¿El directorio asegura la mejora de la Seguridad de la Información?
5.2 Política	**6.** ¿Existe una política de Seguridad de la Información con objetivos definidos o un marco para el establecimiento de objetivos?
5.3 Roles, responsabilidades y autoridades en la organización	**7.** ¿Están asignados y comunicados los roles, responsabilidades y autoridades para la Seguridad de la Información?
6.0 Planificación	
6.1 Acciones para tratar riesgos y oportunidades (6.1.1 Generalidades)	
6.1.2 Valoración de riesgos de Seguridad de la Información	**8.** ¿Hay un proceso documentado para identificar los riesgos de Seguridad de la Información, incluyendo los criterios de aceptación del riesgo y criterios de evaluación del riesgo?
6.1.3 Tratamiento de riesgos de la Seguridad de la Información	**9.** ¿Está documentado el proceso de tratamiento del riesgo, incluyendo las opciones de tratamiento del riesgo?
6.2 Objetivos de Seguridad de la Información y planes para lograrlos	**10.** ¿Existe un plan para lograr los objetivos de Seguridad de la Información incluyendo responsabilidades, método de evaluación y tiempos para el plan?
7.0 Soporte	
7.1 Recursos	**11.** ¿Se cuenta con los recursos adecuados para todos los elementos de un SGSI?
7.2 Competencia	**12.** ¿Es evaluada la competencia, y la capacitación donde sea necesario, para el personal que realiza tareas que puedan afectar a la Seguridad de la Información?
7.3 Concienciación	**13.** ¿La entidad ha promovido la concientización de la Seguridad de la Información, de manera que el personal sea consciente de su papel y las consecuencias de no cumplir con las normas?
7.4 Comunicación	**14.** ¿Hay un proceso de comunicación relacionado con la Seguridad de la Información, incluyendo las responsabilidades, ¿qué se comunica, a quién y cuándo?
7.5 Información documentada	**15.** ¿Se asegura que existe un manejo de documentos y registros, incluyendo quién revisa y aprueba los documentos, ¿cómo y dónde se publican, almacenan y protegen?
8.0 Operación	
8.1 Planificación y control operacional	**16.** ¿La entidad tiene la información documentada necesaria para estar segura de que sus procesos se llevan a cabo según lo planeado?

8.2 Apreciación de los riesgos de seguridad de información	**17.** ¿Los riesgos, sus propietarios, la probabilidad, las consecuencias y el nivel de riesgo son identificados y estos resultados se encuentran documentados?
8.3 Tratamiento de los riesgos de seguridad de información	**18.** ¿Existe un plan de tratamiento del riesgo, aprobado por los propietarios de riesgo?
9.0 Evaluación del desempeño	
9.1 Seguimiento, medición, análisis y evaluación	**19.** ¿Está definido qué tiene que ser medido, a través de qué método, quien es responsable, y quien analizará y evaluará los resultados?
9.2 Auditoría Interna	**20.** ¿Existe un programa de auditoría interna que define las fechas, responsabilidades, reportes, criterios de auditoría y alcance?
9.3 Revisión por la dirección	**21.** ¿La revisión por el directorio se realiza regularmente, y se documentan los resultados en actas de reunión?
10.0 Mejora	
10.1 No conformidad y acciones correctivas	**22.** ¿La entidad reacciona eficazmente a cada no conformidad?
	23. ¿Se registran todas las no conformidades, junto con las acciones correctivas?

ANEXO 4

Procedimiento del Modelo Propuesto

FASE 1: CONTEXTO DE LA EPS

Proceso 1.1: Comprender la EPS y su contexto

A. Definir el contexto interno

El objetivo de este proceso es definir los aspectos de cada factor interno para alcanzar los objetivos estratégicos de la EPS. Para recolectar información se emplea el análisis de documentario, a través de fuentes de información de propias de cada EPS.

Figura 10: Elementos de la actividad - Contexto interno

Entrada	Procedimiento	Salida
- Plan estratégico (visión, misión, valores, objetivos estratégicos). - Plan operativo y presupuesto. - Organigrama, manual y reglamento de organización y funciones. - Cuadro de asignación de personal. - Inventario de activos.	Identificar los parámetros fuente y detalle en cada aspecto identificado del contexto interno: - Normativo: Se identifican cuales son las normas, estándares de referencia adoptados por la EPS. - Metas y objetivos: Determinan lo que se quiere lograr en un tiempo determinado para la EPS. - Valores: Son las particularidades que identifican a la EPS como empresa. - Estructura organizacional: Se precisa como están establecidas las funciones en la EPS. - Recursos tecnológicos: Se refiere a los inventarios de los activos de TI de la EPS.	- Catálogo de definición del contexto interno.

Tabla 1 - Herramienta para definir el contexto interno

FASE 1 - CONTEXTO DE LA EPS **Proceso 1.1 - Comprender la EPS y su contexto** A. Definir el contexto interno			
Objetivo: Identificar los parámetros fuente y detalle en cada aspecto del contexto interno.			
Nº	**Factor**	**Fuente**	**Descripción**
1			
2			
3			
4			
5			
Conclusión:			
Elaborado por:			**Fecha:**

B. Definir el contexto externo

Este proceso tiene como propósito determinar los factores básicos externos para lograr los objetivos estratégicos en la EPS. Para recopilar información se emplearán técnicas e instrumentos como entrevistas, cuestionarios y análisis de documentos.

Figura 2: Elementos de la actividad - Contexto externo

Entrada	Procedimiento	Salida
- Convenios. - SUNASS, OTASS, MVCS, SUNAT, Gobiernos locales. - Marco normativo. - Constitución Política. - Entidades Financieras.	Identificar los parámetros fuente y detalle en cada aspecto identificado del contexto externo: - Ambiente del sector: Se requiere investigar sobre la existencia de convenios con otras entidades que afecten el desempeño de la EPS. - Normativo y político: Indagar si existen normas y leyes que por incumplimiento puedan afectar a la EPS. - Financiero: Se refiere a los aspectos relacionados con la economía.	- Catálogo de definición del contexto externo.

Tabla 2 - Herramienta para definir el contexto externo

FASE 1 - CONTEXTO DE LA EPS **Proceso 1.1 - Comprender la EPS y su contexto** B. Definir el contexto externo			
Objetivo: Identificar los parámetros fuente y detalle en cada aspecto del contexto externo.			
N°	**Factor**	**Fuente**	**Detalle**
1			
2			
3			
Conclusión:			
Elaborado por:		**Fecha:**	

Proceso 1.2: Identificar las necesidades y expectativas de las partes interesadas

En este proceso se identifican las necesidades y expectativas que los interesados esperan de la implementación del SGSI en la EPS. La información referente al tema se obtiene empleando técnicas e instrumentos como son los cuestionarios y las entrevistas.

Figura 3: Elementos del proceso - Partes interesadas

Entrada	Procedimiento	Salida
- Actas de reunión con las partes interesadas. - Documentos legales y reglamentarios. - Obligaciones contractuales. - Pan estratégico. - Convenios, pactos colectivos.	Identificar las partes interesadas y sus necesidades o tipo de información: - Personas o entidades interesadas que tienen transcendencia en la EPS o son afectados por su desempeño. - En el contexto de la SI, se refiere a personas o entidades que influyen o se ven afectadas por la SI o sus actividades relacionadas. - Identificar cuáles son los requisitos que advierten el cumplimiento legal, contractual y reglamentario interno. - Identificar los requisitos que surgen de los resultados esperados respecto a la operación de la EPS. - La plantilla de la tabla 3 se debe llenar empleando un indicador de relación entre la parte interesada y cada tipo de información: ✓ A: Aprobador ✓ O: Origen ✓ I: Informado ✓ U: Destino	- Matriz de necesidades y expectativas de las partes interesadas por tipo de información.

Tabla 3 - Herramienta para identificar necesidades y expectativas de partes interesadas

FASE 1 - CONTEXTO DE LA EPS Proceso 1.2 - Identificar las necesidades y expectativas de las partes interesadas										
Objetivo: Identificar las necesidades y expectativas de las partes interesadas relacionadas con la EPS.										
	Necesidades / Tipo de información									
Parte interesada	Estrategia de SI	Presupuesto de SI	Plan de SI	Políticas de SI	Requerimientos de SI	Plan de Comunicación	Informes de Revisión de SI	Catálogo de Servicios de SI	Perfil de Riesgo de la Inform.	Cuadro de Mando de SI
Interna: EPS										
Directorio										
Gerente General										
Gerente Administración y Finanzas										
Comité de la SI										
Oficial de SI										
Jefe Oficina de Recursos Humanos										
Personal administrativo										
Interna: TI										
Jefe de Oficina de Informática										
Personal de TI										
Externa										
MVCS										
SUNASS										
OTASS										
Gobiernos Locales										
Entidades Financieras										
Proveedores										
Conclusión:										
Elaborado por:					**Fecha:**					

Proceso 1.3: Determinar el alcance del SGSI

La finalidad de esta actividad es tener identificado a los responsables, procesos/funciones e infraestructura de TI relacionados a la aplicación del modelo de SI propuesto. Aquí se consideran las cuestiones internas y externas, partes interesadas y funciones o procesos comprendidos dentro de los límites del SGSI. Para la recolección de información se analizarán los documentos de la EPS.

Figura 4: Elementos del proceso - Determinación del alcance

Entrada	Procedimiento	Salida
- Catálogo de definición del contexto interno. - Catálogo de definición del contexto externo. - Matriz de necesidades y expectativas de las partes interesadas por tipo de información.	- Comprender la EPS. ✓Detallar los procesos o funciones donde se maneja la información a resguardar. ✓Relación del personal responsable del tratamiento de la información. - Identificar lo que necesita ser protegido. ✓Listar los dispositivos físicos (HW) y aplicaciones (SW) que intervienen durante el manejo de la información.	- Listado de dispositivos físicos y aplicaciones de software que intervienen durante el manejo de la información. - Detalle de procesos o funciones donde se maneja la información a resguardar. - Relación de responsables del tratamiento de la información.

Tabla 4 - Herramienta para determinar el alcance del SGSI

FASE 1 - CONTEXTO DE LA EPS Proceso 1.3 - Determinar el alcance del SGSI		
Objetivo: Identificar los responsables, procesos o funciones e infraestructura de TI relacionados con la implementación del SGSI.		
	Detalle	
Procesos/Funciones		
Responsables		
Infraestructura de TI		
Conclusión:		
Elaborado por:		**Fecha:**

FASE 2: LIDERAZGO

Proceso 2.1: Asegurar el liderazgo y compromiso

Tiene la finalidad de verificar el cumplimiento de las funciones de liderazgo por parte del Directorio. Para recolectar información necesaria se realizarán entrevistas al Directorio de la EPS.

Figura 5: Elementos del proceso - Liderazgo

Entrada	Procedimiento	Salida
- Programas de comunicaciones. - Disposiciones, normas. - Planes de incentivos y recompensas.	- Aplicar la plantilla para verificar el cumplimiento del liderazgo (Tabla 5) al Directorio donde se consideran las funciones de SI mínimas requeridas por la ISO/IEC 27001:2022. - Marcar con una X según el cumplimiento de la función: ✓Si = Se cumple con las funciones de liderazgo. ✓No = No se cumple con las funciones de liderazgo. ✓Parcial = la función está incompleta. - Finalmente, se debe especificar la función que falta por cumplir al Directorio.	- Check list de cumplimiento de las funciones del Directorio: ✓Funciones de liderazgo que no cumple el Directorio. ✓Funciones de liderazgo que si cumple el Directorio. ✓Funciones de liderazgo que cumple parcialmente el Directorio.

Tabla 5 - Herramienta para verificar el cumplimiento del liderazgo

FASE 2 - LIDERAZGO Proceso 2.1 - Asegurar el liderazgo y compromiso				
Objetivo: Verificar el cumplimiento de las funciones de liderazgo por parte del Directorio.				
Nº	**Funciones**	**Si**	**Parcial**	**No**
1				
2				
3				
4				
5				
Conclusión:				
Elaborado por:		**Fecha:**		

Proceso 2.2: Establecer políticas y objetivos de SI

Este proceso formaliza el compromiso del Directorio, identificando políticas de SI alineadas a las exigencias de la EPS. Para obtener información pertinente se analizará la documentación relacionada a la SI.

Figura 6: Elementos del proceso - Políticas y objetivos

Entrada	Procedimiento	Salida
- Catálogo de definición del contexto interno. - Catálogo de definición del contexto externo. - Políticas y directivas Institucionales. - Estructura Organizacional. - Políticas planteadas por COBIT 5 para SI, sección II – apéndice A.3.	- Identificar las políticas de SI: ✓Redactar las políticas de acuerdo a las necesidades de la EPS. ✓Debe tener en cuenta los objetivos de la EPS. ✓Demostrar que se tienen en cuenta los requisitos de las partes interesadas. ✓Comunicar la política a las partes interesadas. - Definición: Se explica en qué consiste y cuál es el propósito de cada política. - Alcance: Se identifican las áreas donde se aplicarán las políticas y las personas implicadas en el cumplimiento de la misma. - Objetivo de Seguridad: Se definen los objetivos de SI alineado a cada política de seguridad, acorde a las nuevas tecnologías.	- Documento políticas de SI.

Tabla 6 - Herramienta para establecer las políticas y los objetivos de SI

FASE 2 - LIDERAZGO Proceso 2.2 - Establecer políticas y objetivos de SI				
Objetivo: Identificar y establecer las políticas y los objetivos de SI alineados a la necesidad de la EPS.				
N°	**Política de seguridad**	**Definición**	**Alcance**	**Objetivo de seguridad**
1				
2				
3				
4				
5				
Conclusión:				
Elaborado por:				**Fecha:**

Proceso 2.3: Asignar roles y responsabilidades

El objetivo de este proceso la definición y comunicación de los roles y responsabilidades relacionados con la gestión de la SI en la EPS. Para este fin, se obtendrá información relevante a través del análisis de documentos de la EPS.

Figura 7: Elementos del proceso - Roles y responsabilidades

Entrada	Procedimiento	Salida
- Estructura Organizacional. - Plantilla de determinación del alcance del SGSI.	- Rol: Identificar el rol o cargo del personal de la EPS. Según COBIT 5 para SI, es pertinente la instauración de tres (03) roles: ✓Oficial de SI. ✓Comité de SI. ✓Comité de gestión de riesgos. Además de otros roles y estructuras relacionadas con TI. - Responsabilidad: Identificar las responsabilidades asociadas a cada rol del personal de la EPS. - Nivel de implicancia: Indicar el nivel de repercusión en el personal en la EPS mediante la siguiente calificación: ✓R: Responsable de hacerlo ✓A: Responsable de que se haga ✓C: Consultado ✓I: Informado	- Matriz de roles y responsabilidades de SI claves claramente definidos.

Tabla 7 - Herramienta para asignar roles y responsabilidades

FASE 2 - LIDERAZGO **Proceso 2.3 - Asignar roles y responsabilidades**			
Objetivo: Identificar y asignar roles y responsabilidades del recurso humano que participará en la SI de la EPS.			
Nº	**Rol**	**Responsabilidad**	**Nivel de implicancia**
1			
2			
3			
4			
5			
Conclusión:			
Elaborado por:		**Fecha:**	

FASE 3: PLANIFICACIÓN

Proceso 3.1: Identificar el riesgo

A. Identificar los activos

Tiene como propósito la identificación de los activos existentes dentro de la EPS que, de verse afectados, influiría negativamente en la continuidad de sus operaciones. La información es extraída del inventario de activos de la EPS y la observación directa.

Figura 8: Elementos de la actividad - Identificación de activos

Entrada	Procedimiento	Salida
- Clasificación de los tipos de activos (Cuadro 1).	- Se procede a completar la información en la plantilla para identificar de activos (Tabla 8). - Luego, se identifican los activos de información presentes en la EPS y clasificarlos de acuerdo a la clasificación de los tipos de activos (ver Cuadro 1). - El siguiente paso es codificar los activos de información identificados. - En la columna descripción, indicar la función del activo.	- Listado de activos de información de la EPS.

Cuadro 1 - Clasificación de tipos de activos

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

Tabla 8 - Herramienta para identificar los activos

FASE 3 - PLANIFICACIÓN **Proceso 3.1 - Identificar el riesgo** A. Identificar los activos					
Objetivo: Definir los activos que son críticos para la EPS que, de verse afectados, influiría negativamente en la continuidad de las operaciones de la EPS.					
N°	**Activo**	**Descripción del activo**	**Categoría del activo**	**Cód. de categoría**	**Cód. del activo**
1					
2					
3					
4					
Conclusión:					
Elaborado por:				**Fecha:**	

B. Valorar los activos

Para poder valorar adecuadamente los activos, se ordenan de arriba a abajo, asignando valor en orden de relevancia, considerando los principios de disponibilidad, integridad y confidencialidad, realizando valoraciones tanto cuantitativas como cualitativas. Se recomienda utilizar una escala Likert para el proceso de evaluación, que mide su nivel de cumplimiento. Además de definir el rango de calificación (en este caso de 1 a 5), esto también nos permite tener suficiente amplitud de calificación. Para realizar este paso, los activos deben extraerse de la herramienta utilizada en el proceso anterior.

Figura 9 - Elementos de la actividad - Valoración de activos

Entrada	Procedimiento	Salida
- Listado de activos de información de la EPS.	- Valorar los activos tomando en cuenta los criterios de: ✓Confidencialidad (C): Acceso a la información sólo por el personal autorizado, considerar el cuadro 2. ✓Disponibilidad (D): Acceder a la información cuando se necesite, considerar el cuadro 3. ✓Integridad (I): Exactitud y compleción de la información, considerar el cuadro 4. - Se procede a completar la información del formato de valoración de activos (Cuadro 5). - Nivel de valoración total= C+D+I	- Listado de activos de información valorados.

Cuadro 2 - Valoración de los criterios de confidencialidad

CONFIDENCIALIDAD (C)	
Valor	**Criterio**
1	De naturaleza pública, no requiere control y no tiene impacto negativo en la EPS.
2	De menor importancia, requiere control mínimo, sin impacto negativo en la EPS.
3	Cuasi importante, requiere control bajo, impacta levemente a la EPS.
4	Importante, requiere control medio, impacta negativamente a la EPS.
5	De alta importancia, requiere control alto, impacta seria y negativamente a la EPS.

Cuadro 3 - Valoración de los criterios de disponibilidad

DISPONIBILIDAD (D)	
Valor	**Criterio**
1	Información cual inaccesibilidad no perjudica la realización de los procesos de la EPS.
2	Información cual inaccesibilidad permanente de al menos 10% del tiempo durante la jornada laboral impediría la realización de los procesos de la EPS
3	Información cual inaccesibilidad permanente de al menos 50% del tiempo durante la jornada laboral impediría la realización de los procesos de la EPS
4	Información cual inaccesibilidad permanente de al menos 80% del tiempo durante la jornada laboral impediría la realización de los procesos de la EPS.
5	Información cual inaccesibilidad permanente de al menos el 95% del tiempo durante la jornada laboral ocasionaría un perjuicio significativo para la EPS.

Cuadro 4 - Valoración de los criterios de integridad

INTEGRIDAD (I)	
Valor	**Criterio**
1	No es relevante para la correcta operación de la EPS.
2	Se puede recuperar de una forma bastante fácil.
3	Se puede recuperar guardando la relación pertinente con una molestia razonable.
4	Es posible recuperar la integridad del activo en un tiempo razonable.
5	No es posible recuperar el activo y sus relacionados.

Cuadro 5 - Valoración de los niveles de criticidad de los activos

Rango	Valor	Descripción		Criterio
0	1	Muy Bajo	MB	No es relevante para la operación de la EPS
1 - 3	2	Bajo	B	Perjudica ligeramente la operación de los procesos de la EPS, en 10% del tiempo de la jornada laboral, no involucra pérdida de información.
4 - 6	3	Medio	M	Perjudica la operación de los procesos de la EPS al menos 50% del tiempo de la jornada laboral, no involucra pérdida de información.
7 - 9	4	Alto	A	Perjudica la operación de los procesos de la EPS al menos 80% del tiempo de la jornada laboral, puede involucrar pérdida de información
10 - 12	5	Muy Alto	MA	Interrumpe la operación de los procesos de la EPS al menos 95% del tiempo de la jornada laboral, e involucra pérdida de información.

Tabla 9 - para valorar los activos

FASE 3 - PLANIFICACIÓN **Proceso 3.1 - Identificar el riesgo** B. Valorar los activos								
Objetivo: Identificar el nivel de criticidad de cada activo de información.								
ACTIVO				**VALORACIÓN**				
Nº	**Etiqueta de categoría**	**Código del activo**	**Descripción del activo**	**C**	**D**	**I**	**TOTAL (C+D+I)**	
							Valor	**Descripción**
1								
2								
3								
4								
5								
Conclusión:								
Elaborado por:						**Fecha:**		

C. Identificar y valorar las amenazas y vulnerabilidades

Permite identificar las vulnerabilidades y las amenazas a cada activo previamente valorado. Las vulnerabilidades se refieren a cualquier situación que pueda causar complicaciones de seguridad; las amenazas representan comportamientos específicos que aprovechan las vulnerabilidades que generan incidencias de seguridad.

Figura 10 - Elementos de la actividad - Amenazas y vulnerabilidades

Entrada	Procedimiento	Salida
- Listado de activos de información de la EPS.	- Se analiza la información producida en la fase 1, para identificar las amenazas en la EPS. - Se identifican las amenazas que influyen en cada activo de la EPS teniendo en cuenta el cuadro 6 - Listado de amenazas y vulnerabilidades. - Se procede a llenar la tabla 10 catalogando los activos valorizados en la actividad anterior de acuerdo a las amenazas a las que pueden estar expuestos. Para asignar los valores relacionados a la motivación y capacidad se debe considerar el cuadro 7, y el valor final de la amenaza se obtendrá usando el cuadro 8 - Matriz de valorización de amenazas. - Para establecer cuáles son las vulnerabilidades asociadas a las amenazas de cada uno de los activos identificados se considerará el cuadro 6 - Listado de amenazas y vulnerabilidades. - En base a la valoración considerada en el cuadro 9 - Criterios de valoración de vulnerabilidades, se procede a llenar la tabla 11 - Plantilla para valorar las vulnerabilidades. - Para asignar los valores relacionados a la severidad y exposición, se deberá usar el cuadro 10 - Matriz de valoración de vulnerabilidades.	- Listado de amenazas valoradas. - Listado de vulnerabilidades valoradas.

Cuadro 6 - Criterios de valoración de amenazas

Valor	Capacidad	Motivación
1	Poca o nula capacidad de realizar el ataque.	Poca o nula motivación. No se está inclinando a actuar.
2	(1) Capacidad moderada. Se tiene el conocimiento y habilidades para realizar el ataque, pero pocos recursos. (2) Tiene suficientes recursos, pero conocimiento y habilidades limitadas.	Nivel moderado de motivación. Se actuará si se le pide o provoca.
3	Altamente capaz. Se tienen los conocimientos, habilidad y recursos necesarios para realizar un ataque. Cumple con menos del 80% del perfil del responsable del proceso y con al menos el 70% de los accesos al proceso.	Altamente motivado. Casi seguro que intentará el ataque.

Cuadro 7. Listado de amenazas y vulnerabilidades

ACTIVO	AMENAZAS	VULNERABILIDADES
Hardware	Incumplimiento en el mantenimiento del sistema de información.	Mantenimiento insuficiente /instalación fallida de los medios de almacenamiento.
	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.	Falta de esquemas de reemplazo periódico, susceptibilidad a la humedad, el polvo y la suciedad.
	Radiación electromagnética.	Sensibilidad a la radiación electromagnética.
	Error en el uso.	Falta de control de cambio con configuración eficiente.
	Pérdida del suministro de energía.	Susceptibilidad a las variaciones de tensión.
	Fenómenos meteorológicos.	Susceptibilidad a las variaciones de temperatura.
	Hurto de medios o documentos.	Almacenamiento sin protección.
		Copia no autorizada.
		Falta de cuidado en la disposición final.
Software	Falsificación de derechos.	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.
	Abuso de los derechos.	Falta o insuficiencia de la prueba del software.
		Falta de "terminación de la sesión" cuando se abandona el equipo de cómputo.
		Distribución errada de los derechos de acceso.
		Incompatibilidad.
	Corrupción de datos.	Ataque informático humano.
	Error en el uso.	Interface de usuario complicada.
		Falta de documentación.
		Fechas incorrectas.
	Manipulación con software.	Descarga y uso no controlado de SW.
		Falta de copias de respaldo.
Personal	Incumplimiento en la disponibilidad del personal.	Suplantación de identidad.
	Error en el uso.	Uso incorrecto de software y hardware
		Entrenamiento insuficiente en seguridad.
		Falta de conciencia acerca de la seguridad.
	Procesamiento ilegal de los datos.	Falta de mecanismos de monitoreo
	Hurto de medios o documentos.	Trabajo no supervisado del personal externo o de limpieza.
	Destrucción de equipo o medios.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.
Ambientes físicos	Inundación.	Ubicación en un área susceptible de inundación.
	Pérdida del suministro de energía.	Red energética inestable.
	Hurto de equipo.	Falta de protección física de las puertas y ventanas de la edificación.
Información	Incumplimiento en el mantenimiento de la información.	Información no registrada bajo control.
		Uso inadecuado de la información almacenada.
		Desgaste por manipulación.
	Negación de acciones.	Falta de asignación adecuada de responsabilidades en la SI.

Cuadro 8 - Matriz de valoración de amenazas

	Motivación		
Capacidad	**1**	**2**	**3**
1	1	2	3
2	2	3	4
3	3	4	5

Tabla 10 - Herramienta para valorar de amenazas

FASE 3 - PLANIFICACIÓN **Proceso 3.1 - Identificar el riesgo** C.1 Valorar las amenazas					
Objetivo: Identificar las amenazas bajo los criterios de capacidad y motivación.					
Nº	**Amenazas**	**Activos**	**Capacidad**	**Motivación**	**Valor amenaza**
1					
2					
3					
4					
5					
Conclusión:					
Elaborado por:				**Fecha:**	

Cuadro 9 - Criterios de valoración de vulnerabilidades

Valor	Severidad	Exposición
1	Severidad Baja: Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene poco potencial de pérdida o daño en el activo.	Exposición Baja: Los efectos de vulnerabilidad son mínimos. No incrementa la posibilidad de que vulnerabilidades adicionales sean explotadas.
2	Severidad Moderada: (1) Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo. (2) Se requiere pocos recursos para explotar la vulnerabilidad y tiene un potencial moderado de pérdida o daño en el activo.	Exposición Moderada: La vulnerabilidad puede afectar a más de un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la posibilidad de explotar vulnerabilidades adicionales.
3	Severidad Alta: Se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo.	Exposición Alta: La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la posibilidad de explotar vulnerabilidades adicionales.

Cuadro 10 - Matriz de valoración de vulnerabilidades

	Exposición		
Severidad	**1**	**2**	**3**
1	1	2	3
2	2	3	4
3	3	4	5

Tabla 11 - Herramienta para valorar las vulnerabilidades

FASE 3 - PLANIFICACIÓN **Proceso 3.1 - Identificar el riesgo** C.2 Valorar las vulnerabilidades						
Objetivo: Determinar las vulnerabilidades bajo los criterios de severidad y exposición.						
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**Severidad**	**Exposición**	**Valor vulnerabilidad**
1						
2						
3						
4						
5						
Conclusión:						
Elaborado por:					**Fecha:**	

Proceso 3.2: Analizar el riesgo

A. Valorar la probabilidad e impacto del riesgo

Aquí se determinará la probabilidad que se materialice un riesgo debido a causa de una determinada vulnerabilidad. Además, el análisis de impacto nos permite medir el impacto negativo de la materialización de cada riesgo identificado para cada activo crítico.

Figura 11 - Elementos de la actividad - Impacto del riesgo

Entrada	Procedimiento	Salida
- Listado de amenazas valoradas. - Listado de vulnerabilidades valoradas.	- Se procede a asignar un valor de probabilidad de acuerdo al cuadro 11, para cada vulnerabilidad asociada a cada uno de los activos de información de la EPS. - Luego se procede a llenar la información en la tabla 12 - Plantilla para analizar el riesgo, donde corresponde el valor de la probabilidad. - Enseguida se procede a asignar un valor de impacto de acuerdo al cuadro 12, para cada vulnerabilidad detectada para cada uno de los activos de información de la EPS. - Finalmente se procede a llenar la información en la tabla 12 - Plantilla para analizar el riesgo, donde corresponde el valor del impacto.	- Listado de riesgos valorados.

Cuadro 11 - A.1 Valoración de la probabilidad

Valor	Probabilidad	Descripción
1	Casi imposible	Es casi inconcebible que el suceso ocurra – 0% de ocurrencias históricamente en el norte peruano.
2	Raro	Poco posible que ocurra (no se sabe que haya ocurrido alguna vez) – 0% de ocurrencias históricamente en la EPS.
3	Posible	Posible que ocurra (ha ocurrido raramente) – Menos del 10% del total de incidencias en la EPS.
4	Muy posible	Posible que ocurra algunas veces (no ha ocurrido con frecuencia) – Menos del 50% del total de incidencias en la EPS.
5	Casi cierto	Posible que ocurra muchas veces (ha ocurrido con frecuencia) Más del 80% del total de incidencias en la EPS.

Cuadro 12 - A.2 Valoración del impacto

Valor	Impacto	Descripción
1	Insignificante	No requiere esfuerzo extra para restablecer la operación de procesos de la EPS.
2	Menor	Puede implicar un tiempo de recuperación menor al 10% del tiempo de la jornada laboral y en la pérdida de algunos bienes, material o recursos.
3	Moderado	Puede implicar un tiempo de recuperación menor al 50% del tiempo de la jornada laboral y en la pérdida de bienes, material o recursos.
4	Mayor	Puede implicar un tiempo de recuperación menor al 80% del tiempo de la jornada laboral y en la pérdida de costosa de bienes, material o recursos.
5	Catastrófico	Puede implicar un tiempo mayor al 80.1% del tiempo de la jornada laboral, la paralización total de los procesos de la EPS y la pérdida costosa de bienes, materiales o recursos.

B. Valorar el riesgo

Este proceso determina los niveles de riesgo en función de los valores obtenidos del análisis de vulnerabilidad y amenazas de activos críticos. Al aplicar la escala de magnitud de impacto, se puede determinar cuánto influye en el proceso (bajo, medio, alto, severo).

Figura 12 - Elementos de la actividad - Valoración del riesgo

Entrada	Procedimiento	Salida
- Listado de vulnerabilidades de los activos de información de la EPS.	- Se calcula el nivel de riesgo resultante del producto del valor de amenaza, vulnerabilidad, probabilidad e impacto, fijados en las actividades anteriores. Para determinar el nivel del riesgo se tiene: ✓Valor del Riesgo = Valor de Probabilidad (P) x Valor de Impacto (I) ✓Se utiliza la siguiente escala del 1 al 25. - Acorde al valor del riesgo, ubicar en el cuadro 13 la valoración de la magnitud del riesgo. - Luego se procede a llenar la los datos en la tabla 12 - Plantilla para analizar el riesgo.	- Valoración de la magnitud del riesgo.

Cuadro 13 - B. Valoración de la magnitud del riesgo

Valor del Riesgo	Magnitud del Riesgo
1 – 5	Baja
6 – 10	Moderada
11 – 15	Alta
16 - 25	Extrema

Tabla 12 - Herramienta para analizar el riesgo

FASE 3 - PLANIFICACIÓN Proceso 3.2 - Analizar el riesgo								
Objetivo: Determinar el nivel del riesgo a través del resultado de los valores del análisis de vulnerabilidad y amenazas, sobre los activos críticos.								
Nº	**Cód. riesgo**	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**P x I**	**Magnitud**
1								
2								
3								
4								
5								
Conclusión:								
Elaborado por:						**Fecha:**		

Proceso 3.3: Evaluar el riesgo

Aquí se determina el valor de probabilidad de que una vulnerabilidad específica represente un riesgo. Además, para cada riesgo identificado para cada activo crítico, se puede medir el impacto negativo como consecuencia de materializarse el riesgo.

Figura 13 - Elementos del proceso - Evaluación del riesgo

Entrada	Procedimiento	Salida
- Listado de amenazas valoradas. - Listado de vulnerabilidades valoradas. - Valoración de la magnitud del riesgo.	- Se priorizan los riesgos identificados y se ubican según su impacto y probabilidad en el mapa de calor (Cuadro 14 - Matriz de clasificación de riesgos), donde se obtiene el valor producto de la probabilidad y el impacto, para cada evento de amenaza. - Con el cálculo de los valores del punto anterior se debe ubicar el riesgo y comenzar a completar la información en la tabla 13 - Plantilla para evaluar el riesgo, con los valores obtenidos en las plantillas de valoración de amenazas de la tabla 10 y de valoración de vulnerabilidades de la tabla 11. - Conforme a la semaforización de la matriz de clasificación de riesgos, se identificará la tolerancia al riesgo según la clasificación del cuadro 15 - Identificación de tolerancia al riesgo, procediendo a asignar en la tabla 13 - Plantilla para evaluar el riesgo, la tolerancia para cada riesgo. - Por último, en la tabla 13 - Plantilla para evaluar el riesgo, se agregará el valor del riesgo relacionado con la tolerancia al riesgo, para determinar si es aceptable, tolerable o no tolerable.	- Listado de riesgos según su tolerancia.

Cuadro 14 - Matriz de clasificación de riesgos

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

Cuadro 15 - Identificación de la tolerancia al riesgo

Valor del riesgo	Tolerancia al riesgo	Descripción
1 – 5	Aceptable	El riesgo es aceptable tal y como existe.
6 – 10	Tolerable	El riesgo es tratado basado en la mitigación.
11 – 25	No tolerable	El riesgo es inaceptable por pérdidas mayores.

Tabla 13 - Herramienta para evaluar el riesgo

FASE 3 - PLANIFICACIÓN Proceso 3.3 - Evaluar el riesgo									
Objetivo: Evaluar el riesgo para determinar su tolerancia.									
N°	**Cód. de riesgo**	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PXI)**	**Tolerancia**		
							Aceptable	**Tolerable**	**No Tolerable**
1									
2									
3									
4									
5									
Conclusión:									
Elaborado por:						**Fecha:**			

Proceso 3.4: Tratar el riesgo

El propósito de este proceso es elegir controles pertinentes para el riesgo, dependiendo de la magnitud y la tolerancia del riesgo. Corresponde determinar si se acepta, mitiga, evita o transfiere el riesgo.

Figura 14 - Elementos del proceso - Tratamiento del riesgo

Entrada	Procedimiento	Salida
- Listado de amenazas valoradas. - Valoración de la magnitud del riesgo. - Clasificación de estrategias. - Listado de riesgos según su tolerancia. - Listado de controles del ANEXO A de la ISO/IEC 27001:2022.	- Se deberá llenar los campos correspondientes a cada riesgo, su amenaza, magnitud y la tolerancia al riesgo en la plantilla para tratar el riesgo de la tabla 14. - Seguidamente, para cada riesgo evaluado, teniendo en cuenta su magnitud, se debe seleccionar la estrategia para su tratamiento según la clasificación del cuadro 17. - De acuerdo a la estrategia seleccionada, se deberá elegir los controles pertinentes del ANEXO A de la NTP ISO/IEC 27001:2022 para cada amenaza identificada.	- Listado de controles a aplicar a cada riesgo según la estrategia seleccionada.

Cuadro 16 - Definición de estrategias para el tratamiento del riesgo

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

Cuadro 17 - Clasificación de estrategias para tratar el riesgo

Valor del Riesgo	Magnitud del Riesgo	Estrategia
1 - 5	Baja	Aceptar
6 - 10	Moderada	Aceptar Mitigar
11 - 15	Alta	Mitigar Evitar Transferir
16 - 25	Extrema	Mitigar Evitar Transferir

Tabla 14 - Herramienta para tratar el riesgo

FASE 3 - PLANIFICACIÓN Proceso 3.4 - Tratar el riesgo									
Objetivo: Determinar la estrategia para el tratamiento del riesgo y los controles a aplicar.									
N°	**Cód. de riesgo**	**Magnitud**	**Tolerancia**	**Amenaza**	**Estrategia**				**Controles**
					Aceptar	**Mitigar**	**Evitar**	**Transferir**	
1									
2									
3									
4									
5									
Conclusión: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.									
Elaborado por:				**Fecha:**					

FASE 4: SOPORTE

Proceso 4.1: Asignar recursos

El objetivo de este proceso es determinar las actividades y recursos necesarios para cumplir con la implementación de los controles seleccionados.

Figura 15 - Elementos del proceso - Asignación de recursos

Entrada	Procedimiento	Salida
- Listado de controles a aplicar a cada riesgo según la estrategia seleccionada. - CAP, MOF, Presupuesto.	- En primer lugar, se debe seleccionar los riesgos considerados como altos y extremos obtenidos de la tabla 14 - Plantilla del tratar el riesgo. - Se determinan las actividades a realizar para el cumplir cada uno de los controles elegidos. - En esta etapa se deberá asignar recursos pertinentes para implementar las actividades a realizar para el cumplimiento de cada uno de los controles elegidos. Para lo cual se debe considerar: ✓Inversión económica. ✓Instalaciones. ✓Equipos. ✓Personas. En este escenario podemos contar con personas para que asuman la responsabilidad de preservar la SI en la EPS. En este caso se refiere a recursos humanos ligados exclusivamente SGSI.	- Listado de actividades y recursos asignados a cada riesgo según la estrategia seleccionada.

Tabla 15 - Herramienta para asignar recursos

FASE 4 - SOPORTE Proceso 4.1 - Asignar recursos								
Objetivo: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.								
N°	**Código de riesgo**	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Control**	**Actividad**	**Recursos**
1								
2								
3								
4								
5								
6								
7								
Conclusión:								
Elaborado por:							**Fecha:**	

Proceso 4.2: Capacitar y Concienciar

Este proceso tiene como objetivo definir el plan de acciones a implementar para capacitar y concienciar al personal de la EPS, con el propósito de que entiendan y acepten las políticas y planes de seguridad, y comprendan las implicaciones de no cumplir con las normas de SI propuestas.

Figura 16 - Elementos del proceso - Capacitación y concienciación

Entrada	Procedimiento	Salida
- Estructura Organizacional, MOF, ROF. - Plantilla de determinación del alcance del SGSI. - Matriz de necesidades y expectativas de las partes interesadas. - Matriz de roles y responsabilidades de SI claves claramente definidos. - Documento políticas de SI. - Listado de controles a aplicar a cada riesgo según la estrategia seleccionada. - Listado de actividades y recursos asignados a cada riesgo según la estrategia seleccionada.	- Establecer un programa de capacitación y concienciación. (Oficial de SI, Jefe de TI) - Programar diversas actividades de concienciación. - Utilizar los medios de comunicación que estén al alcance, incluyendo charlas presenciales, videoconferencias, capacitaciones virtuales; adaptadas al ritmo y tiempo del personal de la EPS. - Mantener informado a todo el personal de las actualizaciones en temas de SI. - Impartir con periodicidad capacitaciones y comunicaciones de SI y asegurarse que se incluyan a todos los empleados. Además de incluir a los proveedores que sean necesarios para garantizar que todos los que realizan trabajos en la EPS, que impliquen la SI, estén incluidos.	- Plan de capacitación y concienciación del personal de la EPS.

Tabla 16 - Herramienta para capacitar y concienciar

FASE 4 - SOPORTE Proceso 4.2 - Capacitar y concienciar							
Objetivo: Definir el plan de capacitación y concienciación del personal de la EPS.							
Tipo	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Fecha**
Capacitación …	Evaluar … Charla de …	1° Evaluación completada …	Responsable: … Convocado: …	Documentos: … Presentación: … Ubicación: … Tecnología: ….	1. Diseñar pruebas para evaluar al personal designado para cumplir roles en el sistema. 2. Ejecutar la evaluación del personal.	Resultado esperado: …	Inicio: Fin:
Conclusión:							
Elaborado por:				**Fecha:**			

Proceso 4.3: Determinar la comunicación del SGSI

El propósito de este proceso es determinar actividades que regirán las comunicaciones relevantes para complementar las actividades de operación del SGSI, identificando quién comunicará, qué se logrará, cuál será el contenido, cuándo se comunicará y qué medios se utilizarán.

Figura 17 - Elementos del proceso - Comunicación

Entrada	Procedimiento	Salida
- Listado de controles a aplicar a cada riesgo según la estrategia seleccionada. - Listado de actividades y recursos asignados a cada riesgo según la estrategia seleccionada.	- En primer lugar, se debe establecer lo que se va a comunicar (Qué), especificando cuál es el tema y contenido de la comunicación. - Establecer el responsable (Quién) trasmitirá el mensaje, especificando quién tomará el rol de emisor. - Establecer a quién se trasmitirá el mensaje, especificando quién tomará el rol de receptor. - Seleccionar que medios de comunicación se utilizarán para cada control (verbal, escrito, e-mail, web, video, etc.). - Finalmente, definir el causal o en qué momento (Cuándo) ha de realizarse la comunicación.	- Plan de comunicaciones del SGSI.

Tabla 17 - Herramienta para comunicar el SGSI

FASE 4 - SOPORTE Proceso 4.3 - Determinar la comunicación del SGSI							
Objetivo: Determinar las acciones que guiarán las comunicaciones relevantes que para complementar la operación del SGSI.							
Control	**Actividad**	**Riesgo asociado**	**A quien comunicar**	**Responsable de comunicar**	**Tema a Tratar**	**Medio de comunicación**	**Fecha**
Conclusión:							
Elaborado por:					**Fecha:**		

FASE 5: OPERACIÓN

Proceso 5.1: Planificar y controlar la operación del SGSI

Se realiza el alineamiento de los controles elegidos con los objetivos de SI determinados por la EPS, con la finalidad de que se cumplan. Para desarrollar esta tarea se deberá aplicar los controles señalados al momento de tratar los riesgos.

Figura 18 - Elementos del proceso – Planificación y control de la operación

Entrada	Procedimiento	Salida
- Objetivos de SI establecidos. - Listado de controles a aplicar a cada riesgo según la estrategia seleccionada.	- Usar los controles mencionados en la plantilla para el tratamiento del riesgo - tabla 14. Los cuales se seleccionaron del Anexo A de la NTP ISO/IEC 27001:2022. - Se debe tener en cuenta los objetivos de seguridad establecidos en el proceso 2.2 - Establecer políticas y objetivos de SI (Tabla 6). - Realizar una lista de actividades para implementar dichos controles y dar cumplimiento a los objetivos de SI establecidos. - Definir quién es el responsable de dar cumplimiento al control de seguridad.	- Listado de responsables del cumplimiento de cada control implementado en la EPS.

Tabla 18 - Herramienta para el control operacional

FASE 5 - OPERACIÓN Proceso 5.1 - Planificar y controlar la operación del SGSI			
Objetivo: Alinear los controles elegidos con los objetivos de seguridad establecidos por la EPS.			
Control de seguridad	**Objetivo de seguridad**	**Actividad de control**	**Responsable del control**
Conclusión: En esta sección se especifica el comentario final de lo percibido después de llenada la plantilla.			
Elaborado por:		**Fecha:**	

FASE 06: EVALUACIÓN DEL DESEMPEÑO

Proceso 6.1: Monitorear, analizar y evaluar el SGSI

Este proceso sirve para evaluar el rendimiento, efectividad y cumplimiento de los objetivos de SI, determinando lo que se debe medir y controlar, cuándo, quién y cómo. Para llevar a cabo esta tarea se recomienda realizar entrevistas a los miembros de la alta dirección, así como del área de TI.

Figura 19 - Elementos del proceso - Monitoreo, análisis y evaluación

Entrada	Procedimiento	Salida
- Objetivos de SI establecidos. - Listado de controles a aplicar a cada riesgo según la estrategia seleccionada (Anexo A de la ISO/IEC 27001:2022). - Listado de actividades y recursos asignados a cada riesgo según la estrategia seleccionada.	- Escoger los controles de SI a monitorear, considerar solo los que se necesite realmente. - Indicar que método de monitoreo se va a aplicar a cada control. - Establecer el valor del control, de acuerdo al cuadro 18 - Valoración del nivel de cumplimiento. - Definir el responsable de realizar el monitoreo. - Ingresar el periodo de monitoreo. - Calificar el cumplimiento del control monitoreado.	- Plan de monitoreo.

Cuadro 18 - Valoración del nivel de cumplimiento

Valor	Estado	Descripción
1	Cumple satisfactoriamente	Se cumple como solicita el modelo propuesto, es conocido y aplicado por todos los involucrados del SGSI, cumple al 100%.
2	Cumple parcialmente	Se hace de manera parcial, se definió, pero no se gestiona.
3	No cumple	No existe o no se está haciendo.
4	No aplica	El control no se aplica a la EPS.

Tabla 19 - Herramienta para monitorear, analizar y evaluar el SGSI

FASE 6 - EVALUACIÓN DEL DESEMPEÑO Proceso 6.1 - Monitorear, analizar y evaluar el SGSI						
Objetivo: Establecer un plan de monitoreo, análisis y evaluación del SGSI.						
N°	**Controles**	**Método**	**Valor del control**	**Estado**	**Responsable**	**Periodo**
1						
2						
3						
4						
5						
Conclusión:						
Elaborado por:					**Fecha:**	

FASE 07: MEJORA CONTINUA

Proceso 7.1: Mejorar el SGSI

Se trata de identificar mejoras de acuerdo a los objetivos de SI determinados en el SGSI, con el propósito de encauzar los esfuerzos en el mejoramiento de sus procesos. Una vez sean mejoradas las actividades que correspondan, éstas serán incluidas en el plan de comunicaciones de la EPS a fin de que sea conocida por todas las áreas de interés.

Figura 20 - Elementos del proceso - Mejoramiento continuo

Entrada	Procedimiento	Salida
- Objetivos de SI establecidos. - Listado de controles a aplicar a cada riesgo según la estrategia seleccionada. - Listado de actividades y recursos asignados a cada riesgo según la estrategia seleccionada. - Plan de monitoreo.	- Listar los controles propuestos que contrarrestan los riesgos. - Ingresar las fechas de inicio y de fin del plan de mejora continua. - Plan de acción. Seleccionar herramienta y/o servicio para apoyar a la EPS en mantener y mejorar continuamente el SGSI, por ejemplo: ✓Asesoría para la revisión por el Directorio. ✓Realización de Auditorías internas. ✓Evaluaciones técnicas de cumplimiento. ✓Comentarios de incidentes de SI. ✓Monitoreo de KPIs y SLAs de SI. ✓Evaluaciones de cumplimiento de proveedores de servicios.	- Plan de mejoramiento continuo.

Tabla 20 - Herramienta para la mejora continua

FASE 7 - MEJORA CONTINUA **Proceso 7.1 - Mejorar el SGSI**					
Objetivo: Elaborar un plan de mejora continua					
N°	**Riesgos involucrados**	**Controles**	**Plan de acción (Herramienta/Servicio)**	**Fecha de inicio**	**Fecha de fin**
1					
2					
3					
4					
5					
Conclusión:					
Elaborado por:				**Fecha:**	

ANEXO 5

Validación del contenido del modelo de SI propuesto por juicio de expertos

EXPERTO 1

FICHA DE VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ. Para tal fin, se anexa el cuestionario de validación.

NOMBRES Y APELLIDOS:	Jose García Correa
FORMACIÓN ACADÉMICA:	Ing. Sistemas.
ÁREA DE EXPERIENCIA PROFESIONAL:	Seguridad de la Información
TIEMPO DE EXPRIENCIA:	6 años en S.I. y 38 años en T.I.
CARGO ACTUAL:	Oficial de Seguridad de la Información
INSTITUCIÓN:	Municipalidad Provincial de Chiclayo

Objetivo de la investigación: Contribuir en la seguridad de la información de las entidades prestadoras de servicios de saneamiento del norte del Perú.

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

Objetivo de la prueba: Determinar la utilidad del modelo propuesto en la gestión de las entidades prestadoras de servicios de saneamiento.

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

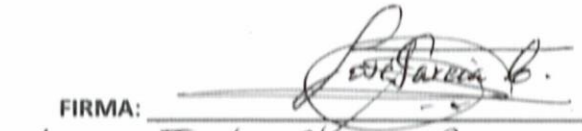
		CALIFICACIÓN			
		1. No cumple con el criterio	2. Bajo Nivel	3. Moderado nivel	4. Alto nivel
CATEGORÍA	**SUFICIENCIA** Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	Los ítems no son suficientes para medir la dimensión.	Los ítems miden algún aspecto de la dimensión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

VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE 01 - Contexto de la EPS						
Proceso 1.1: Comprender la EPS y su contexto						
A. Definir el contexto interno	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y interno	4	4	4	4	
B. Definir el contexto externo	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y externo.	4	4	4	4	
Proceso 1.2: Identificar las necesidades y expectativas de las partes interesadas	Identificar las necesidades y expectativas de las partes interesadas relacionadas con la EPS.	3	4	4	4	
Proceso 1.3: Determinar el alcance del SGSI	Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.	4	4	4	4	
FASE 02 - Liderazgo						
Proceso 2.1: Asegurar el liderazgo y compromiso	Identificar el cumplimiento de las funciones de liderazgo por parte del Directorio.	3	4	4	4	
Proceso 2.2: Establecer políticas y objetivos de seguridad de la información	Identificar y establecer las políticas y objetivos de seguridad de acuerdo a las necesidades de la EPS.	4	4	4	4	
Proceso 2.3: Asignar roles y responsabilidades	Identificar y asignar los roles y responsabilidades del personal que intervendrá en la seguridad de la información de la EPS.	3	4	4	4	
FASE 03 - Planificación						
Proceso 3.1: Identificar el riesgo						
A. Identificar los activos	Definir qué activos son críticos para la EPS, que de haberse afectados se produzca un impacto negativo en la EPS.	4	4	4	4	
B. Valorar los activos	Identificar el nivel de criticidad de cada activo.	4	4	4	4	
C. Identificar y valorar las amenazas y vulnerabilidades	Identificar las amenazas bajo los criterios de capacidad y motivación. Determinar las vulnerabilidades bajos los criterios de severidad y exposición.	4	4	4	4	

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Proceso 3.2: Analizar el riesgo	Determinar la magnitud del riesgo a través de los valores sensibilidad de activos, análisis de amenaza y vulnerabilidad, probabilidad e impacto.					
A. Valorar la probabilidad e impacto del riesgo	Determinar el valor de la probabilidad de que un riesgo se materialice a causa de una determinada vulnerabilidad.	4	4	4	4	
B. Valorar el riesgo	Determinar el nivel del riesgo a través de los valores del análisis de vulnerabilidad y análisis de amenaza, sobre los activos sensibles.	4	4	4	4	
Proceso 3.3: Evaluar el riesgo	Evaluar el riesgo para determinar su tolerancia al riesgo.	4	4	4	4	
Proceso 3.4: Tratar el riesgo	Determinar la estrategia para el tratamiento del riesgo y los controles a aplicar.	4	4	4	4	
FASE 04 - Soporte						
Proceso 4.1: Asignar recursos	Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.	4	4	4	4	
Proceso 4.2: Capacitar y concienciar	Definir el plan de capacitación y concienciación del personal de la EPS.	3	4	4	4	
Proceso 4.3: Determinar la comunicación del SGSI	Determinar las acciones que guiarán las comunicaciones relevantes que se dan para complementar la operación del SGSI.	4	4	4	3	
FASE 05 - Operación						
Proceso 5.1: Planificar y controlar la operación del SGSI	Alinear los controles seleccionados con los objetivos de seguridad establecidos por la EPS.	3	4	4	4	
FASE 06 - Evaluación del Desempeño						
Proceso 6.1: Monitorear, analizar y evaluar el SGSI	Establecer un plan de monitoreo, análisis y evaluación del SGSI.	4	4	4	4	
FASE 07 - Mejora Contínua						
Proceso 7.1: Mejorar el SGSI	Establecer un plan de mejora continua.	4	4	4	4	

FECHA: Chiclayo 05 de agosto de 2019

FIRMA: 

Mg. Ing. José García Correa

EXPERTO 2

FICHA DE VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ. Para tal fin, se anexa el cuestionario de validación.

NOMBRES Y APELLIDOS:	ROBERT EDGAR PUICAN GUTIERREZ
FORMACIÓN ACADÉMICA:	INGENIERIA DE SISTEMAS, ADMINISTRACION DE EMPRESAS
ÁREA DE EXPERIENCIA PROFESIONAL:	TECNOLOGÍAS DE LA INFORMACÓN / ETHICAL HACKING DOCENCIA UNIVERSITARIA
TIEMPO DE EXPRIENCIA:	19 AÑOS
CARGO ACTUAL:	JEFE DE LA OFICINA GENERAL DE SISTEMAS INFORMÁTICOS
INSTITUCIÓN:	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Objetivo de la investigación: Contribuir en la seguridad de la información de las entidades prestadoras de servicios de saneamiento del norte del Perú.

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

Objetivo de la prueba: Determinar la utilidad del modelo propuesto en la gestión de las entidades prestadoras de servicios de saneamiento.

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

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

VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE 01 - Contexto de la EPS						
Proceso 1.1: Comprender la EPS y su contexto						
A. Definir el contexto interno	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y interno	4	4	4	4	
B. Definir el contexto externo	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y externo.	4	4	4	4	
Proceso 1.2: Identificar las necesidades y expectativas de las partes interesadas	Identificar las necesidades y expectativas de las partes interesadas relacionadas con la EPS.	4	4	4	4	
Proceso 1.3: Determinar el alcance del SGSI	Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.	4	4	4	4	
FASE 02 - Liderazgo						
Proceso 2.1: Asegurar el liderazgo y compromiso	Identificar el cumplimiento de las funciones de liderazgo por parte del Directorio.	4	4	4	3	
Proceso 2.2: Establecer políticas y objetivos de seguridad de la información	Identificar y establecer las políticas y objetivos de seguridad de acuerdo a las necesidades de la EPS.	3	3	4	3	PERMITIR CARACTERIZAR LAS POLÍTICAS DE SEGURIDAD SEGÚN LA EPS
Proceso 2.3: Asignar roles y responsabilidades	Identificar y asignar los roles y responsabilidades del personal que intervendrá en la seguridad de la información de la EPS.	3	3	4	3	
FASE 03 - Planificación						
Proceso 3.1: Identificar el riesgo						
A. Identificar los activos	Definir qué activos son críticos para la EPS, que de haberse afectados se produzca un impacto negativo en la EPS.	4	4	4	4	
B. Valorar los activos	Identificar el nivel de criticidad de cada activo.	4	4	4	4	
C. Identificar y valorar las amenazas y vulnerabilidades	Identificar las amenazas bajo los criterios de capacidad y motivación. Determinar las vulnerabilidades bajos los criterios de severidad y exposición.	4	4	4	4	

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Proceso 3.2: Analizar el riesgo	Determinar la magnitud del riesgo a través de los valores sensibilidad de activos, análisis de amenaza y vulnerabilidad, probabilidad e impacto.	4	4	4	4	
A. Valorar la probabilidad e impacto del riesgo	Determinar el valor de la probabilidad de que un riesgo se materialice a causa de una determinada vulnerabilidad.	4	4	4	4	
B. Valorar el riesgo	Determinar el nivel del riesgo a través de los valores del análisis de vulnerabilidad y análisis de amenaza, sobre los activos sensibles.	4	4	4	4	
Proceso 3.3: Evaluar el riesgo	Evaluar el riesgo para determinar su tolerancia al riesgo.	4	4	4	4	
Proceso 3.4: Tratar el riesgo	Determinar la estrategia para el tratamiento del riesgo y los controles a aplicar.	4	4	4	4	
FASE 04 - Soporte						
Proceso 4.1: Asignar recursos	Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.	3	3	3	3	CONSIDERAR UNA BITÁCORA DE RECURSOS
Proceso 4.2: Capacitar y concienciar	Definir el plan de capacitación y concienciación del personal de la EPS.	3	3	3	3	DEFINIR LOS TEMAS INDISPENSABLES PARA CAPACITAR
Proceso 4.3: Determinar la comunicación del SGSI	Determinar las acciones que guiarán las comunicaciones relevantes que se dan para complementar la operación del SGSI.	3	4	4	3	CONSIDERAR UNA LISTA DE PUNTOS A COMUNICAR
FASE 05 - Operación						
Proceso 5.1: Planificar y controlar la operación del SGSI	Alinear los controles seleccionados con los objetivos de seguridad establecidos por la EPS.	3	3	4	4	
FASE 06 - Evaluación del Desempeño						
Proceso 6.1: Monitorear, analizar y evaluar el SGSI	Establecer un plan de monitoreo, análisis y evaluación del SGSI.	4	4	4	4	
FASE 07 - Mejora Contínua						
Proceso 7.1: Mejorar el SGSI	Establecer un plan de mejora continua.	4	4	4	4	

FECHA: 09/08/19

FIRMA: _____

EXPERTO 3

FICHA DE VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ. Para tal fin, se anexa el cuestionario de validación.

NOMBRES Y APELLIDOS:	Alberto Fonseca Sanchez Ayala
FORMACIÓN ACADÉMICA:	Ingeniero de Computación y Sistemas
ÁREA DE EXPERIENCIA PROFESIONAL:	Tecnologías de la Información
TIEMPO DE EXPRIENCIA:	22 años
CARGO ACTUAL:	Gerente Tecnologías de la Información
INSTITUCIÓN:	Municipalidad de Chiclayo.

Objetivo de la investigación: Contribuir en la seguridad de la información de las entidades prestadoras de servicios de saneamiento del norte del Perú.

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

Objetivo de la prueba: Determinar la utilidad del modelo propuesto en la gestión de las entidades prestadoras de servicios de saneamiento.

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

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

VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MARCOS DE TRABAJO ESTANDARIZADOS PARA CONTRIBUIR EN LA GESTIÓN DE LAS ENTIDADES PRESTADORAS DE SERVICIOS DE SANEAMIENTO DEL NORTE DEL PERÚ

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
FASE 01 - Contexto de la EPS						
Proceso 1.1: Comprender la EPS y su contexto						
A. Definir el contexto interno	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y interno	3	4	3	3	
B. Definir el contexto externo	Identificar los parámetros de fuente y detalle en cada criterio del contexto interno y externo.	3	4	3	3	
Proceso 1.2: Identificar las necesidades y expectativas de las partes interesadas	Identificar las necesidades y expectativas de las partes interesadas relacionadas con la EPS.	3	4	3	3	
Proceso 1.3: Determinar el alcance del SGSI	Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.	3	4	3	3	
FASE 02 - Liderazgo						
Proceso 2.1: Asegurar el liderazgo y compromiso	Identificar el cumplimiento de las funciones de liderazgo por parte del Directorio.	4	3	3	3	
Proceso 2.2: Establecer políticas y objetivos de seguridad de la información	Identificar y establecer las políticas y objetivos de seguridad de acuerdo a las necesidades de la EPS.	4	3	3	3	
Proceso 2.3: Asignar roles y responsabilidades	Identificar y asignar los roles y responsabilidades del personal que intervendrá en la seguridad de la información de la EPS.	4	3	3	3	
FASE 03 - Planificación						
Proceso 3.1: Identificar el riesgo						
A. Identificar los activos	Definir qué activos son críticos para la EPS, que de haberse afectados se produzca un impacto negativo en la EPS.	4	4	3	3	
B. Valorar los activos	Identificar el nivel de criticidad de cada activo.	4	4	3	3	
C. Identificar y valorar las amenazas y vulnerabilidades	Identificar las amenazas bajo los criterios de capacidad y motivación. Determinar las vulnerabilidades bajos los criterios de severidad y exposición.	4	4	3	3	

MODELO PROPUESTO	OBJETIVO	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Proceso 3.2: Analizar el riesgo	Determinar la magnitud del riesgo a través de los valores sensibilidad de activos, análisis de amenaza y vulnerabilidad, probabilidad e impacto.	3	4	3	3	
A. Valorar la probabilidad e impacto del riesgo	Determinar el valor de la probabilidad de que un riesgo se materialice a causa de una determinada vulnerabilidad.	3	3	3	4	
B. Valorar el riesgo	Determinar el nivel del riesgo a través de los valores del análisis de vulnerabilidad y análisis de amenaza, sobre los activos sensibles.	3	4	3	4	
Proceso 3.3: Evaluar el riesgo	Evaluar el riesgo para determinar su tolerancia al riesgo.	3	4	3	3	
Proceso 3.4: Tratar el riesgo	Determinar la estrategia para el tratamiento del riesgo y los controles a aplicar.	3	4	3	3	
FASE 04 - Soporte						
Proceso 4.1: Asignar recursos	Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados.	3	3	3	4	
Proceso 4.2: Capacitar y concienciar	Definir el plan de capacitación y concienciación del personal de la EPS.	3	3	4	4	
Proceso 4.3: Determinar la comunicación del SGSI	Determinar las acciones que guiarán las comunicaciones relevantes que se dan para complementar la operación del SGSI.	3	3	3	4	
FASE 05 - Operación						
Proceso 5.1: Planificar y controlar la operación del SGSI	Alinear los controles seleccionados con los objetivos de seguridad establecidos por la EPS.	3	3	3	4	
FASE 06 - Evaluación del Desempeño						
Proceso 6.1: Monitorear, analizar y evaluar el SGSI	Establecer un plan de monitoreo, análisis y evaluación del SGSI.	3	3	4	3	
FASE 07 - Mejora Contínua						
Proceso 7.1: Mejorar el SGSI	Establecer un plan de mejora continua.	3	3	3	4	

FECHA: 11 Agosto 2019

FIRMA: A. Enrique Samillan Ayala
INGENIERO DE SISTEMAS
C.I.P. 59650

DR. EN CIENCIAS AMBIENTALES

ANEXO 6

Aplicación del modelo propuesto como caso de estudio

El Modelo de SI propuesto se aplicó como caso de estudio en EPSEL S.A.

FASE 1 - CONTEXTO DE LA EPS Proceso 1.1 - Comprender la EPS y su contexto A. Definir el contexto interno			
Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto interno.			
N°	**Factor**	**Fuente**	**Detalle**
01	Normativo	Reglamento de prestación de servicios de agua potable y alcantarillado de la EPS EPSEL S.A.	- Ley Orgánica de Municipalidades, Ley N° 27972. - Ley de la Actividad Empresarial del Estado, Ley N° 24948. - Ley General de sociedades, Ley N°26887. - Ley General del Sistema Nacional de Presupuesto, Ley 28411. - Plan Nacional de Saneamiento 2006 – 2015, D.S. N° 007 – 2006 – vivienda. - Ley de Creación de la Superintendencia Nacional de Servicios de Saneamiento, Decreto Ley Nº 25965. - Ley General del Ambiente, Ley N° 28611. - Ley General de Servicios de Saneamiento, Ley Nº 26338 y su Reglamento. - Estatutos de la empresa, reglamento aprobado por D.S N° 09-95-PRES vigente, se cambia la denominación de EMAPAL por el de EPSEL S.A integrando a las municipalidades distritales.
02	Metas y Objetivos	Plan estratégico	- Misión: Contribuir a mejorar la calidad de vida de la población de Lambayeque, brindando servicios de saneamiento eficientes y de calidad que ayuden a preservar el medio ambiente obteniendo niveles de rentabilidad que permitan su desarrollo empresarial y de su personal. - Visión: Ser una organización eficiente, rentable, sólida, entre las más importantes del sector, con recursos humanos altamente capacitados que trabajen en equipo, actuando con permanente esfuerzo para lograr un crecimiento sostenible y brindar servicios de calidad orientados a la satisfacción del cliente. - Objetivos estratégicos: ✓Suministrar y mejorar y ampliar la cobertura de los servicios de agua potable y alcantarillado. ✓Gestionar la calidad de los servicios de agua potable y alcantarillado. ✓Lograr óptimos resultados económicos y financieros. ✓Lograr una óptima gestión empresarial. ✓Fortalecer las competencias del talento humano.
03	Valores		- Trabajo en Equipo: Unamos capacidades para alcanzar nuestros objetivos. - Honestidad: Seamos honestos con nosotros mismos y con los demás. - Protección del medio ambiente: Respeto a las leyes sobre salud pública y protección del medio Ambiente. - Servicio de Calidad a los Clientes: Porque sabemos que desean nuestros clientes, trabajamos para ellos. - Responsabilidad: Asumamos los retos diarios y preparémonos para el futuro. - Respeto por la persona y dignidad humana: Es nuestro compromiso social y responsabilidad de la Empresa.

04	Estructura orgánica de la EPS, Funciones y responsabilidades	Organigrama, MOF, CAP	- Órganos de Dirección y Control: Conformado por la Junta de Accionistas, el Directorio, la Gerencia General y el Órgano de Control Institucional. - Órganos Operativos: Conformado por la Gerencia Operacional, Gerencia Comercial y Gerencia de Proyectos y Obras. - Órganos de Apoyo: Conformado por la Gerencia de Administración y Finanzas, Oficina de Recursos Humanos, Oficina de Comunicación Social y la Oficina de Informática. - Órganos de Asesoramiento y Asistencia Técnica: Conformado por la Oficina de Asesoría Legal, Oficina de Desarrollo Empresarial y Oficina de Coordinación de Plan Maestro Optimizado.
05	Recursos	Procesos, servicios, SW, HW	- Proceso de medición, proceso de facturación, proceso de cobranza, proceso de atención al cliente, proceso de catastro y conexiones. - Servidor Web, servidor ADDS, servidor DNS, firewall, servidor BD, modem, router, switch - Ofimática, sistema de gestión comercial, sistema de gestión administrativa, Sistema de RRHH, SICAP, Antivirus. - Equipo de cómputo, impresoras, ticketeras.
Conclusiones: Se han detallado los aspectos internos que influyen en la SI en EPSEL SA			
Elaborado por: Alejandro Navarro			**Fecha elaboración:** 21/05/2019

FASE 1 - CONTEXTO DE LA EPS **Proceso 1.1 - Comprender la EPS y su contexto** B. Definir el contexto externo			
Objetivo: Identificar los parámetros de fuente y detalle en cada criterio del contexto externo.			
N°	**Factor**	**Fuente**	**Detalle**
01	Ambiente del sector	Convenios	Convenio de operaciones reciprocas con las entidades del estado.
02	Normativo y político	Portal de Transparencia de EPSEL SA, Portales Institucionales: SUNASS, MVCS, OTASS, Otros	- Ley Orgánica de Municipalidades, Ley N° 27972. - Ley de la Actividad Empresarial del Estado, Ley N° 24948. - Ley General de sociedades, Ley N°26887. - Ley General del Sistema Nacional de Presupuesto, Ley 28411. - Plan Nacional de Saneamiento 2006 – 2015, D.S. N° 007 – 2006 – vivienda. - Ley de Creación de la Superintendencia Nacional de Servicios de Saneamiento, Decreto Ley Nº 25965. - Ley General del Ambiente, Ley N° 28611. - Ley General de Servicios de Saneamiento Ley Nº 26338 y su Reglamento. - Estatutos de la empresa, reglamento aprobado por D.S N° 09-95-PRES vigente, se cambia la denominación de EMAPAL por el de EPSEL S.A integrando a las municipalidades distritales. - Resolución Directiva N º 064 - SUNASS. - Resolución Directiva Nº 011 - SUNASS.
03	Financiero	Entidades financieras	- MEF, Gobiernos locales, Gobierno francés, Banco Continental, BCP, Interbank, Banco de la Nación.
04	Reglamentario	CPP, Códigos, Diario El Peruano	- Normas, leyes, decretos, ordenanzas, otros.
Conclusiones: Los cambios en las normativas legales, aspectos políticos de gobiernos locales, regionales, nacionales son los aspectos más relevantes que influyen o limitan el ámbito y desarrollo de las actividades de la EPS EPSEL SA.			
Elaborado por: Alejandro Navarro			**Fecha elaboración:** 21/05/2019

FASE 1 - CONTEXTO DE LA EPS Proceso 1.2 - Identificar las necesidades y expectativas de las partes interesadas										
Objetivo: Identificar las necesidades y expectativas de las partes interesadas relacionadas con la EPS										
	Tipo de información									
Parte Interesada	Estrategia de SI	Presupuesto de SI	Plan de SI	Políticas de SI	Requerimientos de SI	Plan de Comunicación	Informes de Revisión de SI	Catálogo de Servicios de SI	Perfil de Riesgo de Información	Cuadro de Mando de SI
Interna: EPS										
Directorio	A	A	A	A			A	A	A	A
Gerente General	A					A				O
Gerente de Administración y Finanzas		A								O
Comité de la SI	O		O	O	O		O	O	O	O
Oficial de SI	O		O	O	O		O	O	O	O
Jefe de Oficina de Recursos Humanos				U		U	O			
Personal administrativo				U		U				
Interna: TI										
Jefe de Oficina de Informática	A		O	O		O		O		
Personal de TI					I		O	O		
Externa										
MVCS							I			
SUNASS							I			
OTASS							I			
Gobiernos Locales							I			
Entidades Financieras							I			
Proveedores							I			
Conclusiones: En esta sección se han utilizado indicadores de relación entre las partes interesadas de la EPS y el tipo de información. Aprobador(A), Origen/emisor (O), Informado (I), Destino/usuario (U).										
Elaborado por: Alejandro Navarro							**Fecha elaboración:** 21/05/2019			

FASE 1 - CONTEXTO DE LA EPS Proceso 1.3 - Determinar el alcance del SGSI	
Objetivo: Identificar los procesos o funciones, responsables e infraestructura de TI relacionados con la implementación de un SGSI.	
	Detalle
Procesos/Funciones	Planificar, monitorear, dirigir e implementar el SGSI en la EPS EPSEL SA y asegurar el presupuesto para este fin. Todos los procesos administrativos, operativos y comerciales de EPSEL SA.
Responsables	Directorio, Gerente General, Responsable de TI, Jefe de Oficina de Recursos Humanos, Personal de la oficina de informática.
Infraestructura de TI	04 Equipos de cómputo, 01 switch, 01 impresora multifuncional, 02 laptops, 04 estabilizadores UPS y 01 UPS. Servicio de Internet. Material de oficina.
Conclusiones: El modelo propuesto cubre todos los procesos de la EPS EPSEL SA, además las funciones de los responsables de la implementación del SGSI.	
Elaborado por: Alejandro Navarro	**Fecha elaboración:** 21/05/2019

FASE 2 - LIDERAZGO Proceso 2.1 - Asegurar el liderazgo y compromiso				
Objetivo: Identificar el cumplimiento de las funciones de liderazgo por parte del Directorio.				
N°	**Funciones**	**Si**	**Parcial**	**No**
01	Asegurar que la política y los objetivos de seguridad sean establecidos y compatibles con los objetivos estratégicos de la EPS.			x
02	Asegurar la integración de los requisitos del SGSI en los procesos de la EPS.	x		
03	Asegurar que los recursos necesarios para el SGSI estén disponibles.	x		
04	Comunicar la importancia de una efectiva gestión de SI en conformidad con los requisitos del SGSI.	x		
05	Asegurar que el SGSI logre los resultados previstos.			x
06	Dirigir y apoyar a los usuarios para que contribuyan con la efectividad del SGSI.	x		
07	Promover la mejora continua del SGSI.		x	
08	Apoyar otros roles pertinentes de gestión para demostrar su liderazgo aplicado a sus áreas de responsabilidad.	x		
Conclusiones: El Directorio de la EPS EPSEL SA no cumple con todas las funciones solicitadas por la ISO/IEC 27001:2022. Para cumplir completamente con la fase de liderazgo, se debe cumplir con los requisitos referidos en las fases 01, 05, 06 y 07.				
Elaborado por: Alejandro Navarro		**Fecha elaboración:** 21/05/2019		

FASE 2 - LIDERAZGO Proceso 2.2 - Establecer políticas y objetivos de SI				
Objetivo: Identificar y establecer las políticas y objetivos de seguridad de acuerdo a las necesidades de la EPS EPSEL SA				
Nº	**Política de seguridad**	**Definición**	**Alcance**	**Objetivo de seguridad**
01	Política de Control de Acceso	Las políticas son las que otorgan a los usuarios acceso al sitio. A menos que estén autorizados a ejercer sus responsabilidades mediante una o varias políticas de control de acceso, los usuarios no tienen acceso a funciones del sitio.	Unidades de negocio, proveedores y terceros. Las actualizaciones y revalidaciones deben involucrar a RRHH, a los propietarios de datos y sistemas y a SI. Toda política nueva o actualizada debería distribuirse a las correspondientes unidades de negocio, a los proveedores y a terceros.	• Proporcionar un acceso adecuado a las partes interesadas, internas y externas, a fin de que se alcancen los objetivos del negocio. • Garantizar que el acceso de emergencia esté debidamente permitido y revocado en el momento oportuno.
02	Política de SI Relativa al Personal	Los estándares relacionados al personal deben ser aplicados para todos los servidores de la EPS en cualquiera de sus modalidades, y terceros que tengan acceso a la información. Para lo cual estará definido en un acuerdo de confidencialidad.	Unidades de negocio, proveedores y terceros. Las actualizaciones y revalidaciones deben involucrar a RRHH, al director de privacidad, a asesoría jurídica, a SI y al área de protección de instalaciones. Toda política nueva o actualizada deberá ser distribuida a los empleados, a los contratistas, a los proveedores según se especifique en contrato y a los empleados temporales.	• Realizar regularmente una verificación de antecedentes de todos los empleados y las personas en puestos clave. • Obtener información sobre el personal clave en puestos de SI. • Desarrollar un plan de sucesión para todos los puestos clave relacionados con la SI. • Verificar si todo el personal de SI tiene las habilidades pertinentes y las certificaciones afines, vigentes.
03	Política de Seguridad Física y Ambiental	Esta política contempla las normas y procedimientos necesarios a utilizar para asegurar el acceso físico a los edificios, computadoras, información y medios de comunicación.	Empleados, todas las unidades de negocio, proveedores que porten activos/equipos de la organización y todos los visitantes. Las actualizaciones y revalidación deberían involucrar al área de instalaciones, al de asesoría jurídica, a SI y a los titulares de datos y sistemas. Toda política nueva o actualizada debería distribuirse a los empleados, a los contratistas, a los proveedores según se especifique en contrato y a los empleados temporales.	Proporcionar orientación relativa a: • Protección de ubicaciones físicas • Controles ambientales que proporcionen capacidad a las operaciones de soporte. Indirectamente, la política contribuye a la optimización de los costes de los seguros.
04	Política de Respuesta a Incidentes de Seguridad	Esta política busca regular la forma en que la EPS administra la respuesta ante incidentes de SI y definir los procedimientos que se requieren al efecto.	Unidades de negocio y empleados clave. Las actualizaciones y revalidación deberían involucrar a la función de SI. Toda política nueva o actualizada debería distribuirse a los empleados clave.	Responder a los incidentes de una manera oportuna para recuperar las actividades de la EPS.
Conclusiones: Se consideran cuatro políticas de seguridad planteadas por COBIT 5 para SI, sección II – apéndice A.3.				
Elaborado por: Alejandro Navarro				**Fecha elaboración:** 21/05/2019

FASE 2 - LIDERAZGO Proceso 2.3 - Asignar roles y responsabilidades			
Objetivo: Identificar y asignar los roles y responsabilidades del personal que intervendrá en SI de EPSEL SA			
N°	**Rol**	**Responsabilidad**	**Nivel de implicancia**
01	Directorio	Supervisar y monitorear el desarrollo e implementación del SGSI.	I
02	Gerente General	Identificar y comunicar amenazas para la SI, comportamientos deseables y cambios necesarios para tratar estos puntos.	C
03	Personal de TI	Supervisar el registro de la información entrante y la entrega de información solicitada.	R
04	Oficial de SI	Recoger toda la información concerniente a la SI de la organización.	R
05	Comité de Gestión de Riesgos	Evaluar, optimizar, financiar y monitorizar el riesgo de todos los orígenes con el propósito de incrementar el valor de la empresa a corto y largo plazo para las partes interesadas.	A
06	Comité de SI	Responsabilidad general para la gestión de esfuerzos en SI	A
Conclusiones: Según lo examinado por COBIT 5 para SI, he estimado conveniente la creación de los siguientes roles: ✓ Oficial de SI. ✓ Comité de gestión de riesgos. ✓ Comité de SI.			
Elaborado por: Alejandro Navarro		**Fecha elaboración:** 21/05/2019	

FASE 3 - PLANIFICACIÓN Proceso 3.1 - Identificar el riesgo A. Identificar los activos					
Objetivo: Definir qué activos son críticos para la EPS, que de verse afectados se produzca un impacto negativo en la EPS.					
N°	**Activo**	**Descripción del Activo**	**Categoría del Activo**	**Cód. de Categoría**	**Cód. del Activo**
1	Proceso de Medición	Proceso de toma, registro de lecturas y cálculo de consumo de conexiones que usan medidor.	Servicio	S	S_PMED
2	Proceso de Facturación	Proceso de cálculo de montos por los servicios de agua y alcantarillado acuerdo a los consumos registrados en el proceso de medición y a la tarifa establecida para cada conexión, así como otros cargos a facturar.	Servicio	S	S_PFAC
3	Proceso de Cobranza	Proceso que contempla la recaudación y acciones de cobranza.	Servicio	S	S_PCOB
4	Proceso de Atención al Cliente	Proceso que contempla la atención de reclamos y consultas.	Servicio	S	S_PAAC
5	Proceso de Catastro y Conexiones	Proceso de registro y actualización de datos de ubicación y tipo de conexión.	Servicio	S	S_PCYC
6	Sistema de Gestión Comercial	Software que automatiza todos los procesos comerciales.	Software	SW	SW_SICDESA
7	Sistema de Captura de Datos	Software mediante el cual las EPS cumplen con transferir a SUNASS las variables de gestión.	Software	SW	SW_SICAP
8	Ofimática	Software para procesamiento de textos y hojas de cálculo.	Software	SW	SW_OFI
9	Antivirus	Software para detectar y eliminar virus informáticos.	Software	SW	SW_AV
10	Impresoras	Dispositivos láser, inyección, matricial, para impresión de diversos documentos.	Hardware	HW	HW_IMP
11	Equipo de cómputo	Computadora personal.	Hardware	HW	HW_EDC
12	Lectoras de cód. barras	Dispositivos periféricos para lectura recibos.	Hardware	HW	HW_LCB
13	Servidor Web	Servidor configurado para alojar el portal web.	Soporte de Información	SI	SI_SWEB
14	Servidor ADDS-DNS	Servidor que contiene la configuración del dominio, usuarios y traduce nombres de dominio a IPs y viceversa.	Soporte de Información	SI	SI_SADDS-DNS
15	Firewall	Dispositivo que contiene la configuración de las políticas de seguridad y acceso a internet.	Soporte de Información	SI	SI_FW
16	Modem	Dispositivo que recibe el servicio de internet del proveedor responsable.	Soporte de Información	SI	SI_MDM
17	Switch	Dispositivo para la conexión de red.	Soporte de Información	SI	SI_SWT
18	Servidor de Base de Datos	Servidor que contiene el gestor de base de datos que almacena toda la información comercial.	Soporte de Información	SI	SI_SBD
Conclusiones: Se han identificado 18 activos relacionados con las actividades de la EPS EPSEL SA.					
Elaborado por: Alejandro Navarro			**Fecha elaboración:** 21/05/2019		

FASE 3 - PLANIFICACIÓN
Proceso 3.1 - Identificar el riesgo
B. **Valorar** los activos

Objetivo: Identificar el nivel de criticidad de cada activo.

ACTIVO				VALORACIÓN				
N°	Cód. de activo	Cód. de Categoría	Descripción del activo	C	I	D	TOTAL (C+D+I)	
							Valor	Descripción
1	S_PMED	S	Proceso de Medición	5	5	5	15	Muy Alto
2	S_PFAC	S	Proceso de Facturación	5	5	5	15	Muy Alto
3	S_PCOB	S	Proceso de Cobranza	5	5	5	15	Muy Alto
4	S_PAAC	S	Proceso de Atención al Cliente	5	5	4	14	Muy Alto
5	S_PCYC	S	Proceso de Catastro y Conexiones	5	5	5	15	Muy Alto
6	SW_SICDESA	SW	Sistema de Gestión Comercial	5	5	5	15	Muy Alto
7	SW_SICAP	SW	Sistema de Captura de Datos	1	1	1	3	Bajo
8	SW_OFI	SW	Ofimática	1	1	1	3	Bajo
9	SW_AV	SW	Antivirus	2	1	3	6	Medio
10	HW_IMP	HW	Impresoras	3	1	4	8	Alto
11	HW_EDC	HW	Equipo de Cómputo	4	3	4	11	Muy Alto
12	HW_LCB	HW	Lectoras de cód. barras	3	1	3	7	Alto
13	SI_SWEB	SI	Servidor Web	1	1	1	3	Bajo
14	SI_SADDS-DNS	SI	Servidor ADDS-DNS	2	3	3	8	Alto
15	SI_FW	SI	Firewall	1	1	1	3	Bajo
16	SI_MDM	SI	Modem	2	1	3	6	Medio
17	SI_SWT	SI	Switch	2	1	3	6	Medio
18	SI_SBD	SI	Servidor de Base de Datos	5	5	5	15	Muy Alto

Conclusiones: Según los criterios de confidencialidad (C), integridad (I) y disponibilidad (D); se identificaron 2 activos con nivel de criticidad alto y 8 activos de criticidad muy alta.

Elaborado por: Alejandro Navarro | **Fecha elaboración:** 21/05/2019

FASE 3 - PLANIFICACIÓN Proceso 3.1 - Identificar el riesgo C.1 Valorar las amenazas					
Objetivo: Identificar las amenazas bajo los criterios de capacidad y motivación					
N°	**Amenaza**	**Activo**	**Capacidad**	**Motivación**	**Valor amenaza**
1	Fuego	HW_IMP	3	1	3
2	Fuego	HW_EDC	3	1	3
3	Fuego	HW_LCB	3	1	3
4	Fuego	SI_SWEB	3	1	3
5	Fuego	SI_SADDS-DNS	3	1	3
6	Fuego	SI_FW	3	1	3
7	Fuego	SI_MDM	3	1	3
8	Fuego	SI_SWT	3	1	3
9	Fuego	SI_SBD	3	1	3
10	Daños por agua	HW_IMP	3	1	3
11	Daños por agua	HW_EDC	3	1	3
12	Daños por agua	HW_LCB	3	1	3
13	Daños por agua	SI_SWEB	3	1	3
14	Daños por agua	SI_SADDS-DNS	3	1	3
15	Daños por agua	SI_FW	3	1	3
16	Daños por agua	SI_MDM	3	1	3
17	Daños por agua	SI_SWT	3	1	3
18	Daños por agua	SI_SBD	3	1	3
19	Desastres naturales	SW_SICDESA	1	1	1
20	Desastres naturales	HW_IMP	1	1	1
21	Desastres naturales	HW_EDC	1	1	1
22	Desastres naturales	HW_LCB	1	1	1
23	Desastres naturales	SI_SWEB	1	1	1
24	Desastres naturales	SI_SADDS-DNS	1	1	1
25	Desastres naturales	SI_FW	1	1	1
26	Desastres naturales	SI_MDM	1	1	1
27	Desastres naturales	SI_SWT	1	1	1
28	Desastres naturales	SI_SBD	1	1	1
29	Corte de suministro eléctrico	SW_SICDESA	2	2	3
30	Corte de suministro eléctrico	SW_SICAP	2	2	3
31	Corte de suministro eléctrico	SW_OFI	2	2	3
32	Corte de suministro eléctrico	SW_AV	2	2	3
33	Corte de suministro eléctrico	HW_IMP	2	2	3
34	Corte de suministro eléctrico	HW_EDC	2	2	3
35	Corte de suministro eléctrico	HW_LCB	2	2	3
36	Corte de suministro eléctrico	SI_SWEB	2	2	3
37	Corte de suministro eléctrico	SI_SADDS-DNS	2	2	3
38	Corte de suministro eléctrico	SI_FW	2	2	3
39	Corte de suministro eléctrico	SI_MDM	2	2	3
40	Corte de suministro eléctrico	SI_SWT	2	2	3
41	Corte de suministro eléctrico	SI_SBD	2	2	3
42	Condiciones inadecuadas de humedad o temp.	HW_IMP	1	1	1
43	Condiciones inadecuadas de humedad o temp.	HW_EDC	1	1	1
44	Condiciones inadecuadas de humedad o temp.	HW_LCB	1	1	1
45	Condiciones inadecuadas de humedad o temp.	SI_SWEB	1	1	1
46	Condiciones inadecuadas de humedad o temp.	SI_SADDS-DNS	1	1	1
47	Condiciones inadecuadas de humedad o temp.	SI_FW	1	1	1
48	Condiciones inadecuadas de humedad o temp.	SI_MDM	1	1	1
49	Condiciones inadecuadas de humedad o temp.	SI_SWT	1	1	1
50	Condiciones inadecuadas de humedad o temp.	SI_SBD	1	1	1

51	Fallo de servicios de comunicaciones	HW_IMP	2	2	3
52	Fallo de servicios de comunicaciones	HW_EDC	2	2	3
53	Fallo de servicios de comunicaciones	HW_LCB	2	2	3
54	Fallo de servicios de comunicaciones	SI_SWEB	2	2	3
55	Fallo de servicios de comunicaciones	SI_SADDS-DNS	2	2	3
56	Fallo de servicios de comunicaciones	SI_FW	2	2	3
57	Fallo de servicios de comunicaciones	SI_MDM	2	2	3
58	Fallo de servicios de comunicaciones	SI_SWT	2	2	3
59	Fallo de servicios de comunicaciones	SW_SGC	2	2	3
60	Fallo de servicios de comunicaciones	SI_SBD	2	2	3
61	Interrupción de otros serv./suminist. esenciales	HW_IMP	1	2	2
62	Interrupción de otros serv./suminist. esenciales	HW_EDC	1	2	2
63	Interrupción de otros serv./suminist. esenciales	HW_LCB	1	2	2
64	Interrupción de otros serv./suminist. esenciales	SI_SBD	1	2	2
65	Errores de los usuarios	SW_SICDESA	3	3	5
66	Errores de los usuarios	SW_SICAP	3	1	3
67	Errores de los usuarios	HW_IMP	1	1	1
68	Errores de los usuarios	HW_EDC	1	1	1
69	Errores de los usuarios	HW_LCB	1	1	1
70	Errores de configuración	SW_SICDESA	3	3	5
71	Errores de configuración	SW_SICAP	2	1	2
72	Errores de configuración	SW_AV	2	2	3
73	Errores de configuración	HW_IMP	2	1	2
74	Errores de configuración	HW_EDC	2	1	2
75	Errores de configuración	HW_LCB	2	1	2
76	Errores de configuración	SI_SWEB	3	2	4
77	Errores de configuración	SI_SADDS-DNS	3	2	4
78	Errores de configuración	SI_FW	3	1	3
79	Errores de configuración	SI_MDM	3	1	3
80	Errores de configuración	SI_SWT	3	1	3
81	Errores de configuración	SI_SBD	3	3	5
82	Fuga de información	SW_SICDESA	3	3	5
83	Fuga de información	SW_SICAP	1	1	1
84	Fuga de información	HW_IMP	2	1	2
85	Fuga de información	HW_EDC	2	2	3
86	Fuga de información	SI_SBD	3	3	5
87	Introducción de falsa información	SW_SICDESA	3	3	5
88	Introducción de falsa información	SW_SICAP	2	1	2
89	Introducción de falsa información	SI_SBD	3	1	3
90	Alteración de la información	SW_SICDESA	3	3	5
91	Alteración de la información	SW_SICAP	2	1	2
92	Alteración de la información	SI_SBD	3	3	5
93	Corrupción de la información	SW_SICDESA	3	3	5
94	Corrupción de la información	SW_SICAP	2	1	2
95	Corrupción de la información	SI_SBD	3	1	3
96	Destrucción de la información	SW_SICDESA	3	2	4
97	Destrucción de la información	SW_SICAP	2	1	2
98	Destrucción de la información	SI_SBD	3	3	5
99	Degradación de los soportes de almac. de inform.	SI_SBD	3	2	4
100	Difusión de software dañino	HW_EDC	3	3	5
101	Difusión de software dañino	SI_SWEB	3	1	3
102	Difusión de software dañino	SI_SADDS-DNS	3	1	3
103	Difusión de software dañino	SI_FW	3	1	3
104	Difusión de software dañino	SI_SBD	3	1	3
105	Errores de mantenimiento/actualización de SW	SW_SICDESA	3	2	4
106	Errores de mantenimiento/actualización de SW	SI_SBD	3	1	3

108	Errores de mantenimiento/actualización de HW	HW_EDC	2	2	3
109	Errores de mantenimiento/actualización de HW	HW_LCB	1	1	1
110	Errores de mantenimiento/actualización de HW	SI_SWEB	3	1	3
111	Errores de mantenimiento/actualización de HW	SI_SADDS-DNS	3	1	3
112	Errores de mantenimiento/actualización de HW	SI_FW	3	1	3
113	Errores de mantenimiento/actualización de HW	SI_SBD	3	1	3
114	Caída del sistema por sobrecarga	SW_SICDESA	3	1	3
115	Caída del sistema por sobrecarga	SW_SICAP	2	1	2
116	Pérdida de Equipos	HW_IMP	1	3	3
117	Pérdida de Equipos	HW_EDC	2	3	4
118	Pérdida de Equipos	HW_LCB	1	3	3
119	Pérdida de Equipos	SI_SWEB	3	1	3
120	Pérdida de Equipos	SI_SADDS-DNS	3	1	3
121	Pérdida de Equipos	SI_FW	3	1	3
122	Pérdida de Equipos	SI_MDM	3	1	3
123	Pérdida de Equipos	SI_SWT	3	1	3
124	Pérdida de Equipos	SI_SBD	3	1	3
125	Indisponibilidad del personal	SW_SICDESA	3	1	3
126	Indisponibilidad del personal	SI_SBD	3	1	3
127	Abuso de privilegios de acceso	SW_SICDESA	3	3	5
128	Abuso de privilegios de acceso	SI_SBD	3	3	5
129	Acceso no autorizado	SW_SICDESA	3	3	5
130	Acceso no autorizado	SW_SICAP	2	1	2
131	Acceso no autorizado	SI_SBD	3	3	5
132	Denegación del servicio	HW_IMP	1	2	2
133	Denegación del servicio	HW_LCB	1	2	2
134	Denegación del servicio	SI_SWEB	3	1	3
135	Denegación del servicio	SI_SADDS-DNS	3	1	3
136	Denegación del servicio	SI_FW	3	1	3
137	Denegación del servicio	SI_MDM	3	1	3
138	Denegación del servicio	SI_SWT	3	1	3
139	Ingeniería social	SW_SICDESA	3	3	5
140	Ingeniería social	SW_SICAP	2	1	2
Conclusiones: Se obtuvieron 25 amenazas relacionadas a los activos identificados.					
Elaborado por: Alejandro Navarro		**Fecha elaboración:** 21/05/2019			

FASE 3 - PLANIFICACIÓN Proceso 3.1 - Identificar el riesgo C.2 Valorar las vulnerabilidades						
Objetivo: Determinar las vulnerabilidades bajo los criterios de severidad y exposición.						
N°	**Activo**	**Amenaza**	**Vulnerabilidad**	**Severidad**	**Exposición**	**Valor vulnerabilidad**
1	HW_IMP	Fuego	Carencia de sistemas de seguridad anti incendios	3	1	3
2	HW_IMP	Daños por agua	Carencia de plan concientización de cuidado de equipos	3	1	3
3	HW_IMP	Desastres naturales	Infraestructura inadecuada	1	1	1
4	HW_IMP	Corte de suministro eléctrico	Carencia de grupos electrógenos	2	1	2
5	HW_IMP	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	2	1	2
6	HW_IMP	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	3	1	3
7	HW_IMP	Interrupción de otros servicios/suministros esenciales	Carencia de políticas de mantenimiento preventivo	2	1	2
8	HW_IMP	Errores de los usuarios	Carencia de un plan de capacitación	3	2	4
9	HW_IMP	Errores de configuración	Ausencia de un plan de configuración de equipos	3	1	3
10	HW_IMP	Fuga de información	Ausencia de un plan de SI	3	1	3
11	HW_IMP	Error mantenimiento/actualización de SW	Ausencia de un plan de mantenimiento de equipos	2	1	2
12	HW_IMP	Pérdida de Equipos	Carencia de un plan de SI	3	1	3
13	HW_IMP	Denegación del servicio	Carencia de un sistema de información de administración de eventos	3	1	3
14	HW_EDC	Fuego	Carencia de sistemas de seguridad anti incendios	3	2	4
15	HW_EDC	Daños por agua	Carencia de plan concientización de cuidado de equipos	3	2	4
16	HW_EDC	Desastres naturales	Infraestructura inadecuada	1	2	2
17	HW_EDC	Corte de suministro eléctrico	Carencia de grupos electrógenos	2	2	3
18	HW_EDC	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	2	2	3
19	HW_EDC	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	2	2	3
20	HW_EDC	Interrupción de otros serv./suministros esenciales	Carencia de políticas de mantenimiento preventivo	2	2	3
21	HW_EDC	Errores de los usuarios	Carencia de un plan de capacitación	3	2	4
22	HW_EDC	Errores de configuración	Ausencia de un plan de configuración de equipos	3	2	4
23	HW_EDC	Fuga de información	Ausencia de un plan de SI	3	2	4
24	HW_EDC	Difusión de software dañino	Ausencia de un plan de SI	3	2	4
25	HW_EDC	Difusión de software dañino	Ausencia de políticas de software mal intencionado	3	2	4
26	HW_EDC	Error mantenimiento /actualización de HW	Deficiencia en el procedimiento de prevención	3	2	4
27	HW_EDC	Error mantenimiento/actualizació	Ausencia de un plan de mantenimiento de equipos	3	2	4

FASE 3 - PLANIFICACIÓN Proceso 3.2 - Analizar el riesgo								
Objetivo: Determinar el nivel del riesgo a través de los valores resultantes del análisis de vulnerabilidad y análisis de amenaza, sobre los activos críticos.								
N°	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**Valor del riesgo (P x I)**	**Cód. del Riesgo**	**Magnitud del Riesgo**
1	HW_IMP	Fuego	Carencia de sistemas de seguridad anti incendios	2	2	4	R1	Baja
2	HW_IMP	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	2	4	R2	Baja
3	HW_IMP	Desastres naturales	Infraestructura inadecuada	1	2	2	R3	Baja
4	HW_IMP	Corte de suministro eléctrico	Carencia de grupos electrógenos	1	2	2	R4	Baja
5	HW_IMP	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	1	1	1	R5	Baja
6	HW_IMP	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	2	2	4	R6	Baja
7	HW_IMP	Interrupción de otros servicios/suministros esenciales	Carencia de políticas de mantenimiento preventivo	2	2	4	R7	Baja
8	HW_IMP	Errores de los usuarios	Carencia de un plan de capacitación	3	2	6	R8	Moderada
9	HW_IMP	Errores de configuración	Ausencia de un plan de configuración de equipos	3	2	6	R9	Moderada
10	HW_IMP	Fuga de información	Ausencia de un plan de SI	1	1	1	R10	Baja
11	HW_IMP	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	1	1	1	R11	Baja
12	HW_IMP	Pérdida de Equipos	Carencia de un plan de SI	3	3	9	R12	Moderada
13	HW_IMP	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	2	2	R13	Baja
14	HW_EDC	Fuego	Carencia de sistemas de seguridad anti incendios.	2	4	8	R14	Moderada
15	HW_EDC	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	4	8	R15	Moderada
16	HW_EDC	Desastres naturales	Infraestructura inadecuada	1	4	4	R16	Baja
17	HW_EDC	Corte de suministro eléctrico	Carencia de grupos electrógenos	2	3	6	R17	Moderada
18	HW_EDC	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	1	3	3	R18	Baja
19	HW_EDC	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	3	4	12	R19	Alta
20	HW_EDC	Interrupción de otros servicios/suministros esenciales	Carencia de políticas de mantenimiento preventivo	3	4	12	R20	Alta
21	HW_EDC	Errores de los usuarios	Carencia de un plan de capacitación	3	5	15	R21	Alta
22	HW_EDC	Errores de configuración	Ausencia de un plan de configuración de equipos	3	4	12	R22	Alta
23	HW_EDC	Fuga de información	Ausencia de un plan de SI	3	5	15	R23	Alta
24	HW_EDC	Difusión de software dañino	Ausencia de un plan de SI	2	4	8	R24	Moderada
25	HW_EDC	Difusión de software dañino	Ausencia de políticas de software mal intencionado	2	4	8	R25	Moderada

26	HW_EDC	Errores de mant. / actualiz. de HW	Deficiencia en el procedimiento de prevención	2	3	6	R26	Moderada
27	HW_EDC	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	2	3	6	R27	Moderada
28	HW_EDC	Pérdida de Equipos	Deficiencia en la actualización del inventario de equipos	2	4	8	R28	Moderada
29	HW_EDC	Pérdida de Equipos	Carencia de un plan de SI	2	4	8	R29	Moderada
30	SI_MDM	Fuego	Deficiencia en infraestructura de la sala de servidores	2	5	10	R30	Moderada
31	SI_MDM	Daños por agua	Deficiencia en infraestructura de la sala de servidores	1	4	4	R31	Baja
32	SI_MDM	Desastres naturales	Deficiencia en infraestructura de la sala de servidores	2	4	8	R32	Moderada
33	SI_MDM	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores	1	3	3	R33	Baja
34	SI_MDM	Condiciones inadecuadas temperatura/humedad	Deficiencia en infraestructura de la sala de servidores	1	3	3	R34	Baja
35	SI_MDM	Fallo de servicios de comunicaciones	Carencia de un sistema de información de administración de eventos	2	3	6	R35	Moderada
36	SI_MDM	Fallo de servicios de comunicaciones	Deficiencia en las políticas para determinar los SLA	2	3	6	R36	Moderada
37	SI_MDM	Errores de configuración	Ausencia de plan de gestión de configuración	1	3	3	R37	Baja
38	SI_MDM	Pérdida de Equipos	Carencia de un plan de SI	1	3	3	R38	Baja
39	SI_MDM	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	3	3	R39	Baja
40	SI_SWT	Fuego	Deficiencia en infraestructura de la sala de servidores	2	5	10	R40	Moderada
41	SI_SWT	Daños por agua	Deficiencia en infraestructura de la sala de servidores	1	5	5	R41	Baja
42	SI_SWT	Desastres naturales	Deficiencia en infraestructura de la sala de servidores	2	4	8	R42	Moderada
43	SI_SWT	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores	1	4	4	R43	Baja
44	SI_SWT	Condiciones inadecuadas temperatura/humedad	Deficiencia en infraestructura de la sala de servidores	2	5	10	R44	Moderada
45	SI_SWT	Fallo de servicios de comunicaciones	Carencia de un sistema de información de administración de eventos	2	4	8	R45	Moderada
46	SI_SWT	Errores de configuración	Ausencia de plan de gestión de configuración	1	5	5	R46	Baja
47	SI_SWT	Pérdida de Equipos	Carencia de un plan de SI	1	3	3	R47	Baja
48	SI_SWT	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	5	5	R48	Baja
49	SI_SBD	Fuego	Deficiencia en infraestructura de la sala de servidores	2	5	10	R49	Moderada
50	SI_SBD	Fuego	Deficiencia en las políticas de copias de seguridad	2	5	10	R50	Moderada
51	SI_SBD	Daños por agua	Deficiencia en infraestructura de la sala de servidores	2	5	10	R51	Moderada
52	SI_SBD	Daños por agua	Deficiencia en las políticas de copias de seguridad	2	5	10	R52	Moderada
53	SI_SBD	Desastres naturales	Deficiencia en infraestructura de la sala de servidores	1	5	5	R53	Baja
54	SI_SBD	Desastres naturales	Políticas de copias de seguridad deficiente	1	5	5	R54	Baja
55	SI_SBD	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores	2	5	10	R55	Moderada
56	SI_SBD	Condiciones inadecuadas temperatura/humedad	Deficiencia en infraestructura de la sala de servidores	1	5	5	R56	Baja

57	SI_SBD	Fallo de servicios de comunicaciones	Carencia de un sistema de información de administración de eventos	2	5	10	R57	Moderada
58	SI_SBD	Interrupción de otros servicios/suministros esenciales	Carencia de políticas de mantenimiento preventivo	2	5	10	R58	Moderada
59	SI_SBD	Errores de configuración	Ausencia de plan de gestión de configuración	4	5	20	R59	Extrema
60	SI_SBD	Fuga de información	Carencia de un plan de SI	4	5	20	R60	Extrema
61	SI_SBD	Introducción de falsa información	Carencia de políticas de revisión por muestreo	3	5	15	R61	Alta
62	SI_SBD	Introducción de falsa información	Carencia de un plan de supervisión	3	5	15	R62	Alta
63	SI_SBD	Alteración de la información	Carencia de un plan de supervisión	5	5	25	R63	Extrema
64	SI_SBD	Corrupción de la información	Carencia de un plan de supervisión	3	5	15	R64	Alta
65	SI_SBD	Corrupción de la información	Deficiencia en las políticas de copias de seguridad	3	5	15	R65	Alta
66	SI_SBD	Destrucción de la información	Carencia de un plan de supervisión	5	5	25	R66	Extrema
67	SI_SBD	Destrucción de la información	Deficiencia en las políticas de copias de seguridad	5	5	25	R67	Extrema
68	SI_SBD	Degradación de los soportes de almacenamiento de la información	Carencia de un plan de supervisión	3	5	15	R68	Alta
69	SI_SBD	Degradación de los soportes de almacenamiento de la información	Carencia de un sistema de información de administración de eventos	3	5	15	R69	Alta
70	SI_SBD	Difusión de software dañino	Ausencia de un plan de SI	3	5	15	R70	Alta
71	SI_SBD	Difusión de software dañino	Ausencia de políticas de software mal intencionado	3	5	15	R71	Alta
72	SI_SBD	Error mantenimiento/actualización de SW	Carencia de documentación	2	5	10	R72	Moderada
73	SI_SBD	Error mantenimiento/actualización de SW	Carencia de un plan de mantenimiento preventivo	2	5	10	R73	Moderada
74	SI_SBD	Error mantenimiento/actualización de SW	Ausencia de plan de gestión de configuración	2	5	10	R74	Moderada
75	SI_SBD	Errores de mant. / actualiz. de HW	Carencia de documentación	2	5	10	R75	Moderada
76	SI_SBD	Errores de mant. / actualiz. de HW	Carencia de un plan de mantenimiento preventivo	3	5	15	R76	Alta
77	SI_SBD	Errores de mant. / actualiz. de HW	Ausencia de plan de gestión de configuración	3	5	15	R77	Alta
78	SI_SBD	Pérdida de Equipos	Carencia de un plan de SI	3	3	9	R78	Moderada
79	SI_SBD	Indisponibilidad del personal	Dependencia excesiva de personal de gestión de BD	3	4	12	R79	Alta
80	SI_SBD	Abuso de privilegios de acceso	Deficiencia en la política de rotación de personal	5	5	25	R80	Extrema
81	SI_SBD	Abuso de privilegios de acceso	Ausencia fuente inform. de perfil acceso descrito y autoriz.	5	5	25	R81	Extrema
82	SI_SBD	Acceso no autorizado	Carencia de un sistema de información de administración de eventos	3	5	15	R82	Alta
83	SI_SBD	Acceso no autorizado	Carencia de un plan de auditoría de accesos	3	5	15	R83	Alta
84	SW_SICDESA	Corte de suministro eléctrico	Deficiencia en las políticas de copias de seguridad	2	4	8	R84	Moderada
85	SW_SICDESA	Fallo de servicios de comunicaciones	Carencia de una fuente de conocimiento de incidentes	3	4	12	R85	Alta
86	SW_SICDESA	Errores de los usuarios	Carencia de un plan de capacitación	5	5	25	R86	Extrema
87	SW_SICDESA	Errores de configuración	Ausencia de plan de gestión de configuración	5	5	25	R87	Extrema
88	SW_SICDESA	Errores de configuración	Ausencia fuente inform. de perfil acceso descrito y autoriz.	4	5	20	R88	Extrema
89	SW_SICDESA	Fuga de información	Carencia de un plan de SI	4	5	20	R89	Extrema

90	SW_SICDESA	Introducción de falsa información	Carencia de políticas de revisión por muestreo	4	5	20	R90	Extrema
91	SW_SICDESA	Introducción de falsa información	Carencia de un plan de supervisión	4	5	20	R91	Extrema
92	SW_SICDESA	Alteración de la información	Carencia de políticas de revisión por muestreo	4	5	20	R92	Extrema
93	SW_SICDESA	Alteración de la información	Carencia de un plan de supervisión	4	5	20	R93	Extrema
94	SW_SICDESA	Corrupción de la información	Carencia de políticas de revisión por muestreo	4	5	20	R94	Extrema
95	SW_SICDESA	Corrupción de la información	Carencia de un plan de supervisión	4	5	20	R95	Extrema
96	SW_SICDESA	Destrucción de la información	Carencia de políticas de revisión por muestreo	4	5	20	R96	Extrema
97	SW_SICDESA	Destrucción de la información	Carencia de un plan de supervisión	4	5	20	R97	Extrema
98	SW_SICDESA	Error mantenimiento/actualización de SW	Carencia de documentación	2	5	10	R98	Moderada
99	SW_SICDESA	Error mantenimiento/actualización de SW	Carencia de un plan de mantenimiento preventivo	2	5	10	R99	Moderada
100	SW_SICDESA	Error mantenimiento/actualización de SW	Ausencia de plan de gestión de configuración	3	5	15	R100	Alta
101	SW_SICDESA	Caída del sistema por sobrecarga	Carencia de un sistema de información de administración de eventos	2	4	8	R101	Moderada
102	SW_SICDESA	Indisponibilidad del personal	Dependencia excesiva de personal de gestión de BD	3	4	12	R102	Alta
103	SW_SICDESA	Abuso de privilegios de acceso	Deficiencia en la política de rotación de personal	5	5	25	R103	Extrema
104	SW_SICDESA	Abuso de privilegios de acceso	Ausencia fuente inform. de perfil acceso descrito y autoriz.	4	5	20	R104	Extrema
105	SW_SICDESA	Acceso no autorizado	Carencia de un sistema de información de administración de eventos	4	5	20	R105	Extrema
106	SW_SICDESA	Ingeniería social	Carencia de Capacitación sobre ingeniería social	5	5	25	R106	Extrema
107	HW_LCB	Fuego	Carencia de sistemas de seguridad anti incendios	2	1	2	R107	Baja
108	HW_LCB	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	1	2	R108	Baja
109	HW_LCB	Desastres naturales	Infraestructura inadecuada	1	1	1	R109	Baja
110	HW_LCB	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	1	1	1	R110	Baja
111	HW_LCB	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	1	1	1	R111	Baja
112	HW_LCB	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	2	2	4	R112	Baja
113	HW_LCB	Interrupción de otros servicios/suministros esenciales	Infraestructura inadecuada	1	2	2	R113	Baja
114	HW_LCB	Errores de los usuarios	Carencia de un plan de capacitación	3	2	6	R114	Moderada
115	HW_LCB	Errores de configuración	Ausencia de un plan de configuración de equipos	3	2	6	R115	Moderada
116	HW_LCB	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	1	1	1	R116	Baja
117	HW_LCB	Pérdida de Equipos	Carencia de un plan de SI	3	3	9	R117	Moderada
118	HW_LCB	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	2	2	R118	Baja
119	SI_SWEB	Fuego	Carencia de sistemas de seguridad anti incendios	2	5	10	R119	Moderada
120	SI_SWEB	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	5	10	R120	Moderada
121	SI_SWEB	Desastres naturales	Infraestructura inadecuada	1	5	5	R121	Baja
122	SI_SWEB	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	5	10	R122	Moderada

123	SI_SWEB	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	2	5	10	R123	Moderada
124	SI_SWEB	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	3	4	12	R124	Alta
125	SI_SWEB	Errores de los usuarios	Carencia de un plan de capacitación	3	5	15	R125	Alta
126	SI_SWEB	Difusión de software dañino	Ausencia de un plan de SI	1	5	5	R126	Baja
127	SI_SWEB	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	3	5	15	R127	Alta
128	SI_SWEB	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	5	5	R128	Baja
129	SI_SADDS-DNS	Fuego	Carencia de sistemas de seguridad anti incendios	2	5	10	R129	Moderada
130	SI_SADDS-DNS	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	5	10	R130	Moderada
131	SI_SADDS-DNS	Desastres naturales	Infraestructura inadecuada	1	5	5	R131	Baja
132	SI_SADDS-DNS	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	5	10	R132	Moderada
133	SI_SADDS-DNS	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	2	5	10	R133	Moderada
134	SI_SADDS-DNS	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	3	4	12	R134	Alta
135	SI_SADDS-DNS	Errores de configuración	Carencia de un plan de capacitación	1	5	5	R135	Baja
136	SI_SADDS-DNS	Difusión de software dañino	Ausencia de un plan de SI	1	5	5	R136	Baja
137	SI_SADDS-DNS	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	3	5	15	R137	Alta
138	SI_SADDS-DNS	Pérdida de Equipos	Carencia de un plan de SI	3	3	9	R138	Moderada
139	SI_SADDS-DNS	Denegación del servicio	Carencia de un sistema de información de administración de eventos	1	5	5	R139	Baja
140	SI_FW	Fuego	Carencia de sistemas de seguridad anti incendios	2	5	10	R140	Moderada
141	SI_FW	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	5	10	R141	Moderada
142	SI_FW	Desastres naturales	Infraestructura inadecuada	1	5	5	R142	Baja
143	SI_FW	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	5	10	R143	Moderada
144	SI_FW	Condiciones inadecuadas temperatura/humedad	Carencia de infraestructura adecuada	2	5	10	R144	Moderada
145	SI_FW	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	3	4	12	R145	Alta
146	SI_FW	Errores de configuración	Carencia de un plan de capacitación	1	5	5	R146	Baja

147	SI_FW	Difusión de software dañino	Ausencia de un plan de SI	1	5	5	R147	Baja
148	SI_FW	Errores de mant. / actualiz. de HW	Ausencia de un plan de mantenimiento de equipos	3	5	15	R148	Alta
149	SI_FW	Pérdida de Equipos	Carencia de un plan de SI	3	5	15	R149	Alta
150	SI_FW	Denegación del servicio	Carencia de un sistema de información de adm. de eventos	1	5	5	R150	Baja
151	SW_SICAP	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	4	8	R151	Moderada
152	SW_SICAP	Errores de los usuarios	Carencia de un plan de capacitación	3	5	15	R152	Alta
153	SW_SICAP	Errores de configuración	Ausencia de un plan de configuración de equipos	1	5	5	R153	Baja
154	SW_SICAP	Fuga de información	Ausencia de un plan de SI	4	5	20	R154	Extrema
155	SW_SICAP	Introducción de falsa información	Falta de un plan de SI	4	5	20	R155	Extrema
156	SW_SICAP	Alteración de la información	Falta de un plan de SI	4	5	20	R156	Extrema
157	SW_SICAP	Corrupción de la información	Falta de un plan de SI	4	5	20	R157	Extrema
158	SW_SICAP	Destrucción de la información	Falta de un plan de SI	4	5	20	R158	Extrema
159	SW_SICAP	Caída del sistema por sobrecarga	Falta de un control de accesos a los recursos	2	4	8	R159	Moderada
160	SW_SICAP	Acceso no autorizado	Falta de políticas de control de acceso	4	5	20	R160	Extrema
161	SW_SICAP	Acceso no autorizado	Cuentas de usuarios mal configuradas	4	5	20	R161	Extrema
162	SW_SICAP	Ingeniería social	Falta de políticas de seguridad	5	5	25	R162	Extrema
163	SW_OFI	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	3	6	R163	Moderada
164	SW_AV	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	2	5	10	R164	Moderada
165	SW_AV	Errores de configuración	Carencia de un plan de capacitación	2	4	8	R165	Moderada
Conclusiones: De los 165 riesgos identificados, se observa que existen 31 riesgos de magnitud extrema. Del mismo modo, se observan 30 riesgos de magnitud alta.								
Elaborado por: Alejandro Navarro						**Fecha elaboración:** 21/05/2019		

FASE 3 - PLANIFICACIÓN Proceso 3.3 - Evaluar el riesgo									
Objetivo: Evaluar el riesgo para determinar su tolerancia al riesgo									
N°	**Cód. riesgo**	**Magnitud del riesgo**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor riesgo (PXI)**	**Tolerancia**		
							Aceptable	**Tolerable**	**No Tolerable**
1	R1	Baja	HW_IMP	Fuego	Carencia de sistemas de seguridad anti incendios.	4	x		
2	R2	Baja	HW_IMP	Daños por agua	Carencia de plan concientización del cuidado de equipos	4	x		
3	R3	Baja	HW_IMP	Desastres naturales	Infraestructura inadecuada	2	x		
4	R4	Baja	HW_IMP	Corte de suministro eléctrico	Carencia de grupos electrógenos.	2	x		
5	R5	Baja	HW_IMP	Condiciones inadecuadas de temp. o humedad	Carencia de infraestructura adecuada	1	x		
6	R6	Baja	HW_IMP	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	4	x		
7	R7	Baja	HW_IMP	Interrupción de otros serv. y suministros esenciales	Carencia de políticas de mantenimiento preventivo	4	x		
8	R8	Moderada	HW_IMP	Errores de los usuarios	Carencia de un plan de capacitación.	6		x	
9	R9	Moderada	HW_IMP	Errores de configuración	Ausencia de un plan de configuración de equipos.	6		x	
10	R10	Baja	HW_IMP	Fuga de información	Ausencia de un plan de SI	1	x		
11	R11	Baja	HW_IMP	Errores de mantenimiento / actualización de HW	Ausencia de un plan de mantenimiento de equipos.	1	x		
12	R12	Moderada	HW_IMP	Pérdida de Equipos	Carencia de un plan de SI	9		x	
13	R13	Baja	HW_IMP	Denegación del servicio	Carencia de un sist. de informac. de administración de eventos	2	x		
14	R14	Moderada	HW_EDC	Fuego	Carencia de sistemas de seguridad anti incendios.	8		x	
15	R15	Moderada	HW_EDC	Daños por agua	Carencia de plan concientización del cuidado de equipos	8		x	
16	R16	Baja	HW_EDC	Desastres naturales	Infraestructura inadecuada	4	x		
17	R17	Moderada	HW_EDC	Corte de suministro eléctrico	Carencia de grupos electrógenos.	6		x	
18	R18	Baja	HW_EDC	Condiciones inadecuadas	Carencia de infraestructura adecuada	3	x		

				de temp. o humedad					
19	R19	Alta	HW_EDC	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo.	12			x
20	R20	Alta	HW_EDC	Interrupción de otros serv. y suministros esenciales	Carencia de políticas de mantenimiento preventivo.	12			x
21	R21	Alta	HW_EDC	Errores de los usuarios	Carencia de un plan de capacitación.	15			x
22	R22	Alta	HW_EDC	Errores de configuración	Ausencia de un plan de config. de equipos.	12			x
23	R23	Alta	HW_EDC	Fuga de información	Ausencia de un plan de SI	15			x
24	R24	Moderada	HW_EDC	Difusión de software dañino	Ausencia de un plan de SI	8		x	
25	R25	Moderada	HW_EDC	Difusión de software dañino	Ausencia de Políticas de software mal intencionado	8		x	
26	R26	Moderada	HW_EDC	Errores de mantenimiento / actualización de HW	Deficiencia en el procedimiento de prevención.	6		x	
27	R27	Moderada	HW_EDC	Errores de mantenimiento / actualización de HW	Ausencia de un plan de mantenimiento de equipos.	6		x	
28	R28	Moderada	HW_EDC	Pérdida de Equipos	Deficiencia en la actualización del inventario de equipos.	8		x	
29	R29	Moderada	HW_EDC	Pérdida de Equipos	Carencia de un plan de SI	8		x	
30	R30	Moderada	SI_MDM	Fuego	Deficiencia en infraestructura de la sala de servidores.	10		x	
31	R31	Baja	SI_MDM	Daños por agua	Deficiencia en infraestructura de la sala de servidores.	4	x		
32	R32	Moderada	SI_MDM	Desastres naturales	Deficiencia en infraestructura de la sala de servidores.	8		x	
33	R33	Baja	SI_MDM	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores.	3	x		
34	R34	Baja	SI_MDM	Condiciones inadecuadas de temperatura o humedad	Deficiencia en infraestructura de la sala de servidores.	3	x		
35	R35	Moderada	SI_MDM	Fallo de servicios de comunicaciones	Carencia de un sist. de informac. de admin eventos	6		x	
36	R36	Moderada	SI_MDM	Fallo de servicios de	Deficiencia en las políticas para	6		x	

				comunicaciones	determinar los acuerdos de niveles de servicio.				
37	R37	Baja	SI_MDM	Errores de configuración	Ausencia de Plan de Gestión de Config.	3	x		
38	R38	Baja	SI_MDM	Pérdida de Equipos	Carencia de un plan de SI	3	x		
39	R39	Baja	SI_MDM	Denegación del servicio	Carencia de un sist. de informac. de admin eventos	3	x		
40	R40	Moderada	SI_SWT	Fuego	Deficiencia en infraestructura de la sala de servidores.	10		x	
41	R41	Baja	SI_SWT	Daños por agua	Deficiencia en infraestructura de la sala de servidores.	5	x		
42	R42	Moderada	SI_SWT	Desastres naturales	Deficiencia en infraestructura de la sala de servidores.	8		x	
43	R43	Baja	SI_SWT	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores.	4	x		
44	R44	Moderada	SI_SWT	Condiciones inadecuadas de temperatura o humedad	Deficiencia en infraestructura de la sala de servidores.	10		x	
45	R45	Moderada	SI_SWT	Fallo de servicios de comunicaciones	Carencia de un sist. de informac. de admin eventos	8		x	
46	R46	Baja	SI_SWT	Errores de configuración	Ausencia de Plan de Gestión de Configuración	5	x		
47	R47	Baja	SI_SWT	Pérdida de Equipos	Carencia de un plan de SI	3	x		
48	R48	Baja	SI_SWT	Denegación del servicio	Carencia de un sist. de informac. de admin eventos	5	x		
49	R49	Moderada	SI_SBD	Fuego	Deficiencia en infraestructura de la sala de servidores.	10		x	
50	R50	Moderada	SI_SBD	Fuego	Deficiencia en las políticas de copias de seguridad	10		x	
51	R51	Moderada	SI_SBD	Daños por agua	Deficiencia en infraestructura de la sala de servidores.	10		x	
52	R52	Moderada	SI_SBD	Daños por agua	Deficiencia en las políticas de copias de seguridad	10		x	
53	R53	Baja	SI_SBD	Desastres naturales	Deficiencia en infraestructura de la sala de servidores.	5	x		
54	R54	Baja	SI_SBD	Desastres naturales	Políticas de copias de seguridad deficiente	5	x		
55	R55	Moderada	SI_SBD	Corte de suministro eléctrico	Deficiencia en infraestructura de la sala de servidores.	10		x	

56	R56	Baja	SI_SBD	Condiciones inadecuadas de temperatura o humedad	Deficiencia en infraestructura de la sala de servidores.	5	x		
57	R57	Moderada	SI_SBD	Fallo de servicios de comunicaciones	Carencia de un sist. de informac. de admin eventos	10		x	
58	R58	Moderada	SI_SBD	Interrupción de otros serv. y suministros esenciales	Carencia de políticas de mantenimiento preventivo.	10		x	
59	R59	Extrema	SI_SBD	Errores de configuración	Ausencia de Plan de Gestión de Config.	20			x
60	R60	Extrema	SI_SBD	Fuga de información	Carencia de un plan de SI	20			x
61	R61	Alta	SI_SBD	Introducción de falsa información	Carencia de políticas de revisión por muestreo	15			x
62	R62	Alta	SI_SBD	Introducción de falsa información	Carencia de un plan de supervisión	15			x
63	R63	Extrema	SI_SBD	Alteración de la información	Carencia de un plan de supervisión	25			x
64	R64	Alta	SI_SBD	Corrupción de la información	Carencia de un plan de supervisión	15			x
65	R65	Alta	SI_SBD	Corrupción de la información	Deficiencia en las políticas de copias de seguridad	15			x
66	R66	Extrema	SI_SBD	Destrucción de la inform.	Carencia de un plan de supervisión	25			x
67	R67	Extrema	SI_SBD	Destrucción de la información	Deficiencia en las políticas de copias de seguridad	25			x
68	R68	Alta	SI_SBD	Degradación de los soportes de almac. de inform.	Carencia de un plan de supervisión	15			x
69	R69	Alta	SI_SBD	Degradación de los soportes de almac. de inform.	Carencia de un sist. de informac. de admin eventos	15			x
70	R70	Alta	SI_SBD	Difusión de software dañino	Ausencia de un plan de SI	15			x
71	R71	Alta	SI_SBD	Difusión de software dañino	Ausencia de Políticas de software mal intencionado	15			x
72	R72	Moderada	SI_SBD	Errores de mantenimiento / actualización de SW	Carencia de Documentación	10		x	
73	R73	Moderada	SI_SBD	Errores de mantenimiento /	Carencia de un plan de mantenimiento preventivo	10		x	

				actualización de SW					
74	R74	Moderada	SI_SBD	Errores de mantenimiento / actualización de SW	Ausencia de Plan de Gestión de Configuración	10		x	
75	R75	Moderada	SI_SBD	Errores de mantenimiento / actualización de HW	Carencia de Documentación	10		x	
76	R76	Alta	SI_SBD	Errores de mantenimiento / actualización de HW	Carencia de un plan de mantenimiento preventivo	15			x
77	R77	Alta	SI_SBD	Errores de mantenimiento / actualización de HW	Ausencia de Plan de Gestión de Configuración	15			x
78	R78	Moderada	SI_SBD	Pérdida de Equipos	Carencia de un plan de SI	9		x	
79	R79	Alta	SI_SBD	Indisponibilidad del personal	Dependencia excesiva de personal de gestión de BD	12			x
80	R80	Extrema	SI_SBD	Abuso de privilegios de acceso	Deficiencia en la política de rotación de personal.	25			x
81	R81	Extrema	SI_SBD	Abuso de privilegios de acceso	Ausencia de una fuente de información de perfiles de acceso descritos y autoriz.	25			x
82	R82	Alta	SI_SBD	Acceso no autorizado	Carencia de un sist. de informac. de admin eventos	15			x
83	R83	Alta	SI_SBD	Acceso no autorizado	Carencia de un plan de auditoría de accesos	15			x
84	R84	Moderada	SW_SICDESA	Corte de suministro eléctrico	Deficiencia en las políticas de copias de seguridad	8		x	
85	R85	Alta	SW_SICDESA	Fallo de servicios de comunicaciones	Carencia de una fuente de conocimiento de incidentes	12			x
86	R86	Extrema	SW_SICDESA	Errores de los usuarios	Carencia de un plan de capacitación.	25			x
87	R87	Extrema	SW_SICDESA	Errores de configuración	Ausencia de Plan de Gestión de Configuración	25			x
88	R88	Extrema	SW_SICDESA	Errores de configuración	Ausencia de fuente de inform. de perfil de acceso descrito y autoriz.	20			x
89	R89	Extrema	SW_SICDESA	Fuga de información	Carencia de un plan de SI	20			x
90	R90	Extrema	SW_SICDESA	Introducción de falsa informac.	Carencia de políticas de revisión por muestreo	20			x
91	R91	Extrema	SW_SICDESA	Introducción de falsa	Carencia de un plan de supervisión	20			x

				informac.					
92	R92	Extrema	SW_SICDESA	Alteración de la información	Carencia de políticas de revisión por muestreo	20			x
93	R93	Extrema	SW_SICDESA	Alteración de la información	Carencia de un plan de supervisión	20			x
94	R94	Extrema	SW_SICDESA	Corrupción de la información	Carencia de políticas de revisión por muestreo	20			x
95	R95	Extrema	SW_SICDESA	Corrupción de la información	Carencia de un plan de supervisión	20			x
96	R96	Extrema	SW_SICDESA	Destrucción de la información	Carencia de políticas de revisión por muestreo	20			x
97	R97	Extrema	SW_SICDESA	Destrucción de la información	Carencia de un plan de supervisión	20			x
98	R98	Moderada	SW_SICDESA	Errores de mantenimiento / actualización de SW	Carencia de Documentación	10		x	
99	R99	Moderada	SW_SICDESA	Errores de mantenimiento / actualización de SW	Carencia de un plan de mantenimiento preventivo	10		x	
100	R100	Alta	SW_SICDESA	Errores de mantenimiento / actualización de SW	Ausencia de Plan de Gestión de Configuración	15			x
101	R101	Moderada	SW_SICDESA	Caída del sist. por sobrecarga	Carencia de un sist. de informac. de admin eventos	8		x	
102	R102	Alta	SW_SICDESA	Indisponibilidad del personal	Dependencia excesiva de personal de gestión de BD	12			x
103	R103	Extrema	SW_SICDESA	Abuso de privilegios de acceso	Deficiencia en la política de rotación de personal.	25			x
104	R104	Extrema	SW_SICDESA	Abuso de privilegios de acceso	Ausencia de fuente de inform. de perfil de acceso descrito y autoriz.	20			x
105	R105	Extrema	SW_SICDESA	Acceso no autorizado	Carencia de un sist. de informac. de administ. eventos	20			x
106	R106	Extrema	SW_SICDESA	Ingeniería social	Carencia de Capacitación sobre Ing. Social.	25			x
107	R107	Baja	HW_LCB	Fuego	Carencia de sistemas de seguridad anti incendios	2	x		
108	R108	Baja	HW_LCB	Daños por agua	Carencia de plan concientización de cuidado de equipos	2	x		

109	R109	Baja	HW_LCB	Desastres naturales	Infraestructura inadecuada	1	x		
110	R110	Baja	HW_LCB	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	1	x		
111	R111	Baja	HW_LCB	Condiciones inadecuadas de temperatura o humedad	Carencia de infraestructura adecuada	1	x		
112	R112	Baja	HW_LCB	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	4	x		
113	R113	Baja	HW_LCB	Interrupción de otros serv. y suministros esenciales	Infraestructura inadecuada	2	x		
114	R114	Moderada	HW_LCB	Errores de los usuarios	Carencia de un plan de capacitación	6		x	
115	R115	Moderada	HW_LCB	Errores de configuración	Ausencia de un plan de config. de equipos	6		x	
116	R116	Baja	HW_LCB	Errores de mantenimiento / actualización de HW	Ausencia de un plan de mantenimiento de equipos	1	x		
117	R117	Moderada	HW_LCB	Pérdida de Equipos	Carencia de un plan de SI	9		x	
118	R118	Baja	HW_LCB	Denegación del servicio	Carencia de sist. de inform. de administ. de eventos	2	x		
119	R119	Moderada	SI_SWEB	Fuego	Carencia de sistemas de seguridad anti incendios	10		x	
120	R120	Moderada	SI_SWEB	Daños por agua	Carencia de plan concientiz. del cuidado de equipos	10		x	
121	R121	Baja	SI_SWEB	Desastres naturales	Infraestructura inadecuada	5	x		
122	R122	Moderada	SI_SWEB	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	10		x	
123	R123	Moderada	SI_SWEB	Condiciones inadecuadas de temp. o humedad	Carencia de infraestructura adecuada	10		x	
124	R124	Alta	SI_SWEB	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	12			x
125	R125	Alta	SI_SWEB	Errores de los usuarios	Carencia de un plan de capacitación	15			x
126	R126	Baja	SI_SWEB	Difusión de software dañino	Ausencia de un plan de SI	5	x		
127	R127	Alta	SI_SWEB	Errores de mantenimiento / actualización de HW	Ausencia de un plan de mantenimiento de equipos	15			x
128	R128	Baja	SI_SWEB	Denegación del servicio	Carencia de sist. de inform. de administ.	5	x		

					de eventos				
129	R129	Moderada	SI_SADDS-DNS	Fuego	Carencia de sistemas de seguridad anti incendios	10		x	
130	R130	Moderada	SI_SADDS-DNS	Daños por agua	Carencia de plan concientiz. del cuidado de equipos	10		x	
131	R131	Baja	SI_SADDS-DNS	Desastres naturales	Infraestructura inadecuada	5	x		
132	R132	Moderada	SI_SADDS-DNS	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	10		x	
133	R133	Moderada	SI_SADDS-DNS	Condiciones inadecuadas de temp. o humedad	Carencia de infraestructura adecuada	10		x	
134	R134	Alta	SI_SADDS-DNS	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	12			x
135	R135	Baja	SI_SADDS-DNS	Errores de configuración	Carencia de un plan de capacitación	5	x		
136	R136	Baja	SI_SADDS-DNS	Difusión de software dañino	Ausencia de un plan de SI	5	x		
137	R137	Alta	SI_SADDS-DNS	Errores de mantenimiento / actualización de HW	Ausencia de un plan de mantenimiento de equipos	15			x
138	R138	Moderada	SI_SADDS-DNS	Pérdida de Equipos	Carencia de un plan de SI	9		x	
139	R139	Baja	SI_SADDS-DNS	Denegación del servicio	Carencia de sist. de inform. de administ. de eventos	5	x		
140	R140	Moderada	SI_FW	Fuego	Carencia de sistemas de seguridad anti incendios	10		x	
141	R141	Moderada	SI_FW	Daños por agua	Carencia de plan concientiz. del cuidado de equipos	10		x	
142	R142	Baja	SI_FW	Desastres naturales	Infraestructura inadecuada	5	x		
143	R143	Moderada	SI_FW	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	10		x	
144	R144	Moderada	SI_FW	Condiciones inadecuadas de temperatura o humedad	Carencia de infraestructura adecuada	10		x	
145	R145	Alta	SI_FW	Fallo de servicios de comunicaciones	Carencia de políticas de mantenimiento preventivo	12			x
146	R146	Baja	SI_FW	Errores de configuración	Carencia de un plan de capacitación	5	x		
147	R147	Baja	SI_FW	Difusión de software dañino	Ausencia de un plan de SI	5	x		
148	R148	Alta	SI_FW	Errores de mantenimiento /	Ausencia de un plan de mantenimiento de equipos	15			x

				actualización de HW					
149	R149	Alta	SI_FW	Pérdida de Equipos	Carencia de un plan de SI	15			x
150	R150	Baja	SI_FW	Denegación del servicio	Carencia de sist. de inform. de administ. de eventos	5	x		
151	R151	Moderada	SW_SICAP	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	8		x	
152	R152	Alta	SW_SICAP	Errores de los usuarios	Carencia de un plan de capacitación	15			x
153	R153	Baja	SW_SICAP	Errores de configuración	Ausencia de un plan de config. de equipos	5	x		
154	R154	Extrema	SW_SICAP	Fuga de información	Ausencia de un plan de SI	20			x
155	R155	Extrema	SW_SICAP	Introducción de falsa información	Falta de un plan de SI	20			x
156	R156	Extrema	SW_SICAP	Alteración de la información	Falta de un plan de SI	20			x
157	R157	Extrema	SW_SICAP	Corrupción de la información	Falta de un plan de SI	20			x
158	R158	Extrema	SW_SICAP	Destrucción de la información	Falta de un plan de SI	20			x
159	R159	Moderada	SW_SICAP	Caída del sistema por sobrecarga	Falta de un control de accesos a los recursos	8		x	
160	R160	Extrema	SW_SICAP	Acceso no autorizado	Falta de políticas de control de acceso	20			x
161	R161	Extrema	SW_SICAP	Acceso no autorizado	Cuentas de usuarios mal configuradas	20			x
162	R162	Extrema	SW_SICAP	Ingeniería social	Falta de políticas de seguridad	25			x
163	R163	Moderada	SW_OFI	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	6		x	
164	R164	Moderada	SW_AV	Corte de suministro eléctrico	Falta de equipos de respaldo eléctrico	10		x	
165	R165	Moderada	SW_AV	Errores de configuración	Carencia de un plan de capacitación	8		x	
Conclusiones: Según el cuadro 15, se identifica la tolerancia al riesgo y se resume que 61 riesgos son No Tolerables, por lo tanto, deben ser tratados.									
Elaborado por: Alejandro Navarro							**Fecha elaboración:** 21/05/2019		

FASE 3 - PLANIFICACIÓN Proceso 3.4 - Tratar el riesgo									
Objetivo: Determinar la estrategia para el tratamiento del riesgo y los controles a aplicar									
N°	**Cód. riesgo**	**Magnitud del riesgo**	**Tolerancia**	**Amenaza**	**Estrategia**				**Controles**
					Aceptar	**Mitigar**	**Evitar**	**Transferir**	
1	R80	Extrema	No Tolerable	Abuso de privilegios de acceso		x			Restringir y controlar la asignación y uso de derechos de acceso privilegiado.
2	R81	Extrema	No Tolerable	Abuso de privilegios de acceso		x			Restringir y controlar la asignación y uso de derechos de acceso privilegiado.
3	R103	Extrema	No Tolerable	Abuso de privilegios de acceso		x			Restringir y controlar la asignación y uso de derechos de acceso privilegiado.
4	R104	Extrema	No Tolerable	Abuso de privilegios de acceso		x			Restringir y controlar la asignación y uso de derechos de acceso privilegiado.
5	R82	Alta	No Tolerable	Acceso no autorizado		x			Establecer, documentar y revisar una política de control de acceso
6	R83	Alta	No Tolerable	Acceso no autorizado		x			Establecer, documentar y revisar una política de control de acceso
7	R105	Extrema	No Tolerable	Acceso no autorizado		x			Establecer, documentar y revisar una política de control de acceso
8	R160	Extrema	No Tolerable	Acceso no autorizado		x			Establecer, documentar y revisar una política de control de acceso
9	R161	Extrema	No Tolerable	Acceso no autorizado		x			Establecer, documentar y revisar una política de control de acceso
10	R63	Extrema	No Tolerable	Alteración de la información		x			Implementar un plan de supervisión de la información
11	R92	Extrema	No Tolerable	Alteración de la información		x			Implementar un plan de supervisión de la información
12	R93	Extrema	No Tolerable	Alteración de la información		x			Implementar un plan de supervisión de la información
13	R156	Extrema	No Tolerable	Alteración de la información		x			Implementar un plan de supervisión de la información
14	R64	Alta	No Tolerable	Corrupción de la información		x			Definir e implementar política de copias de seguridad
15	R65	Alta	No Tolerable	Corrupción de la información		x			Definir e implementar política de copias de seguridad
16	R94	Extrema	No Tolerable	Corrupción de la información		x			Definir e implementar política de copias de seguridad
17	R95	Extrema	No Tolerable	Corrupción de la información		x			Definir e implementar política de copias de seguridad
18	R157	Extrema	No Tolerable	Corrupción de la información		x			Definir e implementar política de copias de seguridad
19	R69	Alta	No Tolerable	Degradación de los soportes de almac. de inform.		x			Implementar un sistema de administración de eventos.
20	R68	Alta	No Tolerable	Degradación de los soportes de almac. de inform.		x			Implementar un sistema de administración de eventos.
21	R66	Extrema	No Tolerable	Destrucción de la información		x			Implementar un plan de supervisión de la información.
22	R67	Extrema	No Tolerable	Destrucción de la información		x			Implementar un plan de supervisión de la información.

23	R96	Extrema	No Tolerable	Destrucción de la información		x			Implementar un plan de supervisión de la información.
24	R97	Extrema	No Tolerable	Destrucción de la información		x			Implementar un plan de supervisión de la información.
25	R158	Extrema	No Tolerable	Destrucción de la información		x			Implementar un plan de supervisión de la información.
26	R70	Alta	No Tolerable	Difusión de software dañino		x			Definir políticas de software malintencionado
27	R71	Alta	No Tolerable	Difusión de software dañino		x			Definir políticas de software malintencionado
28	R22	Alta	No Tolerable	Errores de configuración		x			Implementar plan de gestión de configuración de todos los equipos
29	R59	Extrema	No Tolerable	Errores de configuración		x			Implementar plan de gestión de configuración de todos los equipos
30	R87	Extrema	No Tolerable	Errores de configuración		x			Implementar plan de gestión de configuración de todos los equipos
31	R88	Extrema	No Tolerable	Errores de configuración		x			Implementar plan de gestión de configuración de todos los equipos
32	R21	Alta	No Tolerable	Errores de los usuarios		x			Asignación de perfiles de usuario
33	R86	Extrema	No Tolerable	Errores de los usuarios		x			Asignación de perfiles de usuario
34	R125	Alta	No Tolerable	Errores de los usuarios				x	Asignación de perfiles de usuario
35	R152	Alta	No Tolerable	Errores de los usuarios		x			Asignación de perfiles de usuario
36	R76	Alta	No Tolerable	Errores de mantenimiento / actualización de HW		x			Implementar plan de mantenimiento preventivo
37	R77	Alta	No Tolerable	Errores de mantenimiento / actualización de HW		x			Implementar plan de mantenimiento preventivo
38	R127	Alta	No Tolerable	Errores de mantenimiento / actualización de HW		x			Implementar plan de mantenimiento preventivo
39	R137	Alta	No Tolerable	Errores de mantenimiento / actualización de HW		x			Implementar plan de mantenimiento preventivo
40	R148	Alta	No Tolerable	Errores de mantenimiento / actualización de HW		x			Implementar plan de mantenimiento preventivo
41	R100	Alta	No Tolerable	Errores de mantenimiento / actualización de SW		x			Implementar plan de mantenimiento preventivo
42	R19	Alta	No Tolerable	Fallo de servicios de comunicaciones		x			Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red
43	R85	Alta	No Tolerable	Fallo de servicios de comunicaciones		x			Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red
44	R124	Alta	No Tolerable	Fallo de servicios de comunicaciones		x			Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red
45	R134	Alta	No Tolerable	Fallo de servicios de comunicaciones		x			Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red
46	R145	Alta	No Tolerable	Fallo de servicios de comunicaciones		x			Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red
47	R23	Alta	No Tolerable	Fuga de información		x			Definir políticas de SI aprobada por Directorio.
48	R60	Extrema	No Tolerable	Fuga de información		x			Definir políticas de SI aprobada por Directorio.
49	R89	Extrema	No Tolerable	Fuga de información		x			Definir políticas de SI aprobada por Directorio.

50	R154	Extrema	No Tolerable	Fuga de información		x			Definir políticas de SI aprobada por Directorio.
51	R79	Alta	No Tolerable	Indisponibilidad del personal		x			Determinar términos y condiciones del empleo
52	R102	Alta	No Tolerable	Indisponibilidad del personal		x			Determinar términos y condiciones del empleo
53	R106	Extrema	No Tolerable	Ingeniería social				x	Aplicar Ingeniería Social.
54	R162	Extrema	No Tolerable	Ingeniería social		x			Aplicar Ingeniería Social.
55	R20	Alta	No Tolerable	Interrupción de otros serv. y suministros esenciales		x			Implementar un Plan de continuidad del Negocio
56	R61	Alta	No Tolerable	Introducción de falsa información		x			Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS
57	R62	Alta	No Tolerable	Introducción de falsa información		x			Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS
58	R90	Extrema	No Tolerable	Introducción de falsa información		x			Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS
59	R91	Extrema	No Tolerable	Introducción de falsa información		x			Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS
60	R155	Extrema	No Tolerable	Introducción de falsa información		x			Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS
61	R149	Alta	No Tolerable	Pérdida de Equipos		x			Implementar plan de seguridad
Conclusiones: Se determinaron estrategias y controles para el tratamiento del riesgo.									
Elaborado por: Alejandro Navarro									**Fecha elaboración:** 21/05/2019

FASE 4 - SOPORTE Proceso 4.1 - Asignar recursos								
Objetivo: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados								
N°	**Cód. de riesgo**	**Magnitud del riesgo**	**Tolerancia al riesgo**	**Amenaza**	**Estrategia**	**Control**	**Actividad**	**Recursos**
1	R80	Extrema	No Tolerable	Abuso de privilegios de acceso	Mitigar	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso	Personal RRHH, Personal de Infraestructura, redes y comunicaciones
2	R81	Extrema	No Tolerable	Abuso de privilegios de acceso	Mitigar	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso	Personal RRHH, Personal de Infraestructura, redes y comunicaciones
3	R103	Extrema	No Tolerable	Abuso de privilegios de acceso	Mitigar	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso	Personal RRHH, Personal de Infraestructura, redes y comunicaciones
4	R104	Extrema	No Tolerable	Abuso de privilegios de acceso	Mitigar	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso	Personal RRHH, Personal de Infraestructura, redes y comunicaciones
5	R82	Alta	No Tolerable	Acceso no autorizado	Mitigar	Establecer, documentar y revisar una política de control de acceso	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
6	R83	Alta	No Tolerable	Acceso no autorizado	Mitigar	Establecer, documentar y revisar una política de control de acceso	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
7	R105	Extrema	No Tolerable	Acceso no autorizado	Mitigar	Establecer, documentar y revisar una política de control de acceso	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
8	R160	Extrema	No Tolerable	Acceso no autorizado	Mitigar	Establecer, documentar y revisar una política de control de acceso	Solicitar el uso de credenciales por área y usuario.	Credenciales de identificación.
9	R161	Extrema	No Tolerable	Acceso no autorizado	Mitigar	Establecer, documentar y revisar una política de control de acceso	Solicitar el uso de cred. por área y usuario.	Credenciales de identificación.
10	R63	Extrema	No Tolerable	Alteración de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitud para selección de proveedor en SGSI	Especialista en gestión de servicios ITIL
11	R92	Extrema	No Tolerable	Alteración de la	Mitigar	Implementar un plan de	Solicitud para selección	Especialista en gestión

				información		supervisión de la información.	de proveedor en SGSI	de servicios ITIL
12	R93	Extrema	No Tolerable	Alteración de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitud para selección de proveedor en SGSI	Especialista en gestión de servicios ITIL
13	R156	Extrema	No Tolerable	Alteración de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitud para selección de proveedor en SGSI	Especialista en gestión de servicios ITIL
14	R64	Alta	No Tolerable	Corrupción de la información	Mitigar	Definir e implementar política de copias de seguridad	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
15	R65	Alta	No Tolerable	Corrupción de la información	Mitigar	Definir e implementar política de copias de seguridad	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
16	R94	Extrema	No Tolerable	Corrupción de la información	Mitigar	Definir e implementar política de copias de seguridad	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
17	R95	Extrema	No Tolerable	Corrupción de la información	Mitigar	Definir e implementar política de copias de seguridad	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
18	R157	Extrema	No Tolerable	Corrupción de la información	Mitigar	Definir e implementar política de copias de seguridad	Comprar, instalar y configurar un servidor de archivos.	Servidor de archivos
19	R69	Alta	No Tolerable	Degradación de los soportes de almac. de inform.	Mitigar	Implementar un sistema de administración de eventos.	Comprar, instalar y configurar un servidor de archivos	Servidor de archivos
20	R68	Alta	No Tolerable	Degradación de los soportes de almac. de inform.	Mitigar	Implementar un sistema de administración de eventos.	Comprar, instalar y configurar un servidor de archivos	Servidor de archivos
21	R66	Extrema	No Tolerable	Destrucción de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitar capacitación en recuperación de la información.	Curso de capacitación. Personal experto en recuperación de inform. y restauración del sistema
22	R67	Extrema	No Tolerable	Destrucción de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitar capacitación en recuperación de la información.	Curso de capacitación. Personal experto en recuperación de Inf. y restauración del sist.
23	R96	Extrema	No Tolerable	Destrucción de la	Mitigar	Implementar un plan de	Solicitar capacitación	Curso de capacitación

				información		supervisión de la información.	en recuperación de la información.	Personal experto en recuperación de inform. y restauración del sistema.
24	R97	Extrema	No Tolerable	Destrucción de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitar capacitación en recuperación de la información.	Curso de capacitación. Personal experto en recuperación de inform. y restauración del sistema.
25	R158	Extrema	No Tolerable	Destrucción de la información	Mitigar	Implementar un plan de supervisión de la información.	Solicitar capacitación en recuperación de la información.	Curso de capacitación. Personal experto en recuperación de información y restauración del sistema.
26	R70	Alta	No Tolerable	Difusión de software dañino	Mitigar	Definir políticas de software malintencionado	Solicitar configuración y actualización de antivirus para la SI.	Personal de soporte técnico. Proveedor de Antivirus
27	R71	Alta	No Tolerable	Difusión de software dañino	Mitigar	Definir políticas de software malintencionado	Solicitar configuración y actualización de antivirus para la SI.	Personal de soporte técnico. Proveedor de Antivirus
28	R22	Alta	No Tolerable	Errores de configuración	Mitigar	Implementar plan de gestión de configuración de todos los equipos	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
29	R59	Extrema	No Tolerable	Errores de configuración	Mitigar	Implementar plan de gestión de configuración de todos los equipos	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
30	R87	Extrema	No Tolerable	Errores de configuración	Mitigar	Implementar plan de gestión de configuración de todos los equipos	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
31	R88	Extrema	No Tolerable	Errores de configuración	Mitigar	Implementar plan de gestión de configuración de todos los equipos	Solicitud para selección de proveedor en gestión de servicios	Especialista en gestión de servicios ITIL

							ITIL	
32	R21	Alta	No Tolerable	Errores de los usuarios	Mitigar	Asignación de perfiles de usuario	Configurar Servidor ADDS	Personal de Redes
33	R86	Extrema	No Tolerable	Errores de los usuarios	Mitigar	Asignación de perfiles de usuario	Configurar Servidor ADDS	Personal de Redes
34	R125	Alta	No Tolerable	Error de los usuarios	Transferir	Asignación de perfiles de usuario	Config. Servidor ADDS	Personal de Redes
35	R152	Alta	No Tolerable	Errores de los usuarios	Mitigar	Asignación de perfiles de usuario	Configurar Servidor ADDS	Personal de Redes
36	R76	Alta	No Tolerable	Errores de mantenimiento / actualización de HW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
37	R77	Alta	No Tolerable	Errores de mantenimiento / actualización de HW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
38	R127	Alta	No Tolerable	Errores de mantenimiento / actualización de HW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
39	R137	Alta	No Tolerable	Errores de mantenimiento / actualización de HW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
40	R148	Alta	No Tolerable	Errores de mantenimiento / actualización de HW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
41	R100	Alta	No Tolerable	Errores de mantenimiento / actualización de SW	Mitigar	Implementar plan de mantenimiento preventivo	Elaborar plan de mantenimiento preventivo	Personal de Soporte Técnico
42	R19	Alta	No Tolerable	Fallo de servicios de comunicaciones	Mitigar	Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
43	R85	Alta	No Tolerable	Fallo de servicios de comunicaciones	Mitigar	Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
44	R124	Alta	No Tolerable	Fallo de servicios de comunicaciones	Mitigar	Identificar mecanismos de seg., niveles de servicio y requisitos de	Solicitud para selección de proveedor en	Especialista en gestión de servicios ITIL

						gestión de servicios de red	gestión de servicios ITIL	
45	R134	Alta	No Tolerable	Fallo de servicios de comunicaciones	Mitigar	Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
46	R145	Alta	No Tolerable	Fallo de servicios de comunicaciones	Mitigar	Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios de red	Solicitud para selección de proveedor en gestión de servicios ITIL	Especialista en gestión de servicios ITIL
47	R23	Alta	No Tolerable	Fuga de información	Mitigar	Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	Consultor en SI.
48	R60	Extrema	No Tolerable	Fuga de información	Mitigar	Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	Consultor en SI.
49	R89	Extrema	No Tolerable	Fuga de información	Mitigar	Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	Consultor en SI.
50	R154	Extrema	No Tolerable	Fuga de información	Mitigar	Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	Consultor en SI.
51	R79	Alta	No Tolerable	Indisponibilidad del personal	Mitigar	Determinar términos y condiciones del empleo.	Solicitar al área de RRHH cubrir todas las plazas	Base de datos de personal calificado.
52	R102	Alta	No Tolerable	Indisponibilidad del personal	Mitigar	Determinar términos y condiciones del empleo.	Solicitar al área de RRHH cubrir todas las plazas	Base de datos de personal calificado.
53	R106	Extrema	No Tolerable	Ingeniería social	Transferir	Aplicar Ingeniería Social.	Solicitar capacitación sobre Ingeniería Social.	Contratar profesional en seg. de la inf. para capacitar al personal
54	R162	Extrema	No Tolerable	Ingeniería social	Mitigar	Aplicar Ingeniería Social.	Solicitar capacitación sobre Ingeniería Social.	Contratar profesional en seg. de la inf. para capacitar al personal
55	R20	Alta	No Tolerable	Interrupción de serv. y sumin. esenciales	Mitigar	Implementar un Plan de continuidad del Negocio	Elaborar proy. del plan de contin. del Negocio	Personal de riesgos. Consultor en Riesgos
56	R61	Alta	No Tolerable	Introducción de falsa información	Mitigar	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	Software de supervisión de eventos de Windows. Supervisor de eventos.

57	R62	Alta	No Tolerable	Introducción de falsa información	Mitigar	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	Software de supervisión de eventos de Windows. Supervisor de eventos.
58	R90	Extrema	No Tolerable	Introducción de falsa información	Mitigar	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	Software de supervisión de eventos de Windows. Supervisor de eventos.
59	R91	Extrema	No Tolerable	Introducción de falsa información	Mitigar	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	Software de supervisión de eventos de Windows. Supervisor de eventos.
60	R155	Extrema	No Tolerable	Introducción de falsa información	Mitigar	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	Software de supervisión de eventos de Windows. Supervisor de eventos.
61	R149	Alta	No Tolerable	Pérdida de Equipos	Mitigar	Definir políticas de SI aprobada por Directorio	Elaborar plan de SI	Consultor en seguridad de la inf.
Conclusiones: Se determinó actividades y recursos necesarios para el cumplimiento de los controles seleccionados.								
Elaborado por: Alejandro Navarro							**Fecha elaboración:** 21/05/2019	

FASE 4 - SOPORTE Proceso 4.2 - Capacitar y concienciar							
Objetivo: Definir el plan de capacitación y concienciación del personal de la EPS.							
Tipo	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Fecha**
Capacitación.	Evaluar la competencia del personal.	Se ha aprobado el plan de concientización, capacitación y evaluación.	**Responsable:** Oficial de SI. **Convocado:** Personal que participa del SGSI.	**Documentos:** - Plan de concientización, capacitación y evaluación. - Evaluaciones para el personal.	- Diseñar pruebas para evaluar personal elegido para cumplir roles en el SGSI. - Ejecutar la evaluación del personal.	**Resultado esperado:** Resultados de evaluación de personal.	Inicio: 15-07 Fin: 31-07
Capacitación.	Charlas de Concienciación.	Se ha aprobado el plan de concientización, capacitación y evaluación.	**Responsable:** Oficial de SI. **Convocado:** Personal de la organización.	**Documentos:** - Plan de concientización, capacitación y evaluación. - Temario de la concientización. **Presentación:** Concientización en SI. **Ubicación:** Sala de reuniones de la EPS. **Tecnología:** Laptop y proyector.	- Ejecutar la charla de concientización general - Grupo 1. - Ejecutar la charla de concientización general - Grupo 2. - Ejecutar la charla de concientización general (rezagados).	**Resultado esperado:** Listas de asistencia a la presentación Personal concienciado.	Inicio: 15-07 Fin: 15-07
Capacitación.	Evaluar la competencia del personal.	- Se ha aprobado el plan de concientización, capacitación y evaluación. - Se ha completado la primera evaluación de la competencia del personal.	**Responsable:** Oficial de SI. **Convocado:** Personal que participa del SGSI.	**Documentos:** - Plan de concientización, capacitación y evaluación. - Evaluaciones para el personal. **Presentación:** Roles, responsabilidades y actividades del SGSI. **Ubicación:** Sala de reuniones de la EPS. **Tecnología:** Laptop y proyector.	- Identificar personal que requiere mejorar o adquirir ciertas competencias, en base a los resultados de las evaluaciones previas. - Ejecutar capacitaciones al personal identificado. - Ejecutar la reevaluación del personal capacitado.	**Resultado esperado:** - Listas de asistencia a la presentación. - Personal del sistema competente.	Inicio: 15-07 Fin: 15-07
Conclusiones: Se elaboró el plan de las acciones a desarrollar para capacitar y concientizar al personal de la EPS, así como también para evaluar si se ha logrado realizar con efectividad.							
Elaborado por: Alejandro Navarro						**Fecha elaboración:** 21/05/2019	

FASE 4 - SOPORTE Proceso 4.3 - Determinar la comunicación del SGSI							
Objetivo: Dar a conocer a las partes interesadas los controles a implementar							
N°	**Control**	**Actividad**	**Riesgo asociado**	**A quien comunicar**	**Responsable de comunicar**	**Medio de comunicación**	**Fecha**
1	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso.	R80, R81, R103, R104	Área de RRHH Área de Informática	Gerencia General	Documento escrito, Reunión informativa	03/06/2019
2	Establecer, documentar y revisar una política de control de acceso.	Solicitar el uso de credenciales por área y usuario.	R82, R83, R105, R160, R161	Todo el Personal	Área de RRHH	Documento escrito, Reunión informativa	03/06/2019
3	Implementar un plan de supervisión de la información.	Solicitar selección de proveedor en SGSI.	R63, R92, R93, R156	Área de Administ.	Oficial de SI	Documento escrito	14/06/2019
		Solicitar capacitación en recuperación de la información.	R66, R67, R96, R97, R158	Área de Administ.	Área de Informática	Documento escrito	03/06/2019
4	Definir e implementar política de copias de seguridad.	Comprar, instalar y configurar un servidor de archivos.	R64, R65, R94, R95, R157	Área de Administ., Área de Informática	Oficial de SI	Reunión informativa	14/06/2019
5	Implementar un sistema de administración de eventos.		R69, R68	Área de Informática	Oficial de SI	Documento escrito	21/06/2019
6	Definir políticas de software malintencionado.	Solicitar configuración y actualización de antivirus para la SI.	R70, R71	Área de Informática	Oficial de SI	Documento escrito	21/06/2019
7	Implementar plan de gestión de configuración de todos los equipos.	Solicitud para selección de proveedor en gestión de servicios ITIL.	R22, R59, R87, R88	Área de Administ.	Área de Informática	Documento escrito	14/06/2019
8	Asignación de perfiles de usuario.	Configurar Servidor ADDS.	R21, R86, R125, R152	Área de Informática	Área de RRHH	Documento escrito, Reunión informativa	07/06/2019
9	Implementar plan de mantenimiento preventivo.	Elaborar plan de mantenimiento preventivo.	R76, R77, R127, R137, R148, R100	Área de Informática	Jefe de Informática	Documento escrito	28/06/2019
10	Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de servicios de red.	Solicitud para selección de proveedor en gestión de servicios ITIL.	R19, R85, R124, R134, R145	Área de Administ.	Área de Informática	Documento escrito	14/06/2019

11	Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	R23, R60, R89, R154, R149	Área de Administ.	Oficial de SI	Documento escrito, Reunión informativa	28/06/2019
12	Determinar términos y condiciones del empleo.	Solicitar al área de RRHH cubrir todas las plazas.	R79, R102	Área de RRHH	Gerencia General	Documento escrito	28/06/2019
13	Aplicar Ingeniería Social.	Solicitar capacitación sobre Ingeniería Social.	R106, R162	Área de Administ.	Área de Informática	Documento escrito	07/06/2019
14	Implementar un Plan de continuidad del Negocio	Elaborar proyecto del plan de continuidad del Negocio	R20	Área de Administ.	Oficial de SI	Documento escrito, Reunión informativa	28/06/2019
15	Implementar política de supervisión por muestreo para los procesos comerciales de la EPS	Solicitar la adquisición de software de supervisión de eventos de Windows.	R61, R62, R90, R91, R155	Área de Administ.	Área de Informática	Documento escrito	14/06/2019
Conclusiones: Se obtuvieron quince (15) controles para ser comunicados a las áreas respectivas de EPSEL SA							
Elaborado por: Alejandro Navarro						**Fecha elaboración:** 21/05/2019	

FASE 5 - OPERACIÓN Proceso 5.1 - Planificar y controlar la operación del SGSI			
Objetivo: Alinear los controles seleccionados con los objetivos de seguridad establecidos por la EPS			
Aprobado por: Maricarmen Soto		**Fecha aprobación:** 21/05/2019	
Objetivo de seguridad	**Control de seguridad**	**Actividad de control**	**Responsable del control**
• Proporcionar un acceso adecuado a las partes interesadas, internas y externas, a fin de que se alcancen los objetivos del negocio.	**C1:** Definir políticas de SI aprobada por Directorio.	Elaborar plan de SI.	Oficial de SI
• Garantizar que el acceso de emergencia esté debidamente permitido y revocado en el momento oportuno.	**C2:** Asignación de perfiles de usuario.	Configurar Servidor ADDS.	Gerente de RRHH
• Realizar regularmente una verificación de antecedentes de todos los empleados y las personas en puestos clave. • Obtener información sobre el personal clave en puestos de SI.	**C3:** Determinar términos y condiciones del empleo.	Solicitar al área de RRHH cubrir todas las plazas.	Gerente General
• Desarrollar un plan de sucesión para todos los puestos clave relacionados con la SI. • Verificar si todo el personal de SI tiene las habilidades pertinentes y las certificaciones afines, vigentes.	**C4:** Aplicar Ingeniería Social.	Solicitar capacitación sobre Ingeniería Social.	Gerente de Administración
Proporcionar orientación relativa a: • Protección de ubicaciones físicas • Controles ambientales que proporcionen capacidad a las operaciones de soporte. Indirectamente, la política contribuye a la optimización de los costes de los seguros.	**C5:** Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Coordinar con RRHH, crear perfiles de acceso.	Gerente General
	C6: Establecer, documentar y revisar una política de control de acceso.	Solicitar el uso de credenciales por área y usuario.	Gerente de RRHH
Responder a los incidentes de una manera oportuna para recuperar las actividades de la EPS.	**C7:** Implementar un Plan de continuidad del Negocio.	Elaborar proyecto del plan de continuidad del Negocio	Oficial de SI
	C8: Definir e implementar política de copias de seguridad.	Comprar, instalar y configurar un servidor de archivos.	Oficial de SI
	C9: Implementar un sistema de administración de eventos.		Oficial de SI
	C10: Implementar plan de gestión de configuración de todos los equipos.	Solicitud para selección de proveedor en gestión de servicios ITIL.	Jefe de Informática
	C11: Definir políticas de software	Solicitar configuración y	Oficial de SI

	malintencionado.	actualización de antivirus para la SI.	
	C12: Implementar un plan de supervisión de la información.	Solicitar selección de proveedor en SGSI. Solicitar capacitación en recuperación de la información.	Oficial de SI, Jefe de Informática
	C13: Implementar plan de mantenimiento preventivo.	Elaborar plan de mantenimiento preventivo.	Jefe de Informática
	C14: Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de servicios de red.	Solicitud para selección de proveedor en gestión de servicios ITIL.	Jefe de Informática
	C15: Implementar política de supervisión por muestreo para los procesos comerciales de la EPS.	Solicitar la adquisición de software de supervisión de eventos de Windows.	Gerente de Administración
Conclusiones: Se alinearon los quince (15) controles seleccionados y sus actividades con los objetivos de seguridad establecidos por EPSEL SA en el proceso 2.2.			
Elaborado por: Alejandro Navarro		**Fecha elaboración:** 21/05/2019	

FASE 6 - EVALUACIÓN DEL DESEMPEÑO Proceso 6.1 - Monitorear, analizar y evaluar el SGSI						
Objetivo: Establecer un plan de monitoreo						
N°	**Controles**	**Método de monitoreo**	**Valor del control**	**Estado**	**Responsable**	**Periodo**
1	Definir políticas de SI aprobada por Directorio.	Informe	2	Cumple parcialmente	Oficial de SI	Mensual
2	Asignación de perfiles de usuario.	Informe	1	Cumple satisfactoriamente	Gerente de RRHH	Anual
3	Determinar términos y condiciones del empleo.	Informe	2	Cumple parcialmente	Gerente General	Semestral
4	Aplicar Ingeniería Social.	Evaluación	2	Cumple parcialmente	Gerente de Administración	Mensual
5	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Visita de campo	1	Cumple satisfactoriamente	Gerente General	Diario
6	Establecer, documentar y revisar una política de control de acceso.	Informe	1	Cumple satisfactoriamente	Gerente de RRHH	Anual
7	Implementar un Plan de continuidad del Negocio.	Informe	2	Cumple parcialmente	Oficial de SI	Anual
8	Definir e implementar política de copias de seguridad.	Visita de campo, Registro	1	Cumple satisfactoriamente	Oficial de SI	Mensual
9	Implementar un sistema de administración de eventos.	Reportes, Registro	2	Cumple parcialmente	Oficial de SI	Diario
10	Implementar plan de gestión de configuración de todos los equipos.	Informe, Registro	2	Cumple parcialmente	Jefe de Informática	Semestral
11	Definir políticas de software malintencionado.	Informe, Evaluación	2	Cumple parcialmente	Oficial de SI	Semanal
12	Implementar un plan de supervisión de la información.	Informe, Reportes	2	Cumple parcialmente	Oficial de SI, Jefe de Informática	Diario
13	Implementar plan de mantenimiento preventivo.	Informe	1	Cumple satisfactoriamente	Jefe de Informática	Semestral
14	Identificar los mecanismos de SI, los niveles de servicio y los requisitos de gestión de servicios de red.	Informe	2	Cumple parcialmente	Jefe de Informática	Semestral
15	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS.	Reportes, Registros	2	Cumple parcialmente	Gerente de Administración	Diario
Conclusiones: De los quince (15) controles seleccionados se observa que: 05 controles se cumplen satisfactoriamente, 10 se están cumpliendo parcialmente.						
Elaborado por: Alejandro Navarro					**Fecha elaboración:** 21/05/2019	

FASE 7 - MEJORA CONTINUA Proceso 7.1 - Mejorar el SGSI					
Objetivo: Establecer un plan de mejora continua					
N°	**Riesgos involucrados**	**Controles**	**Actividades**	**Fecha de inicio**	**Fecha de fin**
1	R23, R60, R89, R154, R149	Definir políticas de SI aprobada por Directorio.	Revisar periódicamente el plan de SI.	01/07/2018	31/07/2018
2	R79, R102	Determinar términos y condiciones del empleo.	Verificar que el área de RRHH cubra todas las plazas.	08/07/2018	12/07/2018
3	R106, R162	Aplicar Ingeniería Social.	Comprobar conocimientos sobre Ingeniería Social	08/07/2018	12/07/2018
4	R20	Implementar un Plan de continuidad del Negocio.	Revisar periódicamente el plan de continuidad del Negocio	01/07/2018	31/07/2018
5	R69, R68	Implementar un sistema de administración de eventos.	Monitorear y reconfigurar el servidor de archivos.	15/07/2018	19/07/2018
6	R22, R59, R87, R88	Implementar plan de gestión de configuración de todos los equipos.	Revisar periódicamente la gestión de servicios ITIL.	01/07/2018	31/07/2018
7	R70, R71	Definir políticas de software malintencionado.	Revisar y actualizar el antivirus para la SI.	15/07/2018	19/07/2018
8	R63, R92, R93, R156, R66, R67, R96, R97, R158	Implementar un plan de supervisión de la información.	Analizar la SI. Comprobar conocimientos en recuperación de la información.	22/07/2018	26/07/2018
9	R19, R85, R124, R134, R145	Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de servicios de red.	Revisar periódicamente la gestión de servicios ITIL.	01/07/2018	31/07/2018
10	R61, R62, R90, R91, R155	Implementar política de supervisión por muestreo para los diferentes procesos comerciales de la EPS.	Monitorear software de supervisión de eventos de Windows.	22/07/2018	26/07/2018
Conclusiones: El plan de mejora continua se ha establecido solo con los diez (10) controles que cumplen parcialmente con su desempeño (valor de control 2).					
Elaborado por: Alejandro Navarro				**Fecha elaboración: 21/05/2019**	