ETAPA DE PLANEACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE GESTIÓN DE INFORMACIÓN EN LA EMPRESA GERS S.A.S.

ANDRES MAURICIO ESPINOSA MAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2022

ETAPA DE PLANEACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE GESTIÓN DE INFORMACIÓN EN LA EMPRESA GERS S.A.S.

ANDRES MAURICIO ESPINOSA MAYA

Proyecto de Grado – Proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2022

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Santiago de Cali, 29 de mayo de 2022

DEDICATORIA

Con gran orgullo dedico este trabajo a mis padres, que con su apoyo incondicional siempre han estado a mi lado a pesar de los tropiezos de la vida. Su esfuerzo por hacer que desde niño me comprometiera firmemente con la consecución de mis objetivos y por inculcar en mí, los principios y valores necesarios para ser una persona íntegra y con gran vocación de aprendizaje continuo

.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD en general, por su compromiso con la educación continua de los colombianos. Agradezco a los tutores que hicieron parte de mi proceso formativo y en especial a los docentes que, desde su experiencia profesional y educativa, me ayudaron a hacer realidad uno de mis principales sueños, graduarme como profesional y ser especialista en mi área de desempeño.

CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVOS DE INFORMACIÓN: es aquel que representa un valor para la organización debido a la información que contiene y por ende debe protegerse.

AMENAZA: es un incidente que es capaz de explotar una vulnerabilidad y materializar un ataque, lo que puede generar un daño sobre uno o más elementos que conforman el sistema de información.

ANEXO A: es una guía para implementar los controles definidos en la ISO/IEC 27001:2013. Está integrado por 14 secciones que a su vez se distribuyen entre 114 controles de seguridad.

CICLO PHVA: el ciclo de vida PHVA consiste en cuatro fases: planear, hacer, verificar y actuar. Es una metodología muy utilizada dentro de los sistemas de gestión por lo práctico y beneficioso que resulta.

CONFIDENCIALIDAD: garantizar que la información esté disponible y accesible en el momento que se requiera por parte de los usuarios y/o procesos autorizados.

DISPONIBILIDAD: garantizar que la información esté disponible y accesible en el momento que se requiera por parte de los usuarios autorizados.

INTEGRIDAD: esta propiedad vela por mantener la exactitud de los datos, es decir que no sea alterada por terceros durante su proceso de almacenamiento o transporte.

ISO/IEC 27001:2013: esta norma define los requisitos y requerimientos necesarios para establecer, implementar, mantener y mejorar un SGSI. Se divide en varias secciones: Introducción, alcance, referencias normativas, términos y definiciones, contexto de la

organización, liderazgo, planificación, apoyo o soporte, funcionamiento u operación, evaluación de desempeño, mejora continua.

ISO/IEC 27002: de acuerdo con los lineamientos de la ISO/IEC 27001:2013, esta guía contiene las buenas prácticas para llevar a cabo la implementación de un SGSI.

MEJORA CONTINUA: es la actividad recurrente que busca que los procesos evolucionen con el fin de cumplir de manera eficiente y eficaz sus objetivos.

POLÍTICA DE SEGURIDAD: es un conjunto de normas y procedimientos que se deben atender para garantizar la seguridad de la información, todo alineado a los objetivos estratégicos de la organización.

RIESGO: se da cuando una amenaza explota una vulnerabilidad y genera un daño o perdida de información.

RIESGO RESIDUAL: aquel riesgo que prevalece aún después de haber actuado ante ciertos riesgos. se convierte en el riesgo aceptable o apetito de riesgo de la organización.

SEGURIDAD DE LA INFORMACIÓN: son aquellas medidas que se implementan dentro de las organizaciones con el fin de salvaguardar su activo más importante: la información.

SGI: sistema de gestión integral.

SGSI: un sistema de gestión de seguridad de la información es el conjunto de políticas definidas para la gestión de la seguridad de la información.

SOA: declaración de aplicabilidad, que lista los controles de seguridad establecidos en el anexo A para su evaluación.

VULNERABILIDAD: es una debilidad dentro de un sistema informático que puede permitir un ataque.

RESUMEN

En la empresa, dentro del proceso de Gestión de Información, como su nombre lo indica, se gestiona la información de la organización independientemente del medio en donde se almacena, ya sea físico o lógico, por ende, es importante iniciar con una planeación que permita identificar las vulnerabilidades que ponen en riesgo la información de la empresa, y todas sus partes interesadas, que son: los clientes tanto internos como externos, los proveedores y los colaboradores, en cualquiera de los tres pilares que define la seguridad de la información, que son: integridad, confidencialidad y disponibilidad.

Para lograrlo se plantea iniciar con la primera etapa del ciclo de vida PHVA (Planear, Hacer, Verificar, Actuar) en sistemas de gestión, es decir, con la planeación, bajo el marco de trabajo de la norma ISO/IEC 27001:2013 y su guía de buenas prácticas, la ISO/IEC 27002:2013. Este par de normas en conjunto ayudarán a iniciar con un proceso de madurez y dejarán todo listo para dar el siguiente paso y poder iniciar con la etapa del hacer y de esta manera, empezar a tomar las medidas correspondientes que ayuden a mitigar los riesgos y amenazas previamente identificados.

La etapa de planeación comprende los siguientes escenarios de cumplimiento:

- Diseño del SGSI
- Análisis de procesos
- Definición del alcance
- Elaboración de la política de seguridad
- Identificación y evaluación del inventario de activos
- Análisis de riesgos
- Generación de la declaración de aplicabilidad (SoA)

Palabras claves: ISO/IEC 27001:2013, ISO/IEC 27002, Magerit, PHVA, SGSI.

ABSTRACT

In the company, within the Information Management process, as its name indicates, the organization's information is managed regardless of the medium where it is stored, whether physical or logical, therefore, it is important to start with a planning that allows identify the vulnerabilities that put the information of the company at risk, and all its interested parties, which are: both internal and external customers, suppliers and collaborators, in any of the three pillars that define information security, which They are: integrity, confidentiality and availability.

To achieve this, it is proposed to start with the first stage of the PDCA life cycle (Plan, Do, Verify, Act) in management systems, that is, with planning, under the framework of the ISO / IEC 27001: 2013 standard and its good practice guide, ISO / IEC 27002: 2013. This couple of rules together will help to start with a maturity process and will leave everything ready to take the next step and be able to start with the doing stage and in this way begin to take the corresponding measures that help mitigate risks and threats previously. identified.

The planning stage comprises the following compliance scenarios:

- Design the ISMS.
- Process analysis
- Definition of scope
- Preparation of the security policy
- Identification and evaluation of the inventory of assets
- Risk analysis
- Generation of the Statement of Applicability (SoA)

Keywords: ISMS, ISO/IEC 27001:2013, ISO/IEC 27002, Magerit, PDCA

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El proceso de Gestión de Información es uno de los más sensibles dentro de la organización, debido a la naturaleza de la información que se maneja. Actualmente se tienen definidas algunas acciones que permiten la mitigación parcial de los riesgos asociados a la seguridad de la información, pero se consideran insuficientes, toda vez que no protege a nivel general la superficie de los ataques que se pueden presentar, los cuales pueden afectar la integridad, disponibilidad y confidencialidad de la información.

Dentro de los problemas que se han presentado por no tener un Sistema de Gestión de Seguridad de la Información (SGSI) implementado se identifican los siguientes:

- Usuarios no sensibilizados que han caído en ataques de *phishing*.
- En el año 2017 un *host* se vio involucrado en un ataque de *Ransomware*, el cual no se propago por toda la red por la respuesta oportuna del personal de TI.
- No existe una cultura organizacional que relacione los procesos de seguridad de la información con los objetivos estratégicos de la organización.
- No existe un método de control eficaz que permita evidenciar y realizar la trazabilidad ante la violación de uno de los tres pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad.
- Existe un ciclo de monitoreo y mejora continua, pero este va asociado al sistema de gestión integral y no precisamente hace énfasis en el SGSI.
- No se ha definido un nivel de riesgo tolerable o asumible dentro de la organización.

La etapa de planeación del SGSI, basado en el ciclo de vida PHVA, es la parte inicial y aquí es donde se diseñan y se construyen las bases del sistema de gestión, el cual puede ser agregado al sistema de gestión integral actual.

Para llevar a buen término lo planteado anteriormente, se propone iniciar con la etapa de planeación, apoyado en el marco de trabajo de la norma ISO/IEC 27001:2013, la cual define una serie de guías, procedimientos y procesos y su guía de buenas prácticas, la ISO/IEC 27002:2013. Esto con el fin de iniciar con un proceso de madurez y dejar todo listo para dar inicio con la etapa del hacer y así empezar a tomar las medidas correspondientes que ayuden a mitigar los riesgos identificados y llevarlos hasta un nivel aceptable.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es la importancia de planear un SGSI dentro del proceso de Gestión de Información en la empresa GERS S.A.S.?

2 JUSTIFICACIÓN

El COVID19 fue sin duda el dinamizador de la migración de las empresas hacia el trabajo en casa, muchas empresas no estaban preparadas y tomaron medidas quizá un poco apresuradas con el fin de permitir los servicios necesitados, pero abriendo brechas y vulnerabilidades de seguridad que, de materializarse se pueden dejar comprometidos los sistemas informáticos.

La ejecución del presente proyecto le permitirá a la empresa iniciar con la solución de una problemática empresarial que requiere de gestión de forma precisa. Esto le servirá para avanzar en la consecución de un nivel de madurez que a su vez se traducirá en un mejor posicionamiento en el mercado.

A continuación, se describen algunos grandes beneficios que aportará la implementación de un SGSI que inicia con la etapa de planeación:

- Reducción de riesgos debido al establecimiento y seguimiento de controles.
- Ahorro de costos derivado de una racionalización de los recursos.
- La seguridad se considera un sistema y se convierte en una actividad de gestión.
- La organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costos innecesarios.
- La certificación del SGSI contribuye a mejorar la competitividad en el mercado, aumenta la confianza de colaboradores, clientes y proveedores e incrementa su prestigio.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar la etapa de planeación de un Sistema de Gestión de Seguridad de la Información para el proceso de Gestión de Información, alineado al estándar ISO/IEC 27001/2013, con el fin de mitigar los riesgos en la empresa GERS S.A.S.

3.2 OBJETIVOS ESPECÍFICOS

Establecer un diagnóstico en cuanto a los dominios de un sistema de gestión de seguridad de la información en la empresa GERS S.A.S.

Analizar los riesgos de los activos del proceso de gestión de información en la empresa GERS S.A.S, a través de la metodología de gestión de riesgos MAGERIT.

Determinar un plan de tratamiento de riesgo por medio de la guía de buenas prácticas ISO/IEC 27002:2013

Elaborar la política de seguridad de la información para mitigar los riesgos de la empresa GERS S.A.S.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Sistema de Gestión. El círculo de calidad consiste en cuatro etapas:

- **Planear:** en la primera fase donde se establece el sistema de gestión.
- **Hacer:** es la fase donde se implementa y se opera el sistema de gestión.
- **Verificar:** en esta fase se monitorea y se revisa el sistema de gestión.
- **Actuar:** en la última fase se mantiene y mejora el sistema de gestión.

De acuerdo con PEREZ, Pastor y MUNERA, Francisco “el PHVA es un ciclo dinámico que puede desarrollarse como un todo”[1] y esto se relaciona directamente entre la planificación, implementación, control y mejora continua de los procesos.

4.1.2 Seguridad de la información. La finalidad de la seguridad de la información es simple: proteger los datos y la información de posibles amenazas o acontecimientos que puedan alterar su ciclo de vida.

Los principios esenciales que vela por preservar son:

- **Confidencialidad:** garantizar que la información esté disponible y accesible en el momento que se requiera por parte de los usuarios y/o procesos autorizados.
- **Disponibilidad:** garantizar que la información esté disponible y accesible en el momento que se requiera por parte de los usuarios autorizados.

[1] PEREZ, Pastor y MUNERA, Francisco. Reflexiones para implementar un sistema de gestión de calidad (ISO 9001: 2000) en cooperativas y empresas de economía solidaria, 2007. p. 50.

- **Integridad:** esta propiedad vela por mantener la exactitud de los datos, es decir que no sea alterada por terceros durante su proceso de almacenamiento o transporte.

Se suman a estos, unas características esenciales que se deben cuidar, estos son:

- **Autenticidad:** garantizar y asegurar la identidad de la persona que genera la información sin suplantación.
- **No repudio:** evitar que ni el emisor ni el receptor nieguen la transmisión de un mensaje.
- **Trazabilidad:** monitorear desde su origen cualquier operación relacionada con la información.

4.1.3 Sistema de Gestión de Seguridad de la Información. "Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales"[2].

El SGSI está enfocado de manera sistemática con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización, todo esto alineado a la consecución de sus objetivos comerciales y/o de servicio.

[2] LOPEZ, Agustín. SGSI. (s.f.).

4.1.4 Importancia de un SGSI dentro de una empresa. Como dice Pérez[3], en la actualidad la información de una organización es considerada el activo más relevante, entonces de aquí radica la necesidad de protegerla frente a los diferentes riesgos a los que se puede exponer tanto en un físico como en un ambiente lógico. Razón por la cual se hace indispensable contar con un sistema de gestión que se enfoque específicamente en la seguridad de la información. El SGSI es este sistema.

4.1.5 Beneficios de un SGSI. Dentro de los beneficios de implementar un SGSI se encuentran los siguientes:

- Reducción de riesgos debido al establecimiento y seguimiento de controles.
- Ahorro de costos derivado de una racionalización de los recursos.
- La seguridad se considera un sistema y se convierte en una actividad de gestión.
- La organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costos innecesarios.
- La certificación del SGSI contribuye a mejorar la competitividad en el mercado, aumenta la confianza e incrementa su prestigio.

4.1.6 Relevancia de identificar los riesgos de seguridad mediante la metodología MAGERIT. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) tiene como objetivo sistematizar el análisis y la gestión de los riesgos que pueden presentar los activos de una organización.

Debido al crecimiento exponencial que ha tenido la tecnología, esta metodología cobra mayor importancia, toda vez que es necesario llevar a un nivel aceptable los riesgos asociados al uso de los sistemas garantizando la confidencialidad, integridad, y

[3] PEREZ, Brigitte. Importancia de un sistema de gestión de seguridad de la información para empresas de tecnología. Trabajo de grado Especialización en seguridad informática. Universidad Piloto de Colombia, 2020. [Consulta: 15 de mayo de 2022]. p. 1. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6841

disponibilidad de estos, con la finalidad de generar confianza de todas las partes interesadas.

“Los objetivos de MAGERIT son:

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

La versión 3 de MAGERIT está compuesta de la siguiente manera:

- Libro I: Método
- Libro II: Catálogo de elementos
- Guía de técnicas: recopilación de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método”[4].

[4] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. p. 8.

4.2 MARCO CONCEPTUAL

4.2.1 Fases para implementar un SGSI. Los pasos que se enumeran a continuación describen aquellas fases necesarias para llevar a cabo un proyecto de implementación de un SGSI de manera exitosa.

- **Definición de la Política:** aquí se definen las directrices que debe cumplir la seguridad de la información. Debe estar alineada con los objetivos estratégicos de la organización y la legislación aplicable.

- **Definición del alcance:** Andrade[5] define el alcance como la fase donde se determinan los procesos más críticos dentro de la organización, se define que se desea proteger y el punto inicial. También se identifican las actividades de la empresa, su ubicación física, infraestructura tecnológica y, por último, se deja claro los procesos y/o áreas que se excluirán del alcance del SGSI.

- **Análisis de riesgos:** se debe realizar el análisis de los activos de información identificados de forma previa. En este análisis se determinan las amenazas y vulnerabilidades que posee cada activo.

- **Gestión del Riesgo:** en esta etapa se generan resultados y conclusiones de acuerdo con las opciones que dispone el *risk management*, tales como: eliminar el riesgo, transferir el riesgo, asumir el riesgo y mitigar el riesgo. Luego de esto, resultará el riesgo residual y el nivel de riesgo aceptable o tolerable por la organización.

[5] ANDRADE, Yovany. Entendiendo el SGSI, Trabajo de grado Especialización en seguridad informática. Universidad Piloto de Colombia, 2016. [Consulta: 15 de mayo de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2748

- **Selección de controles a implementar:** basado en la norma ISO/IEC 27002, que es una guía de buenas prácticas que describe de manera granular cada uno de los controles disponibles para aplicar en un SGSI, se debe definir cuáles de estos controles son aplicables dentro de la organización de acuerdo con los resultados del análisis y la gestión de los riesgos identificados.

- **Declaración de aplicabilidad (SoA):** los controles definidos se deben listar dentro de la declaración de aplicabilidad o SoA por sus siglas en inglés *Stament of Applicability.*

  La lista de controles debe estar acompañada de los objetivos, descripción, razón o no de elección y se condiciona por los siguientes factores: costo del control frente al costo del impacto, necesidad de disponibilidad del control y el costo de la implementación y mantenimiento[6].

- **Revisión del sistema:** como medida de todo sistema, este debe estar sujeto a la mejora continua, la cual sucede de la toma de acciones preventivas y/o correctivas.

  Una práctica común para hallar estas mejoras es por medio de la aplicación de auditorías internas y su plan de desarrollo en el tiempo.

4.2.2 Dominios, objetivos de control y controles de un SGSI. El anexo A (ISO/IEC 27002) de la Norma ISO/27001:2013 está compuesto de 14 dominios, 35 objetivos de control y 114 controles de seguridad. A continuación, se listan los dominios:

- A.5 Política de seguridad.
- A.6 Aspectos organizativos de la seguridad de la información.

[6] EALDE Business School. [Sitio web]. [Consulta: 15 de mayo de 2022]. La Gestión de Riesgos en un SGSI, 2020. Disponible en: https://www.ealde.es/gestion-de-riesgos-sgsi/

- A.7 Seguridad ligada a los recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de accesos.
- A.10 Cifrado.
- A.11 Seguridad física y ambiental.
- A.12 Seguridad en la operativa.
- A.13 Seguridad en las telecomunicaciones.
- A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.15 Relación con proveedores.
- A.16 Gestión de los incidentes en la seguridad de la información.
- A.17 Aspectos de la Seguridad de la Información en la gestión de la continuidad de negocio.
- A.18 Cumplimiento.

4.2.3 Política de seguridad del SGSI. Haciendo énfasis en la definición de la política y basado en el documento guía desarrollado por MINTIC[7] sobre cómo elaborar la política general de seguridad y privacidad de la información, encontramos que esta es sumamente importante porque "aborda la necesidad de la implementación de un SGSI planteado desde la descripción del quién, qué, porqué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI".

En este mismo documento, se describen las fases necesarias para llevar a cabo su implementación:

- Desarrollo de las políticas: justificación, alcance, roles y responsabilidades, revisión de la política, aprobación de la política.
- Cumplimiento.

[7] MINTIC. Elaboración de la política general de seguridad y privacidad de la información, 2016. p. 6.

- Comunicación.
- Monitoreo.
- Mantenimiento.
- Retiro.

En adición a lo anterior, MINTIC realiza las siguientes recomendaciones para la redacción correcta de la política de seguridad de la información:

- “La política debe tener como parte de su texto la declaración en la cual se indica ¿qué es lo que se desea hacer?, ¿qué regula la política?, ¿cuál es la directriz que deben seguir los funcionarios, contratistas y/o terceros?, todo esto alineado con la estrategia de la organización.
- Alinearse con el alcance del Modelo de Seguridad y Privacidad de la Información.
- Debe especificarse a quién (es) va dirigida la política, se debe identificar fácilmente quién (es) deben cumplir la política.
- En los casos que aplique se hace referencia de la regulación mediante la cual se soporta la política.
- En caso de que aplique la política debe indicar las excepciones a la misma y a quienes les aplica la excepción.
- Datos de las personas o roles de la entidad que pueden brindar información sobre la política.
- Nombre, rol o responsable de quien autoriza la política.
- Describir los pasos y procedimientos para realizar ajustes a la política.
- Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política.
- Fecha que inicia la vigencia de la política”.

4.3 ANTECEDENTES O ESTADO ACTUAL

Son cada vez más las empresas que se preocupan por garantizar la seguridad de la información, no solamente por cumplimiento legal sino porque se han dado cuenta de que la información es su activo más importante. De a poco, las organizaciones invierten en la implementación de mecanismos y sistemas de seguridad y también integran dentro de sus sistemas de gestión integral, el sistema de gestión de seguridad de la información.

En la actualidad, debido a los avances tecnológicos y a la nueva era de la virtualidad, las empresas han tomado mayor conciencia de los riesgos que existen en el ciberespacio, se han dado cuenta de que no basta con tener una acceso remoto vía VPN para proteger los datos y que, garantizar el cumplimiento de los tres pilares de la seguridad de la información es tarea de todos y cada uno de los miembros de la organización, es decir que esto dejó de ser responsabilidad exclusiva del jefe de sistemas o coordinador de TI para convertirse en una tarea de cada colaborador, desde la alta dirección hasta el vigilante.

Entonces, se entiende por seguridad de la información al conjunto de políticas, procesos y procedimientos cuyo objetivo es garantizar el cumplimiento de los tres pilares: confidencialidad, integridad y disponibilidad.

El conjunto de normas ISO/IEC 27000 son un gran apoyo para las empresas que necesitan desarrollar sus proyectos de seguridad de la información y lograr una certificación en este aspecto que respalde su compromiso y responsabilidad.

La empresa GERS S.A.S., demuestra un compromiso con el aseguramiento de la información, por ello inicia con la elaboración de la primera etapa del ciclo PHVA del SGSI, correspondiente a la planeación, para de esta manera identificar los riesgos y

amenazas a las cuales está expuesta la organización y en la siguiente etapa tomar las medidas pertinentes para mitigar estos riesgos.

Antes de iniciar con el desarrollo de los objetivos planteados es importante conocer un poco la empresa GERS S.A.S., como está conformada, cuál es su *core* de negocio, sus objetivos estratégicos, su misión y visión, su estructura organizacional y sus partes interesadas, toda vez que alrededor de estos particulares girará el proceso de certificación de un sistema de gestión de seguridad de la información.

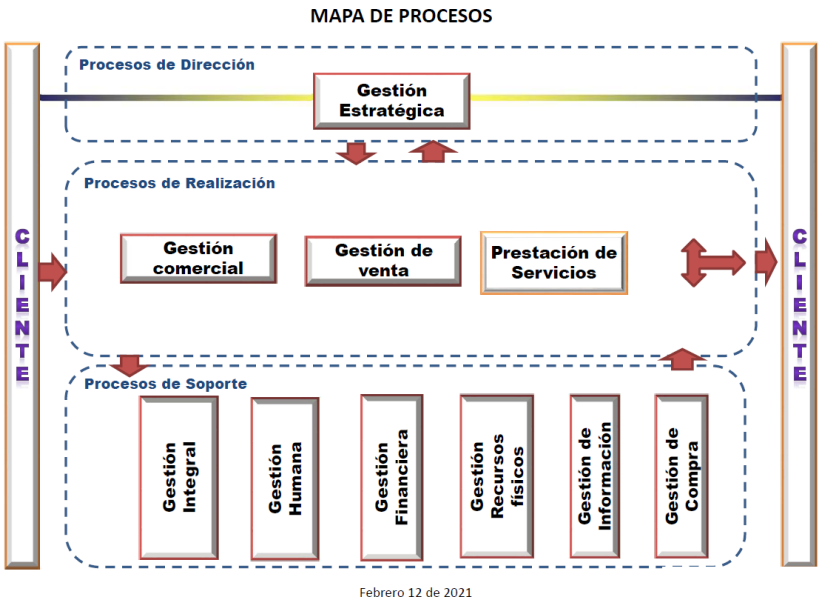
4.3.1 Descripción general. GERS es un grupo empresarial, con 40 años de experiencia en el mercado de la consultoría en ingeniería eléctrica. Tiene sedes en varios países (Colombia, Chile, México, Estados Unidos).

El *core* de su negocio es “Llevar a cabo la ejecución de monitoreo de calidad de potencia y energía, pruebas en equipos de subestaciones eléctricas, sistemas industriales y los más avanzados sistemas de protección, control y transferencia de sistemas de potencia. Así como también ofrecer soluciones para proyectos EPC (Engineering, Procurement and Construction) tanto de subestaciones eléctricas como de proyectos industriales.”[8]

[8] GERS S.A.S. Inicio. [Sitio web]. [Consulta: 15 de mayo de 2022]. Disponible en: https://gers.com.co.

4.3.2 Mapa de procesos. En la figura 1 se muestra el mapa de procesos de la compañía.

Figura 1. Mapa de procesos GERS S.A.S.



Fuente: mapa de procesos GERS 2021

El alcance del SGSI está definido para el proceso de soporte “Gestión de información” toda vez que en este se definen las actividades relacionadas con la seguridad de la información.

4.3.3 Política de gestión integral. “GERS, empresa de consultoría en ingeniería que presta servicios de diseño, estudios, pruebas y puesta en servicio de sistemas eléctricos, comercialización de equipos y software especializados, se compromete a realizar sus actividades cumpliendo la legislación nacional, la internacional y los requisitos suscritos aplicables a sus proyectos. Sus acciones se orientan a la protección ambiental, la seguridad y salud de sus colaboradores y contratistas y se enfocan en la mejora continua de sus procesos y la satisfacción de sus clientes.

Hace parte de la política de GERS:

- Prevenir accidentes y enfermedades identificando los peligros, evaluando y valorando los riesgos, determinando los controles y mejorando continuamente las condiciones de trabajo
- Prevenir la contaminación del medio ambiente, controlando sus impactos, haciendo uso eficiente de sus recursos y asegurando la disposición adecuada de los residuos generados.
- Desarrollar programas de responsabilidad social dirigidos a población vulnerable
- Evitar daños a su propiedad y la de sus clientes
- Prestar sus servicios con oportunidad, confiabilidad y rentabilidad adecuada

Para lograr estos compromisos, la empresa provee los recursos humanos, económicos y técnicos necesarios para el mejoramiento de sus servicios y el desarrollo integral de sus colaboradores”.[9]

Es importante mencionar que la empresa cuenta con un sólido sistema de gestión integral, en consecuencia, el SGSI y por ende la política de seguridad de la información perfectamente pueden ir asociados a esta política de gestión integral.

[9] GERS S.A.S. Política de gestión integral, 2021.

4.3.4 Partes interesadas. Las partes interesadas se listan a continuación:

- Accionistas
- Clientes
- Proveedores de bienes y servicios
- Colaboradores
- Entes de vigilancia y control
- Comunidad
- Academia

4.4 MARCO LEGAL

LEY 1266 DE 2008[10]

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DE 2009[11]

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008) En: Diario Oficial. Diciembre, 2008.
[11] COLOMBIA. SENADO. Ley 1273 (5, enero, 2009) En Diario Oficial. Enero, 2009.

LEY 1341 DE 2009[12]

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

LEY 1581 DE 2012[13]

Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma

DECRETO 1377 DE 2013[14]

Protección De Datos, Decreto Por El Cual Se Reglamenta Parcialmente La Ley 1581 De 2012.

[12] COLOMBIA. SENADO. Ley 1341 (30, julio, 2009), En: Diario Oficial. Julio, 2009.

[13] GOBIERNO DE COLOMBIA. [Sitio web]. Función pública. Ley 1581 de 2012. [Consulta: 15 de mayo de 2022] Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

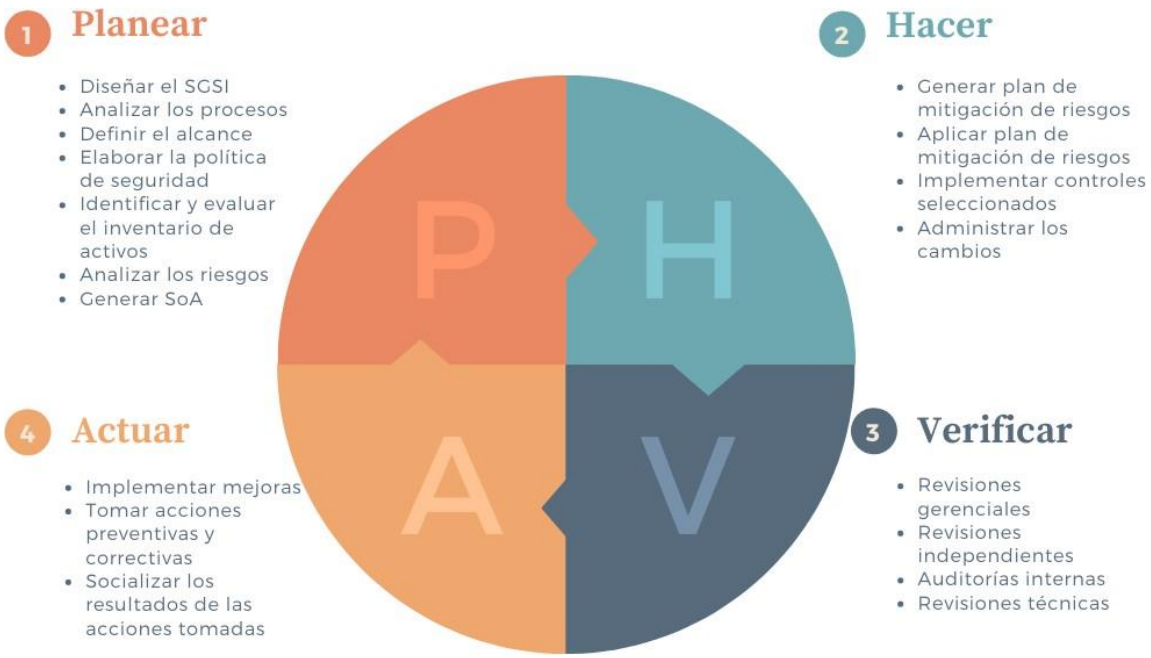
[14] GOBIERNO DE COLOMBIA. [Sitio web]. Función pública. Decreto 1377 DE 2013. [Consulta: 15 de mayo de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA PARA IMPLEMENTAR EL SGSI

La metodología para implementar el SGSI en la empresa GERS S.A.S. es de tipo descriptivo, toda vez que se parte de un problema actual, el cual se pretende analizar y evaluar por medio de la recolección, descripción, registro e interpretación de la información; para que, apoyado en marco de trabajo de la ISO/IEC27001:2013, llevar a cabo el desarrollo de la etapa de planeación de acuerdo con el ciclo de vida PHVA.

Figura 2. Ciclo PHVA



Fuente: “elaboración propia”

5.2 MÉTODOS DE RECOLECCIÓN DE DATOS

- Inspección
- Observación
- Información existente en el SGI y en el proceso de Gestión de Información
- Encuestas a usuarios

En esta etapa de la metodología, se define el alcance del Sistema de Gestión de Seguridad de la Información dentro de la organización teniendo en cuenta las políticas y directrices existentes. A continuación, se describen las fases que se van a desarrollar, de acuerdo con los objetivos planteados:

Fase 1: Establecer un diagnóstico en cuanto a los dominios de un sistema de gestión de seguridad de la información en la empresa GERS S.A.S.

Actividad 1: Recolección de información por medio de inspecciones, observaciones, documentación de auditorías previas y encuestas al personal de la organización con el fin de diligenciar la matriz del estado inicial y aplicabilidad de controles de seguridad de la información, la cual contiene un resumen general de los 14 dominios, 35 objetivos de control y 114 controles definidos en la guía ISO/IEC 27002:2013

Fase 2: Analizar los riesgos de los activos del proceso de gestión de información en la empresa GERS S.A.S, a través la metodología de gestión de riesgos MAGERIT.

Actividad 2: Implementación de la metodología MAGERIT para la gestión de riesgos.

MAGERIT tiene los siguientes objetivos:

- Concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo,
- Ofrecer un método sistemático para analizar tales riesgos,

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control,
- Apoyar la preparación a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda.

Fase 3: Determinar un plan de tratamiento de riesgo por medio de la guía de buenas prácticas ISO/IEC 27002:2013

Actividad 3: Existen cuatro opciones de tratamiento de riesgo:

- "**Mitigar el riesgo:** con esta acción, se trata de disminuir el riesgo hasta un nivel de apetito de riesgo aceptable por medio de la aplicación de controles de seguridad del Anexo A incluidos en el documento "anexo A de la norma ISO 27001" o también conocido como ISO 27002

- **Transferir el riesgo:** la transferencia de riesgos es una estrategia de gestión y control de riesgos que consiste en el cambio contractual de un riesgo puro de una parte a otra.

- **Evitar el riesgo:** evitar un riesgo se logra por medio de la eliminación de peligros, actividades y exposiciones que pueden afectar de manera negativa los activos de información de una organización.

- **Aceptar el riesgo:** significa que, a pesar de que el riesgo está identificado y registrado en el proceso de gestión de riesgos, no se realizará ninguna acción. Simplemente se acepta que pueda suceder y se aplicará un tratamiento específico en caso de darse. Esta es una buena estrategia para usar con riesgos muy pequeños."[15]

[15] ISO 27001. Fase 4 Planificación del SGSI, s.f.

Fase 4: Definir una política de seguridad de la información para mitigar los riesgos de la empresa GERS S.A.S.

Actividad 4: Se debe definir la política de seguridad recogiendo “las directrices que debe seguir la seguridad de la información de acuerdo con las necesidades de la organización y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades”.[16]

[16] INTECO. Implantación de un SGSI en la empresa, s.f. p. 16.

6 DESARROLLO DE LOS OBJETIVOS

6.1 ESTABLECER UN DIAGNÓSTICO EN CUANTO A LOS DOMINIOS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA GERS S.A.S.

Actividad 1: Recolección de información por medio de inspecciones, observaciones, documentación de auditorías previas y encuestas al personal de la organización con el fin de diligenciar la matriz del estado inicial y aplicabilidad de controles de seguridad de la información, la cual contiene un resumen general de los 14 dominios, 35 objetivos de control y 114 controles definidos en la guía ISO/IEC 27002:2013

En la tabla 1 se muestra la escala de calificación con los valores asignables a cada uno de los 114 controles:

Tabla 1 Escala de calificación de controles

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.

Fuente: ISO/IEC 27001 certification standard.

Tabla 2 Escala de calificación de controles (continuación)

Estado	Significado
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo con un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

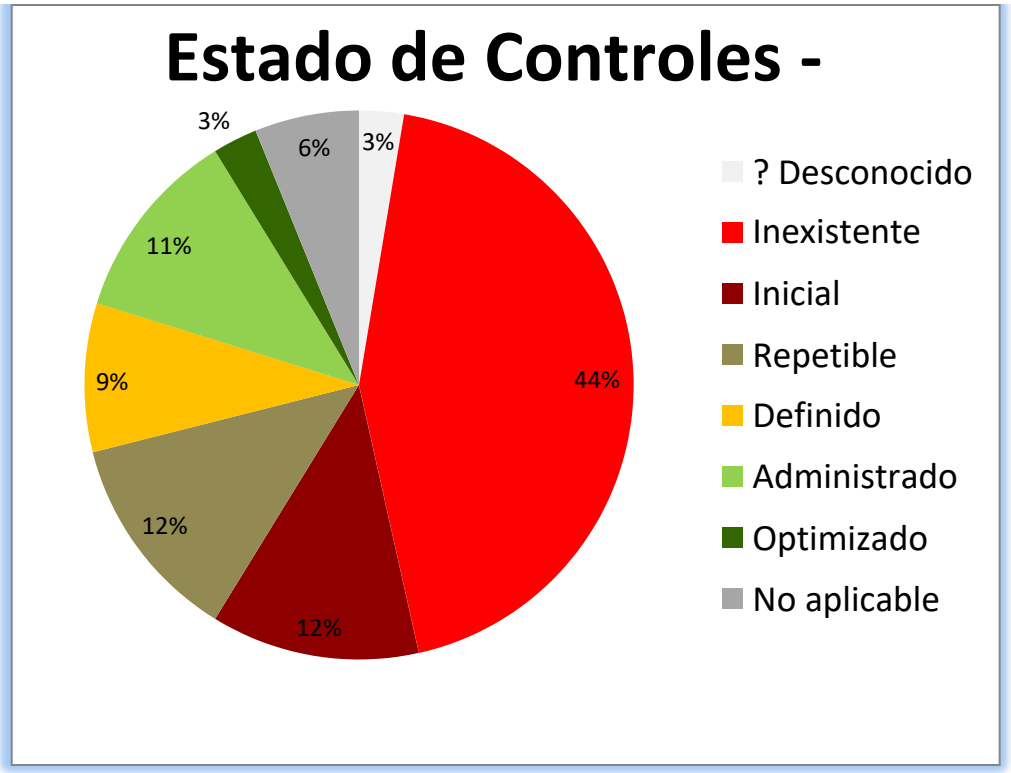
Fuente: ISO/IEC 27001 certification standard.

Al finalizar la evaluación de los 114 controles, se actualiza un diagrama de pastel de manera automática, el cual sirve como un indicador o métrica, insumo confiable para conocer de manera gráfica el estado actual de madurez de la empresa GERS S.A.S., en cuanto a seguridad de la información se refiere.

Ver Anexo A.

A continuación, se presenta el resultado del análisis inicial, donde se muestra el estado de los controles del Anexo A:

Figura 3. Estado de controles - Anexo A



Fuente: “Elaboración propia”

De la gráfica anterior se puede concluir que:

- El estado de madurez en cuanto a seguridad de la información en la empresa GERS S.A.S. es bajo y susceptible a mejorar con la implementación de un SGSI. El 44% de los controles son inexistentes.
- Solo un 14% de los controles está administrado u optimizado, estos son controles que presentan un nivel ideal de gestión al cual deberían llegar los demás controles dentro del proceso de mejora continua.
- Un 24% se divide entre controles con estado inicial y repetible, lo que indica que, si bien se han realizado algunas actividades para mejorar la postura de seguridad, estas carecen de políticas, procesos, procedimientos y registros formales que los respalden.

- Un 9% de los controles evidencian un estado definido, lo que indica que están próximos a madurar si se realizan las aprobaciones gerenciales pertinentes sobre los procesos, procedimientos o políticas.
- Un 6% de los controles no aplican principalmente porque están enfocados al desarrollo de software en sitio y la empresa no realiza esta actividad. Su software es tercerizado.
- Un 3% relacionado con la sección 18.2 no ha sido evaluada, toda vez que no se cuenta con un SGSI implementado.

6.2 ANALIZAR LOS RIESGOS DE LOS ACTIVOS DEL PROCESO DE GESTIÓN DE INFORMACIÓN EN LA EMPRESA GERS S.A.S, A TRAVÉS DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS MAGERIT.

Actividad 2: Implementación de la metodología MAGERIT para la gestión de riesgos.

MAGERIT tiene los siguientes objetivos:

- Concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo,
- Ofrecer un método sistemático para analizar tales riesgos,
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control,
- Apoyar la preparación a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda.

Para la ejecución de cada uno de los pasos que se describen a continuación, se emplea la “Matriz de levantamiento de información de activos según metodología Magerit y Norma ISO 27001:2013” desarrollada por instructores y estudiantes de la UNAD y que se ofrece como material de estudio en algunos cursos dentro del programa de

Especialización en Seguridad Informática.

Ver anexo B.

6.2.1 Identificación de los activos. Como punto inicial se realiza la identificación, clasificación y catalogación de todos los activos de información presentes en la infraestructura de la empresa GERS S.A.S. y que forman parte del alcance del SGSI, es decir, del proceso de Gestión de Información.

En la identificación se define el nombre del activo, el proceso o propietario del activo y el tipo de activo.

El tipo de activo se cataloga, por sus características, como uno de los siguientes:

- [D] Datos / Información
- [K] Claves Criptográficas
- [S] Servicios
- [SW] *Software* / Aplicaciones informáticas
- [HW] Equipamiento informático (*hardware*)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

Realizar la catalogación de manera correcta es de suma importancia porque a partir de esta se deben identificar las amenazas que pueden ser explotadas por una o diversas vulnerabilidades y posterior a ello, definir su nivel de riesgo y el plan de tratamiento que se debe dar a cada uno de estos.

Figura 4. Identificación de activos

No.	DATOS DEL ACTIVO DE INFORMACION		
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo
1	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	Douglas Lopez Fernandez	SERVICIOS
2	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	Douglas Lopez Fernandez	SOFTWARE
3	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	Douglas Lopez Fernandez	SOFTWARE
4	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	Douglas Lopez Fernandez	SOFTWARE
5	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	Douglas Lopez Fernandez	HARDWARE
6	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	Douglas Lopez Fernandez	SOFTWARE
7	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	Douglas Lopez Fernandez	HARDWARE
8	[SW] Servidor proxy - OS Arch Linux 4.14.70	Douglas Lopez Fernandez	SOFTWARE
9	[HW] Servidor proxy - Dell Vostro 200	Douglas Lopez Fernandez	HARDWARE
10	[SW] Servidor SIP - Freepbx 10.13.66	Douglas Lopez Fernandez	SOFTWARE
11	[HW] Servidor SIP - Clon hibrido	Douglas Lopez Fernandez	HARDWARE
12	[SW] Software antivirus (Forticlient v7)	Douglas Lopez Fernandez	SOFTWARE
13	[SW] Suite de ofimática (MS Office 2013)	Douglas Lopez Fernandez	SOFTWARE
14	[SW] Suite de ofimática (MS Office 2016)	Douglas Lopez Fernandez	SOFTWARE
15	[SW] software de estudios (Digsilent 2016-2022)	Douglas Lopez Fernandez	SOFTWARE
16	[SW] Software de estudios (Neplan v10.9.1.1)	Douglas Lopez Fernandez	SOFTWARE
17	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	Douglas Lopez Fernandez	SOFTWARE
18	[SW] Ordenador portatil (OS Windows 10 Single Language)	Douglas Lopez Fernandez	SOFTWARE
19	[HW] Switch * 2 (V1910-48G JE009A)	Douglas Lopez Fernandez	HARDWARE
20	[HW] Switch * 2 (HP 1950-48G JG963A)	Douglas Lopez Fernandez	HARDWARE
21	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	Douglas Lopez Fernandez	SOFTWARE
22	[HW] Access Point (UNIFI Ubiquiti)	Douglas Lopez Fernandez	HARDWARE
23	[S] Correo electronico (G-Suite)	Douglas Lopez Fernandez	SERVICIOS
24	[S] Backup (Google Drive)	Douglas Lopez Fernandez	SERVICIOS
25	[AUX] Sistema de alimentación ininterrumpida (UPS)	Douglas Lopez Fernandez	AUXILIAR
26	[HW] Telefono IP (GrandStream)	Douglas Lopez Fernandez	HARDWARE
27	[COM] Internet (Proveedor C&W fibra optica de 80MB)	Douglas Lopez Fernandez	COMUNICACIONES
28	[D] Hojas de vida de colaboradores	Lizeth Navarro	DATOS
29	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	Douglas Lopez Fernandez	HARDWARE
30	[S] Paginas web corporativas (Servidor Digital Ocean)	Douglas Lopez Fernandez	SERVICIOS
31	[COM] Red de Area Local (LAN)	Douglas Lopez Fernandez	COMUNICACIONES

Fuente: “Elaboración propia”

6.2.2 Valoración de los activos. Se realiza la evaluación cualitativa y cuantitativa de los activos de información.

- **Valoración cualitativa**

Paso seguido, se realiza la valoración de los activos, de acuerdo con su nivel de criticidad para la operación del negocio.

La valoración cualitativa, de acuerdo con MAGERIT, se realiza con base en los siguientes criterios:

Dimensiones

Se evalúan las siguientes dimensiones:

- [D] Disponibilidad
- [I] Integridad
- [C] Confidencialidad
- [A] Autenticidad de los usuarios y de la información
- [T] Trazabilidad

Para esta valoración se toma como referencia la siguiente escala:

- B = Bajo
- M = Medio
- A = Alto
- MA = Muy alto
- MB = Muy bajo

Figura 5. Evaluación por dimensiones

No.	DATOS DEL ACTIVO DE INFORMACION	DIMENSION				
	Nombre del activo de información	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad
1	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	B	B	MA	A	A
2	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	B	B	MA	MA	A
3	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	B	B	MA	MA	A
4	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	B	B	MA	MA	MA
5	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	B	B	B	B	MA
6	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	B	B	MA	MA	MA
7	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	B	B	B	B	MA
8	[SW] Servidor proxy - OS Arch Linux 4.14.70	B	B	MA	MA	B
9	[HW] Servidor proxy - Dell Vostro 200	B	B	B	B	MA
10	[SW] Servidor SIP - Freepbx 10.13.66	B	B	MA	MA	B
11	[HW] Servidor SIP - Clon hibrido	B	B	B	B	MA
12	[SW] Software antivirus (Forticlient v7)	B	B	MA	MA	MA
13	[SW] Suite de ofimática (MS Office 2013)	B	B	MA	MA	MA
14	[SW] Suite de ofimática (MS Office 2016)	B	B	MA	MA	MA
15	[SW] software de estudios (Digsilent 2016-2022)	B	B	MA	MA	MA
16	[SW] Software de estudios (Neplan v10.9.1.1)	B	B	MA	MA	MA
17	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	B	B	MA	B	B
18	[SW] Ordenador portatil (OS Windows 10 Single Language)	B	B	MA	MA	MA
19	[HW] Switch * 2 (V1910-48G JE009A)	B	B	B	MA	MA
20	[HW] Switch * 2 (HP 1950-48G JG963A)	B	B	B	B	MA
21	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	B	B	MA	MA	MA
22	[HW] Access Point (UNIFI Ubiquiti)	B	B	B	B	MA
23	[S] Correo electronico (G-Suite)	B	B	MA	MA	MA
24	[S] Backup (Google Drive)	B	B	MA	MA	B
25	[AUX] Sistema de alimentación ininterrumpida (UPS)	B	B	B	B	MA
26	[HW] Telefono IP (GrandStream)	B	B	MA	B	MA
27	[COM] Internet (Proveedor C&W fibra optica de 80MB)	B	B	B	B	MA
28	[D] Hojas de vida de colaboradores	B	B	MA	MA	B
29	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	B	B	B	B	MA
30	[S] Paginas web corporativas (Servidor Digital Ocean)	B	B	B	B	MA
31	[COM] Red de Area Local (LAN)	MA	B	MA	MA	B

Fuente: “Elaboración propia”

Atributos

Para las siguientes preguntas se espera una respuesta de “SI” o “NO”

- ¿Es activo de información de terceros o de clientes que debe protegerse?
- ¿Activo de información que debe ser restringido a un número limitado de empleados?
- Activo de información que debe ser restringido a personas externas

- Activo de información que puede ser alterado o comprometido para fraudes o corrupción
- Activo de información que es muy crítico para las operaciones internas
- Activo de información que es muy crítico para el servicio hacia terceros

Para la afirmación “Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera”: se debe marcar con una “X” el impacto, sobre alguna de las opciones: leve, importante o grave.

Figura 6. Evaluación por atributos

No.	DATOS DEL ACTIVO DE INFORMACION	ATRIBUTOS								
	Nombre del activo de información	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:		
								Leve	Importante	Grave
1	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	NO	SI	SI	SI	SI	NO			X
2	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	NO	SI	SI	SI	SI	NO			X
3	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	NO	SI	SI	SI	SI	NO			X
4	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	NO	SI	SI	SI	SI	NO			X
5	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	NO	SI	SI	NO	SI	NO			X
6	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	NO	SI	SI	SI	SI	SI			X
7	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	NO	SI	SI	NO	SI	SI			X
8	[SW] Servidor proxy - OS Arch Linux 4.14.70	NO	NO	SI	SI	SI	SI		X	
9	[HW] Servidor proxy - Dell Vostro 200	NO	NO	SI	NO	SI	SI		X	
10	[SW] Servidor SIP - Freepbx 10.13.66	NO	NO	SI	SI	NO	NO	X		
11	[HW] Servidor SIP - Clon hibrido	NO	NO	SI	NO	NO	NO	X		
12	[SW] Software antivirus (Forticlient v7)	NO	NO	SI	SI	SI	NO		X	
13	[SW] Suite de ofimática (MS Office 2013)	NO	SI	SI	SI	SI	SI		X	
14	[SW] Suite de ofimática (MS Office 2016)	NO	SI	SI	SI	SI	SI		X	
15	[SW] software de estudios (Digsilent 2016-2022)	NO	SI	SI	SI	SI	SI			X
16	[SW] Software de estudios (Neplan v10.9.1.1)	NO	SI	SI	SI	SI	SI			X
17	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	NO	SI	SI	SI	NO	NO	X		
18	[SW] Ordenador portatil (OS Windows 10 Single Language)	NO	NO	SI	SI	SI	SI		X	
19	[HW] Switch * 2 (V1910-48G JE009A)	NO	SI	SI	NO	SI	NO	X		
20	[HW] Switch * 2 (HP 1950-48G JG963A)	NO	SI	SI	NO	SI	NO	X		
21	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	NO	SI	SI	SI	SI	SI			X
22	[HW] Access Point (UNIFI Ubiquiti)	NO	SI	SI	SI	NO	NO	X		
23	[S] Correo electronico (G-Suite)	NO	SI	SI	SI	SI	SI			X
24	[S] Backup (Google Drive)	NO	SI	SI	SI	SI	SI			X
25	[AUX] Sistema de alimentación ininterrumpida (UPS)	NO	SI	SI	SI	SI	NO	X		
26	[HW] Telefono IP (GrandStream)	NO	SI	SI	SI	NO	NO	X		
27	[COM] Internet (Proveedor C&W fibra optica de 80MB)	NO	SI	SI	SI	SI	SI			X
28	[D] Hojas de vida de colaboradores	NO	SI	SI	SI	NO	NO			X
29	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	NO	SI	SI	SI	NO	NO	X		
30	[S] Paginas web corporativas (Servidor Digital Ocean)	NO	NO	NO	SI	NO	NO		X	
31	[COM] Red de Area Local (LAN)	NO	NO	SI	SI	SI	NO			X

Fuente: “Elaboración propia”

Ubicación

Marcando con una “X” se debe definir la ubicación del activo de información, es decir, si es activo físico o activo electrónico.

Figura 7. Evaluación por ubicación

No.	DATOS DEL ACTIVO DE INFORMACION	UBICACIÓN	
	Nombre del activo de información	Físico	Electrónico
1	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)		X
2	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS		X
3	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15		X
4	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16		X
5	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	X	
6	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016		X
7	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	X	
8	[SW] Servidor proxy - OS Arch Linux 4.14.70		X
9	[HW] Servidor proxy - Dell Vostro 200	X	
10	[SW] Servidor SIP - Freepbx 10.13.66		X
11	[HW] Servidor SIP - Clon hibrido	X	
12	[SW] Software antivirus (Forticlient v7)		X
13	[SW] Suite de ofimática (MS Office 2013)		X
14	[SW] Suite de ofimática (MS Office 2016)		X
15	[SW] software de estudios (Digsilent 2016-2022)		X
16	[SW] Software de estudios (Neplan v10.9.1.1)		X
17	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)		X
18	[SW] Ordenador portatil (OS Windows 10 Single Language)		X
19	[HW] Switch * 2 (V1910-48G JE009A)	X	
20	[HW] Switch * 2 (HP 1950-48G JG963A)	X	
21	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)		X
22	[HW] Access Point (UNIFI Ubiquiti)	X	
23	[S] Correo electronico (G-Suite)		X
24	[S] Backup (Google Drive)		X
25	[AUX] Sistema de alimentación ininterrumpida (UPS)	X	
26	[HW] Telefono IP (GrandStream)	X	
27	[COM] Internet (Proveedor C&W fibra optica de 80MB)		X
28	[D] Hojas de vida de colaboradores	X	
29	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	X	
30	[S] Paginas web corporativas (Servidor Digital Ocean)		X
31	[COM] Red de Area Local (LAN)		X

Fuente: “Elaboración propia”

Valoración cuantitativa

La valoración cuantitativa está definida por la siguiente escala:

Figura 8. Escala valoración cuantitativa

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Valoracion del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: “Elaboración propia”

A partir de la calificación otorgada a cada activo dentro de los criterios de las cinco dimensiones (figura 5), la siguiente tabla se genera de manera automática.

Figura 9. Valoración cuantitativa

	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	IMPORTANTE	9	9	25	20	20	17
2	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	IMPORTANTE	9	9	25	25	20	18
3	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	IMPORTANTE	9	9	25	25	20	18
4	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	IMPORTANTE	9	9	25	25	25	19
5	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	APRECIABLE	9	9	9	9	25	12
6	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	IMPORTANTE	9	9	25	25	25	19
7	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	APRECIABLE	9	9	9	9	25	12
8	[SW] Servidor proxy - OS Arch Linux 4.14.70	APRECIABLE	9	9	25	25	9	15
9	[HW] Servidor proxy - Dell Vostro 200	APRECIABLE	9	9	9	9	25	12
10	[SW] Servidor SIP - Freepbx 10.13.66	APRECIABLE	9	9	25	25	9	15
11	[HW] Servidor SIP - Clon hibrido	APRECIABLE	9	9	9	9	25	12
12	[SW] Software antivirus (Forticlient v7)	IMPORTANTE	9	9	25	25	25	19
13	[SW] Suite de ofimática (MS Office 2013)	IMPORTANTE	9	9	25	25	25	19
14	[SW] Suite de ofimática (MS Office 2016)	IMPORTANTE	9	9	25	25	25	19
15	[SW] software de estudios (Digsilent 2016-2022)	IMPORTANTE	9	9	25	25	25	19
16	[SW] Software de estudios (Neplan v10.9.1.1)	IMPORTANTE	9	9	25	25	25	19
17	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	APRECIABLE	9	9	25	9	9	12
18	[SW] Ordenador portatil (OS Windows 10 Single Language)	IMPORTANTE	9	9	25	25	25	19
19	[HW] Switch * 2 (V1910-48G JE009A)	APRECIABLE	9	9	9	25	25	15
20	[HW] Switch * 2 (HP 1950-48G JG963A)	APRECIABLE	9	9	9	9	25	12
21	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	IMPORTANTE	9	9	25	25	25	19
22	[HW] Access Point (UNIFI Ubiquiti)	APRECIABLE	9	9	9	9	25	12
23	[S] Correo electronico (G-Suite)	IMPORTANTE	9	9	25	25	25	19
24	[S] Backup (Google Drive)	APRECIABLE	9	9	25	25	9	15
25	[AUX] Sistema de alimentación ininterrumpida (UPS)	APRECIABLE	9	9	9	9	25	12
26	[HW] Telefono IP (GrandStream)	APRECIABLE	9	9	25	9	25	15
27	[COM] Internet (Proveedor C&W fibra optica de 80MB)	APRECIABLE	9	9	9	9	25	12
28	[D] Hojas de vida de colaboradores	APRECIABLE	9	9	25	25	9	15
29	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	APRECIABLE	9	9	9	9	25	12
30	[S] Paginas web corporativas (Servidor Digital Ocean)	APRECIABLE	9	9	9	9	25	12
31	[COM] Red de Area Local (LAN)	IMPORTANTE	25	9	25	25	9	19

Fuente: “Elaboración propia”

Nota: Tanto la valoración cualitativa como la cuantitativa resulta más fácil de elaborar una vez se haya realizado la identificación de amenazas y vulnerabilidades para cada activo.

6.2.3 Identificación de amenazas. Se identifican las amenazas que están latentes sobre cada activo. Se toman las amenazas definidas dentro de la metodología MAGERIT, las cuales se resumen en la tabla 3.

Tabla 3 Identificación de amenazas con Magerit

TIPO AMENAZA	AMENAZA
[N] Desastres naturales	[N1] Fuego
[N] Desastres naturales	[N2] Daños por agua

Fuente: “Elaboración propia”

Tabla 4 Identificación de amenazas con Magerit (continuación)

TIPO AMENAZA	AMENAZA
[N] Desastres naturales	[N*] Desastres naturales
[I] De origen industrial	[I1] Fuego
[I] De origen industrial	[I2] Daños por agua
[I] De origen industrial	[I*] Desastres industriales
[I] De origen industrial	[I3] Contaminación mecánica
[I] De origen industrial	[I4] Contaminación electromagnética
[I] De origen industrial	[I5] Avería de origen físico o lógico
[I] De origen industrial	[I6] Corte del suministro eléctrico
[I] De origen industrial	[I7] Condiciones inadecuadas de temperatura o humedad
[I] De origen industrial	[I8] Fallo de servicios de comunicaciones
[I] De origen industrial	[I9] Interrupción de otros servicios y suministros esenciales
[I] De origen industrial	[I10] Degradación de los soportes de almacenamiento de la información
[I] De origen industrial	[I11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios
[E] Errores y fallos no intencionados	[E2] Errores del administrador
[E] Errores y fallos no intencionados	[E3] Errores de monitorización (log)
[E] Errores y fallos no intencionados	[E4] Errores de configuración
[E] Errores y fallos no intencionados	[E7] Deficiencias en la organización
[E] Errores y fallos no intencionados	[E8] Difusión de software dañino
[E] Errores y fallos no intencionados	[E9] Errores de [re-]encaminamiento
[E] Errores y fallos no intencionados	[E10] Errores de secuencia
[E] Errores y fallos no intencionados	[E14] Escapes de información
[E] Errores y fallos no intencionados	[E15] Alteración accidental de la información
[E] Errores y fallos no intencionados	[E18] Destrucción de información
[E] Errores y fallos no intencionados	[E19] Fugas de información

Fuente: “Elaboración propia”

Tabla 5 Identificación de amenazas con Magerit (continuación)

TIPO AMENAZA	AMENAZA
[E] Errores y fallos no intencionados	[E20] Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	[E21] Errores de mantenimiento / actualización de programas (software)
[E] Errores y fallos no intencionados	[E23] Errores de mantenimiento / actualización de equipos (hardware)
[E] Errores y fallos no intencionados	[E24] Caída del sistema por agotamiento de recursos
[E] Errores y fallos no intencionados	[E25] Pérdida de equipos
[E] Errores y fallos no intencionados	[E28] Indisponibilidad del personal
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)
[A] Ataques intencionados	[A4] Manipulación de la configuración
[A] Ataques intencionados	[A5] Suplantación de la identidad del usuario
[A] Ataques intencionados	[A6] Abuso de privilegios de acceso
[A] Ataques intencionados	[A7] Uso no previsto
[A] Ataques intencionados	[A8] Difusión de software dañino
[A] Ataques intencionados	[A9] [Re-]encaminamiento de mensajes
[A] Ataques intencionados	[A10] Alteración de secuencia
[A] Ataques intencionados	[A11] Acceso no autorizado
[A] Ataques intencionados	[A12] Análisis de tráfico
[A] Ataques intencionados	[A13] Repudio
[A] Ataques intencionados	[A14] Interceptación de información (escucha)
[A] Ataques intencionados	[A15] Modificación deliberada de la información
[A] Ataques intencionados	[A18] Destrucción de información
[A] Ataques intencionados	[A19] Divulgación de información
[A] Ataques intencionados	[A22] Manipulación de programas

Fuente: “Elaboración propia”

Tabla 6 Identificación de amenazas con Magerit (continuación)

TIPO AMENAZA	AMENAZA
[A] Ataques intencionados	[A23] Manipulación de los equipos
[A] Ataques intencionados	[A24] Denegación de servicio
[A] Ataques intencionados	[A25] Robo
[A] Ataques intencionados	[A26] Ataque destructivo
[A] Ataques intencionados	[A27] Ocupación enemiga
[A] Ataques intencionados	[A28] Indisponibilidad del personal
[A] Ataques intencionados	[A29] Extorsión
[A] Ataques intencionados	[A30] Ingeniería social (picaresca)

Fuente: “Elaboración propia”

Como se mencionó anteriormente, la importancia que tiene la catalogación de los activos es muy grande, de aquí parte la correcta relación entre el tipo de activo de información y las diferentes amenazas a las cuales es susceptible el activo.

Luego de esto se relacionan las amenazas con una o varias vulnerabilidades y lo que resta es definir el plan de tratamiento de riesgo de acuerdo con el nivel de aceptación del riesgo que será sustentado más adelante.

Figura 10. Amenazas Metodología Magerit y vulnerabilidades asociadas

No. De Amenazas	Activos de Información	Nombre del activo de información	VALORACIÓN DEL	Amenazas Metodología Magerit	Vulnerabilidades
1	SERVICIOS	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	17	[E19] Fugas de información	Transporte inseguro de los datos desde la oficina del cliente hasta la nube del proveedor
2	SOFTWARE	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	18	[A15] Modificación deliberada de la información	Alteración indebida de la información
3	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	18	[E21] Errores de mantenimiento / actualización de programas (software)	Versión de sistema operativo obsoleto y sin soporte que es vulnerable
4	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - Apps LAMP - PHP5.6.16	19	[E20] Vulnerabilidades de los programas (software)	Versiones 5.x de PHP obsoletas, con multiples vulnerabilidades y sin soporte
5	HARDWARE	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	12	[I5] Avería de origen físico o lógico	Daño de algun componente interno de equipo por una mala manipulación o golpe. Daño humano por mantenimiento preventivo o correctivo mal ejecutado.
6	SOFTWARE	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	19	[E2] Errores del administrador	Un servidor con falencias a nivel de hardening puede permitir la explotación de una serie de vulnerabilidades que ponen en peligro la seguridad de la información
7	HARDWARE	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen8	12	[I6] Corte del suministro eléctrico	Falta de respaldo eléctrico y/o de contingencia electrica
8	SOFTWARE	[SW] Servidor proxy - OS Arch Linux 4.14.70	15	[A11] Acceso no autorizado	No revocación de permisos o eliminación de usuarios privilegiados
9	HARDWARE	[HW] Servidor proxy - Dell Vostro 200	12	[E24] Caída del sistema por agotamiento de recursos	Ataques de denegación de servicios
10	SOFTWARE	[SW] Servidor SIP - Freepbx 10.13.66	15	[A11] Acceso no autorizado	Atacantes pueden infiltrar la planta para generar llamadas internacionales que generan sobrecostos en la facturación
11	HARDWARE	[HW] Servidor SIP - Clon hibrido	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Incumplimiento al plan de mantenimiento que genera deterioro físico de las partes internas del servidor
12	SOFTWARE	[SW] Software antivirus (Forticlient v7)	19	[A6] Abuso de privilegios de acceso	El usuario accede a configuraciones del antivirus para crear excepciones, desactivarlo o desinstalarlo sin autorización ni precaución.
13	SOFTWARE	[SW] Suite de ofimática (MS Office 2013)	19	[E20] Vulnerabilidades de los programas (software)	Omisión en característica seguridad en aplicaciones
14	SOFTWARE	[SW] Suite de ofimática (MS Office 2016)	19	[E20] Vulnerabilidades de los programas (software)	Omisión en característica seguridad en aplicaciones
15	SOFTWARE	[SW] software de estudios (Digsilent 2016-2022)	19	[E2] Errores del administrador	Error de la restecnica al borrar o manipular archivos propios del sistema como servicios, controladores o DLL's causando inestabilidad o daños en el SO.
16	SOFTWARE	[SW] Software de estudios (Neplan v10.9.1.1)	19	[E1] Errores de los usuarios	Consultas generadas por los usuarios que genera consumo excesivo de recursos
17	SOFTWARE	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	12	[E20] Vulnerabilidades de los programas (software)	Extracción de información confidencial como hashes de contraseña simplemente haciendo una llamada maliciosa.
18	SOFTWARE	[SW] Ordenador portatil (OS Windows 10 Single Language)	19	[E21] Errores de mantenimiento / actualización de programas (software)	Se pueden conectar unidades externas y modifica codigo UEFI en la memoria
19	HARDWARE	[HW] Switch * 2 (V1910-48G J8009A)	15	[I5] Avería de origen físico o lógico	Degradación del firmware por falta de mantenimiento que genera indisponibilidad de acceso a la red de los dispositivos conectados
20	HARDWARE	[HW] Switch * 2 (HP 1950-48G JG963A)	12	[I7] Condiciones inadecuadas de temperatura o humedad	Sistema de refrigeración deficiente o inexistente en el area dispuesta para centralizar equipos servidores y de networking.
21	SOFTWARE	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	19	[E20] Vulnerabilidades de los programas (software)	Firmware obsoleto y vulnerable que permite la escalada de privilegios
22	HARDWARE	[HW] Access Point (UNIFI Ubiquiti)	12	[I6] Corte del suministro eléctrico	Susceptibilidad a las variaciones de voltaje
23	SERVICIOS	[S] Correo electronico (G-Suite)	19	[A5] Suplantación de la identidad del usuario	Por medio del correo electronico se envían campañas de Phishing que conducen a los usuarios hacia enlaces o paginas que aperentan ser legitimas, pero tienen intenciones maliciosas, como el robo de credenciales, por ejemplo.
24	SERVICIOS	[S] Backup (Google Drive)	15	[A11] Acceso no autorizado	Por falta de politicas o restricciones a nivel de directorios almacenados en esta herramienta, se pueden presentar accesos no autorizados a información confidencial, lo cual impacta precisa y directamente a la confidencialidad de la información
25	AUXILIAR	[AUX] Sistema de alimentación ininterrumpida (UPS)	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Daño de sistema de respando UPS por falta de mantenimiento o seguimiento al estado de baterias.
26	HARDWARE	[HW] Telefono IP (GrandStream)	15	[A25] Roto	Telefonos en escritorios expuestos y sin mecanismos de seguridad fisica
27	COMUNICACIONES	[COM] Internet (Proveedor C&W fibra optica de 80MB)	12	[I8] Fallo de servicios de comunicaciones	Al contar con un solo ISP, si este falla genera indisponibilidad de servicios esenciales
28	DATOS	[D] Hojas de vida de colaboradores	15	[A11] Acceso no autorizado	Control inadecuado al acceso físico
29	HARDWARE	[HW] Equipos de computo (En alquiler RcCom, Milenio PC y Zinko)	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Incumplimiento en el mantenimiento del sistema de información
30	SERVICIOS	[S] Paginas web corporativas (Servidor Digital Ocean)	12	[A24] Denegación de servicio	Puertos inseguros abiertos
31	SERVICIOS	[COM] Red de Area Local (LAN)	19	[A5] Suplantación de la identidad del usuario	Un atacante puede hacerse pasar por un usuario autorizado y escalar privilegios

Fuente: “Elaboración propia”

Se realizan los siguientes cálculos para identificar el nivel de aceptación de riesgos y definir los riesgos que se deben tratar en el plan de tratamiento de riesgos:

- Cálculo de riesgo neto = Valoración del riesgo de los activos * Probabilidad de la vulneración, donde: 1 muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente seguro)
- Criticidad neta = Ubicar el valor del cálculo de riesgo neto, donde: 1 a 4 despreciable (D), 5 a 9 baja (B), 10 a 15 apreciable (A), 16 a 20 importante (I), 21 a 25 crítico(C)
- Calificación de gestión = Un valor de la siguiente escala: 1 control no existe, 2 existe, pero no efectivo, 3 efectivo, pero no documentado, 4 efectivo y documentado.
- Riesgo residual = Calificación del riesgo neto / Calificación de gestión
- Criticidad residual = Ubicar el valor del cálculo de riesgo residual, donde: 1 a 4 despreciable (D), 5 a 9 baja (B), 10 a 15 apreciable (A), 16 a 20 importante (I), 21 a 25 crítico(C)
- Nivel de aceptación del riesgo = Ubicar el valor del riesgo residual, donde: 1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I)

Figura 11. Niveles de aceptación del riesgo

No. De Amenazas	Activos de Información	Nombre del activo de información	VALORACIÓN DEL	Niveles de aceptació	Probabilidad de	Calculo del riesgo net	Criticidad neta	Calificación de Gestión	Si la opciónes 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
1	SERVICIOS	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	17	I	3	51	C	1		51	C
2	SOFTWARE	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	18	I	2	36	C	1		36	C
3	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	18	I	3	54	C	1		54	C
4	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - Apps LAMP - PHP 5.6.16	19	I	3	57	C	1		57	C
5	HARDWARE	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	12	I	3	36	C	1		36	C
6	SOFTWARE	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	19	I	3	57	C	1		57	C
7	HARDWARE	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	12	I	3	36	C	2	Existe una UPS para alimentar los activos criticos mientras se hace la transferencia a las plantas manuales o se recupera el fluido electrico	18	I
8	SOFTWARE	[SW] Servidor proxy - OS Arch Linux 4.14.70	15	I	4	60	C	1		60	C
9	HARDWARE	[HW] Servidor proxy - Dell Vostro 200	12	I	3	36	C	1		36	C
10	SOFTWARE	[SW] Servidor SIP - Freepbx 10.13.66	15	I	3	45	C	1		45	C
11	HARDWARE	[HW] Servidor SIP - Clon hibrido	12	I	3	36	C	2	Existe un cronograma de mantenimiento para los servidores	18	I
12	SOFTWARE	[SW] Software antivirus (Forticlient v7)	19	I	5	95	C	1		95	C
13	SOFTWARE	[SW] Suite de ofimática (MS Office 2013)	19	I	5	95	C	1		95	C
14	SOFTWARE	[SW] Suite de ofimática (MS Office 2016)	19	I	4	76	C	1		76	C
15	SOFTWARE	[SW] software de estudios (Digsilent 2016-2022)	19	I	2	38	C	1		38	C
16	SOFTWARE	[SW] Software de estudios (Neplan v10.9.1.1)	19	I	3	57	C	1		57	C
17	SOFTWARE	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	12	I	3	36	C	1		36	C
18	SOFTWARE	[SW] Ordenador portatil (OS Windows 10 Single Language)	19	I	4	76	C	1		76	C
19	HARDWARE	[HW] Switch * 2 (V1910-48G JE009A)	15	I	3	45	C	1		45	C
20	HARDWARE	[HW] Switch * 2 (HP 1950-48G JG963A)	12	I	4	48	C	3	Existe un cuarto de comunicaciones con refrigeración permanente y un cornograma de mantenimiento de aire acondicionado	16	I
21	SOFTWARE	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	19	I	3	57	C	2	Existe un contrato con el tercero que administra el Firewall, donde detalla la existencia de un plan de actualización recurrente	29	C
22	HARDWARE	[HW] Access Point (UNIFI Ubiquiti)	12	I	4	48	C	2	Existe una UPS para alimentar los activos criticos mientras se hace la transferencia a las plantas manuales o se recupera el fluido electrico	24	C
23	SERVICIOS	[S] Correo electronico (G-Suite)	19	I	1	19	I	1		19	I
24	SERVICIOS	[S] Backup (Google Drive)	15	I	3	45	C	1		45	C
25	AUXILIAR	[AUX] Sistema de alimentación ininterrumpida (UPS)	12	M	3	36	C	3	Existe un procedimiento que indica el plan de mantenimiento que se realiza sobre las UPS	12	A
26	HARDWARE	[HW] Telefono IP (GrandStream)	15	M	1	15	A	3	Existe vigilancia física privada con apoyo en camaras de seguridad al interior y exterior de la empresa	5	B
27	COMUNICACIONES	[COM] Internet (Proveedor C&W fibra optica de 80MB)	12	M	2	24	C	2	El ISP garantiza un 99.96% de disponiilidad del servicio. Existe un procedmiento de conexión alterno, si llegase a fallar el ISP principal	12	A
28	DATOS	[D] Hojas de vida de colaboradores	15	M	2	30	C	4	Existe una politica de restricción de acceso solo a personal autorizado al centro de documentación. Área monitoreda por camaras de seguridad	8	B
29	HARDWARE	[HW] Equipos de computo (En alquiler PcCom, Milenio PC y Zinko)	12	A	1	12	A	3	En conjunto con los proveedores, se tiene defindo un plan de mantenimiento de equipos de computo	4	D
30	SERVICIOS	[S] Paginas web corporativas (Servidor Digital Ocean)	12	M	2	24	C	3	El proveedor que administra los sitios web se encarga de la seguridad de estos	8	B
31	SERVICIOS	[COM] Red de Area Local (LAN)	19	I	2	38	C	1		38	C

Fuente: “Elaboración propia”

6.3 DETERMINAR UN PLAN DE TRATAMIENTO DE RIESGO POR MEDIO DE LA GUÍA DE BUENAS PRÁCTICAS ISO/IEC 27002:2013

Actividad 3: Existen cuatro opciones de tratamiento de riesgo:

- **Mitigar el riesgo:** se trata de disminuir los riesgos hasta un nivel de riesgo aceptable mediante la aplicación de controles de seguridad del Anexo A incluidos en el documento “anexo A de la norma ISO 27001” o también referenciado como ISO 27002

- **Transferir el riesgo:** dependiendo del tipo de riesgo se puede pensar en transferir el riesgo. La transferencia de riesgos es una estrategia de gestión y control de riesgos que implica el cambio contractual de un riesgo puro de una parte a otra. Un ejemplo es la compra de una póliza de seguro, por la cual se transfiere un riesgo específico de pérdida del titular de la póliza a la aseguradora.

- **Evitar el riesgo:** prevenir o evitar un riesgo mediante la eliminación de peligros, actividades y exposiciones que impacten de manera negativa los activos de información de la organización. No se trata de una gestión propia de los riesgos que tiene como objetivo controlar los daños y las consecuencias financieras de los eventos amenazantes, la prevención de riesgos busca evitar por completo el compromiso de los eventos.

- **Aceptar el riesgo:** aceptar el riesgo significa que, aunque el riesgo está identificado y registrado en el proceso de gestión de riesgos, no se realizará ninguna acción. Simplemente se acepta que pueda suceder y se aplicará un tratamiento específico si así ocurre.

  Esta es una buena estrategia para usar con riesgos muy pequeños: riesgos que no tendrán un gran impacto en la actividad de la organización si llega a ocurrir y existe

una solución fácil en caso de que surja. Esto lo haremos en el caso que el coste de una estrategia alternativa de gestión de riesgos para enfrentar el riesgo sea mayor que los recursos empleados en asumir el riesgo".[17]

La gran mayoría de los riesgos, debido a su nivel de aceptación de riesgo definido como inaceptable, se deben tratar y en lo posible mitigarlos. Algunos, se pueden aceptar porque presentan un nivel aceptable o moderado.

En la figura 12, se evidencia la primera clasificación antes de pasar con la implementación de los controles del Anexo A.

[17] ISO 27001. Fase 4 Planificación del SGSI, s.f.

Figura 12. Tratamiento de riesgos

No. De Amenazas y Vulnerabilidades	Activos de Informacion	Nombre del activo de información	Niveles de aceptación del riesgo	Transefir	Aceptar	Eliminar	Mitigar
1	SERVICIOS	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	I				X
2	SOFTWARE	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	I				X
3	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	I				X
4	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	I				X
5	HARDWARE	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	I				X
6	SOFTWARE	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	I				X
7	HARDWARE	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	I				X
8	SOFTWARE	[SW] Servidor proxy - OS Arch Linux 4.14.70	I				X
9	HARDWARE	[HW] Servidor proxy - Dell Vostro 200	I				X
10	SOFTWARE	[SW] Servidor SIP - Freepbx 10.13.66	I				X
11	HARDWARE	[HW] Servidor SIP - Clon hibrido	I				X
12	SOFTWARE	[SW] Software antivirus (Forticlient v7)	I				X
13	SOFTWARE	[SW] Suite de ofimática (MS Office 2013)	I				X
14	SOFTWARE	[SW] Suite de ofimática (MS Office 2016)	I				X
15	SOFTWARE	[SW] software de estudios (Digsilent 2016-2022)	I				X
16	SOFTWARE	[SW] Software de estudios (Neplan v10.9.1.1)	I				X
17	SOFTWARE	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	I				X
18	SOFTWARE	[SW] Ordenador portatil (OS Windows 10 Single Language)	I				X
19	HARDWARE	[HW] Switch * 2 (V1910-48G JE009A)	I				X
20	HARDWARE	[HW] Switch * 2 (HP 1950-48G JG963A)	I				X
21	SOFTWARE	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	I	X			
22	HARDWARE	[HW] Access Point (UNIFI Ubiquiti)	I				X
23	SERVICIOS	[S] Correo electronico (G-Suite)	I				X
24	SERVICIOS	[S] Backup (Google Drive)	I				X
25	AUXILIAR	[AUX] Sistema de alimentación ininterrumpida (UPS)	M		X		
26	HARDWARE	[HW] Telefono IP (GrandStream)	M		X		
27	COMUNICACIONES	[COM] Internet (Proveedor C&W fibra optica de 80MB)	M		X		
28	DATOS	[D] Hojas de vida de colaboradores	M		X		

Fuente: “Elaboración propia”

Luego, basados en el Anexo A, se definen los dominios, los objetivos de control y los controles aplicables a cada uno de los activos a tratar.

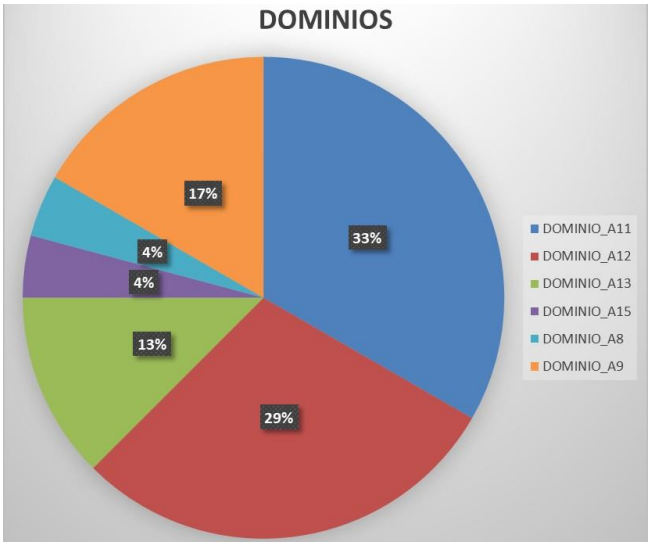
Figura 13. Aplicación de controles Anexo A

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre de la Activo de información	Plan de Tratamiento			
			Indique el control a aplicar a partir de la norma ISO 27001:2013			
			DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación de los control
1	SERVICIOS	[S] Sistema de gestión financiera [Siesa ERP Nube AWS]	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.6 Seguridad de equipos y activos fuera de las instalaciones –Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas	Se debe implementar una política de seguridad y un procedimiento que defina el control sobre los activos de información que se han trasladado a la nube, su tratamiento, la seguridad en todas sus capas, transporte y acceso, etc, lo involucra al proveedor de nube para establecer el modelo de
2	SOFTWARE	[SW] Servidor para sistema de gestión del recurso humano [Nomina web] - OS Windows Server 2016 - AWS	DOMINIO_A.15	OBJETIVO_A.15.1	A15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores –Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o	Se debe implementar una política de seguridad donde se definan los requisitos de seguridad que debe ofrecer el proveedor de nube en cuanto a la gestión del sistema operativo del servidor donde se aloja este servicio
3	SOFTWARE	[SW] Servidor de aplicaciones web [GDP - Wiki - Transferencias] - OS Arch Linux 4.11.5	DOMINIO_A.12	OBJETIVO_A.12.5	A12.5.1 Instalación de software en sistemas operativos –Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Se debe implementar un procedimiento para programar ventanas de actualización sobre el sistema operativo y de hierro previo a la instalación de una actualización del SO o de un software,
4	SOFTWARE	[SW] Servidor de aplicaciones web [GDP - Wiki - Transferencias]- Apps LAMP - PHP 5.6.36	DOMINIO_A.12	OBJETIVO_A.12.6	A12.6.1 Gestión de las vulnerabilidades técnicas –Control: Se debe obtener oportuna mente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	Se debe implementar y socializar una política de seguridad y un procedimiento de control que defina el tratamiento sobre las vulnerabilidades técnicas sobre software obsoleto
5	HARDWARE	[HW] Servidor de aplicaciones web [GDP - Wiki - Transferencias] - HP Proliant DL380 G6	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.4 Mantenimiento de los equipos. –Control: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe contar con indicadores que midan el cumplimiento y la eficacia del programa de mantenimiento y su periodicidad
6	SOFTWARE	[SW] Servidor de aplicaciones técnicas [DigSilent, ELCAD, Primtech NEPLAN V5] - OS Windows Server 2016	DOMINIO_A.12	OBJETIVO_A.12.6	A12.6.2 Restricciones sobre la instalación de software –Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Se debe establecer una política de seguridad y un procedimiento de control que describa las reglas los permisos, los responsables de realizar la instalación y configuración sobre los diferentes sistemas operativos de la organización, los cuales deben garantizar un nivel adecuado de
7	HARDWARE	[HW] Servidor de aplicaciones técnicas [DigSilent, ELCAD, Primtech NEPLAN V5] - HP Proliant DL380 Gen8	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.2 Servicios de suministro –Control: los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Se debe contar con un sistema de suministro de energía alterno con capacidad de soportar los servidores, mientras se hace la transferencia manual a las plantas o se restablece el servicio
8	SOFTWARE	[SW] Servidor proxy - OS Arch Linux 4.14.70	DOMINIO_A.9	OBJETIVO_A.9.2	A9.2.5 Revisión de los derechos de acceso de usuarios –Control: los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Implementar un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o
9	HARDWARE	[HW] Servidor proxy - Dell Vostro 260	DOMINIO_A.13	OBJETIVO_A.13.1	A13.1.2 Seguridad de los servicios de red –Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o	Se deben implementar y documentar mecanismos de seguridad robustos que proteja n el activo de ataques de denegación de servicios los cuales puede agotar sus recursos físicos y desencadenen indisponibilidad
10	SOFTWARE	[SW] Servidor SIP - Freepbx 10.13.66	DOMINIO_A.9	OBJETIVO_A.9.4	A9.4.3 Sistema de gestión de contraseñas –Control: los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Se debe establecer y socializar una política de seguridad para contraseñas seguras, que incluya periodicidad de cambio, robustez, complejidad, entre otros para nuestros
11	HARDWARE	[HW] Servidor SIP - Clon híbrido	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.4 Mantenimiento de los equipos. –Control: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe contar con indicadores que midan el cumplimiento y la eficacia del programa de mantenimiento y su periodicidad
12	SOFTWARE	[SW] Software antivirus [Forticlient VP]	DOMINIO_A.9	OBJETIVO_A.9.2	A9.2.3 Gestión de derechos de acceso privilegiado –Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Se deben establecer y documentar los accesos privilegiados basados en roles sobre cualquier activo de información para evitar la manipulación no autorizada de los sistemas
13	SOFTWARE	[SW] Suite de ofimática [MS Office 2013]	DOMINIO_A.12	OBJETIVO_A.12.2	A12.2.1 Controles contra códigos maliciosos –Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Se deben documentar todas las acciones de protección que realiza el Firewall perimetral con el fin de conocer si puede existir alguna brecha de seguridad que permita la explotación de este tipo de vulnerabilidades. Adicional mente, se debe tener un informe periódico de las amenazas contenidas
14	SOFTWARE	[SW] Suite de ofimática [MS Office 2016]	DOMINIO_A.12	OBJETIVO_A.12.6	A12.6.1 Gestión de las vulnerabilidades técnicas –Control: Se debe obtener oportuna mente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	Se debe implementar y socializar una política de seguridad y un procedimiento de control que defina el tratamiento sobre las vulnerabilidades técnicas sobre software obsoleto
15	SOFTWARE	[SW] software de estudios [Digsilent 2016-2022]	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.4 Mantenimiento de los equipos. –Control: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe implementar y socializar una política de seguridad y un procedimiento que defina las mejores practicas para realizar el mantenimiento de los servidores, para disminuir fallas al
16	SOFTWARE	[SW] Software de estudios [Neplan v109.1.1]	DOMINIO_A.8	OBJETIVO_A.8.1	A8.1.3 Uso aceptable de los activos –Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con	Se debe implementar y socializar una política de seguridad y un procedimiento donde se especifique el uso adecuado de los activos y la formación o el entrenamiento para apropiar de
17	SOFTWARE	[SW] Software de llamadas telefónicas [Softphone Microsip 3.20.7]	DOMINIO_A.12	OBJETIVO_A.12.2	A12.2.1 Controles contra códigos maliciosos –Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia	Se debe fortalecer el software que se utiliza para las llamadas telefónicas, tanto servidor como cliente. Asi mismo, se debe fortalecer la protección de dispositivos finales por medio de un software
18	SOFTWARE	[SW] Ordenador portatil [OS Windows 10 Single Language]	DOMINIO_A.12	OBJETIVO_A.12.6	A12.6.1 Gestión de las vulnerabilidades técnicas –Control: Se debe obtener oportuna mente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las	Se debe implementar y socializar una política de seguridad y un procedimiento para la gestión de vulnerabilidades técnicas de los sistemas de información. En el procedimiento se debe detallar periodicidad de aplicación de parches de seguridad, sitios de descarga, fuentes de información,
19	HARDWARE	[HW] Switch ^2 [WS-C3560-48PS-E]	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.4 Mantenimiento de los equipos. –Control: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se deben incluir estos dispositivos dentro del programa de mantenimiento preventivo y correctivo y documentar su ejecución con indicadores de cumplimiento
20	HARDWARE	[HW] Switch ^2 [HP 1950-48G J9830A]	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.1 Ubicación y protección de los equipos –Control: los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las	Se debe llevar registro del cumplimiento del plan de mantenimiento de los equipos de aire acondicionado en esta área
21	SOFTWARE	[SW] Firewall [Fortinet 100E Version de Firmware 6.4.6]				Se trasfiere el riesgo
22	HARDWARE	[HW] Access Point [UNIFI Ubiquiti]	DOMINIO_A.11	OBJETIVO_A.11.2	A11.2.2 Servicios de suministro –Control: los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Se debe contar con un sistema de control que regule la energía que se suministra a l dispositivo para evitar fallos por sobrecargas. Integrar los APs a la conexión electrica con la UPS
23	SERVICIOS	[S] Correo electronico [G-Suite]	DOMINIO_A.13	OBJETIVO_A.13.2	A13.2.3 Mensajería Electronica –Control: Se debe proteger adecuada mente la información incluida en la mensajería electrónica.	Se deben implementar mecanismos de seguridad de tipo DLP, para prevenir la exfiltración de datos por medio del correo electronico. Herramientas que filtren el spam y sensibilización constante a los
24	SERVICIOS	[S] Backup [Google Drive]	DOMINIO_A.9	OBJETIVO_A.9.1	A9.1.1 Política de control de acceso –Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Se debe establecer y socializar una política de seguridad y un procedimiento que defina el control de acceso a los diferentes directorios de la herramienta de backups. Esto debe ser en función de roles de usuarios, áreas de trabajo, entre otros. Separando así el acceso a datos sensibles de la
25	AUXILIAR	[ALM] Sistema de alimentación ininterrumpida [UPS]				Se acepta el riesgo
26	HARDWARE	[HW] Telefono IP [Grandstream]				Se acepta el riesgo
27	COMUNICACIONES	[COM] Internet [Proveedor C&W fibra optica de 30MB]				Se acepta el riesgo
28	DATOS	[D] Hojas de vida de colaboradores				Se acepta el riesgo
29	HARDWARE	[HW] Equipos de computo [Enalquiler PcCom, Millenio PCy Zinko]				Se trasfiere el riesgo
30	SERVICIOS	[S] Paginas web corporativas [Servidor Digital Ocean]				Se trasfiere el riesgo
31	SERVICIOS	[COM] Red de Area Local [LAN]	DOMINIO_A.13	OBJETIVO_A.13.1	A13.1.3 Separación en las redes –Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Se debe esta blecer la separación de las redes por medio de la implementación de VLANs y DMZs, con el fin de controlar el acceso a los recursos solo a personal permitido de acuerdo con su rol dentro

Fuente: “Elaboración propia”

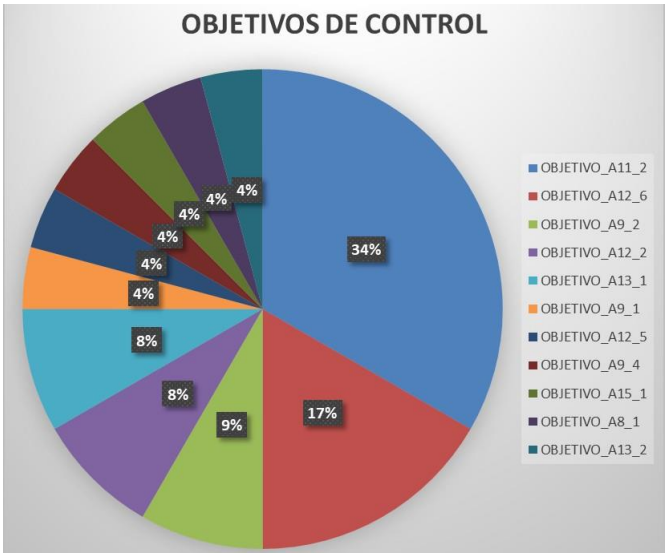
Los resultados de la adopción del Anexo A, están representados en las figuras 14, 15 y 16.

Figura 14. Dominios Anexo A



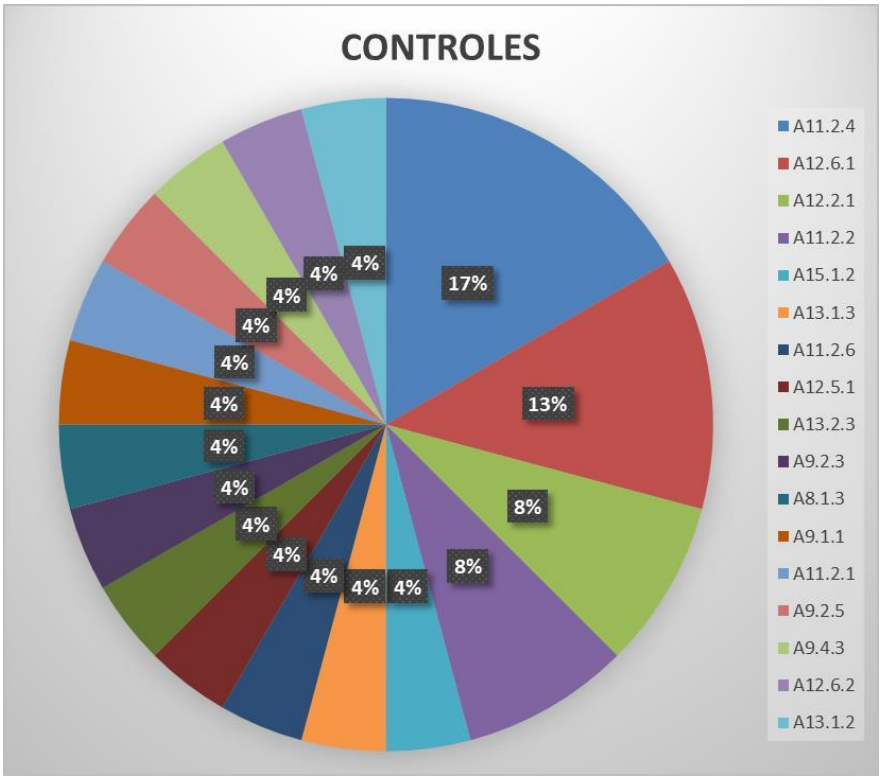
Fuente: “Elaboración propia”

Figura 15. Objetivos de control Anexo A



Fuente: “Elaboración propia”

Figura 16. Controles Anexo A



Fuente: “Elaboración propia”

Los dominios A11 – Seguridad física y del entorno y A12 – Seguridad de las operaciones son los dominios que predominan después de la aplicación de los controles del Anexo A.

Los objetivos de control A11.2 - Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. y A12.6 - Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas son los dominios que predominan después de la aplicación de los controles del Anexo A.

Los controles A11.2.4 – Mantenimiento de los equipos y A12.6.1 – gestión de las vulnerabilidades técnicas son los dominios que predominan después de la aplicación de los controles del Anexo A.

Esto quiere decir que en función de estos dos últimos controles mencionados se deben enfocar los esfuerzos para mitigar o contener la mayoría de los riesgos identificados en los diferentes activos de información.

6.4 ELABORAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA MITIGAR LOS RIESGOS DE LA EMPRESA GERS S.A.S.

Actividad 4: Se debe definir la política de seguridad recogiendo "las directrices que debe seguir la seguridad de la información de acuerdo con las necesidades de la organización y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades".[18]

Con base en el ejemplo que plasma MINTIC en su guía "Elaboración de la política general de seguridad y privacidad de la información"[19], se elabora la siguiente política para el SGSI:

Política para el SGSI de GERS S.A.S.

"La dirección de GERS S.A.S., entendiendo la importancia de una adecuada gestión de la información se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.

[18] INTECO. Implantación de un SGSI en la empresa, s.f. p. 16.
[19] MINTIC. Elaboración de la política general de seguridad y privacidad de la información. 2012. [Consulta: 05 de noviembre de 2022]. p. 9. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Para GERS S.A.S., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la empresa según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la empresa.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de GERS S.A.S.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la empresa, sus funcionarios, contratistas y terceros de GERS S.A.S. y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de GERS S.A.S.:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- GERS S.A.S. protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- GERS S.A.S. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- GERS S.A.S. protegerá su información de las amenazas originadas por parte del personal.
- GERS S.A.S. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- GERS S.A.S. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- GERS S.A.S. implementará control de acceso a la información, sistemas y recursos de red.
- GERS S.A.S. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- GERS S.A.S. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- GERS S.A.S. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- GERS S.A.S. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

El incumplimiento a la Política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la empresa, incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.”

CONCLUSIONES

- Después de diagnosticar los diferentes dominios y controles presentes en la Norma ISO/IEC 27002:2013, se puede concluir que, a pesar de que la empresa tiene total disposición para implementar un SGSI y que su nivel de madurez en otros sistemas de gestión evidenciados en su SGI es óptimo, se nota debilidad en los procesos relacionados con la seguridad de la información y por ende la implementación del presente proyecto fue de gran ayuda para determinar las falencias y mejorar este sistema.

  Por lo anterior, se concluye que el desarrollo adecuado de la etapa inicial del SGSI (la planeación) fue de suma importancia dentro de la organización y más específicamente para el área de Gestión de la Información, toda vez que esta fase permitió dar un orden al proceso por medio de la definición de una serie de objetivos claros, la identificación de activos y amenazas, el análisis y la evaluación de los riesgos y la relación de los controles de seguridad de la información en la declaración de aplicabilidad donde se formalizó el tratamiento de cada riesgo identificado.

- Al analizar los riesgos por medio de la metodología MAGERIT, se concluye que existe un alto nivel de riesgo el cual se debe abordar con prontitud, no solamente para cumplir con la norma y llegar a establecer el SGSI, sino para realmente salvaguardar el activo más importante de la organización: la información.

  Implementar esta metodología es bastante interesante porque abre el panorama y se visualizan los riesgos desde lo general a lo específico y adicionalmente deja recursos muy importantes como lo es el inventario de activos, por ejemplo.

- Dentro de las cuatro opciones disponibles para tratar el riesgo, la acción más eficaz es sin duda la de mitigar el riesgo, pero en ciertos escenarios, ya sea por

funcionamiento u operación propia de la organización, esta acción no es viable al ciento por ciento, entonces es necesario evaluar las siguientes acciones.

La transferencia del riesgo se presenta en muchos escenarios en donde los servicios son tercerizados. GERS S.A.S., en su constante evolución tecnológica, a encaminado grandes esfuerzos por adoptar esta práctica.

La aceptación del riesgo es sin duda la acción más arriesgada que se puede tomar dentro del plan de tratamiento de riesgos, esta debe ser la última opción y no debe ser permanente.

- La política de seguridad de la información tiene un significado importante y va más allá de un simple documento que se genera por cumplimiento. Esta política va relacionada directamente con los objetivos estratégicos de la organización y debe acogerse a la legislación vigente.

  La política debe ser clara y sencilla y debe ser socializada con todos los colaboradores y las partes interesadas, y esta debe ser interiorizada por parte de ellos.

RECOMENDACIONES

- Se debe iniciar con la documentación de todos las políticas, procesos y procedimientos que hacen parte del diagnóstico inicial y que se evidenciaron con un grado de madurez bajo para relacionarlo con el plan de tratamiento de riesgos.

- Es importante que la organización alimente constantemente la matriz de riesgos existente y que dentro de esta se de valor a los activos de información, puesto que se evidencia que la matriz actual evalúa con rigor otros aspectos de la organización, pero a nivel de activos de información es muy superficial.

- Se recomienda iniciar con el plan de tratamiento de riesgos con el fin de tomar las medidas que permitan asegurar aquellos activos que tienen un nivel de riesgo inaceptable. En este punto es importante definir un cronograma de actividades que permita hacer seguimiento y medir su cumplimiento.

- Los controles A11.2.4 – Mantenimiento de los equipos y A12.6.1 – gestión de las vulnerabilidades técnicas son los dominios que predominan después de la aplicación de los controles del Anexo A. Esto quiere decir que en función de estos dos últimos controles mencionados se deben enfocar los esfuerzos para mitigar o contener la mayoría de los riesgos identificados en los diferentes activos de información.

- Se debe ajustar la política de seguridad de la información y/o integrarla a la política actual del sistema de gestión integral. Una vez hecho esto, se debe socializar con todos los colaboradores y con las partes interesadas.

BIBLIOGRAFÍA

ANDRADE, Yovany. Entendiendo el SGSI, Trabajo de grado Especialización en seguridad informática. Universidad Piloto de Colombia, 2016. [Consulta: 15 de mayo de 2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2748

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008) En: Diario Oficial. Diciembre, 2008. Disponible en: https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008

COLOMBIA. SENADO. Ley 1273 (5, enero, 2009) En Diario Oficial. Enero, 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. SENADO. Ley 1341 (30, julio, 2009), En: Diario Oficial. Julio, 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

GOBIERNO DE COLOMBIA. [Sitio web]. Función pública. Decreto 1377 DE 2013. [Consulta: 15 de mayo de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

EALDE Business School. La Gestión de Riesgos en un SGSI, 2020. Disponible en: https://www.ealde.es/gestion-de-riesgos-sgsi/

ESPINOSA, Andrés., *et al*. Establecer e implementar el SGSI, 2021.

GOBIERNO DE COLOMBIA. [Sitio web]. Función pública. Ley 1581 de 2012. [Consulta: 15 de mayo de 2022] Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

FONSECA, Omar. Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS, 2019. Disponible en: http://hdl.handle.net/10882/9521.

GERS S.A.S. Inducción departamento de TI, s,f.

-------- Mapa de procesos GERS 2021, 2021

-------- Matriz de riesgos y oportunidades, 2021

-------- Organigrama, 2021

-------- Perfiles de cargo, 2020

-------- Pensamiento estratégico. Revisión por la dirección, 2021

-------- Política de gestión integral 2021, 2021

-------- Política de protección de datos, 2013

-------- Procedimiento para control de información y software, 2018

-------- Reglamento interno de trabajo. 2018

GÓMEZ, F. L., & Fernández, R. P. P. Cómo implantar un SGSI según une-en ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad, 2018. p. 57-132. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=58

ICONTEC. Norma Técnica Colombiana NTC-ISO-IEC 27001 Técnicas de Seguridad y Requisitos para un Sistema de Gestión de Seguridad de la Información. Colombia, 2013

ICONTEC. Norma Técnica Colombiana NTC-ISO-IEC 27002 Técnicas de Seguridad, Código de Práctica para Controles de Seguridad de la Información. Colombia, 2013

NORMAISO27001. Implantando ISO 27001 paso a paso - La Planificación del SGSI. ISO 27001, s.f. Disponible en: https://normaiso27001.es/fase-4-planificacion-del-sgsi/#h6

INTECO. Implantación de un SGSI en la empresa. p. 16. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO/IEC 27001 certification standard. ISO/IEC 27001:2013. Disponible en: https://www.iso27001security.com/html/27001.html

ISOTools. ¿Cuál es la situación de la norma ISO 27001 en Sudamérica?, 2017. Disponible en: https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

ISO27001security. ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook, 2014. Disponible en: www.ISO27001security.com

ISOTOOLS. 12 beneficios de Implantar un SGSI de acuerdo a ISO 27001, 2016. Disponible en: https://www.isotools.cl/12-beneficios-de-implantar-un-sgsi-de-acuerdo-a-iso-27001/

LALINDE, J. Investigación y desarrollo en seguridad de la información. Disponible en: http://acistente.acis.org.co/typo43/fileadmin/Base_de_Conocimiento/X_JornadaSeguridad/ConferenciaJuanLalinde1.pdf

LOPEZ, Agustín. SGSI. Disponible en: https://www.iso27000.es/sgsi.html

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MINTIC. Elaboración de la política general de seguridad y privacidad de la información, 2012. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

PEREZ, Brigitte. Importancia de un sistema de gestión de seguridad de la información para empresas de tecnología. Trabajo de grado Especialización en seguridad informática. Universidad Piloto de Colombia, 2020. [Consulta: 15 de mayo de 2022]. p. 1. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6841

PEREZ, Pastor y MUNERA, Francisco. Reflexiones para implementar un sistema de gestión de calidad (ISO 9001: 2000) en cooperativas y empresas de economía solidaria, 2007. p. 50. Disponible en: https://books.google.com.co/books?id=-9q8MV_4pXcC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información. 5.2. Política. Disponible en: https://www.pmg-ssi.com/norma-27001/5-2-politica/

WeLiveSecurity. ¿Cómo definir el alcance del SGSI?, 2021. Disponible en: https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/

ANEXOS

Anexo A. Estado inicial y aplicabilidad de controles de seguridad de la información en GERS S.A.S

Anexo B. Análisis de riesgos GERS S.A.S

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A.5	**Políticas de seguridad de la información**				
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.					
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Inexistente	¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)? ¿Están las políticas bien escritas, legible, razonable y viable? ¿Incorporan controles adecuados y suficientes? ¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? ¿Cuán madura es la organización en esta área?	No existe política definida para el SGSI o integrada dentro de la política SGI
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	Inexistente	¿Todas las políticas tienen un formato y estilo consistentes? ¿Están todos al día, habiendo completado todas las revisiones debidas? ¿Se han vuelto a autorizar y se han distribuido?	No existe política definidita para el SGSI o integrada dentro de la política SGI
A.6	**Organización de la seguridad de la información**				
A.6.1	**Organización interna**				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.					
A6.1.1	Roles y responsabilidades en seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Inexistente	¿Se le da suficiente énfasis a la seguridad y al riesgo de la información? ¿Hay apoyo de la administración? ¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad? ¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas? ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? ¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información? ¿Hay coordinación dentro de la organización entre las unidades de negocio? ¿funciona efectivamente en la práctica? ¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?	No se evidencia separación de roles, toda la responsabilidad recae en el Coordinador de TI.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Administrado	¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas? ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed ¿Existe una política que cubra la segregación de deberes? ¿Cómo llegan las decisiones con respecto a tal segregación? ¿Quién tiene la autoridad para tomar tales decisiones? ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?	La empresa cuenta con un mapa de procesos y un perfil de cargo definido para cada área.
A6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	Inexistente	¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias? ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo? ¿La lista es actual y correcta? ¿Hay un proceso de mantenimiento?	No se evidencia un listado de contacto de autoridades a quien se pueda acudir en caso de presentarse un incidente o emergencia.
A6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Inexistente	¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k? ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?	No se evidencia un listado de contacto de grupos especiales a quien se pueda acudir en caso de presentarse un incidente o emergencia.
A6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Inicial	¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? ¿La etapa del proyecto incluye actividades apropiadas?	Los proyectos se ejecutan por las fases adecuadas, pero no se evidencia la existencia de un procedimiento para la correcta ejecución de estos.
A.6.2	**Dispositivos móviles y teletrabajo**				
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles					
A6.2.1	Política de dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Inexistente	¿Existen política y controles seguridad relacionados con los usuarios móviles? ¿Se distinguen los dispositivos personales de los empresariales? ¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad? ¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?	No se evidencia política de seguridad ni medidas de control para el uso de dispositivos móviles.
A6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Inicial	¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina? ¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?	Se implementan algunos controles para acceso remoto seguro, como el uso de VPN, pero no existe un procedimiento ni política formal.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A.7.1	**Antes de asumir el empleo**				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.					
A7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Administrado	¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo? ¿Se hace en la empresa o se subcontrata a un tercero? Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables? ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección? ¿Existen procesos de selección mejorados para los trabajadores en roles críticos? ¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?	El proceso de selección evidencia madurez, se ha actualizado recientemente para dar a conocer a los aspirantes los temas relacionados con la seguridad y privacidad de los datos personales. El proceso está debidamente documentado.
A7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Administrado	¿Están claramente definidos los términos y condiciones de empleo? ¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general? ¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles? ¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?	Dentro del contrato de trabajo se tiene estipulada una clausula que abarca el tema de seguridad de la información.
A.7.2	**Durante la ejecución del empleo**				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.					
A7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Inexistente	¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia? ¿Se hace de forma regular y está a día? ¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados? ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? ¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?	No se evidencia la existencia de un programa de concientización sobre seguridad de la información. Esto se hace esporádicamente y de manera informal.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Inexistente	¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? ¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores? ¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos? ¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos? ¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas? ¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento? ¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?	No existe un programa de capacitación enfocado a dar catedra o sensibilización en temas de seguridad de la información.
A7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Inexistente	¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores? ¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? ¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo? ¿Se actualiza el proceso de forma regular?	No existe un proceso disciplinario que aplique para aquellos que se vean involucrados con incidentes de seguridad de la información.
A.7.3	**Terminación y cambio de empleo**				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.					
A7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Definido	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización? ¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos? ¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?	Se evidencia la existencia de políticas y procedimientos para la eliminación de accesos y recuperación de activos una vez finalice el contrato de trabajo, pero no se tiene contemplado la sustitución de roles y/o privilegios cuando los empleados se mueven vertical u horizontalmente dentro de la organización.
A.8	**GESTION DE ACTIVOS**				
A.8.1	**Responsabilidad sobre los activos**				
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Administrado	¿Hay un inventario de activos de la información? ¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas ¿A quién pertenece el inventario? ¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI? ¿Es suficientemente detallado y está estructurado adecuadamente?	Existe un procedimiento formalizado para hacer uso del software asset manager para gestionar el inventario de los activos de la información.
A8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	Administrado	¿Los activos tienen propietario de riesgo? ¿Los activos tienen responsable técnico? ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos? ¿Cómo se etiquetan los activos? ¿Cómo se informa ante incidentes de seguridad de la información que los afectan?	Se tiene definido el propietario de los activos dentro del inventario. Se elabora acta de entrega a los usuarios, la cual se firma al recibir y al regresar el activo.
A8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Inicial	¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.? ¿Cubre el comportamiento del usuario en Internet y en las redes sociales? ¿Se permite el uso personal de los activos de la empresa? En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto? ¿Se describe de forma explícita lo qué constituye un uso inapropiado? ¿Se distribuye esta información a toda la empresa? ¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?	No se evidencia una política o una guía que defina las responsabilidades de los usuarios para hacer uso de los recursos y activos de información. Algunos están documentados como por ejemplo el uso de correo electrónico.
A8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Administrado	¿Existe un procedimiento para recuperar los activos tras una baja o despido? ¿Es un procedimiento automatizado o manual? Si es manual, ¿Cómo se garantiza que no haya desvíos? ¿Cómo se abordan los casos en los que los activos no han sido devueltos?	Existe un procedimiento formal que aplica cuando un empleado finaliza su contrato, existe un check list de activos por devolver y credenciales y accesos por eliminar.
A.8.2	**Clasificación de la información**				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.					
A8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Repetible	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información? ¿La clasificación es impulsada por obligaciones legales o contractuales? ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad? ¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen? ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?	Existe clasificación parcial de la información, pero no esta respaldada por una política que formalice el proceso.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Inexistente	¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica? ¿Está sincronizado con la política de clasificación de la información? ¿Cómo se garantiza el correcto etiquetado? ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante? ¿Cómo se garantiza que no haya acceso no autorizado? ¿Se revisan los niveles de clasificación en intervalos predefinidos?	No existe un procedimiento para etiquetar la información.
A8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Inexistente	Más allá de A.8.2.1 ¿Están los niveles de clasificación adecuadamente asignados a los activos? ¿Se considera los gimiente? Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.	No existe un procedimiento para el manejo y clasificación de los activos de información.
A.8.3	**Manejo de medios**				
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios					
A8.3.1	Gestión de medio removibles	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Inicial	¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles? ¿Los medios extraíbles están debidamente etiquetados y clasificados? ¿Los medios se mantienen y almacenan de forma adecuada? ¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?	No existe un procedimiento formal para gestionar los medios removibles, aunque se controla su almacenamiento.
A8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Administrado	Más allá de A.8.3.1 ¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios? ¿Se documenta la aprobación en cada etapa para la eliminación de los medios? ¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación? ¿Se tiene en cuenta los periodos de retención?	Se hace disposición adecuada de los medios una vez finaliza su vida útil. Está alineado al PGIR de la organización.
A8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Administrado	¿Se utiliza un transporte o servicio de mensajería confiable? ¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia? ¿Se verifica la recepción por el destino?	Se evidencia una procedimiento formal para el transporte de información por medio de un servicio de mensajería propio y otro externo. Y se verifica la recepción por parte del destinatario.
A.9	**Control de acceso**				
A.9.1	**Requisitos de negocio para el control de acceso**				
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.					
A9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Repetible	¿Existe una política de control de acceso? ¿Es consistente con la política de clasificación? ¿Hay una segregación de deberes apropiada? ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?	No existe política para el control de acceso, pero existen unos procedimientos informales para la segregación de deberes.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Inicial	¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?	Se evidencia el acceso remoto por medio de VPN con los controles adecuados, pero no se acompaña de otras medidas de control. No tiene gestión ni análisis de métricas de incidentes.
A.9.2	**Gestión de acceso de usuario**				
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.					
A9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Repetible	¿Se utiliza un ID de usuario únicos para cada usuario? ¿Se genera en función a una solicitud con aprobaciones y registros apropiados? ¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido? ¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos? ¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes? ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios? ¿Qué impide que los ID de usuario sean reasignados a otros usuarios?	Se utilizan usuarios únicos para cada empleado y se deshabilitan una vez finalizan su contrato laboral, pero el proceso no evidencia formalización.
A9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Inicial	¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Existe un registro documental de la solicitud y aprobación de acceso?	Existe un procedimiento para suministrar accesos de acuerdo con los roles y responsabilidades, pero se evidencian falencias en los controles aplicados.
A9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Inexistente	Más allá de A.9.2.2 ¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios? ¿Se genera un ID de usuario separado para otorgar privilegios elevados? ¿Se ha establecido una caducidad para los ID de usuario con privilegios? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?	No existe un proceso para gestionar las cuentas privilegiadas.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A9.2.4	Gestión de información de autenticación secreta de los usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Inexistente	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.? ¿Se verifica rutinariamente si hay contraseñas débiles? ¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas? ¿Se transmite dicha información por medios seguros? ¿Se generan contraseñas temporales suficientemente fuertes? ¿Se cambian las contraseñas por defecto de los fabricantes? ¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas? ¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?	No existen políticas para la gestión de contraseñas. Se usan contraseña por defecto.
A9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Inexistente	¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones? ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios? ¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?	No se realiza revisión periódica de los derechos de los usuarios de la información.
A9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Repetible	¿Existe un proceso de ajuste de derechos de acceso? ¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo? ¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red? En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?	Existe un procedimiento informal para retirar los accesos a los usuarios que se desvinculen de la empresa.
A.9.3	**Responsabilidades del usuario**				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Inexistente	¿Cómo se asegura la confidencialidad de las credenciales de autenticación? ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida? ¿Existen controles de seguridad relativas a las cuentas compartidas?	No existen políticas o procedimientos para asegurar que los usuarios cumplan con las buenas prácticas de uso de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Inicial	Más allá de A.9.2.2 ¿Existen controles de acceso adecuados? ¿Se identifican los usuarios de forma individual individuales? ¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?	Se tiene restricción parcial a las aplicaciones, pero no existe documento formalizado.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Inexistente	¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado? ¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión? ¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.? ¿La información de inicio de sesión solo se valida una vez imputadas las credenciales? ¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas? ¿Se registran los inicios de sesión exitosos? ¿Se transmiten las contraseñas de modo seguro mediante el uso	No existen políticas o procedimientos para garantizar el acceso seguro al sistema o a las aplicaciones.
A9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Inexistente	¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos? ¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación ¿Se almacenan y transmiten de forma segura (cifrado)?	No existe una política para la gestión de contraseñas.
A9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Inexistente	¿Quién controla los servicios privilegiados? ¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines? ¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? ¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado? ¿Se tiene en cuenta la segregación de tareas?	No existe una política para el uso de programas privilegiados.
A9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso a los códigos fuente de los programas.	No aplicable	¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios? ¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.? ¿Cómo se modifica el código fuente? ¿Cómo se publica y se compila el código? ¿Se almacenan y revisan los registros de acceso y cambios?	NA
A.10	**Criptografía**				
A.10.1	**Controles criptográficos**				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información					
A10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Inexistente	¿Existe una política que cubra el uso de controles criptográficos? ¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables ¿Se cumple con la política y requerimientos de cifrado?	No existe una política para el uso de controles criptográficos.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Inexistente	¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)? ¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas? ¿Se generan claves diferentes para sistemas y aplicaciones? ¿Se evitan claves débiles? ¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)? ¿Se hacen copias de respaldo de las claves? ¿Se registran las actividades clave de gestión? ¿Cómo se cumplen todos estos requisitos?	No existe una política para la gestión de llaves.
A.11	**Seguridad física y del entorno**				
A.11.1	**Áreas seguras**				
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.					
A11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de información.	Administrado	¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?	Se tiene definido una política de seguridad física donde el área de comunicaciones se encuentra aislada de las demás áreas. Se realiza monitoreo con cámaras de seguridad.
A11.1.2	Controles de acceso físicos	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Repetible	¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multifactor de autenticación (ej. Biométrico más el código PIN)? ¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?	El acceso a áreas seguras está protegido con algunos controles de acceso como CCTV, llaves de seguridad, pero no se encuentra documentado.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Definido	¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?	Existen controles para vigilar el acceso a las oficinas como vigilancia privada, CCTV, alarmas de seguridad, pero no están integradas dentro de una política formal.
A11.1.4	Protección contra las amenazas externas y ambientales	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Definido	¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?	Existen mecanismos de protección en caso de incendios, como extintores, adicional la brigada de emergencia esta capacitada para actuar en caso de conatos de incendios. No existe procedimiento para recuperación de desastres.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Definido	¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?	Se cuenta con control de acceso físico, CCTV, las áreas son consideradas seguras, pero no está formalizado en algún documento.
A11.1.6	Áreas de carga, despacho y acceso público	Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Administrado	¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?	Existe un área definida para la carga y descarga de equipos. Existe un procedimiento definido para este fin.
A.11.2	**Equipos**				
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.					
A11.2.1	Ubicación y protección de los equipos	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Definido	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?	Los equipos se encuentran ubicados en zonas seguras, se realizan pruebas de manera periódica. No está formalizado.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Administrado	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?	Existe un sistema de UPS para mantener los servicios críticos operativos mientras se realiza la activación de las plantas (de gasolina) para alimentar el circuito eléctrico. También tienen un sistema solar fotovoltaico que sirve para alimentar ciertas áreas de trabajo.
A11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Definido	¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado? ¿Existen procedimientos adecuados para todo ello?	Los circuitos de cableado eléctrico y de telecomunicaciones está protegido. Se controla el acceso a personal autorizado al rack de comunicaciones. No existe procedimiento formal.
A11.2.4	Mantenimiento de los equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Optimizado	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabajo, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?	Existe un procedimiento formal y se evidencia con registros el cumplimiento de este. Aquí se define el programa de mantenimiento de los equipos de computo, de red, de monitoreo.
A11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Inexistente	¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?	No existe control para retirar equipos de la oficina.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Inexistente	¿Existe una “política de uso aceptable” que cubra los requisitos de seguridad y “obligaciones” con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?	No existe una política de uso aceptable de los equipos por fuera de las oficinas.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Administrado	¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?	Se realiza el proceso de backup y borrado seguro de la información. El proceso se encuentra documentado.
A11.2.8	Equipo de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Repetible	¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña? ¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?	Se tienen algunas medidas de usuarios desentendidos, pero no existe política como tal.
A11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Inexistente	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?	No existe una política de escritorio limpio. Ocasionalmente se realizan jornadas de 5S.
A.12	**Seguridad de las operaciones**				
A.12.1	**Procedimientos y responsabilidades operacionales**				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.					
A12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Optimizado	¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?	Dentro del SGI se encuentran documentados los procedimientos de todos los procesos de la organización, incluyendo gestión de información y gestión de recursos físicos.
A12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Inexistente	¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?	No se evidencia la existencia de una política relacionada con la gestión de cambios.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Inexistente	¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?	No se evidencia la existencia de una política relacionada con la gestión de capacidad.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Repetible	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?	Se separan los ambientes de producción y desarrollo a nivel de instancias y bases de datos, pero no de infraestructura física.
A.12.2	**Protección contra códigos maliciosos**				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.					
A12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Definido	¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de “escaneado en acceso” y “escaneo programático” en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?	Existen controles parciales contra códigos maliciosos, pero son insuficientes para gestionar las vulnerabilidades.
A.12.3	**Copias de respaldo**				
Objetivo: Proteger contra la perdida de datos					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A12.3.1	Copias de seguridad de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Optimizado	¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de Ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?	Existe un proceso definido y optimizado para realizar las copias de seguridad de la información.
A.12.4	**Registro y seguimiento**				
Objetivo: Registrar eventos y generar evidencia					
A12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Inexistente	¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos? ¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?	No se evidencia el registro de eventos de seguridad.
A12.4.2	Protección de la información del registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Inexistente	¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?	No se evidencia el registro de eventos de seguridad por ende no hay protección sobre este.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Inexistente	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?	No se evidencia el registro de las actividades realizadas por el administrador o por el operador.
A12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Inexistente	¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?	No existe sincronización de los relojes de los sistemas contra un servidor NTP central.
A.12.5	**Control de software operacional**				
Objetivo: Asegurarse de la integridad de los sistemas operacionales.					
A12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Definido	¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?	Existe un control informal para la instalación de software, pero no hay restricción para que los usuarios puedan instalar software.
A.12.6	**Gestión de la vulnerabilidad técnica**				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Inexistente	¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?	No existe una política para la gestión de vulnerabilidad técnicas ni para la identificación oportuna de los riesgos. Existe una matriz de riesgos, pero no está aterrizada a la realidad actual.
A12.6.2	Restricción en la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Repetible	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?	La instalación de software no está limitada solo al personal autorizado. Existe un documento que acepta el usuario para no hacer instalación de software no autorizado. Existe una línea base de software autorizado.
A.12.7	**Consideraciones sobre la auditoria de sistemas de información**				
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos					
A12.7.1	Controles de auditoría de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Inicial	¿Existe una política que requiera auditorias de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?	Existe un plan de auditorias tanto internas como externas dentro del SGI, pero este no contempla el SGSI.
A.13	**Seguridad de las comunicaciones**				
A.13.1	**Gestión de la seguridad de las redes**				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Repetible	¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red? ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?	Existen algunos controles informales para asegurar las redes, pero no hay segmentación por medio de VLAN, DMZ, entre otras.
A13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Definido	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?	Se gestionan de manera parcial los servicio de red. Se revisan de forma esporádica los SLA de los terceros. Se hace revisión de los dispositivos de seguridad, pero esta no está programada.
A13.1.3	Separación de las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Inicial	¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?	Existe separación parcial de las redes, pero no está formalizado el procedimiento.
A.13.2	**Intercambio de información**				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Repetible	¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), Wifi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?	Existen algunos procedimientos para la transferencia de información, pero no se encuentran formalizados por medio de una política o control

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Inexistente	Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?	No existen acuerdo sobre la transferencia de información con los terceros.
A13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Inicial	¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.? ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?	Existen mecanismos parciales para proteger la comunicación vía correo electrónico.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Inexistente	¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?	Existen acuerdos de confidencialidad sobre la información que se transfiere a externos.
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**				
A.14.1	**Requisitos de seguridad en los sistemas de información**				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que					
A14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Inexistente	¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software? ¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo? ¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.) ¿Se aplican estos controles para sistemas / software comercial, incluidos los productos “a medida” o personalizados?	La empresa no cuenta con los requisitos mínimos de seguridad de la información.
A14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Inicial	¿La organización usa o proporciona aplicaciones web de comercio electrónico? ¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio? ¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad? ¿Se fuerza https? ¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)? ¿Se analizan y documentan las amenazas de forma rutinaria? ¿Existe una gestión de incidentes y cambios para tratarlos?	Algunos de los sitios publicados por la organización cumplen con las especificadores mínimas de seguridad, pero otras aplicaciones carecen de esto.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A14.1.3	Protección de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Inicial	Más allá de A.14.1.2 ¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet? ¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?	Algunos de los sitios publicados por la organización cumplen con las especificadores mínimas de seguridad, pero otras aplicaciones carecen de esto.
A.14.2	**Seguridad en los procesos de Desarrollo y de Soporte**				
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A14.2.1	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplicable	¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad? ¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios? ¿Los métodos de desarrollo incluyen pautas de programación segura? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	NA
A14.2.2	Procedimiento de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplicable	¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios? ¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión? ¿Incluye un procedimiento para cambios de emergencia? ¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones? ¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?	NA
A14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No aplicable	¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado? ¿Hay registros de estas actividades?	NA
A14.2.4	Restricciones a los cambios en los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Inexistente	¿Se hacen cambios a paquetes software adquiridos? ¿Se verifica que los controles originales no han sido comprometidos? ¿Se obtuvo el consentimiento y la participación del proveedor? ¿El proveedor continúa dando soporte tras los cambios? ¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores? ¿Se hace una comprobación de compatibilidad con otro software en uso?	No se controla de manera adecuada los cambios que involucran al proveedor desarrollador de software.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A14.2.5	Principio de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No aplicable	¿Se siguen principios de SDLC que incluye controles de seguridad? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	NA
A14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No aplicable	¿Se aíslan los entornos de desarrollo? ¿Cómo se desarrolla, prueba y lanza el software? ¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones? ¿Se realizan comprobaciones de antecedentes de los desarrolladores? ¿Tienen que cumplir con un NDA? ¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo? ¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?	NA
A14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Repetible	Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento	Los desarrollos son ejecutados a medida por un tercero, pero a estos desarrollos no se les hace el seguimiento adecuado.
A14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Inexistente	Más allá de A.14.2.7 ¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados? ¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?	No existe un plan de pruebas de seguridad en los sistemas.
A14.2.9	Pruebas de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Inexistente	¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red? ¿Las pruebas replican situaciones y entornos operativos realistas? ¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado? ¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo? ¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?	No existe un plan de pruebas para la aceptación de los sistemas.
A.14.3	**Datos de prueba**				
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A14.3.1	Protección de los datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	No aplicable	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?	NA
A.15	**Relaciones con los proveedores**				
A.15.1	**Seguridad de la información en las relaciones con los proveedores**				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Inexistente	¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización ¿Existe una obligación contractual de cumplimento? ¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?	La empresa no cuenta con una política de seguridad de la información para la relación con proveedores. Esta debe aplicar para todos los proveedores que tenga algún tipo de acceso, ya sea parcial o completo a algún activo de información de la empresa.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Inexistente	¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, “robo de empleados”, etc.)	La empresa no cuenta con una política para el tratamiento de la seguridad dentro de los acuerdos en la relación con proveedores.
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Inexistente	Más allá de A.15.1.1 y A.15.1.2 ¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos? ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? ¿Se puede rastrear el origen del producto o servicio?	No existe un análisis de riesgos relacionado con la seguridad de la información dentro de la cadena de suministros.
A.15.2	**Gestión de la prestación de servicios de proveedores**				
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Administrado	¿Existe una monitorización de servicios y quien responsable de esta actividad? ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia? ¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas? ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría? ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?	Existe un proceso definido para la evaluación constante de los proveedores, se debe fortalecer la parte de seguridad de la información dentro de este.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	Inexistente	¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados? ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización? ¿Se actualizan los acuerdos relacionados con los cambios?	No existe control de cambios en los servicios de los proveedores relacionados con la seguridad de la información.
A.16	**Gestión de incidentes de seguridad de la información**				
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.					
A16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Inexistente	¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes? ¿Qué cubre? • El plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?	No se tienen definidos los roles y responsabilidades para atender incidentes de seguridad. Tampoco existen procedimientos para tal fin.
A16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Inicial	¿Cómo se informan los eventos de seguridad de la información? ¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución. ¿Qué pasa con esos informes?	No se realiza reporte de los incidentes de seguridad ni se documentan de manera adecuada.

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Inicial	Más allá de A.16.1.2 ¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual? ¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?	Los empleados son consientes de que deben reportar los eventos de seguridad, pero este no es un procedimiento formal dentro de la organización.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Inexistente	¿Qué tipos de eventos se espera que informen los empleados? ¿A quién informan? ¿Cómo se evalúan estos eventos para decidir si califican como incidentes? ¿Hay una escala de clasificación? ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves? ¿En qué se basa?	No existe evaluación ni clasificación de los eventos de seguridad.
A16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Inexistente	¿Cómo se recolecta, almacena y evalúa la evidencia? ¿Hay una matriz de escalación para usar según sea necesario? ¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes? ¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?	No se evidencia una política o procedimiento para dar respuesta ante incidentes de seguridad de la información.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Inexistente	¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes? ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias? Además, ¿Se está utilizado para formación y concienciación? ¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro? ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	Al no tener reportes o visibilidad de los incidentes de seguridad de la información, no existe un mecanismo que permita el aprendizaje sobre estos.
A16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Inexistente	¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área? ¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas) ¿Quién decide emprender un análisis forense, y en qué criterio se base? ¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?	No existe un procedimiento definido para la recolección de evidencia de incidentes de seguridad de la información.
A.17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**				
A.17.1	**Continuidad de la seguridad de la información**				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Repetible	¿Cómo se determinan los requisitos de continuidad del negocio? ¿Existe un plan de continuidad de negocio? ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos? ¿Se identifica el impacto potencial de los incidentes? ¿Se evalúan los planes de continuidad del negocio? ¿Se llevan a cabo ensayos de continuidad?	Existe un plan no formalizado para dar continuidad del negocio en caso de una crisis o desastre.
A17.1.2	Implementar la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Repetible	¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción? ¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares? ¿La planificación de la continuidad es consistente e identifica las prioridades de restauración? ¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades? ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?	El plan no formalizado no se encuentra implementado en su totalidad, carece de madurez.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Inexistente	¿Existe un método de pruebas del plan de continuidad? ¿Con qué frecuencia se llevan a cabo dichas pruebas? ¿Hay evidencia de las pruebas reales y sus resultados? ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?	No se realizan pruebas de continuidad de negocio.
A.17.2	**Redundancias**				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.					
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Inexistente	¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	No existe un sistema de redundancia para garantizar la disponibilidad de los servicios de procesamiento de información.
A.18	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**				
A.18.1	**Cumplimiento de requisitos legales y contractuales**				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Repetible	¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, PDP, etc. ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables? ¿Hay una persona encargada de mantener, usar y controlar el registro? ¿Cómo se logra y se garantiza el cumplimiento? ¿Existen controles adecuados para cumplir con los requisitos?	La empresa tiene identificado dentro de su SGI los requisitos de legislación y contractuales que le aplican. Se deben integrar los aplicables a la seguridad de la información.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Inexistente	¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?	No existe una política o procedimiento para garantizar los derechos de propiedad intelectual.
A18.1.3	Protección de los registros de la organización	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Inexistente	¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos. ¿Se almacenan las firmas digitales de forma segura? ¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado? ¿Se verifica periódicamente la integridad de los registros? ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?	No existe una política para clasificar, categorizar ni definir los medios de almacenamiento permitidos.
A18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Definido	¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal? ¿Hay un responsable de privacidad en la organización? ¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización? ¿Cuáles son los controles de acceso a información de carácter personal? ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?	Existe un procedimiento informal para el tratamiento de la privacidad de los datos personales.
A18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Inexistente	¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico? ¿Estas actividades cumplen con los requisitos legales y reglamentarios?	No existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico.
A.18.2	**Revisiones de la seguridad de la información**				
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales					

Anexo A. Estado inicial y Aplicabilidad de controles de Seguridad de la Información en GERS S.A.S.					
Sección	**Objetivo de control**	**Control**	**Estado**	**Preguntas**	**Observaciones**
A18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	? Desconocido	¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información? ¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos? ¿Están los objetivos y el alcance de auditoria autorizados por la gerencia? ¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información? ¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?	Como no existe un SGSI, aún no se tiene programada realizar alguna auditoria dentro del programa de auditorias del SGI.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	? Desconocido	¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente? ¿Se hace una verificación periódica?	Como no existe un SGSI, aún no se evalúa el desempeño del sistema.
A18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	? Desconocido	¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares? ¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables? ¿Cómo informa, analiza y utilizan los resultados de dichas pruebas? ¿La prioridad de tratamiento se basa en un análisis de riesgos? ¿Hay evidencias de medidas tomadas para abordar los problemas identificados?	Como no existe un SGSI, aún no se realiza revisión del cumplimiento técnico de este sistema.
			114	Número de Controles	

ANEXO B

No. De Amenazas y Vulnerabilidades	Activos de información	Nombre del activo de información	VALORACIÓN DEL MEDIO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad nota	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual	Plan de Tratamiento							Requerimiento	Obligación	Requerimiento	Análisis de Riesgo	Exclusión
														Indique el control a aplicar a partir de la norma ISO 27001:2013												
														Transefir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control					
1	SERVICIOS	[S] Sistema de gestión financiera (Siesa ERP Nube AWS)	17	[E19] Fugas de información	Transporte inseguro de los datos desde la oficina del cliente hasta la nube del proveedor	I	3	51	C	1		51	C				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.6 Seguridad de equipos y activos fuera de las instalaciones --Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Se debe implementar una política de seguridad y un procedimiento que defina el control sobre los activos de información que se han trasladado a la nube, su tratamiento, la seguridad en todas sus capas (transportem acceso, etc.) e involucrar al proveedor de nube para establecer el modelo de responsabilidad compartida de seguridad de la información			X		
2	SOFTWARE	[SW] Servidor para sistema de gestión del recurso humano (Nomina web) - OS Windows Server 2016 - AWS	18	[A15] Modificación deliberada de la información	Alteración indebida de la información	I	2	36	C	1		36	C				X	DOMINIO_A15	OBJETIVO_A15_1	A15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores --Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Se debe implementar una política de seguridad donde se definan los requisitos de seguridad que debe ofrecer el proveedor de nube en cuanto a la gestión del sistema operativo del servidor donde se aloja este servicio			X		
3	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - OS Arch Linux 4.1.15	18	[E21] Errores de mantenimiento / actualización de programas (software)	Versión de sistema operativo obsoleto y sin soporte que es vulnerable	I	3	54	C	1		54	C				X	DOMINIO_A12	OBJETIVO_A12_5	A12.5.1 Instalación de software en sistemas operativos --Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Se debe implementar un procedimiento para programar ventanas de actualización sobre el sistema operativo y de chequeo previo a la instalación de una actualización del SO o de un software, verificando su configuración y si es seguro.				X	
4	SOFTWARE	[SW] Servidor de aplicaciones web (GDP - Wiki - Transferencias)- Apps LAMP - PHP 5.6.16	19	[E20] Vulnerabilidades de los programas (software)	Versiones 5.x de PHP obsoletas, con multiples vulnerabilidades y sin soporte	I	3	57	C	1		57	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Se debe implementar y socializar una política de seguridad y un procedimiento de control que defina el tratamiento sobre las vulnerabilidades tecnicas sobre software obsoleto				X	
5	HARDWARE	[HW] Servidor de aplicaciones web (GDP - Wiki - Transferencias) - HP Proliant DL180 G6	12	[IS] Avería de origen físico o lógico	Daño de algun componente interno del equipo por una mala manipulacion o golpe. Daño humano por mantenimiento preventivo o correctivo mal ejecutado.	I	3	36	C	1		36	C				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe contar con indicadores que midan el cumplimiento y la eficacia del programa de mantenimiento y su periodicidad				X	
6	SOFTWARE	[SW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - OS Windows Server 2016	19	[E2] Errores del administrador	Un servidor con fallencias a nivel de hardening puede permitir la explotación de una serie de vulnerabilidades que ponen en peligro la seguridad de la información	I	3	57	C	1		57	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.2 Restricciones sobre la instalación de software --Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Se debe establecer una política de seguridad y un procedimiento de control que describa las reglas los permisos, los responsables de realizar la instalación y configuración sobre los diferentes sistemas operativos de la organización, los cuales deben garantizar un nivel adecuado de hardening				X	
7	HARDWARE	[HW] Servidor de aplicaciones técnicas (DigSilent, ELCAD, Primtech NEPLAN V5) - HP Proliant DL360 Gen9	12	[I6] Corte del suministro eléctrico	Falta de respaldo eléctrico y/o de contingencia electrica	I	3	36	C	2	Existe una UPS para alimentar los activos criticos mientras se hace la transferencia a las plantas manuales o se recupera el fluido electrico	18	I				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Se debe contar con un sistema de suministro de energia alterno con capacidad de soportar los servidores, mientras se hace la transferencia manual a las plantas o se restablece elservicio electrico				X	
8	SOFTWARE	[SW] Servidor proxy - OS Arch Linux 4.14.70	15	[A11] Acceso no autorizado	No revocación de permisos o eliminación de usuarios privilegiados	I	4	60	C	1		60	C				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Implementar un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
9	HARDWARE	[HW] Servidor proxy - Dell Vostro 200	12	[E24] Caída del sistema por agotamiento de recursos	Ataques de denegación de servicios	I	3	36	C	1		36	C				X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.2 Seguridad de los servicios de red --Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se deben implementar y documentar mecanismos de seguridad robustos que protejan el activo de ataques de denegación de servicios los cuales puede agotar sus recursos físicos y desencadenen indisponibilidad				X	
10	SOFTWARE	[SW] Servidor SIP - Freepbx 10.13.66	15	[A11] Acceso no autorizado	Atacantes pueden infiltrar la planta para generar llamadas internacionales que generan sobrecostos en la facturación	I	3	45	C	1		45	C				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.3 Sistema de gestión de contraseñas --Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Se debe establecer y socializar una política de seguridad para contraseñas seguras, que incluya periodicidad de cambio, robustez, complejidad, entre otros parametros				X	
11	HARDWARE	[HW] Servidor SIP - Clon hibrido	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Incumplimiento al plan de mantenimiento que genera deterioro físico de las partes internas del servidor	I	3	36	C	2	Existe un cronograma de mantenimiento para los servidores	18	I				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe contar con indicadores que midan el cumplimiento y la eficacia del programa de mantenimiento y su periodicidad				X	
12	SOFTWARE	[SW] Software antivirus (Forticlient v7)	19	[A6] Abuso de privilegios de acceso	El usuario accede a configuraciones del antivirus para crear excepciones, desactivarlo o desinstalarlo sin autorización ni precaución.	I	5	95	C	1		95	C				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Se deben establecer y documentar los accesos privilegiados basados en roles sobre cualquier activo de información para evitar la manipulación no autorizada de los sistemas				X	
13	SOFTWARE	[SW] Suite de ofimática (MS Office 2013)	19	[E20] Vulnerabilidades de los programas (software)	Omisión en caracteristica seguidad en aplicaciones	I	5	95	C	1		95	C				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Se deben documentar todas las acciones de protección que realiza el Firewall perimetral con el fin de conocer si puede existitir alguna brecha de seguridad que permita la explotación de este tipo de vulnerabilidades. Adicionalmente, se debe tener un informe peridico de las amenazas contenidas por este dispositivo de seguridad.				X	
14	SOFTWARE	[SW] Suite de ofimática (MS Office 2016)	19	[E20] Vulnerabilidades de los programas (software)	Omisión en caracteristica seguidad en aplicaciones	I	4	76	C	1		76	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Se debe implementar y socializar una política de seguridad y un procedimiento de control que defina el tratamiento sobre las vulnerabilidades tecnicas sobre software obsoleto				X	
15	SOFTWARE	[SW] software de estudios (Digsilent 2016-2022)	19	[E2] Errores del administrador	Error del area tecnica al borrar o manipular archivos propios del sistema como servicios, controladores o DLL´s causando inestabilidad o daños en el SO.	I	2	38	C	1		38	C				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe implementar y socializar una política de seguridad y un procedimiento que defina las mejores practicas para realizar el mantenimiento de los servidores, para disminuir fallas al momento de realizar soporte, reparación física o logica.				X	
16	SOFTWARE	[SW] Software de estudios (Neplan v10.9.1.1)	19	[E1] Errores de los usuarios	Consultas generadas por los usuarios que generan consumo excesivo de recursos	I	3	57	C	1		57	C				X	DOMINIO_A8	OBJETIVO_A8_1	A8.1.3 Uso aceptable de los activos --Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Se debe implementar y socializar una política de seguridad y un procedimiento donde se especifique el uso adecuado de los activos y la formación o el entrenamiento para aperar de manera eficiente las herramientas de trabajo				X	
17	SOFTWARE	[SW] Software de llamadas telefonicas (Softphone Microsip 3.20.7)	12	[E20] Vulnerabilidades de los programas (software)	Extracción de información confidencial como hashes de contraseña simplemente haciendo una llamada maliciosa.	I	3	36	C	1		36	C				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Se debe fortalecer el software que se utiliza para las llamadas telefonicas, tanto servidor como cliente. Asimismo, se debe fortalecer la protección de dispositivos finales por medio de un software antivirus con caracteristicas avanzadas de protección y respuesta.				X	
18	SOFTWARE	[SW] Ordenador portatil (OS Windows 10 Single Language)	19	[E21] Errores de mantenimiento / actualización de programas (software)	Se pueden conectar unidades externas y modificar codigo UEFI en la memoria	I	4	76	C	1		76	C				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las vulnerabilidades técnicas --Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Se debe implementar y socializar una política de seguridad y un procedimiento para la gestión de vulnerabilidades tecnicas de los sistemas de información. En el procedimiento se debe detallar periodicidad de aplicación de parches de seguridad, sitios de descarga, fuentes de información, riesgos que se pueden derivar despues de la actualización, entre otros				X	
19	HARDWARE	[HW] Switch * 2 (V1910-48G JE009A)	15	[IS] Avería de origen físico o lógico	Degradición del firmware por falta de mantenimiento que genera indisponibilidad de acceso a la red de los dispositivos conectados	I	3	45	C	1		45	C				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se deben incluir estos dispositivos dentro del programa de mantenimiento preventivo y correctivo y documentar su ejecución con indicadores de cumplimiento				X	
20	HARDWARE	[HW] Switch * 2 (HP 1950-48G JG963A)	12	[I7] Condiciones inadecuadas de temperatura o humedad	Sistema de refrigeracion deficiente o inexistente en el area dispuesta para centralizar equipos servidores y de networking.	I	4	48	C	3	Existe un cuarto de comunicaciones con refrigeración permanente y un cronograma de mantenimiento de aire acondicionado	16	I				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.1 Ubicación y protección de los equipos --Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Se debe llevar registro del cumplimiento del plan de mantenimiento de los equipos de aire acondicionado en esta área				X	
21	SOFTWARE	[SW] Firewall (Fortinet 100E Version de Firmware 6.4.6)	19	[E20] Vulnerabilidades de los programas (software)	Firmware obsoleto y vulnerable que permite la escalada de privilegios	I	3	57	C	2	Existe un contrato con el tercero que administra el Firewall, donde detalla la existencia de un plan de actualizacion recurrente	29	C	X							Se transfiere el riesgo				X	
22	HARDWARE	[HW] Access Point (UNIFI Ubiquiti)	12	[I6] Corte del suministro eléctrico	Susceptibilidad a las variaciones de voltaje	I	4	48	C	2	Existe una UPS para alimentar los activos criticos mientras se hace la transferencia a las plantas manuales o se recupera el fluido electrico	24	C				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Se debe contar con un sistema de control que regule la energía que se le suministra al dispositivo para evitar fallos por sobrecargas. Integrar los AP a la conexión electrica con la UPS				X	
23	SERVICIOS	[S] Correo electronico (G-Suite)	19	[A5] Suplantación de la identidad del usuario	Por medio del correo electronico se envian campañas de Phishing que conducen a los usuarios hacia enlaces o paginas que aperentan ser legitimas, pero tienen intenciones maliciosas, como el robo de credenciales, por ejemplo.	I	1	19	I	1		19	I				X	DOMINIO_A13	OBJETIVO_A13_2	A13.2.3 Mensajería Electronica --Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Se deben implementar mecanismos de seguridad de tipo DLP, para prevenir la exfiltración de datos por medio del correo electronico. Herramientas que filtren el spam y sensibilización constante a los usuarios finales				X	
24	SERVICIOS	[S] Backup (Google Drive)	15	[A11] Acceso no autorizado	Por falta de politicas o restricciones a nivel de directorios almacenados en esta herramienta, se pueden presentar accesos no autorizados a información confidencial, lo cual impacta precisa y directamente a la confidencialidad de la información	I	3	45	C	1		45	C				X	DOMINIO_A9	OBJETIVO_A9_1	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Se debe establecer y socializar una política de seguridad y un procedimiento que defina el control del acceso a los diferentes directorios de la herramienta de backups. Esto debe ser en función de roles de usuarios, áreas de trabajo, entre otros. Separando así el acceso a datos sensibles de la organización			X		
25	AUXILIAR	[AUX] Sistema de alimentación ininterrumpida (UPS)	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Daño de sistema de respando UPS por falta de mantenimiento o seguimiento al estado de baterias.	M	3	36	C	3	Existe un procedimiento que indica el plan de mantenimiento que se realiza sobre las UPS	12	A		X						Se acepta el riesgo					
26	HARDWARE	[HW] Telefono IP (GrandStream)	15	[A25] Robo	Telefonos en escritorios expuestos y sin mecanismos de seguridad fisica	M	1	15	A	3	Existe vigilancia física privada con apoyo en camaras de seguridad al interior y exterior de la empresa	5	B		X						Se acepta el riesgo					
27	COMUNICACIONES	[COM] Internet (Proveedor C&W fibra optica de 80MB)	12	[I8] Fallo de servicios de comunicaciones	Al contar con un solo ISP, si este falla genera indisponibilidad de servicios esenciales	M	2	24	C	2	El ISP garantiza un 99.96% de disponilidad del servicio. Existe un procedimiento de conexión alterno, si llegase a fallar el ISP principal	12	A		X						Se acepta el riesgo					
28	DATOS	[D] Hojas de vida de colaboradores	15	[A11] Acceso no autorizado	Control inadecuado al acceso físico	M	2	30	C	4	Existe una política de restricción de acceso solo a personal autorizado al centro de documentación. Área monitoreda por camaras de seguridad	8	B		X						Se acepta el riesgo					
29	HARDWARE	[HW] Equipos de computo (En alquiler PcCom, MilenioPC y Zinko)	12	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Incumplimiento en el mantenimiento del sistema de información	A	1	12	A	3	En conjunto con los proveedores, se tiene definido un plan de mantenimiento de equipos de computo	4	D	X							Se transfiere el riesgo					
30	SERVICIOS	[S] Paginas web corporativas (Servidor Digital Ocean)	12	[A24] Denegación de servicio	Puertos inseguros abiertos	M	2	24	C	3	El proveedor que administra los sitios web se encarga de la seguridad de estos	8	B	X							Se transfiere el riesgo					
31	SERVICIOS	[COM] Red de Area Local (LAN)	19	[A5] Suplantación de la identidad del usuario	Un atacante puede hacerse pasar por un usuario autorizado y escalar privilegios	I	2	38	C	1		38	C				X	DOMINIO_A13	OBJETIVO_A13_1	A13.1.3 Separación en las redes --Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Se debe establecer la separación de las redes por medio de la implementación de VLANs y DMZs, con el fin de controlar el acceso a los recursos solo a personal permitido de acuerdo con su rol dentro de la organización			X		