UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Modelo de seguridad de la información basado en la normativa ISO/IEC 27001 :2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SITEMAS

AUTOR:

Ticona Bustinza, Osmar Raúl (ORCID: 0000-0003-4061-7681)

ASESOR:

Dr. Alfredo Daza Vergaray (ORCID: 0000-0002-2259-1070)

LÍNEA DE INVESTIGACIÓN:

Auditoria de sistemas y seguridad de la información.

LIMA — PERÚ

2022

DEDICATORIA

A mis padres por haberme formado como la persona que soy mucho de lo logrado se lo debo a ellos que me motivaron a cumplir un logro. Me formaron con reglas y algunas libertades, pero siempre me ayudaron y me motivaron para cumplir las metas que me propuse.

AGRADECIMIENTO

Agradecimiento a la empresa SEVEROX SAC por brindarme la información y permisos necesarios que fueron esenciales para llevar a cabo el proceso de investigación. A la persona encargada que compartió su conocimiento y ánimos para cumplir esta meta de convertirme en profesional.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

El presente trabajo de investigación tiene como objetivo determinar el efecto que tiene un modelo de seguridad de la información basado en la normativa ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú S.A.C, Arequipa, 2021.

En la investigación realizada se consideró como muestra 32 trabajadores de la empresa Severox Perú S.A.C teniendo como hipótesis del trabajo de investigación establecer un modelo para la seguridad de la información basado en la normativa ISO/IEC 27001:2013 que tiene un efecto significativo en la mitigación de los riesgos de los activos de la información. Podemos confluir que el trabajo de investigación logro demostrar que la implementación de un modelo se seguridad de la información basada en la norma ISO/IEC 27001:2013 tiene un efecto positivo en la mitigación de los riesgos de los activos de la información en la empresa Severox Perú S.A.C.

Palabras Clave: modelo de seguridad de la información, normativa ISO/27001:2013, riesgos de los activos de la información, amenazas y vulnerabilidades.

ABSTRACT

The objective of this research work is to determine the effect of an information security model based on the ISO/IEC 27001:2013 standard to mitigate the risks of information assets in the private entity Severox Perú SAC, Arequipa, 2021.

In the investigation carried out, 32 workers of the company Severox Perú SAC were considered as a sample, having as a hypothesis of the research work to establish a model for information security based on the ISO / IEC 27001: 2013 standard that has a significant effect in the mitigation information asset risks. We can conclude that the research work was able to demonstrate that the implementation of an information security model based on the ISO / IEC 27001: 2013 standard has a positive effect in mitigating the risks of information assets in the Severox company. Peru S.A.C.

Keywords: information security model, ISO/27001:2013 standard, risks of information assets, threats and vulnerabilities.

I. INTRODUCCIÓN

En la actualidad se han desarrollado grandes avances tecnológicos y con ello también grandes amenazas, es por ello que el manejo y resguarda de la información se convierte en un gran inconveniente, al no tener control y ninguna estandarización en procedimientos cónsonos para manejar la protección de la información ya que podemos decir que el bien más preciado de las diferentes organizaciones o empresas es la información que maneja y es por ello que se necesita un adecuada manipulación y resguardo de este activo (Medina Iriarte, 2006).

Según la investigación (BlackBerry, 2020) observo diversos procedimientos que atañen la SI, los más importantes por el momento en 2020 y los temas que se presentan y afectarán en 2024. El estudio permitió generar una base de datos en base a las amenazas que se presentan en las diferentes industrias tecnológicas y corporaciones. El informe referencio el cambio de la seguridad de la información en épocas de Covid-19 y como se modificó la seguridad de la información en las industrias tecnológicas y corporaciones del mundo, esto permitió adaptar nuevos procesos. para mitigar las distintas amenazas que se generaron en las diferentes industrias, hasta el momento los sistemas operativos tales como Windows, MacOS y Linux, son los que han recibido grandes cantidades de ataques cibernéticos, lo cual permitió mostrar las diferentes vulnerabilidades de estos sistemas y lo que se quiere lograr es minimizar los ataques teniendo como precedente la base generada.

En el mundo de los negocios, existe una tendencia general a tratar los activos tangibles solo como activos comerciales: muebles, máquinas, servidores, etc. Sin embargo, no hay que olvidar que existen activos intangibles como la cartera de clientes, los intereses, el conocimiento empresarial, la propiedad intelectual o la reputación. Todos estos son parte de nuestra inteligencia comercial y se encuentran entre los activos más importantes de nuestra organización. (Instituto Nacional de Ciberseguridad, 2010).

La seguridad de la información, corresponde un problema de vital importancia tanto para los diferentes sectores tanto empresarial como público. Hoy en día viene siendo uno de los problemas actuales que se da en las instituciones del sector público y privadas, esto ha conllevado a luchar constantemente por proteger información y datos que son activos esenciales. Y los principales factores que atentan la seguridad de información de forma física y digital.

Según (Pérez, 2017) La enorme importancia que tiene hoy en día el hecho de resguardar los información relevante y el poder que implica el uso de esta información es un tema muy delicado que muchos usuarios desconocen. Esto conlleva a que estos usuarios; que no tiene conocimiento generen un portal de acceso al activo de la información y esto se da por medio del acceso que tiene los usuarios a portales de poca reputación y sin protocolos de seguridad, permitiendo que puedan acceder a la institución o empresa por medio de ese canal.

Cada vez que la tecnología mejora y evoluciona, evidencia diferentes nuevos riesgos que comprometen la forma en que se protege la información, como (malware, ransomware, hackeos, manipulaciones, etc.) y posibles vulnerabilidades a estas mismas amenazas (Instituto Español de Estudios Estratégicos, 2010).

Muchas Instituciones internacionales enfrentan varios problemas para proteger su información porque se colocan de manera vulnerable y en riesgo de perder su activo que es vital para la empresa. Es por ello que, en el Perú, para implementar y gestionar la SI, se consideran tres principios básicos de preservación de la información tales como la confiabilidad, integridad y disponibilidad. Esto de acuerdo a las especificaciones de las normas 27001:2013.(ISOTools, 2019).

La empresa Severox Perú contempla mecanismos de difusión tanto física como digital, por lo que sus activos tangibles e intangibles contemplan vulnerabilidades. Por consiguiente, el objetivo de este estudio fue identificar posibles riesgos. activos de seguridad de la información para que estos riesgos puedan ser mitigados Análisis previo y posterior a la falla para determinar el

impacto del modelo de SI, basado en las normas 27001, para reducir al mínimo el riesgo de los activos de seguridad de la información de la empresa Severox Perú SAC.

El problema general que tiene Severox Perú S.A.C es poder determinar ¿cuál es la influencia de modelo de SI, basado en la normativa ISO/IEC 270001:2013, para poder atenuar los riesgos de los activos de información en la empresa Severox Perú S.A.C?

Por otro lado, los problemas específicos que han surgido en Severox Perú SAC plantearán las siguientes preguntas: ¿Cómo afecta el modelo de SI, basado en la norma ISO / IEC 27001: 2013 a la aminoración de amenazas a los activos de información en Severox Perú SAC? En la cual se analizarán los siguientes indiciadores: Disponibilidad del personal, salida de información, entrada de información falsa, variación de la información, corruptela de la información y destrozo de la información. Otra pregunta es, ¿cuál es el impacto del modelo de SI, basado en la norma ISO / IEC 27001: 2013 en la mitigación de las vulnerabilidades de los activos de información de Severox Perú SAC? En la cual se analizarán los siguientes indiciadores: Incidentes de seguridad de la información, privilegios de información excesivos, acceso no autorizado, seguridad física del entorno y mantenimiento de todos los sistemas.

Esto permite generar el objetivo general, que es determinar la identidad del modelo de SI, de acuerdo con la norma ISO / IEC 27001: 2013, con el fin de reducir el riesgo de los activos de información de la empresa Severox Perú SAC.

Considerar como objetivo específico el establecer un modelo de SI y determinar su impacto para aminorar las amenazas a los activos de información de Severox Perú SAC, y establecer un modelo de SI, y determinar su impacto para mitigar las vulnerabilidades de los activos de información de la empresa Severox Perú SAC.

Es por esto que en este estudio se utiliza la norma de SI, ISO/IEC 27001:2013 con el propósito de seguridad de los activos de información, para identificar diferentes niveles de riesgo de los activos de información para mejorar la

seguridad de la información. Activos como equipos y sistemas utilizados por la empresa Severox Perú SAC.

Se puede decir que, bajo el supuesto general, hemos establecido un modelo de SI, basado en la norma ISO/IEC 27001:2013, el cual ha incidido significativamente en la reducción del riesgo a la información de la empresa Severox Perú SAC.

Por otro lado, el supuesto específico es establecer un modelo de SI, basado en la norma ISO / IEC 27001: 2013, que incide directamente en la mitigación de las amenazas a los activos de información de la empresa Severox Perú SAC, y establece un modelo de seguridad de la información basado en la norma estándar 27001. Para aminorar las vulnerabilidades de los activos de información de la empresa Severox Perú SAC.

Por otro lado, tenemos una variable independiente, “Sistema de Gestión de Seguridad de la Información”. ella se encuentran las dimensiones (confiabilidad, integridad y disponibilidad). Y una variable dependiente de ella. Que son los riesgos de los activos de información que contiene las siguientes dimensiones (amenazas y vulnerabilidades).

II.MARCO TEÓRICO

En el siguiente punto tenemos los antecedentes a nuestra problemática en el entorno nacional:

Lo implementado sigue los requisitos de la norma internacional 27001:2013 que define los objetivos del plan de implementación de sistemas encargados de aspectos de seguridad en la información, que gestionan la seguridad de información en el plano público. Se tomaron muestras de todos los empleados de las empresas del sector público. Por tanto, la ejecución de estos sistemas han de considerar los intereses de la entidad, ya que mejora la seguridad del sistema de información y contribuye al logro de los objetivos de mejora.(Cruz Diaz & Fukusaki Infantas, 2017).

Según autor (Yañez, 2017), el propósito de esta investigación es determinar el efecto de aplicar la norma internacional 27001 a los expedientes académicos de la institución en estudio. La investigación realizada está orientada a aplicaciones y tiene un diseño experimental pre experimental. El total está compuesto por 26 registros de índices de riesgo y 26 registros de índices de cambios autorizados, y el muestreo es un censo. La observación, fue la técnica de recopilación de datos, por medio de una ficha de observación. Los resultados de este estudio confirmaron que la aplicación de la norma internacional 27001 tuvo un impacto positivo y en cuanto a cambios de autorización, lo redujo de la etapa de pre prueba al 80,8%. Después de las pruebas y con respecto a los riesgos, se redujeron en un 19%.

En trabajo de investigación de los autores (Luna Castillo, Francisco Daniel, Prado Correa, 2020) Podría decirse que el objetivo de su investigación fue recomendar controles seleccionados basados en el (SGSI) existente para la División Piura de la Agencia Regional de Empleo y Promoción Laboral. En el análisis de información de la Institución, a través de encuestas y registros, se determinó que existían 30 vulnerabilidades y 20 riesgos. Se utilizó Magerit para en la mejora continua; se han seleccionado 75 controles adaptativos para estos riesgos a través de una declaración de aplicabilidad. Luego, dependiendo del control

seleccionado, se introducen controles y políticas de seguridad. El SGSI requiere que las entidades planifiquen el uso aceptable de los activos y establezcan mecanismos para tratar adecuadamente los accidentes a través de un plan de tratamiento de riesgos.

Según los autores (Vásquez Zevallos, José Luis Delgado Saavedra, 2019) nos informa que se ha desarrollado un modelo de “SGSI” el cual es idóneo para la pequeña y mediana empresa con base en la norma ISO 27001. Desde su implementación y mantenimiento. Dado que la implementación de ISO 27001 requiere un costo muy alto, se intentó aplicar la norma en distintas empresas dado su tamaño. Para obtener información, las personas piensan que es conveniente utilizar encuestas y otras técnicas para la interpretación de seguimiento; y de esta manera medir la realidad de los problemas soportados por la norma ISO 27001, se pueden identificar defectos para mejorar la seguridad y confiabilidad de nivel del SI, de Berendson Natación SRL.

Según los autores, muestran que los resultados se obtienen minimizando los riesgos por medio de un plan de seguridad de la información ya que en el sector público se basan de acuerdo a la ISO/IEC 27001:2008 (Fernández Peñaloza & Pacheco Vargas, 2014).

Según los autores (Sota; Mechan, 2018), El objetivo del proyecto fue implementar controles en la empresa según ISO/IEC 270001. Para ello implementaron mecanismos para mejorar un (SGSI) en la empresa en estudio, haciendo énfasis al método Deming. Teniendo como principal evidencia que es posible implementar mejoras en la SI, es por ello que la empresa ha determinado el estado de cumplimiento inicial y final de la norma ISO/IEC 27001:2013. Además, la evaluación de riesgos, implementación de controles, satisfacción de requisitos y percepciones de los empleados. Todo esto nos ayuda a sentar las bases para futuras certificaciones de estándares. Este estudio nos permite sacar conclusiones sobre la relevancia de un SGSI dada la importancia en el manejo y resguardo de activos cruciales para la organización sin importar el nivel ni el tamaño.

Según el autor (Narváez Barreiros, 2013), la información corresponde a un activo de trascendencia para las empresas. Con base en esto, se puede observar que gobiernos, instituciones financieras, instituciones reguladoras, centros médicos, organismos gubernamentales y empresas privadas están trabajando en la automatización de sus procesos, lo que para lograr una mayor productividad y eficiencia requiere y genera grandes cantidades de información, que puede ser confidencial (sujeto a ciertos requisitos legales y reglamentarios o al secreto de investigación o de producción), desde información de gestión interna, como datos personales, productos, situación financiera de los empleados, hasta información de pago, seguimiento de paquetes, información del cliente , etc.

Tenemos también que mencionar los antecedentes internacionales:

Según los autores (Lumbantoruan & Hidayat, 2013), Un sistema que gestione la seguridad de información implica implementar un sistema para proteger activos importantes y lo más significativo, también puede asesorar y apoyar en la mejora continua de PHVA. La seguridad de información enfocado como sistema, ayuda a mantener el ritmo de las grandes organizaciones que buscan certificaciones. En el mercado aún hay disponibilidad de generación de ventajas competitivas en la medida que el crecimiento global se vuelve necesario para contratar con otros países, grandes contratos a gran escala de transacciones electrónicas y beneficiarse de ello a través de diferentes modalidades de pago, que permitan gestionar con usuarios nacionales e internacionales.

Según el autor, (Pallas Mega, 2009) Esto nos dice la necesidad de implementación de acciones en torno a la seguridad de información. Considerando a diferentes empresas en el que dos o más se integran verticalmente, gestionando así los desafíos de seguridad de la información de manera práctica, permitiendo el análisis de métodos y estándares, existen diferentes estándares para describir los métodos que se toman para administrar y gestionar la SGSI. Esto permite el análisis de diferentes enfoques de gestión y el análisis de riesgos.

Según los autores, (Lopes & De Sá-Soares, 2010) las medidas de seguridad, la política juega un papel central en la literatura. Sin embargo, el número de trabajos prácticos sobre la adopción de estrategias de sistemas de información con enfoques de seguridad es limitado. Este presentó hallazgos sobre la adopción de políticas de seguridad. Con base en los resultados de la discusión bibliográfica, se determina que el objetivo del trabajo futuro es adoptar estrategias de seguridad en la gestión pública.

Podemos indicar también cuál es la definición de información y por qué es tan importante. "Es un conjunto de datos significativos que sujeta la inseguridad o desarrolla el conocimiento sobre algo. De hecho, la información es información significativa en un contexto dado que se puede utilizar de inmediato y brinda orientación. Actuar reduciendo la incertidumbre de nuestras decisiones" (Thompson, 2008).

Según los autores, (Pan & Tomlinson, 2016), “existen muchos estándares para guiar el proceso de evaluación de riesgos. Puesto que, se han generado definiciones sutiles y diferentes de análisis, valoración y valoración de riesgos. Por lo tanto, los investigadores a menudo confunden estos términos y disciplinas, lo que genera una mayor confusión en la comunidad. En este sentido, es importante llegar a un consenso sobre procesos y terminología para aclarar la investigación en este campo. La forma habitual de lograr este objetivo es consultar la literatura. Este artículo se basa en las ideas del grupo Cochrane y adopta un método formal para revisar la literatura.

El resultado es una revisión sistemática del examen y evaluación de inseguridades. Realizamos una revisión sistemática de más de 80 artículos de investigación publicados entre 2004 y 2014. La principal contribución de nuestro artículo es dividir estos artículos publicados en siete tipos. Esta clasificación tiene como objetivo ayudar a los investigadores a comprender de manera clara y justa la terminología, el desarrollo del ámbito académico.

Al implementarse un sistema encargado de aspectos de seguridad en la información nos permite organizar y tratar datos valiosos, sin importar cómo se almacenaron o transmitan, todo ello cubre la protección de la confidencialidad,

integridad y disponibilidad. Para garantizar la confidencialidad del SGSI la información se procesa y mantiene de manera precisa (ISOTools, 2019).

La investigación según el autor (Vásquez, 2018), “es una aplicación descriptiva, y su diseño corresponde a un trabajo experimental. El total está compuesto por 56 personas. Es decir, 56 personas, que son utilizados por técnicos el método es el siguiente: investigación, análisis documental y auditoría”. En resumen, los supuestos generales que el apego a las normas estándar de seguridad de información, permite proteger datos de diversas amenazas al cumplir con los objetivos de seguridad, y no será multado ni sancionado por pérdida de información en el proceso de tecnología de la información TI.

Según el trabajo de (Rodríguez, 2014), “se realiza con la identificación de verificar vulnerabilidades de los activos más críticos de las empresas industriales, entendiendo la vulnerabilidad de estos activos, y recomendando las medidas de control adecuadas de acuerdo a la norma estándar ISO 27001, para que la empresa pueda minimizar sus riesgos. Además, se desarrollaron planes de contingencia para los riesgos que enfrenta el centro de cómputo y los servicios de TI de la empresa”.

Según el trabajo de investigación de los autores (Angarita Leiva & Bautista Bohorquez, 2014) indica que una organización que maneja grandes cantidades de información en cada uno de sus procesos. Se permiten, a su vez manejar adecuadamente los flujos de información interna y proteger todo el contenido que se considera confidencial. El sistema es principalmente responsable de procesar y almacenar la información dentro de la entidad, y su objetivo es implementar un sistema de acuerdo a las normas 27001 para lograr una gestión eficiente de la información.

La definición ciclo de mejora continua, para (Beetrack, 2019) “El ciclo PHVA es un sistema de mejora continua aplicado a los procesos de negocio, su nombre proviene de las fases que componen el ciclo: planificar, ejecutar, verificar y actuar”. Este sistema también se denomina ciclo Deming, el primero está compuesto por siglas en inglés para cada etapa: Plan, Do, Check y Act, que se aplica a la logística de última milla de manera práctica, ya que la empresa debe

reevaluar constantemente el proceso de entrega para identificar, oportunidades de mejora continua.

También tenemos que tener en cuenta los algunos conceptos básicos como: información podemos decir que es una serie de datos con significado, que se de acuerdo a la disposición de seres humanos. (conceptodefinicion.de, s/f). “La información es un activo valioso para una empresa. Se presenta de muchas formas, en papel, digitales, por correo, en video y habladas en conversaciones, debido a que pueden usarse en un entorno cada vez más interconectado, están sujetos a amenazas y vulnerabilidades”.(Gómez Fernández & Andrés Álvarez, 2012).

Se puede decir que le SGSI, forma parte del conjunto, permitiendo planificar, operar, coordinar y mantener la seguridad en aspectos de sistemas de información, es decir, dejar de actuar de manera intuitiva y comprender lo que sucede en los sistemas de información (Security, 2020). El SGSI en primer lugar, combina procesos para gestionar eficazmente la información de la institución. Cada segundo aseguramos los recursos de información con los que trabajamos. Y para lograr nuestras funciones y objetivos, minimizamos la vulnerabilidad de la información. (Pronabec, 2022).

Figura 1. Procesamiento de datos a información

Podemos especificar qué periodos de ciclos con la intención de mejora permiten administrar los sistemas de gestión. Ciclos PDCA; la mejora organizativa es posible para que sea posible crear un indicador y un modelo métrico a lo largo del tiempo. El progreso puede determinarse cuantitativamente. Primero, este

paso corresponde a el establecimiento de SGSI. Este programa planea planificar y diseñar la sistematización de la política que se aplicará a la organización. Segunda hacer: SGSI se implementa y el paso operacional. Tercera inspección: Esta es la etapa para monitorear y verificar el SGSI. Cuarta Acción: las acciones preventivas y correctivas necesarias para la acción correctiva.(Escuela europea excelencia, 2020).

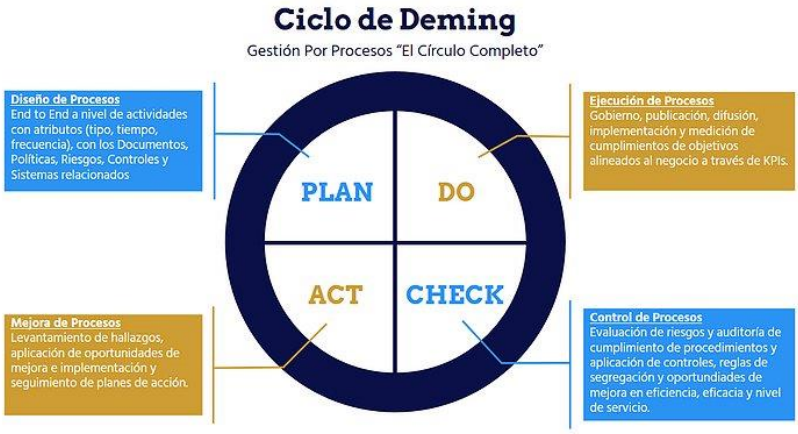


Figura 2. Ciclo de Deming

También debe recordarse debido al auge paulatino del uso del Internet, devienen consideraciones con respecto al uso de la información y a las normas de seguridad en cuanto a su uso; se debe considerar el hecho, de que las empresas establecen las normas y medidas con orientación de empresas del ramo auditor de seguridad

Dado lo anterior, se pueden considerar eventos ubicados en la década de los años 70 cuando comenzaron aparecer las computadoras, allí se perfilaba la utilización de ámbitos de redes tanto públicas como privadas fue aquí cuando la industria consideró una serie de amenazas para la estructura global, por lo cual fueron apareciendo las primeras normas, adoptadas algunas en principio con orden estandarizado mediante la Organización Internacional de Normas (ISO) haciendo énfasis en la interconexión de sistemas abiertos. Estas normas sirven para prevenir los distintos tipos de agresión para la seguridad de un sistema dentro de las cuales cabe destacar las siguientes:

- Interrupción: se presenta cuando ocurre una distorsión o agresión premeditada a los sistemas por ejemplo la destrucción de un disco duro, corte de las líneas de comunicación, etc.

- Intercepción: ocurre cuando una persona no autorizada accede a los sistemas, transgrediendo la confidencialidad, de manera externa o interna, de manera física o mediante software por ejemplo intercepción de manera ilícita en los sistemas de comunicación.

- Modificación: se presenta cuando una persona no se encuentra autorizada para la manipulación de un sistema y ésta genera distorsiones dentro del sistºema, realizando cambios de valores y registros, alterando el programa y generando que este no funcione

- Fabricación: se presenta cunado una persona ajena al sistema implementa o inserta partes desconocidas en el sistema, con énfasis a registros que no existían o incorporando mensajes y actividades distintas

Un eje central de las 27001 es resguardar la confidencialidad, probidad y disponibilidad de la información en las empresas o entes que lo requieran. Para esta actividad, investiga y analiza (evaluación de riesgos) problemas potenciales que pueden afectar la información y luego decide qué se debe hacer para prevenir la ocurrencia o eventual manifestación de estos problemas (reducir o eliminar el riesgo).(advisera, 2022)

Las medidas de seguridad (o controles) a implementar suelen ser políticas, procedimientos e implementaciones técnicas como software y hardware (OSRI, 2018).(ssi.com, 2018).

Figura 3. Estructura de la ISO 27001

Como parte del proceso se tienen diferentes métodos:

- Definir políticas de SI
- Definición hasta dónde llega el modelo
- Evaluación y análisis de riesgos
- Definición en opciones de riesgo
- Elija qué controles implementar
- Preparar una declaración de aplicabilidad

Hay cuatro beneficios comerciales principales que las empresas pueden lograr al implementar este estándar de SI (UPCplus, 2022):

- Cumplir con las normas legales
- Obtenga una ventaja comercial
- reducir el dinero
- Mejor organización

Donde interviene ISO 27001, la SI es fundamentalmente parte de la gestión de riesgos globales de una empresa y los aspectos de intersección con la gestión de la encadenamiento del negocio y la tecnología de la información (UNIR, 2022).

La gestión de cualquier incidente o actividad ilegal o maliciosa que comprometa la disponibilidad, confiabilidad, integridad y confidencialidad de los datos y servicios almacenados o transmitidos. proporcionada o proporcionada por el sistema.(Excellence, 2022).

Esta metodología Magerit analiza y gestionan de manera pronta los riesgos desarrollados por el excelente consejo de gestión electrónica para dar respuesta a los requerimientos de los administraciones (Magerit, 2012). Objetivo Magerit: Primero, es responsable de la información sobre la información sobre la existencia y las necesidades de gestión del riesgo. Se proporciona un método analítico para analizar el riesgo derivado del uso de (TIC) como segundo. Luego en tercer lugar, ayuda a detectar y proyectar un

procedimiento oportuno para mantenerlo peligroso en el control indirecto. Cada uno en cada caso, dependiendo de la situación en cada caso, evaluación, auditoría, autenticación o proceso de autenticación, gracias, agradecimiento, autenticación o procesos de autenticación (Interpolados, 2018).

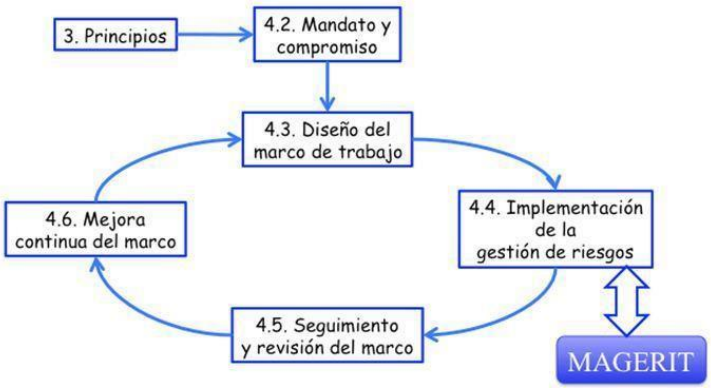


Figura 4. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

III.METODOLOGÍA

3.1. Tipos y diseño de la investigación

3.1.1. Tipo de estudio

El presente es de diseño, de tipo de documental aplicado, por estudios realizados por medio de documentos y es por ello que se conoce la situación de la empresa privada Severox Perú SAC, para poder tener un progreso claro y extenso, estableciendo la realidad se observó el problema y sus posibles efectos.

Según (Alba E., 2010), la meta de este tipo de estudio es reconocer la realidad y las situaciones preponderantes por medio de la figura clara de sus actividades, procesos y otro; con el fin de establecer una relación entre estas variables.

3.1.2. Diseño del estudio

Tenemos peculiaridad metodológica de una investigación de diseño experimental, ya que describe las variables en el estudio, su estilo se muestra en un entorno de forma real ya que afecta a los activos es decir la información dentro de una organización.

3.2. Variables y operacionalización

3.2.1. Dimensiones

Variable independiente

- El “Sistema de Gestión de Seguridad de la Información” SGSI (confiabilidad, integridad y disponibilidad).

Variables dependientes

- Riesgos de los activos de información **(**Amenazas, Vulnerabilidades).

3.2.2. Indicadores

Variable independiente

- Confiabilidad
- Integridad
- Disponibilidad

Variables dependientes

A. Amenazas

- Disponibilidad del, personal
- Salida de la información
- Entrada de información falsa
- Variación, corrupción y destrucción de la información

B. Vulnerabilidades

- Incidentes de la seguridad de la información
- Exceso de privilegios de la información
- Accesos no considerados
- Seguridad física del entorno
- Mantenimiento de todos los sistemas

3.3. Población, muestra y muestreo

3.3.1. Población

Nuestra población está determinada por todos los integrantes de la empresa Severox Perú SAC y todos sus activos de la información que tiene. En el presente proyecto de investigación, no se ha realizado el muestreo, dado que se ha considerado la totalidad de la población de activos de información.

3.3.2. Muestra

Es un grupo de personas donde se extrae la población, con la intención de hacer una investigación estadística para adquirir una cantidad de muestras para este estudio. Para este proyecto se

considera 32 trabajadores es por ello ya tenemos una muestra poblacional.

3.3.3. Muestreo

En este caso se determina toda la población, por consiguiente, no hay muestreo.

3.4. Técnicas instrumentos y recolección de datos

3.4.1. Técnicas

Según (Gerardo & Od, 2016) nos indica que las metodologías para la compilación de información son múltiples, los mismos que se utilizan de diferentes maneras para poder obtienen información. Las técnicas e instrumentos que utilizaremos en este proyecto para la recolección de datos o información son:

- Fichas de observación y verificación
- Encuestas
- Análisis de riesgos.

3.4.2. Instrumentos

Según (Gerardo & Od, 2016) los instrumentos son los medios utilizados para recaudar y almacenar información. Como los que se mencionaran:

- Cuestionario de preguntas, donde el investigador realizara una evaluación de la persecución y adopción de las políticas de seguridad.
- Guía de observación de incidencias por fugas y perdida de la información, por lo que, se utilizaron las guías de observación que indicaran el número de incidentes por fugas y perdidas de información de la empresa Severox Perú S.A.C.

- Análisis de riesgos Magerit utilizando la herramienta Pilar para determinar el nivel de riesgos.
- Fichas bibliográficas, donde el investigador se referenciará a otras bibliografías.

3.5. Procedimiento de recolección de datos

El proyecto de investigación es de tipo aplicada y el estudio realizado consiste en la recopilación de datos. Por lo cual primeramente se realizará la búsqueda de colaboradores que guarden relación con la temática de la investigación. Por segunda parte se conoce la población de estudio y se definió las técnicas e instrumentos que fueron revisados por expertos. Para culminar se aplicará los instrumentos, teniendo como consideración la normativa del SGSI (Vargas Cordero, 2009) .

3.6. Métodos de análisis de datos

Se utilizarán los principios teóricos de la estadística descriptiva para poder analizar los datos recopilados, tales como tabla de frecuencias y pruebas de media (National & Pillars, 2012).

3.7. Aspectos éticos

El investigar cumple con la responsabilidad del tratamiento de los datos brindados por parte de la empresa permitiendo tener una discreción por manejo de los datos brindados. Y se compromete a poder utilizar los datos de la investigación a favor de la empresa. Se respetará la autoría de las diferentes referencias seleccionadas por parte de la investigación realizada. Se garantiza un proyecto de calidad e información veraz para el uso futuro de este proyecto de investigación (Ana Garriga Domínguez y Susana Álvarez González, 2018).

IV.RESULTADOS

Los resultados de los análisis obtenidos en este estudio indican que la seguridad de los activos de información de la empresa Severox Perú S.A.C.

4.1. Análisis descriptivo de las dimensiones

En este proyecto se utilizó la metodología de análisis de riesgos MARGERIT para evaluar el impacto del modelo de SI encargados de aspectos de seguridad en la información en Severox Perú SAC mediante el uso de políticas de seguridad previas al análisis de riesgos. Se logró la implementación del sistema de gestión de SI teniendo en cuenta los fundamentos de la norma ISO 27001:2013, la cual recibió otra evaluación posteriormente. Se generó mediante postest y los resultados se describen en la siguiente tabla.

a. Dimensión de las amenazas

En las siguientes tablas se mostrarán los resultados descriptos que se obtuvieron con el análisis de las amenazas tanto en la tabla pre como del post test y el efecto significativo que tiene el modelo de seguridad de la información al aminorar las amenazas de los activos de la infamación en la empresa Severox Perú S.A.C.

Tabla 1: Frecuencias Pretest de las Amenazas

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
amenazas pretest	.	32	.	.	32	.

Fuente: elaboración propia

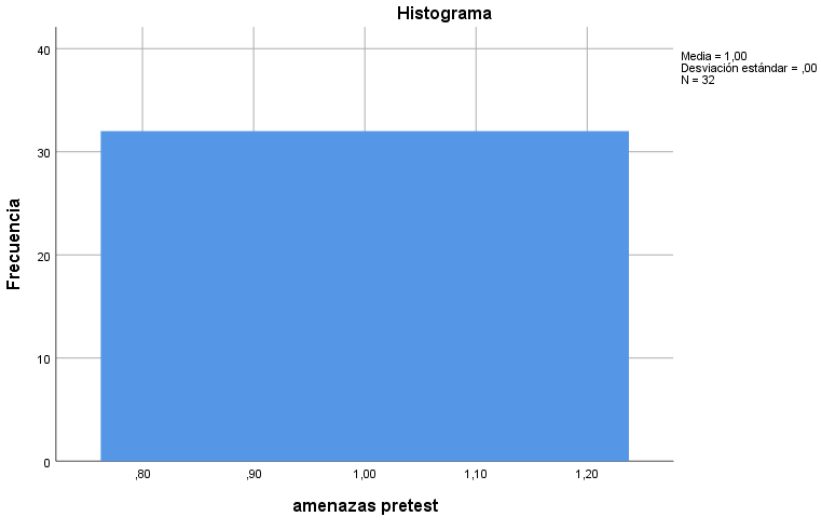


Figura 5: Frecuencia del Pretest - Dimensión de las Amenazas

Fuente: elaboración propia

Tabla 2: Frecuencias Postest de las Amenazas

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
amenazas pretest	.	32	.	.	32	.
amenazas postet	,530	32	,000	,334	32	,000

Fuente: elaboración propia

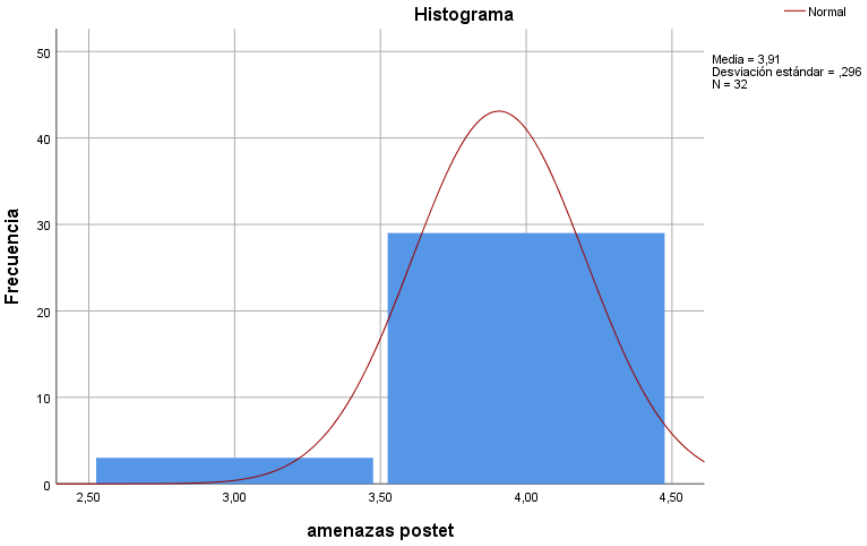


Figura 6: Frecuencia Postest - Dimensión de las Amenazas

Fuente: elaboración propia

La medida de amenaza previa a la prueba que teniendo una muestra de 32 se tuvo una media de 1.00, posteriormente se obtuvo una media a la de 3.91. Esto demuestra la diferencia significativa entre el antes y el después de la implementación de un modelo de seguridad de la información basado en el estándar ISO/IEC27001:2013 en el sentido de que se lograron los objetivos de reducción de amenazas establecidos.

b. Dimensión de las vulnerabilidades

En esta dimensión se muestran resultados de tipo descriptivos de la influencia del modelo de SI para aminorar las debilidades de los activos de la información de la empresa Severox Perú S.A.C.

Se muestran las tablas con las medidas descriptivas del pre y post test de la dimensión de debilidades, donde se observó la influencia del modelo de SI para la atenuar las vulnerabilidades de los activos de la información de la empresa Severox Perú S.A.C.

Tabla 3: Frecuencias pretest de las Vulnerabilidades

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
vulnerabilidades pretest	,338	32	,000	,638	32	,000

Fuente: elaboración propia

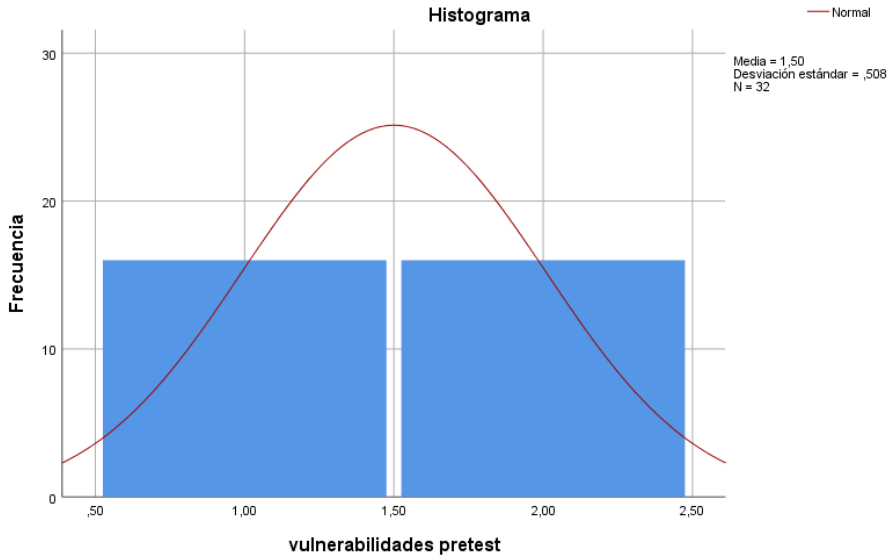


Figura 7: Frecuencia pretest – Dimensión de las Vulnerabilidades

Fuente: elaboración propia

Tabla 4: Frecuencias postest de las Vulnerabilidades

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
vulnerabilidades pretest	,338	32	,000	,638	32	,000
vulnerabilidades postest	,354	32	,000	,637	32	,000

Fuente: elaboración propia

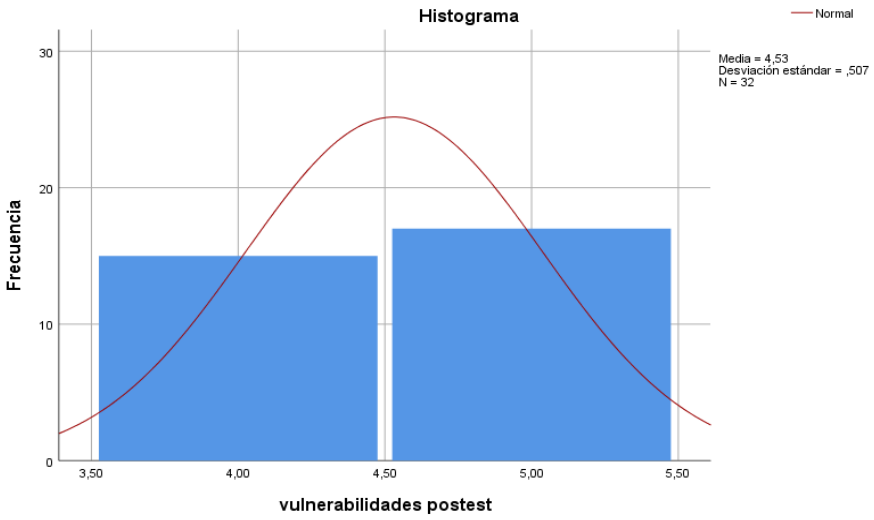


Figura 8: Frecuencia postest – Dimensión de las Vulnerabilidades

Fuente: elaboración propia

Por otra parte, en lo que respecta a los resultados en la dimensión de vulnerabilidades del pretest de la muestra 32, tiene una media de 1.50, mientras en el postest la muestra de 32 tiene una media de 4.53.

Esto nos revela que hay una discrepancia importante entre la pre y post implementación del modelo de SI, basada en la normativa ISO/IEC27001:2013, teniendo en consideración que se logró el objetivo establecido el cual es mitigar las vulnerabilidades.

c. Dimensión del sistema de seguridad de la información

Considerando los resultados descriptivos de la influencia de un modelo de SI para aminorar los riesgos en activos de información de la empresa Severox Perú S.A.C

Aquí observaran las medidas del pre y post test de la dimensión de la seguridad de la información donde se observa una influencia significativa de la mitigación de los riesgos de los activos en la empresa Severox Perú S.A.C.

Tabla 5: Frecuencias pretest sistema de gestión de seguridad de la información

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
sgsi pretetst	,530	32	,000	,334	32	,000

Fuente: elaboración propia

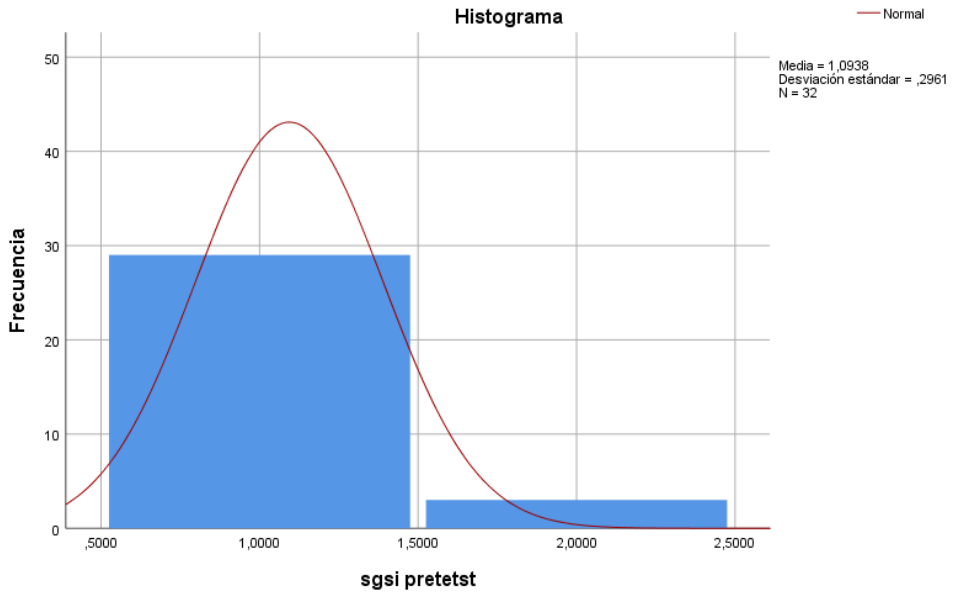


Figura 9: Frecuencia pretest - Dimensión sistema de gestión de seguridad de la información

Fuente: elaboración propia

Tabla 6: Frecuencias postest sistema de gestión de seguridad de la información

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
sgsi pretetst	,530	32	,000	,334	32	,000
sgsi postest	,450	32	,000	,565	32	,000

Fuente: elaboración propia

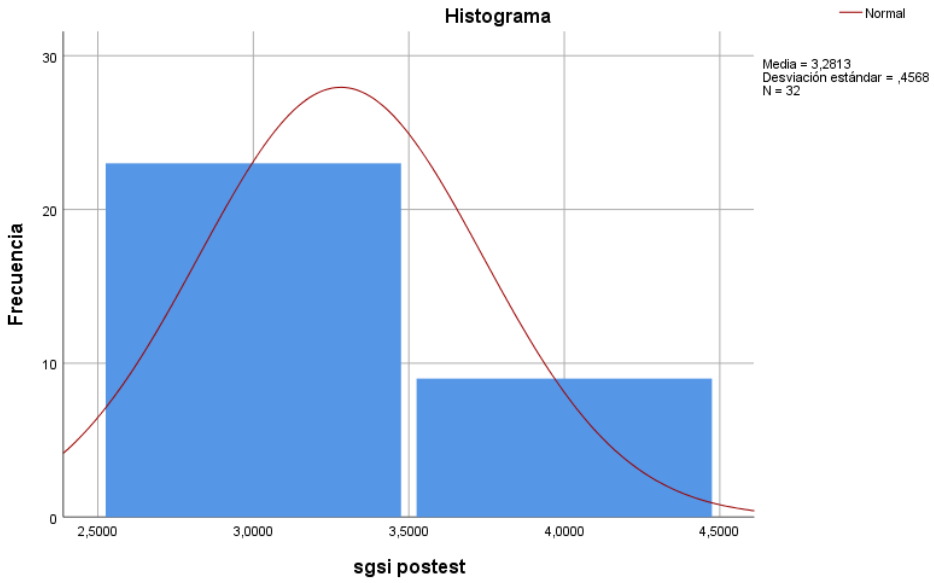


Figura 10: Frecuencia postest - Dimensión sistema de gestión de seguridad de la información

Fuente: elaboración propia

En los resultados de la dimensión de SGSI del pretest de una muestra de 32, tiene una media de 1.09, mientras en el postest la muestra de 32 tiene una media de 3.28.

Esto nos revela que hay una discrepancia de importancia entre la pre y post implementación de la modelo de seguridad de la información, basada en la normativa ISO 27001, teniendo en consideración que se logró el objetivo establecido el cual es determinar la identidad del modelo SI, permitiendo atenuar los riesgos.

4.2. Pruebas de hipótesis

a. Hipótesis de la dimensión de las amenazas

Para cotejar la hipótesis se aplicó la prueba de Wilcoxon, ya que la dimensión de la amenaza adopta una distribución no normal (Sig. es menor a 0.05) es por ello que se rechazó la hipótesis nula y se aceptó la hipótesis de establecer un modelo de la información basada en la norma ISO 27001 que incide directamente en la mitigación de las amenazas los activos de la información de la empresa Severox Perú SAC.

Tabla 7:Estadísticos de prueba de la dimensión amenazas

Estadísticos de prueba[a]

	amenazas postet - amenazas pretest
Z	-5,444[b]
Sig. asintótica(bilateral)	,000

Fuente: elaboración propia

b. Hipótesis de la dimensión de las vulnerabilidades

Para Cotejar la hipótesis se aplicó la prueba de Wilcoxon, ya que la dimensión contempla una distribución no normal la cual es de (Sig. es menor a 0.05). por tal motivo, se rechazó la hipótesis nula y se aceptó la hipótesis de establecer un modelo de la información basada en la norma ISO 27001, que incide directamente en la mitigación de las vulnerabilidades los activos de la información de la empresa Severox Perú SAC.

Tabla 8: Estadísticos de prueba de la dimensión vulnerabilidades

Estadísticos de prueba[a]

	vulnerabilidades postest - vulnerabilidades pretest
Z	-5,334[b]
Sig. asintótica(bilateral)	,000

Fuente: elaboración propia

c. Hipótesis de la dimensión del sistema de gestión de seguridad de la información

Para verificar y comprobar la hipótesis se aplicó la prueba de Wilcoxon, visto que la dimensión evidenció una distribución no normal (Sig. es menor a 0.05) Es por ello que se rechazó la hipótesis nula y se aceptó la hipótesis de establecer un modelo de sistemas de la información basada en la norma ISO 27001, el cual ha afectado significativamente los riesgos de los activos de la información de la empresa Severox Perú SAC.

Tabla 9: Estadísticos de prueba de la dimensión gestión seguridad de la información

Estadísticos de prueba[a]

	sgsi postest - sgsi pretetst
Z	-5,212[b]
Sig. asintótica(bilateral)	,000

Fuente: elaboración propia

V. DISCUSIÓN

En el trabajo de investigación se buscó la comparación con otros trabajos enfocados en la ejecución de sistemas de seguridad de la información, y el primer estudio comparativo fue el trabajo. (Cruz Diaz & Fukusaki Infantas, 2017) el cual tiene como título “Diseño e implementación de un Sistema de Gestión de SI para resguardar los activos de la empresa en estudio en Perú”. Donde se implementó un sistema de gestión de seguridad de la información en una empresa del sector salud, en base a la ISO 27001. En estos resultados que se obtuvieron se identificaron los activos de la seguridad de la información con la valoración correspondiente permitiendo identificar los riesgos y declarar la aplicabilidad de la implementación de los controles y políticas lo que logro una reducción de los riesgos identificados. Esto coincide con este trabajo de investigación que ratifica que la implementación del sistema de gestión de seguridad de la información permitió la disminución de riesgos que se encuentran en los activos de la información de cualquier rubro de empresa y sector.

Cabe mencionar que se logró la coincidencia del personal sobre los diferentes temas de seguridad, al igual que este trabajo de investigación ya que es la base de una mejora continua; adicionalmente a ello uno de los problemas que enfrento la empresa Medcam del sector salud, era que no contaba con ninguna política de seguridad de la información, así como también de controles los cuales son necesario en una empresa que maneja activos de la información.

Es por ello que tanto en este proyecto de investigación como en el comparado se tiene mucho énfasis en la mitigación de los riesgos, amenazas y vulnerabilidades que son un factor importante en el tratamiento de los activos de la información de una empresa.

El segundo trabajo de investigación con el cual se realizó la comparativa es el de (Yañez, 2017) el cual tiene como título “Norma ISO 27001 para la seguridad de información del área de registros académicos del Colegio Nuestra Señora del Carmen ” es un trabajo que se centra en la implementación de la normativa ISO 27001 en las áreas de Institución educativa (Colegio), la cual permite el cumplimiento de marcos de trabajo para la implementación de un SGSI esto con

el fin de proporcionar confiabilidad, probidad y disponibilidad continua de la información manejada den la institución educativa.

El tercer trabajo de investigación con el cual se realizó la comparación es el de (Luna Castillo, Francisco Daniel, Prado Correa, 2020) el cual tiene el titulo “Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura ” en este trabajo se centra en proponer un SI basada en los controles seleccionados en la organización mencionada en el titulo donde determina el diagnostico de los equipos físicos, lógicos y de información recogiendo esta información por medio de encuestas las cuales fueron procesadas y obtuvieron la siguiente data determinante la cual es que se tiene 30 vulnerabilidades 20 riegos y estos riesgos fueron evaluados atraves de la metodología Margerit.

También se basaron la normativa ISO 27001:2014 para la propuesta de su sistema integrado de gestión de SI, al aplicarse esta metodología y basándose en la normativa mencionada obtuvieron mejoras en los diferentes procesos y reducción de vulnerabilidades permitiendo de esa manera mitigarlas.

En el trabajo de investigación también utilizamos la metodología Margerit la cual nos permite mejorar de manera continua en lo que atañe a los procesos que se van realizando en base a la normativa ISO 27001: 2013, en nuestro caso la normativa es una versión anterior, pero cumple con todos los marcos de trabajo e ítems correspondientes a la versión utilizada. Ello permitió una mejora significativa en la mitigación de nuestras vulnerabilidades y amenazas la cuales tenían un alto.

El cuarto trabajo de investigación con el cual se realizó la comparación es el de (Vásquez Zevallos, José Luis Delgado Saavedra, 2019), la cual tiene como título “Modelo de Seguridad Informática Aplicando la Norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson Natación S.R.L”, en este trabajo de investigación tiene como objetivo determinar un modelo basado en la normativa ISO/IEC 27001 para protección de los activos de una organización y determinar el análisis de los riegos y amenazas; ello permitirá asegurar la confidencialidad y disponibilidad de la información dentro de

organización. Propusieron métodos para la implementación de la ISO 27001 y su aplicación en la empresa Berendson Natación S.R.L. buscó flexibilizar los procesos, con la metodología PHVA la cual se utilizó para la implementación del sistema integrado de gestión de la información en la empresa Berendson Natación S.R.L.

Cabe mencionar que a diferencia del trabajo de investigación que se realizó de la empresa Severox Perú S.A.C el cual se implementó un sistema de gestión de seguridad de la información baso el estándar de la ISO 27001 teniendo en cuenta el modelo de mejora continua utilizando la metodología de Margerit la cual se utilizó en este proyecto de investigación, adicionalmente también se utilizó la herramienta Pilar, que nos permitió hacer una análisis de riegos de las amenazas, vulnerabilidades de los activos de la información.

También nos basamos en la normativa ISO: 27001:2013 la cual nos ayuda a la implementación del SIGSI para el tratamiento de los activos de la información, permitiéndonos así generar políticas, las cuales son tomadas y llevadas a la practica en la empresa Severox Perú S.A.C. Lo cual tomo un tiempo para poder ser aplicado en la empresa, pero al final se logró lo que se empraba que era reducir los riesgos tanto en las vulnerabilidades como en las amenas de los activos de la información, teniendo buenos

El quinto trabajo de investigación con el cual se realizó la comparación es el de (Vásquez, 2018), la cual tiene como título “Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI”, este trabajo nos detalla la correcta implementación de un sistema de gestión de seguridad de la información, como también hace un énfasis en importancia de concientizar al personal en salvaguardar la información que se manipula en sus actividades diarias. En este trabajo de investigación a diferencia de mi trabajo se enfoca en sus tres dimensiones la cuales son confiabilidad, integridad y disponibilidad ello se da mediante la implementación de una metodología de riesgos que permite identificar las amenazas que atentan contra la seguridad de la información en los procesos del área de TI de la ONP. Como podemos ver a diferencia de mi trabajo de investigación que va enfocada a mitigar los riesgos teniendo en cuenta dos dimensiones las cuales son amenazas y vulnerabilidades

que se encuentran en los activos de la información, estos activos son los datos que se manejan de los clientes los cuales son sensibles, es por ello que al igual que el trabajo de investigación que se está comparado se da importancia en a la sensibilización del personal que trabaja en la organización, ya que el personal es pieza fundamental en el tratamiento de la información, es por ello que al implementar un sistema integrado de gestión de seguridad de la información se considera la capacitación del personal en las políticas que se implementan y también se considera que cada trabajador de la organización sepa que hay un sistema integrado de seguridad de la información implementado en la empresa o institución.

VI.CONCLUSIONES

- ✓ Al implementarse el modelo de seguridad de información basada en la norma ISO 27001 de 2013 influyo de manera positiva en la disminución de riesgos de los activos de la información que se encuentran en la empresa Severox Perú S.A.C. Ya que el nivel que se obtuvo para mitigar la amenazas es de 90.6 % que indica que posiblemente si se está cumpliendo con las políticas de la implementación del SGSI basada en la normativa; y el 9.4 % indica que no sabe si cumple con las políticas de la implementación del SGSI basada en la normativa.

- ✓ Al implementarse el modelo de seguridad de la información basada en la norma ISO 27001 de 2013 influyo de manera positiva en la disminución de riesgos de los activos de la información que se encuentran en la empresa Severox Perú S.A.C. Ya que el nivel que se obtuvo para mitigar las vulnerabilidades es de 53.1 % donde indica que definitivamente si se cumple con las políticas de la implementación del SGSI basada en la normativa; y que el 46.9 % indica que posiblemente si cumple con las políticas de la implementación del SGSI basada en la normativa.

- ✓ Al implementarse el modelo de seguridad de la información basada en la norma ISO 27001 de 2013 influyo de manera positiva en la disminución de riesgos de los activos de la información que se encuentran en la empresa Severox Perú S.A.C. Ya que el nivel de concientización y percepción del personal sobre la mitigación de los riesgos de 71.9 % que indico que no sabe si cuenta con un sistema integrado de gestión de la información, y que 28.1 % indico que posiblemente si se tiene un sistema de gestión de la información. Estos resultados tienen mucha confluencia ya el personal de la empresa Severox Perú S.A.C, tiene personal rotativo (cambia continuamente), por el rubro en el que se encuentra.

VII.RECOMENDACIONES

1. Se recomienda aumentar el alcance en las diferentes metodologías que se usan para la implementación de un SI basada en la normativa ISO/27001:2013.

2. Se recomienda aumentar el alcance en la implementación del sistema integrado teniendo en cuenta la normativa más actual, para su elaboración y de esa manera mitigar algunos puntos que no se contemplaban en la normativa anterior.

3. Se recomienda la implementación de la normativa ISO/27001:2013 en la totalidad de los procesos dentro de una organización pública o privada para lograr mejorar y les permita certificarse internacionalmente y de esa manera ganar más confianza con los clientes y proveedores en el mercado competitivo de hoy en día.

4. Se recomienda considerar en futuras investigaciones la complementación de herramientas, como ITIL para las buenas prácticas en la ejecución de un sistema, teniendo en cuenta siempre las necesidades y procesos de la empresa.

.

VIII.REFERENCIAS

1. advisera. (2022). *¿Qué es norma ISO 27001?* https://advisera.com/27001academy/es/que-es-iso-27001/
2. Alba E. (2010). *Metodología de la Investigación*. *1986*.
3. Ana Garriga Domínguez y Susana Álvarez González. (2018). *Aplicación del principio de responsabilidad proactiva al tratamiento de los datos personales en el ámbito del proyecto Securhome | CENIE*. https://cenie.eu/es/blogs/securhome/aplicacion-del-principio-de-responsabilidad-proactiva-al-tratamiento-de-los-datos
4. Angarita Leiva, J. A., & Bautista Bohorquez, C. L. (2014). *Diseño De Un Modelo De Control Interno En La Empresa Prestadora De Servicios Hoteleros Eco Turisticos Nativos Activos Eco Hotel La Cocotera, Que Permitira El Mejoramiento De La Informacion Financiera*. 97.
5. Beetrack. (2019). *Ciclo PHVA: Ciclo de mejora continua*. https://www.beetrack.com/es/blog/ciclo-phva-ejemplo-logística-última-mill
6. BlackBerry. (2020). *Informe de amenazas de BlackBerry 2021*. https://www.blackberry.com/la/es/forms/enterprise/report-bb-2021-threat-report-sp?utm_source=google&utm_medium=cpc&utm_campaign=smb_enterprise_es-pe&_bt=519925328332&_bk=ciberseguridad&_bm=b&_bn=g&_bg=124852802591&gclid=EAIaIQobChMIxoXRxp6x9AIVB7KGCh2QYwQ
7. conceptodefinicion.de. (s/f). *¿Qué es Información? » Su Definición y Significado [2021]*. Recuperado el 5 de febrero de 2022, de https://conceptodefinicion.de/informacion/
8. Cruz Diaz, M. A., & Fukusaki Infantas, S. (2017). *Diseño e implementación de un Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la clínica Medcam Perú Sac*. 209. http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/3369/1/cruz_fukusaki.pdf
9. Docplayer. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC sobre seguridad en sistemas de información para pymes*. https://docplayer.es/4467956-Guia-de-aplicacion-de-la-norma-une-iso-

iec-27001-sobre-seguridad-en-sistemas-de-informacion-para-pymes.html

10. Escuela europea excelencia. (2020). *Ciclo PDCA para la mejora continua*. https://www.escuelaeuropeaexcelencia.com/2020/07/en-que-consiste-el-ciclo-pdca-para-la-mejora-continua/
11. Excellence, Isot. (2022). *Metodología Margerit para el análisis e identificación de riesgos en SGSI*. https://www.pmg-ssi.com/2021/07/metodologia-margerit-para-el-analisis-e-identificacion-de-riesgos-en-sgsi/
12. Fernández Peñaloza, D. A., & Pacheco Vargas, O. A. (2014). *Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana ntp-iso/iec 27001:2008*.
13. Gerardo, F., & Od, A. (2016). *EL PROYECTO DE INVESTIGACIÓN 6a EDICIÓN* (Número May).
14. Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. 216. https://books.google.com/books/about/Guía_de_aplicación_de_la_Norma_UNE_ISO.html?hl=es&id=0LW5MQEACAAJ
15. Instituto Español de Estudios Estratégicos. (2010). Ciberseguridad. Retos Y Amenazas a La Seguridad Nacional En El Ciberespacio. En *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio- cuaderno de estudios estrategicos* (Número 149). http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html
16. Instituto Nacional de Ciberseguridad. (2010). *Colección Protege tu Empresa*.
17. Interpolados. (2018). *MAGERIT V.3 : METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN – Interpolados*. https://interpolados.wordpress.com/2018/10/02/magerit-v-3-metodologia-de-analisis-y-gestion-de-riesgos-de-los-sistemas-de-informacion/
18. ISOTools. (2019). *ISO 27001 de Sistemas de Gestión*. Isotools.org. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

19. Lopes, I. M., & De Sá-Soares, F. (2010). Information Systems Security Policies: A survey in Portuguese Public Administration. *Proceedings of the IADIS International Conference Information Systems 2010*, 61–69.
20. Lumbantoruan, E. P., & Hidayat, P. (2013). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA*. 14–27.
21. Luna Castillo, Francisco Daniel, Prado Correa, P. B. (2020). Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura". *Universidad Andina del Cusco*, 1–118. http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47102/Gutierrez_RS-SD.pdf?sequence=1&isAllowed=y
22. Magerit. (2012). *Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*. *2006*. http://administracionelectronica.gob.es/
23. Medina Iriarte, J. (2006). Estandares Para La Seguridad De Información Con Tecnologias De Información. *Universidad De Chile*, 1–193. http://repositorio.uchile.cl/bitstream/handle/2250/108414/medina_j.pdf?sequence=4&isAllowed=y
24. Narváez Barreiros, I. R. (2013). *Aplicación De La Norma Iso 27001 Para La Implementación De Un Sgsi En La Fiscalía General Del Estado*. http://repositorio.puce.edu.ec/bitstream/handle/22000/9780/TESIS_SGSI.pdf?sequence=1&isAllowed=y
25. National, G., & Pillars, H. (2012). *Métodos de análisis de datos*.
26. OSRI. (2018). Metodología para la gestión de la seguridad informática. *Oficina de Seguridad para las Redes Informaticas*, 1–68. http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf
27. Pallas Mega, G. (2009). Metodología de Implantacion de un SGSI en un grupo empresarial jerárquico. *Universidad de la República*, 186. http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf
28. Pan, L., & Tomlinson, A. (2016). A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*, *6*(2), 270–281. https://doi.org/10.2495/SAFE-V6-N2-270-

281

29. Pérez, A. (2017). *Seguridad de la información, un conocimiento imprecindible*. Business School. https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible
30. Pronabec. (2022). *Sistema de Gestión de Seguridad de la Información*. https://www.pronabec.gob.pe/sistema-de-gestion-de-seguridad-de-la-informacion/
31. Rodríguez, L. C. (2014). *"Análisis para la integración de un sistema de información (SGSI) ISO-27001 utilizando OSSIM para empresa industrial"*.
32. Security, A.-I. (2020). *Academy - Internet Security Auditors*. https://academy.isecauditors.com/certificacion-iso-27001-implantacion-espana
33. Sota; Mechan. (2018). Implementación de controles y cumplimiento de requisitos de la ISO / IEC 27001 : 2013 para la seguridad. *Universidad San Martin de Porres*.
34. ssi.com. (2018). Confidencialidad, integridad y disponibilidad en los SG-SSI. En *Febrero 1* (p. 1). https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/
35. Thompson. (2008). Definición de Información. *Definición de Información*, 3.
36. UNIR. (2022). *ISO 27001 ¿En qué consiste esta norma de seguridad?* | *UNIR*. https://www.unir.net/ingenieria/revista/iso-27001/
37. UPCplus. (2022). *Las 4 ventajas comerciales de implementar la ISO 27001 | UPCplus*. https://www.prevencionintegral.com/comunidad/blog/upcplus/2017/02/06/4-ventajas-comerciales-implementar-iso-27001
38. Vargas Cordero, Z. R. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, *33*(1), 155. https://doi.org/10.15517/revedu.v33i1.538
39. Vásquez, J. F. (2018). Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. *Universidad Nacional Mayor de San Marcos*.

https://cybertesis.unmsm.edu.pe/handle/20.500.12672/8436

40. Vásquez Zevallos, José Luis Delgado Saavedra, M. M. (2019). *Modelo de Seguridad Informática aplicando la Norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson natación S.R.L.* 1–79. https://repositorio.udl.edu.pe/bitstream/UDL/339/1/Tesis Guarniz y Meoño.pdf.
41. Yañez, M. B. (2017). Norma ISO 27001 para la seguridad de información del área de registros académicos del Colegio Nuestra Señora del Carmen. *Ucv*, 358.

Anexo

Anexo 1: Matriz de Consistencia

PROBLEAMA	OBEJTIVOS	HIPÓTESIS	OPERACIONALIZACIÓN DE VARIABLES			
			Variables	**Dimensiones**	**Indicadores**	**Metodología**
(PG) ¿Cuál es la influencia de modelo de SI, basado en la normativa ISO/IEC 270001:2013, para poder atenuar los riesgos de los activos de información en la empresa Severox Perú S.A.C?	(OG) Determinar la identidad del modelo de SI, de acuerdo con la norma ISO / IEC 27001: 2013, con el fin de reducir el riesgo de los activos de información de la empresa Severox Perú SAC.	(HG) Establecer un modelo de seguridad de la información basado en la norma ISO / IEC 27001: 2013, el cual ha incidido significativamente la reducción de los riesgos de los activos de información de Severox Perú SAC	**(Variable Independiente) Modelo de seguridad de la información basada en la ISO/IEC 27001:2013**	Sistema de gestión de la seguridad de la información	(Confidencialidad, integridad y disponibilidad)	**Tipo de investigación:** documental Aplicada **Diseño de la investigación:** Experimental
PE1 ¿Cómo afecta el modelo de SI, basado en la norma ISO / IEC 27001: 2013 a la aminoración de amenazas a los activos de información en Severox Perú SAC?	OE1 Establecer un modelo de SI y determinar su impacto para aminorar las amenazas a los activos de información de Severox Perú SAC	HE1 Establecer un modelo de SI basado en la norma ISO / IEC 27001: 2013, que incide directamente en la mitigación de las amenazas a los activos de información de Severox Perú SAC	**(Variable Dependiente) Riesgos de los activos de información**	Amenazas	1. Disponibilidad del personal 2. Salida de información 3. Entrada de falsa información 4. Variación de la información 5. Corruptela de la información 6. Destrucción de la información	

PE2 ¿Cuál es el impacto del modelo de seguridad de la información basado en la norma ISO / IEC 27001: 2013 en la mitigación de las vulnerabilidades de los activos de información de Severox Perú SAC?	OE2 Establecer un modelo de SI, y determinar su impacto para mitigar las vulnerabilidades de los activos de información de la empresa Severox Perú SAC.	HE2 Establecer un modelo de seguridad de la información basado en la norma ISO / IEC 27001: 2013. Para mitigar las vulnerabilidades de los activos de información de Severox Perú SAC que tiene un impacto directo		Vulnerabilidades	7. Incidentes de seguridad de la información 8. Exceso de privilegios de la información 9. Accesos no autorizados 10. Seguridad física del entorno 11. Mantenimiento de todos los sistemas	

Anexo 2: Variables y Operacionalización

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
(Variable Independiente) Modelo de seguridad de la información basada en la ISO/IEC 27001:2013	El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos (ISOTools, 2019).	Esta variable se midió por medio de guías de observación, cuestionarios y listas de cotejo para establecer los indicadores en base a tres pilares importantes del estándar ISO 27001 que son Confidencialidad, integridad y disponibilidad.	Sistema de gestión de la seguridad de la información	Confidencialidad, disponibilidad e integridad)	de intervalo
(Variable Dependiente) Riesgos de los activos de información	Consiste en determinar qué activos de información van a hacer parte del inventario y cuáles son los riegos, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder del cada proceso (o quien haga sus veces… Líder requerido en gestión de calidad) ayude en realización de la actividad (MINTIC, 2016).	En esta variable se mide por medio del análisis de riesgos que se desplegaran después de haber analizado las guías de observación las dimensiones a analizar son las Amenazas y vulnerabilidades	Amenazas	• Disponibilidad del personal • Salida de información • Entrada de falsa información • Variación de la información • Corruptela de la información • Destrozo de la información	de intervalo

			Vulnerabilidades	• Incidentes de seguridad de la información • Exceso de privilegios de la información • Accesos no autorizados • Seguridad física del entorno • Mantenimiento de todos los sistemas	de intervalo

Anexo 3: Cuestionario de evolución al personal de la empresa Severox Perú S.A.C

CUESTIONARIO DE EVOLUCIÓN AL PERSONAL DE LA EMPRESA SEVEROX PERÚ S.A.C

UNIVERSIDAD CÉSAR VALLEJO

ENCUESTA EN SEGURIDAD DE LA INFORMACIÓN PARA LA TESIS TITULADA:

"MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMATIVA ISO/IEC 27001 :2013 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE LA INFORMACIÓN EN LA ENTIDAD PRIVADA SEVEROX PERÚ SAC, AREQUIPA, 2021"

Objetivo:

En la empresa privada Severox Perú SAC, realizar la valoración técnica informática y obtener el diagnóstico general y situación actual de la seguridad informática para verificar las deficiencias y proponer estrategias de control y seguridad en base a los resultados y recomendaciones obtenidos, permitido minimizar las ocurrencias futuras y obtener una prevención concreta en un tratamiento adecuado de los datos y una atención más allá de la información que tratan las empresas que son vitales. Responda las siguientes preguntas de manera honesta y específica, y marque la respuesta que crea que es correcta.

Fecha: __/__/2021

NRO.	PREGUNTAS	DEFINITIVAMENTE NO	POSIBLEMENTE NO	NO SE	POSIBLEMENTE SI	DEFINITIVAMENTE SI
	CONFIDENCIALIDAD					
1	En su opinión, ¿existe un acuerdo de confidencialidad de la información a la que se accede?					
2	En su opinión, ¿es aceptable compartir información textual o imágenes sobre clientes que cuenta la empresa Severox Perú SAC sabiendo que se trata de un hecho de fuga de información y puede constituirse en delito de infidencia?					
	INTEGRIDAD					
3	En su opinión, ¿es aceptable recibir documentos de texto digitales vía correo electrónico sobre clientes y acuerdos de carácter reservado sin verificar su procedencia y/o fuente?					
4	En su opinión, ¿es aceptable recibir documentos de texto digitales (información) vía correo electrónico, sin verificar su procedencia y/o fuente					
	DISPONIBILIDAD					
5	En su opinión, ¿se dispone de una clasificación de la información según la criticidad de la misma?					
6	En su opinión, ¿existe un responsable de los activos?					
7	En su opinión, ¿existen procedimientos para clasificar la información?					

	DISPONIBILIDAD DEL PERSONAL					
8	En su opinión, ¿existen documentos de políticas de seguridad de los Sistemas de Información en la empresa privada Severox Perú SAC?					
9	En su opinión, ¿existe normativa relativa a la seguridad de los Sistemas de Información en la empresa?					
10	En su opinión, ¿existen procedimientos relativos a la seguridad de los Sistemas de Información en la empresa?					
11	En su opinión, ¿existe un responsable de las políticas, normas y procedimientos en Seguridad Informática?					
12	En su opinión, ¿existen mecanismos para la comunicación a los usuarios de las normas?					
13	En su opinión, ¿existen controles regulares para verificar la efectividad de las políticas?					
14	En su opinión, ¿existe un inventario de activos actualizado?					
15	En su opinión ¿el inventario contiene activos de datos, software, equipos y servicios?					
	SALIDA DE INFORMACIÓN					
16	En su opinión, ¿existen roles y responsabilidades definidas para las personas implicadas en la seguridad?					
17	En su opinión, ¿un responsable encargado de evaluar la adquisición y cambios de los Sistemas de Información en la empresa Severox Perú SAC?					
18	En su opinión, ¿la empresa Severox Perú SAC, participan en temas de seguridad Información?					
19	En su opinión, ¿existen programas de formación en seguridad informática para el personal de la empresa Severox Perú SAC?					
	ENTRADA DE FALSA INFORMACIÓN					
20	En su opinión, ¿es inútil tener documentos físicos de la información que se recibe, centraliza, genera y procesa?					
21	En su opinión, ¿es inútil configurar pantallas de bloqueo en los equipos de cómputo dado el tiempo de inactividad?					

22	En su opinión ¿sería inútil mantener un registro de los documentos de información que se formulan y remiten a los distintos niveles de la empresa Severox Perú SAC?					
	VARIACIÓN DE LA INFORMACIÓN					
23	En su opinión, ¿informan a los usuarios de las vulnerabilidades observadas o sospechosas?					
24	En su opinión, ¿son nulos los errores involuntarios en el uso de las aplicaciones informáticas?					
25	En su opinión, ¿existe un proceso disciplinario de la seguridad de la información, implantado?					
	CORRUPTELA DE LA INFORMACIÓN					
26	En su opinión, ¿se tienen definidas las responsabilidades y roles de seguridad?					
27	En su opinión, ¿se tiene en cuenta la seguridad en la selección del personal?					
28	En su opinión, ¿se plasman las condiciones de confidencialidad y responsabilidad al ingresar a laborar a la empresa Severox Perú SAC?					
29	En su opinión, ¿se imparte la formación y/o capacitación adecuada de seguridad y tratamiento de activos?					
	DESTROZO DE LA INFORMACIÓN					
30	En su opinión, ¿es inútil mantener un registro de pérdidas de datos o información en la empresa Severox Perú SAC?					
31	En su opinión, ¿existe algún control en las redes para compartir archivos digitales?					
32	¿Existen medidas de seguridad en el uso del correo electrónico?					
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
33	En su opinión, ¿existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?					
34	En su opinión, ¿están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?					

35	En su opinión, ¿se comunican las debilidades de seguridad?					
36	En su opinión, ¿existen definidas las responsabilidades antes de un incidente?					
37	En su opinión, ¿existe un procedimiento formal de respuesta?					
38	En su opinión, ¿existe un marco de planificación para la continuidad del negocio?					
	EXCESO DE PRIVILEGIOS DE LA INFORMACION					
39	En su opinión, ¿se tiene en cuenta el cumplimiento de las normas dentro de la empresa?					
40	En su opinión, ¿existe una revisión de la política de seguridad y de la conformidad técnica?					
	ACCESO NO AUTORIZADO					
41	En su opinión, ¿existe el uso de passwords?					
42	En su opinión, ¿existe una política de uso de los servicios de red?					
	SEGURIDAD FÍSICA DEL ENTORNO					
43	En su opinión, ¿falta un perímetro de seguridad física eficiente (una pared, puerta con llave, control de acceso físico) en la empresa Severox Perú SAC?					
44	En su opinión, ¿existen controles de entrada para protegerse frente al acceso de personal no autorizado?					
45	En su opinión, ¿un área vulnerable ha de estar cerrada, aislada y protegida de eventos naturales?					
46	En su opinión, ¿existen protecciones frente a fallos en la alimentación eléctrica?					
	MANTENIMIENTO DE TODOS LOS SISTEMAS					
47	En su opinión, ¿se realiza mantenimiento y control en las vulnerabilidades de los equipos?					
48	En su opinión, ¿están actualizados los sistemas operativos, antivirus, aplicaciones y programas de los equipos de cómputo de la empresa Severox Perú SAC?					

49	En su opinión, ¿la oficina de informática de la empresa Severox Perú SAC, cuentan con hardware o equipamiento apropiado?					

Anexo 4: Entregables Definidos por la norma ISO/IEC 27001

Anexo 4: Entregables Definidos por la norma ISO/IEC 27001

SEVEROX
PASIÓN E INGENIO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO PARA EL CONTROL Y REGISTRO DE DOCUMENTOS

Versión: 01

Código	:	**PPCRDD**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

PROCEDIMIENTO PARA EL CONTROL DE DOCUMENTOS Y REGISTROS

1. OBJETIVOS Y USUARIOS

1.1. Objetivo general

Establecer los procedimientos, principios y normas para la elaboración y control de los documentos y registros asociados al Sistema de Gestión de Seguridad de la Información de la empresa Severox Perú S.A.C.

1.2. Objetivos específicos

- Definir los procedimientos a seguir en la cadena de producción documental del Sistema de Gestión de Seguridad de la Información de la empresa Severox Perú S.A.C.
- Viabilizar el manejo de la documentación del Sistema de Gestión de Seguridad de la Información de la empresa Severox Perú S.A.C, reflejando el fortalecimiento de la identidad institucional.
- Permitir un control eficaz y eficiente de la información y documentación, por medio de actividades de seguimiento, control y verificación.
- Permitir la difusión a todo el personal que forma parte del Sistema de Gestión de Seguridad de la Información de la empresa Severox Perú S.A.C, a fin de que tengan conocimiento de la elaboración y control de los documentos que se generan.

2. ALCANCE

Se aplica a todos los documentos que soportan y componen el Sistema de Gestión de la Seguridad de la Información (SGSI) de la de la empresa Severox Perú S.A.C, de conformidad a la norma ISO/IEC 27001:2013.

3. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS INTERNOS

Se establece el procedimiento con el fin de determinar las actividades concernientes a la elaboración, aprobación, actualización, distribución y conservación de los documentos de la empresa Severox Perú S.A.C, a fin de disponer y obtener la información de manera ágil y eficiente, contribuyendo a la correcta preservación de la documentación del Sistema de Gestión del Sistema de Información.

Los parámetros a cumplir en la elaboración de los documentos son los siguientes:

3.1. Formatos y cuerpo de los documentos

Los documentos del SGSI, como manuales, instructivos, guías, informes, protocolos y programas se deben elaborar en papel bond blanco, tamaño A4, con peso de 60 a 80 gr., con márgenes superior 2,5 e izquierda 3 cm, inferior 2,5 y derecha 3 cm, fuente tipográfica Arial tamaño 12.

3.2. Portada

El texto de la portada se escribe en fuente tipográfica Arial, tamaño 12, el nombre del documento en fuente tipográfica Arial, tamaño 14,

negrita y alineado en el centro. La estructura de la portada debe encontrarse como se indica en la siguiente gráfica:

ENTREGABLES DEFINIDOS POR LA NORMA ISO/IEC 27001

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO PARA EL CONTROL Y REGISTRO DE DOCUMENTOS

Versión: 01

Código	:	
Fecha	:	
Creado por	:	Osmar Raúl, Ticona Bustinza
Aprobado por	:	Jefe del área de TI
Confidencialidad	:	Intimo / Intermedio / Superficial

En la parte superior del documento, seis (6) interlineaciones bajo el margen superior, en el centro, encontramos el logo empresa Severox Perú S.A.C.
Seis (6) interlineaciones bajo los logos símbolos encontraremos los datos requeridos por el documento. Estos datos son: el texto Sistema de Gestión de Sistemas de Información en fuente Arial negrita tamaño 16.
Tres (3) interlineaciones después, encontramos el nombre del documento en fuente Arial negrita tamaño 14.
Tres (3) interlineaciones bajo el nombre del documento, se encuentra la versión del documento, cinco (3) interlineaciones después se encuentra el código que identifica al documento, una (1) interlineación más abajo se registra el nombre del proceso del

documento, seguido de la fecha de vigencia del documento, nombre del que formula, aprueba y nivel de confidencialidad.
Estos últimos datos se registran con fuente Arial negrita con tamaño 12. La interlineación de la portada debe ser sencilla.

3.3. Contenido del documento

El contenido del documento debe ser claro, conciso, evitando redundancias y errores gramaticales y ortográficos, teniendo en cuenta que los documentos son la carta de presentación de la institución. Por razones de variación en los formatos, se recomienda que la fuente sea Arial, el tamaño de fuente depende del tipo y tamaño del formato.

3.4. Control de cambios

El Control de Cambios consiste en una tabla que permite llevar control sobre las solicitudes de modificación del documento, cuántas veces se han llevado a cabo las modificaciones y por qué se realizó. Esta tabla se debe incluir al final del documento, bajo los datos de elaboración y generar un formato denominado Control de Cambios, código SGSI-FR-19. Los datos contenidos en el Control de Cambios son los siguientes:

Versión: corresponde al número de versiones existentes del mismo documento. Cabe indicar que la última versión es la que se toma en cuenta para difusión.

Fecha de aprobación: corresponde a la fecha de aprobación de la versión que se encuentra vigente.

Descripción del cambio: referencia de la razón por la cual fue modificado el documento.

Gráfica del control de cambios

CONTROL DE CAMBIOS		
VERSIÓN N°	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**

Nota: los datos de cierre del documento y control de cambios únicamente se registran en los documentos y no en los registros o libros de registros.

4. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS EXTERNOS

Procedimiento establecido con el fin de establecer controles para la identificación y control de los documentos externos que afectan al SGSI, con el fin de disponer de la información de manera adecuada, evitando el uso de documentos obsoletos, contribuyendo al mejoramiento continuo de los Procesos y Procedimientos en la organización.

Los Documentos Externos que afectan al SGSI son:

- Documentos generados, por otras instituciones y que tengan relación directa con las actividades y funciones realizadas por las diferentes áreas.

5. PROCEDIMIENTO DE CONTROL DE REGISTROS

Procedimiento que establecen las actividades necesarias para la identificación, almacenamiento, conservación, recuperación, retención y

disposición de los registros que se generan en cumplimiento de las funciones y procedimientos establecidos por el SGSI.

5.1. Diligenciamiento

El diligenciamiento de los registros puede llevarse a cabo de manera digital o manual.

En los casos en que el formato se diligencie de manera manual, se deben tener en cuenta los siguientes aspectos:

- Escribir con letra clara y legible
- Usar tinta indeleble
- Diligenciar todas las casillas que el formato solicita.
- Evitar tachones y enmendaduras.
- Cuando ocurra un error que requiera la anulación del documento debe tacharse con una sola línea diagonal y dejar constancia mediante la firma y fecha del funcionario responsable.
- Cuando una casilla del formato que requiera diligenciamiento, no se diligenció, debe trazarse una línea para evitar diligenciamientos posteriores de información.

5.2. Responsabilidad

Para identificar quién es el responsable de diligenciar el documento es necesario implementar la Línea de Responsabilidad que se encuentra al final de los formatos establecidos, dicha línea de responsabilidad contiene los siguientes datos, de acuerdo a la naturaleza de cada formato:

	DILIGENCIADO POR
NOMBRE	
CARGO	
FIRMA	
FECHA	

	DILIGENCIADO POR	APROBADO POR
NOMBRE		
CARGO		
FIRMA		
FECHA		

	DILIGENCIADO POR	REVISADO POR	APROBADO POR
NOMBRE			
CARGO			
FIRMA			
FECHA			

Los Registros se relacionan en un Listado Maestro de Registros, código SGSI-FR-16, formato en el que se registran los siguientes datos:
Código, Nombre, Versión, Vigencia, Fecha de Vigencia, Ubicación o Área, Lugar de Almacenamiento, Cargo del responsable del Manejo del Archivo, Medio de Almacenamiento, Nivel de Acceso de la Información, Tiempo de Retención, Disposición Final y Observaciones. El responsable del

diligenciamiento del listado maestro de registros es el líder de cada proceso, quien debe reportar dentro de los cinco (5) últimos días de cada mes a la Unidad de Archivo y Correspondencia los cambios realizados en el listado.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	:	**PPISGSI**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos, las funciones y responsables del proyecto.
El Plan del proyecto se aplica a todas las actividades realizadas en el proyecto de implementación del SGSI.
El Plan del proyecto se aplica en una primera etapa a los datos, sistemas de información, medios de enlace y redes de comunicación, infraestructura tecnológica, soportes de información, infraestructura física y funcionarios que apoyan la ejecución de los tres (3) primeros procesos identificados como críticos dentro de la empresa Severox Perú S.A.C, lo cual nos permitirá identificar la metodología de implementación adecuada, para cada año adaptar los demás procesos críticos del negocio con el SGSI, hasta obtener un grado de madurez que luego nos permita gestionar de una manera adecuada todos los procesos en la empresa Severox Perú S.A.C.
Los usuarios de este documento son los empleados de la empresa Severox Perú S.A.C y los miembros del equipo del proyecto. Para este caso el gerente general de la empresa, jefe del área de TI, componen la Institución, los mismos que tomarán las decisiones; asimismo, el equipo del proyecto está conformado por Osmar Raúl, Ticona Bustinza.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001
- Norma ISO 22301

3. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

3.1. Objetivo del proyecto

La implementación del Sistema de Gestión de Seguridad de la Información de conformidad con la norma ISO 27001:2013, se realizará hasta finales del mes de diciembre del 2020, para obtener los documentos necesarios que permitan gestionar de manera segura el flujo de información derivado de los diferentes procesos de la empresa.

3.2. Resultados del proyecto

Durante el proyecto de implementación del SGSI, se redactarán los siguientes documentos:

a. Situación actual
b. Políticas que incluyen controles para:
1) Aspectos organizativos de la seguridad de la información.
2) Gestión de activos.

3) Seguridad relacionada al personal.
4) Gestión de comunicaciones y operaciones.
5) Control de acceso.
6) Adquisición, desarrollo, mantenimiento de sistemas informáticos.
7) Gestión de los incidentes de seguridad.
8) Gestión de la continuidad del negocio.
9) Cumplimiento.

c. Compromiso por parte de los miembros de la empresa Severox Perú S.A.C, quienes conformarán el Comité de Administración Integral de Riesgo (CAIR), para apoyar decididamente a la implementación del SGSI.
d. Enfoque de evaluación de riesgos cuya metodología debe contemplar inventario de activos, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos y tratamiento de riesgos.
e. Declaración de aplicabilidad SOA.
f. Estrategias para formación y concientización.
g. Planes de acción correctiva/preventiva.
h. Planes de monitoreo y revisión.
i. Revisión del SGSI por parte de la gerencia.
j. Planes de auditoría.

3.3. Plazos

El Sistema de Gestión de Seguridad de la Información tiene como fecha límite para su desarrollo el mes de mayo del 2022, fecha en la cual se habrá pasado por las fases del ciclo de Deaming o PDCA (Plan-Do- Check-Act) que nos permitirá, como la mejor práctica, hacer una mejora continua de las fases que son necesarias a fin de llevar a cabo una satisfactoria implementación del SGSI.

3.4. Organización del proyecto

3.4.1. Promotor del proyecto

El promotor y responsable del presente proyecto será Osmar Raúl, Ticona Bustinza, quien deberá coordinar cada una de las fases, solicitar, organizar o generar la documentación que sea necesaria a fin de dar cumplimiento a la implementación del SGSI.

3.4.2. Gerente del proyecto

El Ing. Jorge Luis Rodríguez, jefe del área de Planeamiento Administrativo de la empresa Severox Perú S.A.C, informará de los avances en el desarrollo del presente proyecto al Ing. Lennon Rojas Sanz Gerente General de la empresa Severox Perú S.A.C.

3.4.3. Equipo del proyecto

Para el desarrollo del presente proyecto será necesario contar con la colaboración de un miembro del área de Planeamiento Administrativo de la empresa Severox Perú S.A.C,

Administrador del área de Tecnologías de la Información y Comunicación de la empresa Severox Perú S.A.C que dará el visto bueno.

3.5. Principales riesgos del plan

En cualquier proyecto, el recurso más importante son las personas. Idealmente un proyecto debería tener disponibles a un número adecuado de personas, con las habilidades y experiencia correctas, comprometidos y motivados con el proyecto. Sin embargo, las cosas pueden ser diferentes, por lo que hemos identificado los siguientes riesgos:

- ¿El personal del proyecto está comprometido con la entera duración para lo que son necesarios?
- ¿Todos los miembros del equipo están disponibles a tiempo completo?
- ¿El movimiento de personal de un mismo proyecto es suficientemente bajo como para permitir la continuidad del proyecto?
- ¿Se han establecido los mecanismos apropiados para permitir la comunicación entre los miembros del equipo?
- ¿El entorno de trabajo del equipo es el apropiado?

3.6. Herramientas para Implementación del proyecto y generación de informes

Se han evaluado varias herramientas, una de las mejores cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001, además el análisis de riesgo se realizara con la herramienta Pilar. La herramienta seleccionada es actualizada periódicamente y cuenta con manuales de implementación y uso en español, adicionalmente se usarán hojas de cálculo lo cual permitirá llevar un control del avance de la implementación del SGSI.

4. GESTIÓN DE RIESGOS GUARDADOS EN BASE A ESTE DOCUMENTO

Se realizará una revisión de los documentos de políticas y archivos generados del desarrollo e implementación del SGSI, se gestionará la implementación de un sistema de versionamiento que permita validar los cambios documentales y las versiones finales donde adicionalmente se llevará el control de la documentación en las herramientas seleccionadas.

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.

Todos los documentos serán debatidos por los involucrados, recoger los comentarios ayudará a enriquecer las políticas que se definan, solo entrará en vigencia cuando se los apruebe por los canales establecidos en la empresa Severox Perú S.A.C, y una vez

canales establecidos en la empresa Severox Perú S.A.C, y una vez que se tengan implementadas todas las correcciones solicitadas por los involucrados del SGSI.

6. DIAGNÓSTICO SITUACIÓN ACTUAL

6.1. Objetivos

- Verificar la implementación de una metodología que permita gestionar los riesgos de la empresa Severox Perú S.A.C, la identificación y valoración de activos y las amenazas sobre estos.
- Verificar la administración de accesos lógicos a los servicios internos y externos.
- Verificar las configuraciones de los servicios y la documentación generada.
- Evaluación de la arquitectura de red implementada.
- Seleccionar los controles que nos van a permitir cubrir los distintos aspectos al implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Revisar las políticas, normas, procedimientos y documentos de control que nos permiten determinar el grado de cumplimiento en la implementación del SGSI.

6.2. Metodología

La metodología seleccionada para la implementación se basa en la metodología de la mejora continua la cual nos permitirá aplicar un método riguroso y comprensivo para describir el comportamiento de los procesos de seguridad, sistemas de seguridad de información, para que se alineen con las metas comunes de la organización.

Preguntas que responde a de la mejora continua: Un proceso de Arquitectura de Seguridad de Información en la empresa ayuda a contestar preguntas básicas como:

- ¿Está la arquitectura actual apoyando y añadiendo valor a la seguridad de la organización?
- ¿Cómo podría una arquitectura de seguridad ser modificada para que añada más valor a la organización?

Para implementar una arquitectura de seguridad de información que se alinee con la estrategia de la organización y otros detalles necesarios tales como dónde y cómo opera, es necesario contar con competencias esenciales, procesos de negocio y cómo la organización interactúa consigo misma.

Cuadro 1: Requerimientos en la empresa Severox Perú S.A.C.

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades y flujo de procesos de las operacionesde TI	SÍ	NO

Ciclos, periodos y distribución en el tiempo de la organización	NO	NO
Proveedores de tecnología hardware, software y servicios	SÍ	NO
Inventarios y diagramas de aplicaciones y software	SÍ	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos y modelos de datos soportados.	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos deseguridad y dónde se conservan	NO	NO
Redes de área local y abiertas, diagramas de conectividad a Internet	NO	NO

Para el desarrollo del presente plan se utilizarán los siguientes procedimientos:

- Reuniones con los involucrados en el Plan de implementación del SGSI, que nos permitirá debatir y contar con la aceptación de los controles de la norma ISO 27002 a implementar en la empresa Severox Perú S.A.C.
- Reunión para establecer el compromiso y delegados en el proceso de implementación del SGSI.

El objetivo de esta etapa es sentar las bases del proceso de mejora continua en materia de seguridad, permitiendo a la empresa Severox Perú S.A.C, conocer el estado del mismo y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Identificación y valoración de los activos y amenazas sobre los activos de la empresa Severox Perú S.A.C.
- Auditoría de cumplimiento de la ISO/IEC 27002:2008.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Presentación de resultados.

Para adaptar el Sistema de Gestión de Seguridad de la Información será importante que el proyecto se ajuste a las 4 fases definidas por la serie de normas ISO 27000 como la mejor práctica para poder implementar el SGSI, en el siguiente esquema se presentan las etapas, en las cuales el SGSI será adaptado a la empresa

Severox Perú S.A.C, las mismas etapas serán la guía para la presentación de avances.

6.2.1. Documentación normativa sobre las mejores prácticas en seguridad de la información

Para la ejecución de la presente etapa se selecciona a Magerit V3 como metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, también es posible que para la consecución de los objetivos.

6.2.2. Identificación y valoración de los activos y amenazas sobre los activos de la institución

6.2.2.1. Inventario de activos

Como primera actividad a ejecutar es necesario realizar la evaluación de los activos de información en los procesos seleccionados, considerando las áreas entre estos y realizando una valoración.

Cuadro 2 : Activos de la Institución

INVENTARIO DE ACTIVOS	DETALLES
INSTALACIONES	Ubicación de equipos informáticos y de comunicaciones
HARDWARE (HW)	Equipos que alojan datos, aplicaciones y servicios
APLICACIONES (SW)	Aplicativos que permiten manejar los datos
DATOS	El principal recurso, todos los demás activos se identifican alrededor de éste activo
RED	Equipamiento que permite intercambiar datos
SERVICIOS	Que se brindan gracias a los datos y que se necesitan para gestionar los datos
EQUIPAMIENTO AUXILIAR	Todo aquello que complemente al material informático
SOPORTES DE INFORMACIÓN	Dispositivos que permiten el almacenamiento de datos (temporal)
PERSONAL	Quienes explotan u operan todos los demás elementos

Cuadro 3 : Dimensiones de Seguridad

DIMENSIONES DE SEGURIDAD		
VA	VALOR	CRITERIO

MA	10	Daño muy grave a la organización
A	7-9	Daño grave a la organización
M	4-6	Daño importante a la organización
B	1-3	Daño menor a la organización
MB	0	Daño irrelevante para la organización

Fuente: Magerit V3

Cuadro 4 :Ámbito y Activos

ÁMBITO	ACTIVO	VALOR
DATOS	Información personal	MA
	Imágenes digitales	MA
SERVICIO	Trámites documentarios	M
	Consultas al sistema	M
SW	*Telegram*	MA
	Correo electrónico	MA
HW	Terminales de usuario	A
REDES Y COMUNICACIONES	Red LAN	A
SOPORTE DE INFORMACIÓN	Documentos Informes	MA
	Documentos Solicitudes	MA
INSTALACIONES	Oficinas	A
PERSONAL	Oficial de órdenes	MA
	Analistas de información	MA
	Personal técnico	MA

6.2.3. Análisis de amenazas

Para el entendimiento de la presente etapa es necesario indicar que se establecen según Magerit V3, ciertas amenazas típicas identificadas y que reducen la utilización del activo en diferentes ámbitos de los pilares de la seguridad de la información, estos activos están frecuentemente expuestos a las amenazas, por lo cual la frecuencia de ocurrencia se expresará como tasa anual o incidencias por año; finalmente la frecuencia con la que una amenaza se materialice sobre un activo hará que este activo disminuya en un porcentaje de su valor.

6.2.4. Cálculo del riesgo

El cálculo del riesgo actual es una valoración en la que interviene el valor que le hemos dado a los activos en cada una de las dimensiones, la frecuencia con la que una amenaza puede degradar a un activo y el impacto de daño o disminución que la amenaza puede causarle al activo.

6.2.5. Selección de controles - salvaguardas

Para ejecutar la actividad de selección de salvaguardas, debemos tomar en consideración los elementos de protección actual que

tienen nuestros activos y los posibles elementos de control de los que podemos dotar a nuestros activos, es decir a los grupos de activos que hemos definido, validar los controles del Anexo a la Norma UNE-ISO/IEC 27001:2013 son aplicables en el contexto de nuestras capacidades, para esto se han considerado 2 ámbitos esenciales con los que debemos trabajar las salvaguardas, los aspectos y el tipo de protección de las salvaguardas que vamos a implementar, los cuales resumimos en los siguientes cuadros.

ASPECTOS DE LAS SALVAGUARDAS	
PR	Procedimientos
PP	Política personal
SW	Aplicaciones
HW	Dispositivos físicos
SF	Seguridad física

TIPO DE PROTECCIÓN	
PTG	Protección de tipo general
PdS	Protección de servicios
PDI	Protección de datos/información
PSW	Protección de aplicaciones
PHW	Protección de equipos
PdC	Protección de comunicaciones
PSF	Seguridad física
PRP	Relativas al personal

Fuente: Magerit V3

6.2.6. Auditoria de cumplimiento de la ISO 27001

Con el propósito de proteger la información de la organización y como futura guía para implementar o mejorar las medidas de seguridad, esta etapa nos va a permitir obtener una radiografía de la situación actual en torno a la seguridad de la empresa Severox Perú S.A.C.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE REQUERIMIENTOS

Versión: 01

Código	:	**PIDR**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE REQUISITOS

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información y con la continuidad del negocio, como también los responsables de su cumplimiento. Este documento se aplica a todo el Sistema de gestión de seguridad de la información (SGSI). Los usuarios de este documento son todo el personal de la empresa Severox Perú S.A.C.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4.2; control A.18.1.1
- Norma ISO 22301, punto 4.2
- Política del sistema de gestión de seguridad de la información
- Política de la Continuidad del Negocio

3. IDENTIFICACIÓN DE REQUISITOS Y PARTES INTERESADAS

El Ing. Jorge Luis Rodríguez, será el responsable de brindar toda la información requerida para la determinación y levantamiento de requisitos.

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades yflujo de procesos de las operaciones de TI	SÍ	NO
Ciclos, periodos y distribución en el tiempode la organización	NO	NO
Proveedores detecnología hardware,software y servicios	SÍ	NO
Inventarios y diagramas de aplicaciones ysoftware	SÍ	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos ymodelos de datos soportados	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se	NO	NO

conservan		
Redes de área local y abiertas, diagramasde conectividad a Internet	NO	NO

4. RESPONSABLES

Responsables de la información
R: Responsabilidad - C: Colaboración

	Jefe TI	CTSG
Recopilación de legislación de seguridad		R
Identificación de requisitos legales de seguridad		R
Evaluación del riesgo de cumplimiento	C	R
Adopción de medidas para asegurar el cumplimiento		R
Actualización de lista de requisitos legales	C	R
Comunicación	R	C
Cumplimiento y archivos de registros		R

SEVEROX
PASIÓN E INGENIO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	:	**ASGSI**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este documento es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa Severox Perú S.A.C.

Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los empleados de la empresa Severox Perú S.A.C.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4,3
- Plan del proyecto para la implementación de la norma ISO 27001
- Lista de requisitos legales, normativos, contractuales y de otra índole

3. DEFINICIÓN DEL ALCANCE DEL SGSI

La organización necesita definir los límites del SGSI para decidir qué información quiere proteger, dicha información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad, esto implica que la responsabilidad por la aplicación y de las medidas de seguridad serán transferidas a un tercero que administre dicha información.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

3.1. Procesos y servicios

Dentro de los procesos que se dan en la empresa Severox Perú S.A.C, tenemos los siguientes:

- Mantener informado al gerente general, utilizando la aplicación de escritorio Telegram Whtasapp, mediante comunicaciones telefónicas y documentos impresos.
- Recibir notas informativas e imágenes digitales vía correo electrónico sobre las operaciones que se ejecutan en las áreas de la empresa.
- Centralizar y procesar la información operativa como administrativa para dar cuenta a la gerencia.
- Procesa la documentación en general proveniente de gerencia, para su distribución a las diferentes áreas y sedes.
- Remite vía correo electrónico diferentes documentos a los clientes.
- Formular informes y demás documentos que se tramitan de la gerencia o áreas correspondientes.

- Anota el ingreso y egreso de documentos en general en la bitácora de registros.
- Transmite las Ordenes Telefónicas dispuesta por la gerencia.
- Recibe información telefónica sobre cualquier hecho las sedes durante el día.
- Orienta a los analistas de información para la captación de información complementaria que se requiere para su procesamiento respectivo.
- Imparte instrucción al personal de las oficinas a fin de que cumplan las funciones en forma eficaz, eficiente y oportuna.
- Realiza otras funciones que le asigne el jefe.
-

3.2. Unidades organizativas

La empresa Severox Perú S.A.C se organiza de la siguiente manera.

a. Gerencia
b. Secretaria
c. Área de TI.
d. Área de Recursos Humanos.
e. Área de Planeamiento
f. Área de Logística
g. Área de Contabilidad
h. Área de Ventas

3.3. Redes e infraestructura de TI

Cuadro 5: Infraestructura de TI de la institución

GRUPO	TIPO	DESCRIPCIÓN	UNIDADES
Hardware	Equipos de cómputo - oficina	PCs de escritorio	50
		Celulares	03
	Impresoras	Impresora Láser B/N	07
		Impresora multifuncional escáner oficina	04
	Dispositivos de red	*Switches* distribución oficinas	04
		Switches distribución Cuarto de telecom	03
		Routers	03

Cuadro 6 : Cuadro 1: Infraestructura de TI de la institución

GRUPO	TIPO	DESCRIPCIÓN	UNIDADES
Infraestructura	CPD	Generador eléctrico	01
		Radio de comunicaciones	03
		Armarios de comunicaciones	01
		Armarios	04

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	:	**PSI**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SEVEROX PERÚ S.A.C.

1. Objetivo, alcance y usuarios

La presente política de alto nivel tiene como propósito definir el objetivo, dirección, principios, disposiciones y reglas básicas para la gestión de la seguridad de la información en la de empresa Severox Perú S.A.C. Además, esta política está dirigida a todos los operadores de información y usuarios de los sistemas de información de la empresa Severox Perú S.A.C.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales (MOF CEOPOL).
- Ley N° 29733 Ley de protección de datos personales 03JUL11.

3. Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información que está disponible solo para personas o sistemas autorizados. Integridad: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida. Disponibilidad: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario. Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información. Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Objetivos de la gestión de la seguridad de la información

4.1. Objetivo general

Lograr niveles aceptables de integridad, confidencialidad y disponibilidad de la información, con el objeto de asegurar continuidad operacional de los procesos que desarrolla la empresa Severox Perú S.A.C, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

4.2. Objetivos específicos

- Identificar, clasificar y asignar los activos de información de la organización, para lograr niveles adecuados de

integridad, confidencialidad y disponibilidad de la información.

- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas que enfrentan los activos, para asegurar la continuidad del negocio.
- Establecer políticas, normativas y procedimientos que permitan resguardar y proteger los activos de información de la organización.
- Definir un Plan de Instrucción y Capacitación que permita difundir los alcances y buenas prácticas asociadas a la seguridad de la información institucional.

5. Alcance de la política de seguridad de la información

5.1. Alcance general

La Política General de Seguridad de la Información de la empresa Severox Perú S.A.C, se establece en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.

La presente política debe ser conocida y cumplida por todo el personal de la empresa Severox Perú S.A.C, involucrada en el uso de los sistemas y tecnologías de Información y las actividades con su sistema.

Esta política se aplica en todo el ámbito de la organización a nivel de la sede principal y sucursales, a sus recursos y a la totalidad de los procesos, internos y externos.

De lo anterior, la información que genera y gestiona la organización constituye un activo estratégico clave para asegurar la continuidad del negocio; por lo que, la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

5.2. Definición de los activos de información

Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización, en la que se distinguen tres niveles:

- La información propiamente dicha, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los equipos, sistemas e infraestructura que soportan la información.
- El personal que utiliza la información y que tienen conocimiento de los procesos institucionales.

ACTIVOS DE INFORMACIÓN

ACTIVOS DE INFORMACIÓN	ACTIVOS FÍSICOS	ACTIVOS DE SERVICIOS DE TI	ACTIVOS HUMANOS
Informes y solicitudes formatos digital y físico	Infraestructura de TI	Servicios de autenticación	Personal que labora en la empresa
Datos digitales en BBDD Postgres	Oficinas y muebles	Servicios de red, conectividad, red LAN	
Imágenes digitales	Ordenadores y equipos informáticos (HW)	Servicios del sistema Propio	
Correo electrónico institucionales, app *Telegram y Whtasapp Desktop*	Instalaciones		

CAPITAL HUMANO ESTRUCTURACIÓN Y VALOR DE LOS ACTIVOS

GRUPO	DESCRIPCIÓN	UNID.	VALOR	CRITICIDAD
Personal	Operadores	30	Muy alta	Alta
	Jefes	02	Muy alta	Alta

DESCRIPCIÓN Y VALOR CRÍTICO DE LOS ACTIVOS

TIPO	DESCRIPCIÓN	UNID	VALOR	CRITICIDAD
Equipos de oficina	Equipos de cómputo	25	Media	Media
	Impresoras	07	Baja	Baja

5.3. Definición de la seguridad de la información

La empresa Severox Perú S.A.C, entiende que la seguridad de la información es la protección de los activos de información contra una amplia gama de amenazas y vulnerabilidades; por lo que, se debe asegurar la continuidad de las operaciones, minimizar el daño a la institución y maximizar la eficiencia y las oportunidades de mejora de la gestión.

6. Políticas y objetivos de seguridad de la información

Las políticas de seguridad que se plantean en este documento, están basadas en un análisis estratégico acorde con cada una de las fases de la estrategia, misión y visión de la organización.

Estas políticas representan directrices generales de alto nivel que deben ser adoptadas por los integrantes en la cadena de prestación de servicios durante las fases de la evolución de la estrategia de la organización. Para asegurar el cumplimiento de las políticas de seguridad para la institución, se establecieron objetivos de control asociados a cada política:

6.1. Política de control de acceso

Del análisis y evaluación de riesgos se determinó que se requiere mayor nivel de seguridad; por lo que, se debe implementar mecanismos y controles que aseguren un registro efectivo, identificación y autenticación de los usuarios de dichos servicios. Asimismo, se debe implementar mecanismos y controles que aseguren el acceso bajo el principio del menor privilegio, necesario para realizar únicamente las labores de cada usuario de dicho servicio.

Objetivos control

PS1.1	Otorgar acceso al sistema web solo a usuarios autorizados. Se requiere limitar el acceso solo para usuarios identificados y autenticados apropiadamente que se encuentren laborando en la organización.
PS1.2	Otorgar privilegios de acceso a servicios que requieren mayor nivel de seguridad en el uso del sistema web. Se requiere minimizar el daño potencial causado por usuarios autorizados lo cual implica establecer segregación de funciones para separar usuarios de los servicios y usuarios con roles administrativos.
PS1.3	Otorgar acceso a servicios que requieren mayor nivel de seguridad condicionado a la presentación de información que soporte la identidad del individuo que requiere el acceso y sus credenciales de autenticación.
PS1.4	Otorgar privilegios de acceso a servicios de la institución, sólo cuando se satisfaga la verdadera identidad del usuario, es decir, que el usuario sea quien realmente dice ser y que no esté registrado bajo otra identidad con un acceso legítimo. Se debe evitar y prevenir la creación de usuarios múltiples. Un usuario puede tener múltiples roles con respecto a los servicios de la institución, pero solo puede poseer una única identidad.
PS1.5	Otorgar acceso a los usuarios sobre los servicios y activos necesarios para soportar el servicio específico requerido. No se deben alterar datos.
PS1.6	Implementar una administración efectiva de los derechos de acceso de usuarios y asignar dicha responsabilidad al personal apropiado, ello en coordinación con personal de administradores de accesos.
PS1.7	Implementar la vigencia de los derechos de acceso y su revocación, una vez finalice el período asignado o haya pérdida de las credenciales, o se detecte uso indebido de los recursos por parte de

	los usuarios. Las credenciales de acceso deben quedar inválidos ante eventos de revocación o cambio de colocación a otra subunidad.

6.2. Política de no repudio

Se debe garantizar el no repudio de las transacciones en los sistemas informáticos y aplicaciones web poniendo en práctica mecanismos de seguridad que permitan crear un ambiente de confianza entre el Gerente General y personal operador de la empresa con relación a la autenticidad, trazabilidad y no repudio de las transacciones electrónicas.

Objetivos control.

PS2.1	Proveer evidencia del origen y la integridad del mensaje, es decir, se deben crear mecanismos en el servicio para crear una prueba de origen de la información de manera que se pueda evitar que una de las partes niegue suresponsabilidad en el envío del mensaje ya sea por correo electrónico o vía sistema web; por lo que se debe guardar la informativa de origen en formato digital e impreso. Asimismo, se deben implementar mecanismos para probar si el mensaje ha sido alterado.
PS2.2	Proveer evidencia del acuse del mensaje, es decir, se deben implementar mecanismos en el servicio de correo, como respuesta automática para crear una prueba de recibo, acuse recibo y almacenarla para su recuperación posterior, en caso de controversia entre las partes, de igual manera se trabajará con el sistema web, verificando su síntesis diaria.
PS2.3	Proveer evidencia que el servicio es proporcionado realmente por una entidad pública con relación al sistema web. Se deben implementar credenciales del servicio, registrar correos oficiales, teléfonos de soporte y ser presentadas a los operadores para la autenticación del sistema web de Severox Perú.
PS2.4	Proveer evidencia de la fecha y hora de la transacción electrónica efectuada a través del servicio de correo y sistema web de Severox Perú.

6.3. Política de privacidad y confidencialidad

Los datos personales, imágenes digitales e impresas de la información recaudada y demás información enviada a través de los servicios de la institución, deben ser protegidos y manejados de manera responsable y segura.

Objetivos control.

PS3.1	Proveer protección adecuada de la información personal y privada contra divulgación no autorizada cuando se transmite a través de redes vulnerables, llámese sistema web, correo electrónico y app WhatsApp y*Telegram*.
PS3.2	Normar y autorizar los destinatarios de los mensajes de correo que se remiten desde las áreas y sucursales; asimismo, normar y filtrar periódicamente a los usuarios autorizados a la visualización de la información que se propaga en el Grupo de la Empresa Severox Perú por las apps de WhatsApp y*Telegram*.
PS3.3	Proteger la información personal y privada de uso indebido y divulgación no autorizada en medios de fuente abierta, así como las imágenes y promociones de ventas, cuando se procesa y almacena dentro del dominio de implementación de los servicios de la institución.

6.4. Política de integridad

La información que se recibe o se envía a través de los servicios de la institución, debe conservar los atributos de correcta y completa durante la transmisión, el procesamiento y el almacenamiento. Deben garantizar la integridad de la información.

Objetivos control.

PS4.1	Proteger la información que se transmite a través de redes públicas contra modificación, borrado o repetición accidental o intencional. Se debe asegurar la fuerte integridad de las comunicaciones para prevenir contra manipulación de datos en tránsito o contra fuga, pérdida y corrupción causada por fallas de equipos, comunicaciones y otros.
PS4.2	Proteger la información que se almacena contra modificación accidental o intencional. Se deben implementar mecanismos para prevenir que los operadores manipulen la información del servicio almacenada en su estación de trabajo con el fin de obtener algún beneficio.
PS4.3	Proteger la información almacenada dentro de las áreas de la institución (correo electrónico, app WhatsApp y*Telegram* y sistema web) contra modificación o destrucción intencional por parte de atacantes externos. Se deben implementar fuertes medidas para frustrar la alteración mal intencionada de los datos de usuarios o de información de dominio público que puedan disminuir la confianza de la empresa. Los proveedores de servicios tienen la obligación del debido cuidado, para asegurar que la información proporcionada sea veraz.

PS4.4	Proteger la información trasmitida o almacenada dentro de la institución contra pérdida o corrupción accidental. Se deben implementar procedimientos probados de respaldo y recuperación de datos y asegurar que se mantienen las listas de usuarios autorizados, dando cuenta al área de informática en caso de modificación no comunicada.

6.5. Política de disponibilidad del servicio

Es de preponderante importancia poder asegurar la disponibilidad continua de los servicios bajo un control estricto y adecuado.

Objetivos control.

PS5.1	Proteger los servicios de la institución contra daños, intrusión o negación por parte de atacantes externos, implementar un plan de contingencia ante este tipo de eventos.
PS5.2	Proteger los servicios de la institución contra daños o provisión intermitente del servicio por fallas internas de los equipos y/o redes. Se deben implementar mecanismos de redundancia y alta disponibilidad acordes con la criticidad de la provisión continua del servicio y la capacidad para realizar reparaciones rápidas.
PS5.3	Proteger los servicios de la institución contra pérdida de datos,pérdida de equipos y otros eventos adversos. Se debe implementar un plan de continuidad del Negocio (BCP-*Business Continuity Plan*), para asegurar que se toman las medidas necesarias y evitar en lo posible, la pérdida de información por ocurrencia de incidentes.

6.6. Política de disponibilidad de información

Las entidades de Gobierno deben asegurar que los datos de los usuarios y clientes se mantienen protegidos contra pérdida, alteración o divulgación por actos accidentales o malintencionados, o por fallas de los equipos y/o redes.

Objetivos control.

PS6.1	Recuperar los datos personales o críticos que han sido dañados, destruidos, alterados o modificados por acciones malintencionadas o accidentales. Se deben implementar procedimientos de copias de respaldo y recuperación, archivos digitales de notas informativas, para asegurar que exista recuperación de los datos sensibles y que puedan ser restaurados en el evento de una falla. También se deben implementar mecanismos para que los datos personales no sean divulgados sin autorización expresa del propietario de la información, que viene a ser el gerente de la empresa Severox Perú.

PS6.2	Recuperar la información protegida en el evento en el que un usuario no pueda suministrar las credenciales de acceso necesarias en el caso del uso de la web. Se deben implementar procedimientos para recuperar datos de usuario en el evento que la contraseña se pierda. Esto permite soportar investigaciones de posible uso indebido del sistema.

6.7. Política de protección del servicio

Se debe asegurar que los servicios y sus activos de información relacionados, estén adecuadamente protegidos contra ataques externos o internos.

Objetivos control.

PS7.1	Proteger los sistemas de información, equipos y redes que soportan los servicios de la institución contra ataques a la provisión continua y segura del servicio. Se deben asegurar los equipos y las redes implementando medidas como aseguramiento de servidores, implementación de topologías seguras de red y escaneo de vulnerabilidades. Los sistemas de información y las aplicaciones, deben ser diseñados e implementados de manera que se minimicen las vulnerabilidades y los ataques externos e internos se reduzcan a un nivel despreciable.

6.8. Política de registro y auditoria

Es importante el poder mantener y proteger los registros de las transacciones electrónicas como evidencia para los requerimientos de las auditorias (internas) y como mecanismo para establecer responsabilidades de los usuarios ante incidencias.

Objetivos control.

PS8.1	Mantener un registro de transacciones que pueda ser requerido después del análisis de eventos y/o incidentes. Se deben mantener registros y pistas de auditoría con el fin de establecer responsabilidad por las transacciones, reconstruir transacciones fallidas y suministrar registros apropiados en caso de conflictos o disputas por el servicio. Debe existir trazabilidad de los registros de transacciones según sea apropiado.

7. Marco general de las Políticas de Seguridad Institucional

7.1. Aspectos generales

La Política General de Seguridad de la Información ha sido elaborada considerando su compatibilidad con las prácticas sugeridas por la Norma ISO/IEC 27001.
La Gerente general de Severox Perú se compromete a realizar las acciones que estén a su alcance para permitir la continuidad

operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

7.2. Aprobación de la política

Las políticas de seguridad de la información serán aprobadas por el Gerente General de la empresa Severox Perú S.A.C, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en la organización.

7.3. Difusión de la política

Será responsabilidad del jefe del área de Sistemas Integrados de Gestión y el jefe de Tecnologías de la Información difundir los temas relevantes en materia de seguridad. Las políticas de seguridad de la información serán comunicadas a todo el personal de la empresa.
Para la difusión de los contenidos de las políticas de seguridad de la información en el interior de la organización se deberán utilizar los medios de difusión que disponga como (correo electrónico, boletín digital informativo, etc.), así como también el área de potencial humano.

Los principales medios utilizados serán:

- Boletín digital informativo de la institución.
- Manual de concientización.
- Inducción a personal que ingresa a la empresa.
- Comunicaciones a través de charlas personalizadas y reuniones
- Se deberá definir, implementar y evaluar las acciones e iniciativas contenidas en un Plan de Difusión, Sensibilización, Instrucción y Capacitación en materia de seguridad de la información.

7.4. Revisión de la política

La Política General de Seguridad de la Información será revisada de manera anual o en las siguientes circunstancias:

- A requerimiento del gerente general, frente a cambios en el ambiente de la organización, debido a las circunstancias del servicio, cambios generales, a las condiciones legales y al ambiente técnico.
- La modificación del presente documento está a cargo del Comité de Seguridad de la Información y será aprobado por el gerente general de la empresa Severox Perú.

7.5. Evaluación del cumplimiento de la política

Los jefes son responsables de la implementación de estas políticas de seguridad de la información, dentro de sus áreas de

responsabilidad, así como el cumplimiento de las políticas, normativas y procedimientos por parte de su equipo de trabajo.
La institución realizará auditorías internas anuales al sistema de seguridad de la información para verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.
El incumplimiento de la Política General de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de las omisiones, dando cuenta documentadamente al órgano de control institucional.

7.6. Análisis diferencial de la Organización

POLÍTICA DE SEGURIDAD				
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN				
Documento de política de seguridad de la información	POLITICA SEGURIDAD	Existen normas que hacen referencia en cuanto al uso de los recursos informáticos e información de la institución.	No existe	No se cumple
Revisión de la política de seguridad	POLITICA SEGURIDAD	Existen Políticas de Seguridad, aprobadas por la Dirección General o Dirección Ejecutiva de Información y Tecnologías de la Comunicación.	No existe	No se cumple
Procedimientos de seguridad de la información	POLITICA SEGURIDAD	Existen procedimientos relativos a la seguridad de los Sistemas de Información	No existe	No se cumple
Responsable de las políticas, normas y procedimientos en Seguridad de la información	ORGANIZACION SEGURIDAD	Existe un responsable de las políticas, normas y procedimientos en Seguridad Informática	No existe	No se cumple
Comunicación de las normas	ORGANIZACION SEGURIDAD	Existen mecanismos para la comunicación a los usuarios de las normas	No existe	No se cumple

Verificar efectividad de las políticas	ORGANIZACION SEGURIDAD	Existen controles regulares para verificar la efectividad de las políticas	No existe	No se cumple

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD				
ORGANIZACIÓN INTERNA				
Compromiso de la jefatura en temas de seguridad con la información	COMUNICACION	Existe un comité de gestión de la seguridad de la información y se ha realizado una asignación adecuada y definida de responsabilidades.	No existe	No se cumple
Evaluación de la adquisición y cambios de los Sistemas de Información	ADQUISICION	Existe un responsable encargado de evaluar la adquisición y cambios de los Sistemas de Información	No existe	No se cumple
Coordinación en temas de seguridad dentro de la institución	ADQUISICION	Existe coordinación entre los diferentes roles y funciones.	No existe	No se cumple
Responsables en temas de seguridad de información en la institución	SEGURIDAD	Están definidos los activos de información y aunque en algunos casos existe alguna asignación de responsabilidades, esta no se da de manera formal.	No existe	No se cumple

Acuerdo de confidencialidad	COMUNICACION	Existe un acuerdo de confidencialidad de la información a la que se accede, se cree que es aceptable compartir información textual o imágenes sobre operaciones de carácter confidencial sabiendoque se trata de un hecho de fuga de información y puede constituirse en delito de infidencia.	Existe	No se cumple
Niveles y acuerdos en temas de confidencialidad	COMUNICACION	En algunos casos dentro de la institución se han realizado algunos acuerdos en temas de confidencialidad, pero muchas veces estos no se monitorean de manera periódica, mucho menos cuando se incorporan nuevos activos de información en la institución.	Existe	No se cumple
Autorización de recursos asociados a la seguridad de la información	COMUNICACION	Existe un proceso de autorización para los nuevos recursos orientados a procesos de información, pero este proceso no es del todo formal, ya que no existe una documentación correspondiente.	No existe	No se cumple

Relación conotras áreas	COMUNICACION	Existen algunos procedimientos referenciados a prevenir algunos riesgos, pero en el caso de la seguridad de la información no se establece un procedimiento formal adecuado.	No existe	No se cumple
Revisión independiente del referente a la seguridad de la información	COMUNICACION	No específicamente en todas las áreas de la institución se realizan revisiones orientadas a temas de seguridad, ya que no cuentan con una política clara específica que termine definiendo la frecuencia y la metodología de la revisión.	No existe	No se cumple

GESTIÓN DE ACTIVOS				
RESPONSABLES DE LOS ACTIVOS EN LA INSTITUCIÓN				
Inventario de activos	SISTEMAS / REDES	El inventario de activos que son propiedad de la institución es adecuado.	No existe	No se cumple
Propietario de los activos	SISTEMAS / REDES	Al no existir un inventario, es asignado un propietario al activo de forma genérica y no específica.	No existe	No se cumple
Clasificación por criticidad	SISTEMAS / REDES	Se dispone de una clasificación de la información según la criticidad de la misma	No existe	No se cumple
Soporte a los activos de información	SISTEMAS / REDES	Están actualizados los sistemas operativos, antivirus, aplicaciones y programas de los equipos de cómputo; asimismo, estos son los adecuados.	No existe	No se cumple
Controles y autenticación	SISTEMAS / REDES	Existe algún control en las redes para compartir archivos digitales	No existe	No se cumple
Controles y autenticación	SEGURIDAD FÍSICA	Están configuradas pantallas de bloqueo en los equipos de cómputo dado el tiempo de inactividad	No existe	Cumple
Perímetro de seguridad	SEGURIDAD FÍSICA	El perímetro de seguridad física es eficiente (una pared, puerta con llave, control de acceso físico)	No existe	No se cumple
Registro de incidentes	RR.HH.	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	No existe	No se cumple
Uso aceptable de los recursos informáticos en la institución	RR.HH.	En la institución existe una publicación orientada a términos de conducta y guía	No existe	No se cumple

		generalizada sobre el buen uso adecuado de los recursos de información.		

CLASIFICACIÓN DE LA INFORMACIÓN				
INFORMACIÓN DE LA INSTITUCIÓN				
Directrices de clasificación	RR.HH.	Se cuenta con una clasificación de información del personal de la institución, clasificando los activos de información que no contengan datos personales y tampoco se identifican según su criticidad para la institución.	No existe	No se cumple
Etiquetado y tratamiento en temas de seguridad	SEGURIDAD FÍSICA	La información clasificada suele estar etiquetada y tiene un tratamiento adecuado a las características, aunque con algunas limitaciones ya que a veces no está correctamente clasificada.	No existe	No se cumple
CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD				
POLÍTICAS DE SEGURIDAD				
Cumplimiento de las políticas y normas de seguridad	CUMPLIMIENTO	Ausencia de informes formales sobre revisiones del cumplimiento por parte de la jefatura, aunque en algunos casos de manera informal se suele realizar este seguimiento.	No existe	No se cumple
Comprobación del cumplimiento técnicos	CUMPLIMIENTO	Se han realizados algunas auditorías técnicas y procedimentales, la	No existe	No se cumple

		institución posee los informes, se analizan los resultados e informes y se implementan los resultados para beneficio de la institución.		

GLOSARIO DE TÉRMINOS:

- **Evaluación de riesgos**
  Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del organismo.

- **Administración de riesgos**
  Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

- **Comité de Seguridad de la Información**
  El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas de la empresa Severox Perú, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

- **Responsable de Seguridad Informática**
  Es la persona que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a los integrantes del organismo que así lo requieran.

- **Incidente de seguridad**
  Un incidente de seguridad es un evento adverso en un sistema de computadoras, aplicación informática o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN DE APLICABILIDAD

Versión: 01

Código	:	**DDA**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

CONTENIDO

DECLARACIÓN DE APLICABILIDAD

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir los controles adecuados a implementarse en la empresa Severox Perú S.A.C, además de identificar los objetivos, forma de implementación, aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.
Este documento incluye todos los controles detallados en el Anexo A de la Norma ISO/IEC 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).
Los usuarios de este documento son el personal de la empresa Severox Perú S.A.C, que se encuentran inmersos en las funciones del SGSI.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- informe de evaluación y tratamientos de riesgos

3. APLICABILIDAD DE LOS CONTROLES

Son aplicables los siguientes controles del Anexo A de la norma ISO/IEC 27001:2013

ID	Controles norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos deControl	Método de implementación	Estado
A.5	Políticas de la seguridad de la información	Si	Políticas de seguridad de la información	La Dirección de la organización dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables.	Planificado
A.5.1	Dirección de la gerencia para la seguridad de la información	Si	Documento de política de seguridad de la información	La dirección deberá aprobar un documento de políticas de seguridad de la información, publicarlo y distribuirlo a todo el personal de la empresa Severox Perú S.A.C	Planificado
A.5.1.1	Políticas para seguridad de la información	Si	Políticas de seguridad de la información	La dirección de la organización dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables. Todas las políticas indicadas bajo esta columna	Planificado
A.5.1.2	Revisión de políticas para seguridad de la información.	Si	Revisión de políticas para seguridad de la información.	Cada política tiene un propietario designado que deberá revisar el documento según un intervalo planificado.	Planificado

A.6	Organización de la seguridad de la información.	Si	Organización Interna	Gestionar la seguridad de la información dentro de la organización, mediante cargos y jerarquías	Planificado
A.6.1	Organización interna	Si	Organización Interna	Gestionar la seguridad de la información dentro de la organización, mediante cargos y jerarquías	Planificado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si	Responsabilidades sobre los Activos de información	Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información	Planificado
A.6.1.2	Segregación de deberes	Si	Asignación de responsabilidades relativas a la seguridad de la información	Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra. Donde se definirán claramente las responsabilidades y deberes relativos a la seguridad de la información.	Planificado
A.6.1.3	Contacto con autoridades	Si	Contacto con las autoridades	Se deben mantener los contactos adecuados con las autoridades competentes de la organización, tomando en cuenta las estrategias de continuidad del negocio y el plan de respuesta ante incidentes.	Planificado

A.6.1.4	Contacto con grupos de interés especial	Si	Contacto con grupos de especial interés	El jefe de SIG es el responsable de supervisar (detallar los nombres de grupos de interés y foros de seguridad), donde se mantendrán los contactos adecuados con grupos de interés especial u otros, asociaciones profesionales especializadas en seguridad.	Planificado
A.6.1.5	Seguridad de la información en gestión de proyecto	SI	Ordenadores portátiles, comunicaciones móviles y teletrabajo	El gerente de proyecto debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto, así como las acciones y tareas a cumplir que le sean asignadas a cada integrante del grupo.	
A.6.2	Dispositivos móviles y teletrabajos	Si	Ordenadores portátiles, comunicaciones móviles y teletrabajo	Se implantará una política formal, adoptando las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y dispositivos móviles.	Planificado
A.6.2.1	Política sobre dispositivos móviles	Si	Ordenadores portátiles y comunicación es móviles	El equipamiento puede ser llevado fuera de las instalaciones solamente en caso sea requerido, pero no se podrá filtrar ni copiar ninguna información que salga de los sistemas de información de la organización, así como el uso de tarjetas de memoria, medios de transferencia de datos.	Planificado

A.6.2.2	Teletrabajo	Si	Teletrabajo	Se redactará e implementará una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondiente.	Planificado

4. DOCUMENTOS DE REFERENCIA

En adelante se recogen las funciones y obligaciones, para el personal de la empresa Severox Perú S.A.C con acceso a los sistemas de información. Así como la previa definición de las funciones y obligaciones del personal, teniendo como objeto:
Proteger los sistemas de información, así como las redes de comunicación propiedad de la organización o bajo su responsabilidad, contra el acceso o uso que no sea autorizado, así como la alteración indebida, destrucción o mal uso.
Proteger la información perteneciente o proporcionada a la organización en contra de revelaciones no autorizadas o de modo accidental.
A efecto de dar cumplimiento con estas obligaciones independientemente de la función que desempeña o responsabilidades que tiene, la organización exige un carácter general a cualquier empleado el cumplimiento de los siguientes aspectos:

- Confidencialidad de la información
- Propiedad intelectual
- Control de acceso físico
- Salidas y entradas de información
- Incidencias
- Uso apropiado de los recursos
- Software
- Hardware
- Conectividad a la red de internet

4.4. Confidencialidad de la información

a) Se debe proteger la información propia o confiada de la empresa evitando el uso indebido o su envío no autorizado al exterior a través de cualquier medio de comunicación.
b) Se deberá guardar máxima reserva, por un tiempo indefinido, la información, documentos, claves, análisis, programas y el resto de información a la cual se tenga acceso dentro de la empresa.
c) En caso de manejar información confidencial, en cualquier tipo de soporte, se deberá entender que la posesión de la misma es temporal, con una obligación de secreto por parte del personal y sin que ello le considere derecho alguno de posesión, titularidad o copia de la misma, inmediatamente después de haber realizado y finalizado las tareas que se hubieran originado, esta debería devolverse a la organización.

4.5. Propiedad intelectual

Queda totalmente prohibido en los sistemas de información de la organización:
a) El uso de aplicaciones informáticas sin la correspondiente licencia. Así como los programas informáticos propiedad de la organización, están protegidos por la propiedad intelectual por lo tanto queda

rotundamente prohibida su reproducción, modificación, cesión o comunicación sin ninguna autorización previa.
b) El uso, reproducción, modificación, cesión o comunicación de cualquier otro tipo de obra protegida por la propiedad intelectual sin la debida autorización correspondiente.

4.6. Control de accesos físicos

a) Las normas orientadas al acceso físico de las instalaciones de la empresa que albergan los sistemas de información y los locales de tratamiento son los siguientes:
b) El acceso a las instalaciones de la organización donde se encuentran los sistemas de información y locales de tratamiento, será realizado previo paso por un sistema de control de acceso físico o con la autorización del responsable(s) de las instalaciones de la empresa.

4.7. Salidas y entradas de información

a) Todo tipo de salida y entrada de información de la organización sea esta de carácter personal, deberá ser realizada por el personal autorizado y será necesaria la autorización formal del responsable del fichero de donde provienen los datos.
b) Para la salida de la información de alto nivel confidencial, se deberán cifrar los mismos o utilizar cualquier otro mecanismo que no permitan el acceso o su manipulación durante el transporte.

4.8. Incidencias

a) El personal de la organización y de terceras partes, tiene como obligación la comunicación de cualquier incidencia que se pueda producir la cual esté relacionada con los sistemas de información o de cualquier otro recurso informático de la organización.
b) La comunicación, gestión y resolución de las incidencias de seguridad se realizarán mediante el sistema de gestión de incidencias es cual es habilitado por la organización.

4.9. Uso apropiado de los recursos informáticos

Los recursos informáticos ofrecidos por la organización (datos, software, comunicaciones, etc.), están disponibles exclusivamente para cumplir con las obligaciones labores y con una finalidad corporativa. Por lo que queda terminantemente prohibido cualquier uso distinto del indicado, algunos ejemplos:

a) El uso de los recursos de la organización, así como los que están bajo su supervisión para actividades no relacionadas con la finalidad de la organización.

b) El uso de los equipos, dispositivos o aplicaciones los cuales no estén especificados como parte de software y/o hardware contenidos en la organización.
c) Introducir en los sistemas de información o red corporativa contenidos ilegales, inmorales u ofensivos y en general, sin utilidad alguna en los procesos del negocio de la organización.
d) Introducir voluntariamente programas, virus, spyware o cualquier otro software malicioso que sean susceptibles de causar alteraciones en los recursos informáticos de la organización hacia terceros.
e) Desactivar o inutilizar los programas antivirus y de protección de los equipos y sus actualizaciones.
f) Intentar eliminar, modificar, inutilizar los datos, programas o cualquier otra información propios de la organización.
g) Conectarse a la red corporativa a través de otros medios que no sean los definidos y administrados por la organización.
h) Intentar descubrir o descifrar las claves de acceso o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la empresa.

4.10. Uso apropiado de los recursos y sistemas operativos

a) Los usuarios deben utilizar únicamente las versiones de software facilitadas por la organización y así seguir las normas de utilización.

b) La oficina de Tecnologías de la Información y Comunicación de la empresa, es el responsable de definir los programas de uso estandarizado en la organización y de realizar las instalaciones en los PCs.
c) Los usuarios no deben instalar ni borrar ningún tipo de programa informático en su PC.

4.11. Hardware

a) El personal en su actividad laboral, deben hacer uso únicamente del hardware instalado en los equipos propiedad de la organización y cuya función lo requiere para el trabajo que desempeña.
b) El personal en ningún caso accederá físicamente al interior del equipo que tiene asignado para su trabajo o que pertenezca a la propiedad de la organización. En caso necesario se comunicará la incidencia, según el protocolo habilitado, para que el departamento indicado o en su defecto el encargado de su función, realice las tareas de reparación, instalación o mantenimiento.
c) Los usuarios no manipularán los mecanismos de seguridad que la organización implemente en los dispositivos (equipos, portátiles, móviles, etc.)
d) No sacar equipos, dispositivos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles y medidas que se hayan establecido para cada supuesto.

4.12. Conectividad a la red de Internet

Las normas referentes al correo electrónico son:

a) El servicio de correo electrónico que la organización pone a disposición de los usuarios tiene un uso estrictamente profesional y destinado a cubrir las necesidades del puesto.
b) Queda terminantemente prohibido intentar leer, copiar o borrar mensajes de correo electrónico de otros usuarios.
c) El personal no debe enviar mensajes de correo electrónico de manera masiva o de tipo primordial con fines publicitarios o comerciales. En el caso que sea necesario, dada la función del usuario, este tipo de mensajes se gestionará con la dirección de la organización y con el responsable de seguridad.

SEVEROX
PASIÓN E INGENIO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DE TRATAMIENTO DE RIESGOS

Versión: 01

Código	:	**PTDR**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

Actividad	Recursos generales y financieros requeridos	Recursos humanos requeridos	Recursos de capacitación	Control de riesgos (evitar, prevenir y proteger)	Función del riesgo (aceptar, retener o transferir)	Opciones del riesgo
Políticas para seguridad de la información	Documentación en papel oformato digital, recursos asumidos la empresa.	Personal encargado de gestionar la documentación referente a las políticas de seguridad	Ciclos de capacitación al personal, dado por personal experto o especialista en seguridad de la información e informática.	Prevenir	Transferir	Elección de controles
Revisión de las políticas para seguridad de la información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal la empresa TI experto en temas de seguridad, con apoyode personal especializado.	Ciclos de capacitación dirigida al personal que interactúa con los sistemas de información.	Proteger	Retener	Evitar el riesgo
Inventario de activos	Inventario de los activos de la institución a cargo de personal de la empresa.	Personal experto en levantamiento de políticas de la seguridad de la información	Registros para entender mejor las necesidades de seguridad de información y determinar los controlespara asegurar la confidencialidad, integridad y disponibilidad de la información	Prevenir	Aceptar	Elección de controles
Mantenimiento de equipo	Recursos del presupuesto alcanzado para los equipos e infraestructura de la institución.	Personal técnico especializado en el área de tecnologías de información e infraestructura de hardware y software.	Mantenimiento para los equipos de la institución bajo tres aspectosde capacitación: mantenimiento preventivo, correctivo y predictivo.	Prevenir	Aceptar	Evitar el riesgo
Procedimientos y políticas sobre transferencia de información	Recursos utilizados por la institución asignados en el presupuesto de la empresa	Personal encargadode velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas adefinir y mejorar procedimientos de manejo de información, así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo
Cumplimiento con las políticas y estándares de seguridad	Recursos utilizados porla institución.	Personal encargado de velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas adefinir y mejorar procedimientos de manejo de información, así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo

Revisión independiente de la seguridad de lainformación	Documentación en papel o formato electrónico, Recursos asumidos la empresa.	Personal encargado de gestionar la documentación referente a las políticas de seguridad	Programas de capacitación al personal, dadopor personal experto en temas de seguridad.	Prevenir	Transferir	Elección de controles
Reporte de debilidades en la seguridad dela información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal de la empresa experto en temas de seguridad.	Programas de capacitación dirigida a losempleados de la institución que interactúan con los sistemas de información	Proteger	Retener	Evitar el riesgo
Análisis y especificación de los requerimientos de seguridad de la información	Recursos utilizados por la institución orientados al levantamiento de requisitos de seguridad para la institución y próximos a su implantación	Personal experto en toma de requerimientos y necesidades de la institución enfocadosa la seguridad en los sistemas de información	Programas de capacitación al personal, dado por personal experto en temas de seguridad.	Evitar	Aceptar	Elección de controles
Procedimientos documentados de operación	Recursos necesarios apoyados por la empresa.	Personal capacitado en labores de documentación y operación.	Recurso asignado por la empresa orientado a brindar capacitación al personal en términos documentarios.	Proteger	Transferir	Elección de controles

SEVEROX
PASIÓN E INGENIO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DE INSTRUCCIÓN Y CAPACITACIÓN

Versión: 01

Código	:	**PIYC**
Fecha	:	**06/01/2022**
Creado por	:	**Osmar Raúl, Ticona Bustinza**
Aprobado por	:	**Jefe del área de TI**
Confidencialidad	:	**Intimo / Intermedio / Superficial**

PLAN DE INSTRUCCIÓN NO 001 -2022 SEVEROX

(PARA EJECUTAR CICLO DE CHARLAS PERSONALIZADAS DE INSTRUCCIÓN AL PERSONAL DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, DIRIGIDO AL PERSONAL DE LA EMPRESA SEVEROX PERU S.A.C)

I. GENERALIDADES

1.1. OBJETIVOS

Establecer normas y procedimientos para impartir conocimientos y procedimientos para la aplicación adecuada del Sistema de Gestión de Seguridad de la Información, dirigido al personal de la empresa Severox Perú S.A.C.

1.2. FINALIDAD

a. Unificar criterios para la organización y ejecución del "Ciclo de Charlas teórico-practicas", relacionados a la aplicación adecuada del Sistema de Gestión de Seguridad de la Información.
b. Orientar al personal de la empresa Severox Perú S.A.C, el cumplimiento de los dispositivos legales y normas vigentes y la aplicación del Sistema de Gestión de Seguridad de la Información.
c. Establecer los principios ético-profesionales y de disciplina en el comportamiento del personal, para lograr exitosamente la implementación del Sistema de Gestión de Seguridad de la Información.

1.3. ALCANCES

El presente Plan de Instrucción, rige para todo el personal de la empresa Severox Perú S.A.C

II. OBJETIVOS

2.1. GENERAL

a. Lograr que el personal de la empresa Severox Perú S.A.C, a través del ciclo de charlas personalizadas desarrolladas por Jorge Luis Rodriguez Pinto, sean capacitados en el uso adecuado del Sistema de Gestión de Seguridad de la Información y pleno conocimiento de las Políticas de Seguridad, que conlleven a elevar los niveles de seguridad en el manejo de la información para mitigar los riesgos de los activos de información identificados.
b. Reducir las deficiencias en el uso y manejo de la información confidencial de Severox Perú que propician fugas o pérdidas de información.

2.2. ESPECÍFICOS

Lograr que el personal de la empresa Severox Perú S.A.C, adquiera conocimientos, habilidades y destrezas relativos a:

a. La observancia y práctica de normas relacionadas sobre el uso adecuado del Sistema de Gestión de Seguridad de la Información y pleno conocimiento de las Políticas de Seguridad.
b. Instruir al personal de la empresa Severox Perú S.A.C. en el empleo de los métodos, técnicas y procedimientos de protección de los activos de la información.
c. Consolidar en los participantes los valores ético-morales que les permita actuar con cautela en sus labores sobre uso y manejo de información.
d. Preparar teórica, práctica y psicológicamente al personal en su totalidad, para cumplir eficientemente con el uso adecuado de la información de carácter secreto, reservado y confidencial.

III. METAS

3.1. DE ATENCIÓN

El objetivo es capacitar a la totalidad del personal, que este laborando en la empresa Severox Perú S.A.C.

3.2. DE OCUPACIÓN

La instrucción teórico y práctica estará a cargo de Jorge Luis Rodriguez Pinto, con experiencia académica, especialmente en las políticas y normas de seguridad de la información.

IV. PERFIL EDUCATIVO

4.1. COMO PERSONA

1. Demostrar equilibrio emocional.
2. Demostrar honestidad, moralidad y ética profesional.
3. Demostrar respeto por la persona humana profesional.
4. Demostrar vocación de servicio, espíritu de equilibrio y justicia.
5. Desarrollar perseverancia y sentido de responsabilidad.

4.2. COMO CIUDADANO

1. Demostrar respeto por las leyes y normas de cortesía.
2. Demostrar espíritu de solidaridad con sus semejantes.
3. Demostrar capacidad de diálogo y/o comunicación.
4. Demostrar capacidad de convivencia fraterna dentro de la comunidad.

4.3. COMO PROFESIONAL

1. Los participantes al término del ciclo de charlas del uso adecuado del Sistema de Gestión de Seguridad de la Información, tendrán pleno conocimiento de las Políticas de Seguridad, evitando en el futuro posibles deficiencias en el uso y manejo del Sistema de Gestión de Seguridad de la Información.

2. Dominio y seguridad en su accionar, demostrando experiencia, tino y profundo conocimiento de las normas y políticas legales vigentes y de seguridad de los activos de información.

3. Lograr que los participantes se familiaricen y amplíen sus conocimientos en los métodos y técnicas del uso del Sistema de Gestión de Seguridad de la Información.

4. Dominio total del Sistema de Gestión de Seguridad de la Información, con conocimiento de las políticas y normas de seguridad para los activos de la información.

V. ESTRUCTURA CURRICULAR

5.1. ORGANIZACIÓN CURRICULAR

5.1.1. TEMARIO

- Definición de información
- Definición de un Sistema de Gestión de Seguridad de la Información
- La Norma UNE-ISO/IEC 27001:2013
- Gestión de riesgos
- Políticas de seguridad de la información

5.1.2. DISTRIBUCIÓN DEL TIEMPO

- El presente ciclo de charlas se ejecutará del 26 al 20FEB22, antes de iniciar de la jornada (08:00 hrs.)
- El tiempo de exposiciones tendrán una duración de 30 minutos.
- Asimismo, se realizará una retroalimentación el 30MAR22, de 08:00 a 09:30 hrs.

5.2. ADMINISTRACIÓN CURRICULAR

5.2.1. METODOLOGÍA DE LA ENSEÑANZA

- La enseñanza se efectuará mediante charlas por 4 días (20 al 28FEB22) durante 30 minutos y un Taller de retroalimentación que se realizará en única fecha el 30MAR22, por espacio de 1:30 horas.

- Se ejercitará la capacidad analítica y critica del participante el día de la retroalimentación (30MAR22).
- Se atenderá por igual las necesidades individuales de los participantes, las consultas se realizarán en cualquier momento de la jornada laboral.
- Los conocimientos impartidos se aplicarán a situaciones reales, buscando la participación activa del participante.

VI. RECURSOS

6.1. FINANCIAMIENTO

Los recursos logísticos serán proporcionados por el área de planeamiento autorizado por el gerente general de la empresa.

6.2. INFRAESTRUCTURA

El presente ciclo de charlas se realizará en las oficinas de la empresa Severox Perú S.A.C del 20 al 28FEB22 y en el auditorio empresa el 30MAR22.

Arequipa, 20 de febrero del 2022

Anexo 5: Permiso de Autorización de la empresa

Permiso de autorización de la Empresa

Arequipa, 10 de enero de 2022

La empresa SEVEROX PERU SOCIEDAD ANONIMA CERRADA con R.U.C. N° 20605834788 se compromete a brindar la información solicitada para el desarrollo del trabajo/tesis, la misma que solo puede ser utilizada para fines estrictamente académicos vinculados al trabajo.

Declaramos conocer que el trabajo de investigación/tesis Modelo de seguridad de la información basado en la normativa ISO/IEC 27001 :2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021

será de público conocimiento a través del repositorio institucional de la universidad.

Cordialmente,

NOMBRES Y APELLIDOS DEL REPRESENTANTE DE LA INSTITUCIÓN:	**LENNON POUL ROJAS SANZ**
D.N.I.	**73249257**
CARGO QUE OCUPA:	**GERENTE GENERAL**
FIRMA Y SELLO:	

Anexo 6: Permiso de autorización de la Universidad

UNIVERSIDAD CÉSAR VALLEJO

"Año del Fortalecimiento de la Soberanía Nacional"

LOS OLIVOS, 15 de febrero de 2022

Señor(a)
ROJAS SANZ LENNON POUL
GERENTE GENERAL
SEVEROX PERÚ SAC
AV. MIGUEL GRAU NRO. 578 ACEQUIA ALTA

Asunto: Autorizar para la ejecución del Proyecto de Investigación de INGENIERÍA DE SISTEMAS

De mi mayor consideración:

Es muy grato dirigirme a usted, para saludarlo muy cordialmente en nombre de la Universidad Cesar Vallejo Filial LOS OLIVOS y en el mío propio, desearle la continuidad y éxitos en la gestión que viene desempeñando.

A su vez, la presente tiene como objetivo solicitar su autorización, a fin de que el Bach. OSMAR RAUL TICONA BUSTINZA del Programa de Titulación para universidades no licenciadas, Taller de Elaboración de Tesis de la Escuela Académica Profesional de INGENIERÍA DE SISTEMAS, pueda ejecutar su investigación titulada: **"MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMATIVA ISO/IEC 27001 :2013 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE LA INFORMACIÓN EN LA ENTIDAD PRIVADA SEVEROX PERÚ SAC, AREQUIPA, 2021."**, en la institución que pertenece a su digna Dirección; agradeceré se le brinden las facilidades correspondientes.

Sin otro particular, me despido de Usted, no sin antes expresar los sentimientos de mi especial consideración personal.

Atentamente,

UCV UNIVERSIDAD CÉSAR VALLEJO ING. DE SISTEMAS COORDINADOR

Ing. M. Sc. Janina Cotrina Linares.
Coordinadora de la Escuela de Ingeniería de Sistemas
UCV - Tarapoto

cc: Archivo PTUN.

Anexo 7: Informe de reunión con los interesados

INFORME DE LA REUNION

En la empresa SEVEROX PERU SAC el día 11 enero del 2022 se hizo una entrevista a representantes de la empresa esto para obtener información sobre procesos y conocimiento de la de la estructura ti lo cual ayudara para el desarrollo del proyecto y tener conocimiento sobre la empresa.

Primeramente, la entrevista con el gerente y el jefe de área TI donde se nos brindó información necesaria y se nos permitirá reuniones para presentación de avances y correcciones si es necesario.

En la entrevista con el jefe de ti donde se ingresó al área de TI, se nos informó la cantidad de equipos que utilizan en la empresa,

Se dio conocer que el ingreso a áreas no autorizadas o el I cuarto de telecom que se encuentra en el área de TI, al ingreso se procede a llenar una bitácora de ingreso al igual un registro de salida.

En el cuarto de telecom se pudo observar 2 servidores, 3 switch, 3 router.

El primer servidor es un servidor de dominio el cual permite autentificar a los usuarios trabajadores de la empresa.

El segundo servidor es un servidor de archivos file server el cual tiene una unidad compartida para cada área dependiendo del perfil de cada usuario.

Después se procedió a ir con el jefe de planificación el cual nos mostró todas las demás áreas de la empresa y nos indico como era el proceso de cada área. Se pudo observar que tenían 3 switch instalados replicadores.

Y al ingresar a cada área se pudo observar que utilizan los medios de tratamiento de información o comunicación tales como Telegram, WhatsApp, y correos institucionales(corporativos) medio por el cual se comunican con los clientes muy independientemente de los números telefónicos por vía celular.

Osmar Raúl, Ticona Bustinza

Anexo 8: Acta de Conformidad de la empresa

ACTA DE CONFORMIDAD DEL DESARROLLO DE INVESTIGACIÓN

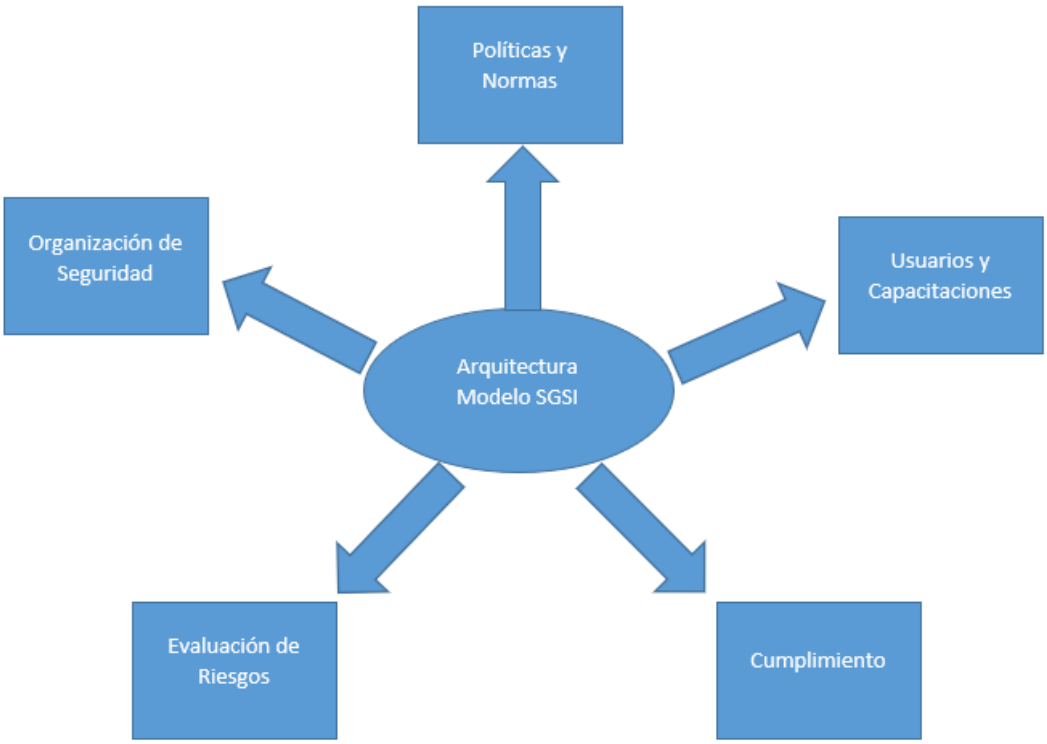
Mediante los documentos de la referencia, el Gerente General de la empresa Severox Peru S.A.C da la conformidad del levantamiento de requerimientos en el marco de investigación realizada por el bachiller.

Antes de iniciar el desarrollo del presente análisis, es necesario precisar de que todos los requerimientos levantados por el investigado son aprobados por él área de informática de la empresa y validados con él encargados de la misma, es por ello que se da conformidad al levantamiento de información y el análisis que el investigador está haciendo para la mejora de los procesos y continuidad del negocio en la empresa Severox Peru S.A.C.
Teniendo en cuenta que el investigador encontró algunas inconformidades que en el proceso del análisis nos irá haciendo llegar según valla avanzando su investigación.

Sin otro particular doy por aprobada esta acta de conformidad por parte de la empresa Severox Peru S.A.C teniendo conocimiento del estado actual de los procesos y modo de trabajo de las diferentes áreas.

Lennon Rojas Sanz
Gerente general

Anexo 9: Arquitectura sistema de gestión de seguridad de la información



Anexo 10: Análisis de Riesgos con Herramienta Pilar

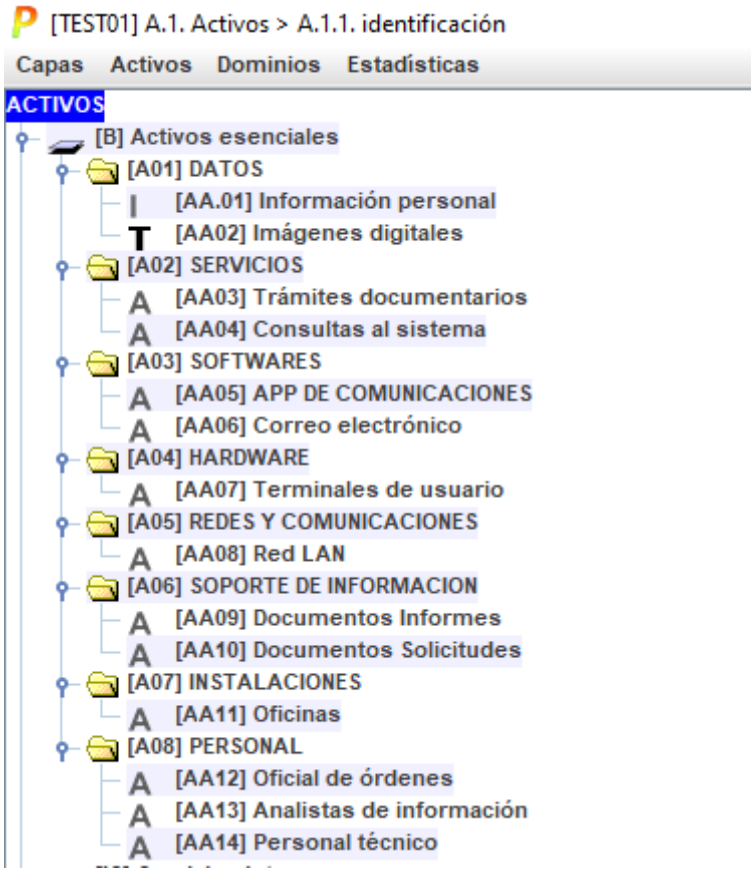
DATOS GENERALES

[TEST01] Contexto

biblioteca [std] Biblioteca INFOSEC (8.10.2019) (basic_74.pl5)
código TEST01
nombre ANALISIS DE RIESGO_SEVEROX
proyecto - clasificación DIFUSIÓN LIMITADA
RGPD contexto

código	nombre	
org	Organización	SEVEROX SAC
desc	Descripción	ANILISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION
author	Autor	SEVEROX SAC
version	Versión	1.0
date	Fecha	24/01/2022
owner	Responsable del Sistema	OSMAR TICONA
ciso	Responsable de la Seguridad de la Información	JORGE RODRIGUEZ

ACTIVOS IDENTIFICACION



CLASIFICACION DE ACTIVOS

[TEST01] A.1. Activos > A.1.2. clases de activos

clases de activos

ACTIVOS

- [B] Activos esenciales
  - [A01] DATOS
    - [AA.01] Información personal
      - {essential.{info.{biz, classified.{TS, S, C, R, UC}}}}
    - [AA02] Imágenes digitales
      - {essential.{ppd.{1, 2, 3}}}
  - [A02] SERVICIOS
    - [AA03] Trámites documentarios
      - {S.{client.{email, www, telework}}}
    - [AA04] Consultas al sistema
      - {S.{prov.{int, edi}}}
  - [A03] SOFTWARES
    - [AA05] APP DE COMUNICACIONES
      - {SW.std.other}
    - [AA06] Correo electrónico
      - {SW.{std.{email_client, email_server}}}
  - [A04] HARDWARE
    - [AA07] Terminales de usuario
      - {HW.{pc, peripheral.{print, scan}}}
  - [A05] REDES Y COMUNICACIONES
    - [AA08] Red LAN
      - {COM.{radio, wifi, LAN}}
  - [A06] SOPORTE DE INFORMACION
    - [AA09] Documentos Informes
      - {Media.{electronic.{disk, san, usb}, non_electronic.printed}}
    - [AA10] Documentos Solicitudes
      - {Media.{electronic.{disk, san, usb}, non_electronic.printed}}
  - [A07] INSTALACIONES
    - [AA11] Oficinas
      - {L.building}
  - [A08] PERSONAL
    - [AA12] Oficial de órdenes
      - {P.ui}
    - [AA13] Analistas de información
      - {P.ui}
    - [AA14] Personal técnico
      - {P.ui}

CLASES DE ACTIVOS

- [essential] Activos esenciales
- [arch] Arquitectura del sistema
- [availability] disponibilidad
- [evaluated] Productos o servicios evaluados
- [D] Datos / Información
- [keys] Claves criptográficas
- [S] Servicios
- [SW] Aplicaciones (software)
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal
- [other] Otras clases

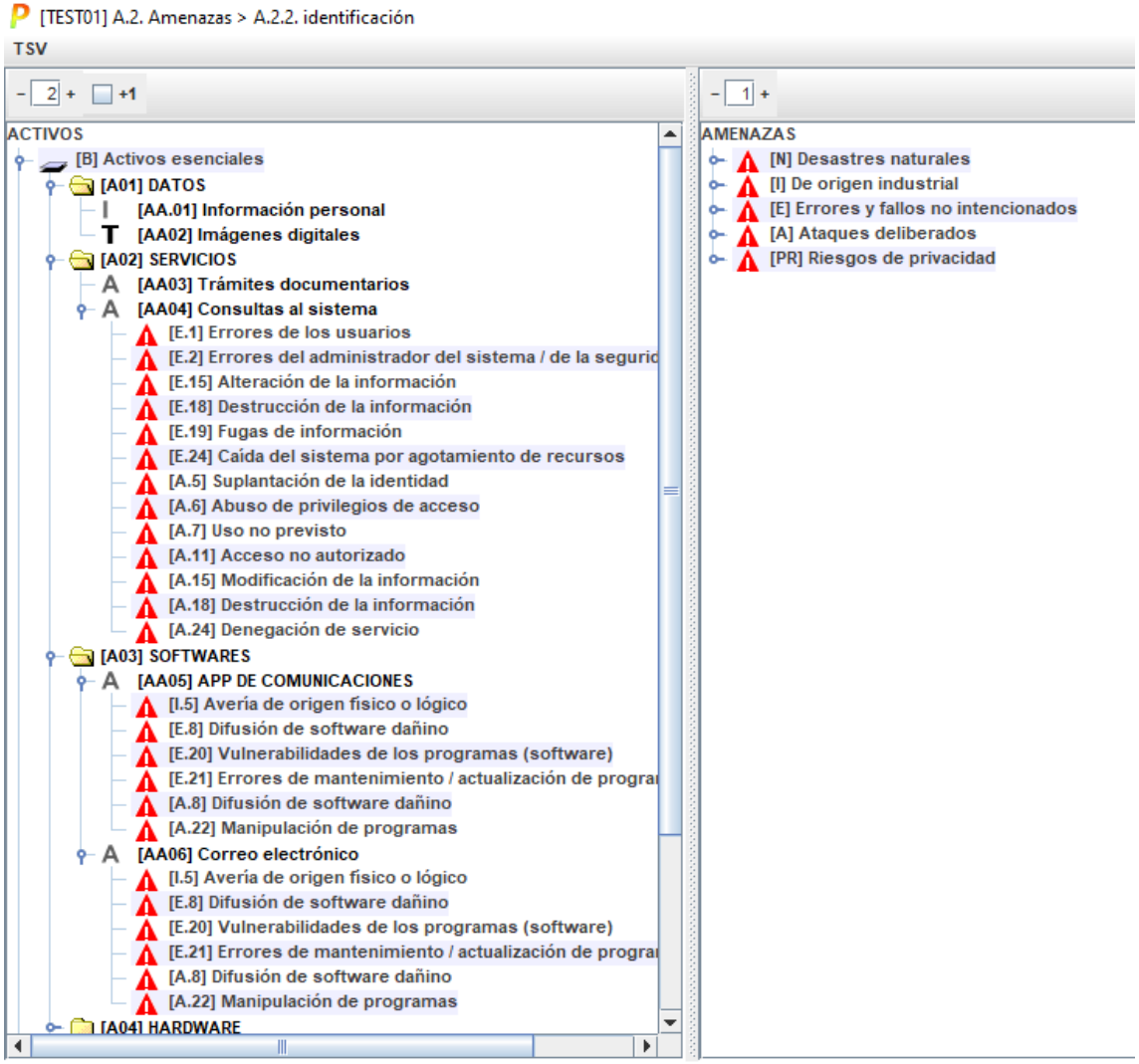
VALORACION DE LOS ACTIVOS

[TEST01] A.1. Activos > A.1.4. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[A01] DATOS				
[AA.01] Información personal	[10]	[10]	[10]	[10]
[AA02] Imágenes digitales	[10]	[10]	[10]	[10]
[A02] SERVICIOS				
[AA03] Trámites documentarios	[6]	[5]	[6]	[6]
[AA04] Consultas al sistema				
[A03] SOFTWARES				
[AA05] APP DE COMUNICACIONES	[10]	[10]	[10]	[10]
[AA06] Correo electrónico	[10]	[10]	[10]	[10]
[A04] HARDWARE				
[AA07] Terminales de usuario	[7]	[7]	[7]	[9]
[A05] REDES Y COMUNICACIONES				
[AA08] Red LAN	[7]	[7]	[9]	[8]
[A06] SOPORTE DE INFORMACION				
[AA09] Documentos Informes	[10]	[10]	[10]	[10]
[AA10] Documentos Solicitudes	[10]	[10]	[10]	[10]
[A07] INSTALACIONES				
[AA11] Oficinas	[8]	[8]	[7]	[7]
[A08] PERSONAL				
[AA12] Oficial de órdenes	[10]	[10]	[10]	[10]
[AA13] Analistas de información	[10]	[10]	[10]	[10]
[AA14] Personal técnico	[9]	[10]	[9]	[9]

AMENAZAS IDENTIFICACION



APLICABILIDAD CONTROLES SEGÚN PILAR

[TEST01] A.3. Medidas técnicas y o ... > A.3.1. aplicabilidad

Expandir Exportar Importar

...	tdp	salvaguarda
		SALVAGUARDAS
G	EL	[IA] Identificación y autenticación
G	std	[IA.1] Se dispone de normativa de identificación y autenticación
G	proc	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación
G	EL	[IA.3] Identificación de los usuarios
G	EL	[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)
G	EL	[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios
T	EL	[IA.3.3] Las cuentas de invitados están sometidas a un control estricto
G	EL	[IA.4] Gestión de la identificación y autenticación de usuario
G	AD	[IA.4.1] Se mantiene un registro de todos los usuarios con su identificador
G	AD	[IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario
G	EL	[IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador
G	EL	[IA.4.4] Se limita el número de autenticadores necesarios por usuario
G	EL	[IA.4.5] Los autenticadores se distribuyen de forma segura
G	AD	[IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticador
G	AD	[IA.4.7] El usuario confirma la recepción del autenticador
G	AD	[IA.4.8] El usuario se hace cargo personalmente del control del autenticador
G	MN	[IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)
G	IM	[IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello
G	EL	[IA.5] Cuentas especiales (administración)
T	EL	[IA.6] Canal seguro de autenticación
G	PR	[IA.7] {xor} Factores de autenticación que se requieren:
T	EL	[AC] Control de acceso lógico
G	PR	[D] Protección de la Información
G	AD	[D.1] modo evaluación
G	std	[D.2] modo evaluación
G	PR	[D.3] modo evaluación
G	PR	[D.I] modo evaluación
G	PR	[D.5] modo evaluación
G	RC	[D.backup] modo evaluación
T	EL	[D.DS] modo evaluación
G	IM	[D.TS] modo evaluación
G	EL	[K] Protección de claves criptográficas
G	EL	[K.IC] modo evaluación
G	EL	[K.DS] modo evaluación
G	EL	[K.disk] modo evaluación
G	EL	[K.comms] modo evaluación
T	EL	[K.509] modo evaluación
G	PR	[S] Protección de los Servicios

CUADRO DE INCIDENCIA DE RIESGOS

Cód	Identificación								Análisis Cualitativo					Análisis cuantitativo					
	Riesgo/oportunidad			Fuente	Propietario	Fechas clave			Prob	Impacto	*Risk rating*			Costo			Tiempo		
	Causa	Evento	Efecto			Identificación	materialización	¿Puede repetirse?			Prob	Impacto	*Risk Score*	Prob %	Impacto	VME	Prob %	Impacto (días)	VME

Cód	Planificación de respuesta								
	Estrategia					Plan de contingencia			
	Evitar Explotar	Mitigar Mejorar	Transferir Compartir	Aceptar	Escalar	Descripción	Disparador	Plan B (*fallback*). Descripción	Disparador	Riesgos secundarios

Cód	Implantación y control					
	Estatus	Ejecutor del riesgo	Acción	% ejecución	comentarios	Lecciones aprendidas

Categoría	
TEC	Técnicos
DIS	Diseño
EQ	Equipo
REC	Recursos
COM	Comerciales
CL	Cliente
INT	Interna
EXT	Externa

Estatus	
ACT	Activo
PEN	Pendiente de decisión
RES	Resuelto
ESC	Escalado

Anexo 11: Aceptación de políticas de seguridad

ACEPTACIÓN DE POLITICAS DE SEGURIDAD

En el presente documento se dejan establecidos los parámetros internos de Severox Perú S.A.C, frente a la publicación, lectura y aceptación de las políticas de seguridad de la empresa.

- Teniendo en cuenta lo anterior, con la firma del presente documento manifiesta conocer las políticas de seguridad publicadas en el manual único de políticas y procedimientos numeral **(1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN)**, publicado en la Intranet de la empresa. Se da por terminado con justa causa la correspondiente labor del Sr Osmar Raúl, Ticona Bustinza.

Para constancia se firma en Arequipa, el 25 de febrero del 2021

Acepto.

Firma:

Nombre: Lennon Rojas Sanz

Cargo: Gerente General

Anexo 12: Conducta de Responsabilidad

PERFIL

OSMAR RAUL TICONA BUSTINZA