FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA ELÉCTRICA

Autoras:

Martínez Mendieta Andrea Marcela

Olmedo Salazar Silvia Alejandra

Año:

2022

FACULTAD DE POSGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA ELÉCTRICA

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Máster en Gestión de la Seguridad de la Información.

Autoras:
Martínez Mendieta Andrea Marcela
Olmedo Salazar Silvia Alejandra

Año:
2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Andrea Marcela Martínez Mendieta

2000062493

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Silvia Alejandra Olmedo Salazar

1720076460

AGRADECIMIENTOS

Mi padre me dijo que la vida es como un tren y que tú decides si te subes o si solo la ves pasar, muchas veces tenemos tantos sueños y metas, para alcanzarlas la mejor manera es compartirlas junto a personas que te ayudan a creer que son posibles; a ellos les agradezco por siempre creer en mí.

Andrea

AGRADECIMIENTOS

Agradezco a la UDLA por brindarme la oportunidad de realizar mis estudios en tan prestigiosa Universidad, a mi familia que durante el recorrido de mi formación profesional me enseñaron que la constancia y esfuerzo siempre dará frutos.

Silvia

DEDICATORIA

A mis padres por su amor y apoyo incondicional.

Andrea

DEDICATORIA

A mi madre, con mucho cariño y amor le dedico mi esfuerzo y dedicación plasmado en este trabajo de titulación.

Silvia

RESUMEN

El presente trabajo de titulación corresponde al desarrollo del programa del sistema de gestión de seguridad de la información para una Empresa Eléctrica Provincial, cuyas actividades se centran en: suministrar, generar, transmitir, distribuir y comercializar energía eléctrica para sus consumidores dentro del área de concesión otorgada.

El programa de gestión de seguridad de la información permite implementar un modelo de gobierno y gestión, el cual se encuentra alineado con los objetivos y estrategia que tiene la Empresa.

El desarrollo inicia con una evaluación de diagnóstico de la situación actual de la Empresa Eléctrica. Se desarrolló con base en dos marcos de referencia internacionales: NIST y COBIT 2019, que fueron utilizados como herramientas de apoyo con el fin de identificar, evaluar, controlar y mejorar la gestión de la seguridad de la información. En la fase de diagnóstico se identificaron varias necesidades que la Empresa requiere solventar.

A continuación, se realizó un análisis sobre la clasificación de entidades y activos de información para determinar su criticidad con respecto a la Integridad, Confidencialidad, Disponibilidad y Privacidad.

Partiendo de la clasificación de activos, se seleccionaron dos activos que manejan información crítica para la operación del negocio, sobre ellos se efectuó el análisis y la evaluación de riesgos para identificar controles existentes, controles propuestos, a través de ello definir planes de acción que permitan mitigarlos con el apoyo de la elaboración de políticas que formen las bases para la gestión del sistema de seguridad de la información.

ABSTRACT

This thesis corresponds to the development of an information security management program (ISMP) for a Provincial Electricity Company, whose activities are focused on supplying, generating, transmitting, distributing, and selling electricity to its consumers within the concession area granted.

The information security management program allows the implementation of a governance and management model, which is aligned with the objectives and strategy of the Company.

The design begins with a diagnostic assessment of the current situation of the Electricity Company and was developed with the support of two international reference frameworks: NIST and COBIT 2019, which were used as tools to identify, evaluate, control, and improve the information security management. From the diagnostic phase, several needs were identified that the Company needs to solve.

Subsequently, an analysis was conducted on the classification of information entities and assets to determine their criticality related to Integrity, Confidentiality, Availability and Privacy.

Based on the asset classification, two assets were selected that handle critical information for the business operation. Risk and assessment analysis were conducted to identify existing controls, proposed controls and finally define action plans to mitigate them, supported by the development of policies, thus laying the foundations for the management of the information security system.

INDICE DEL CONTENIDO

Índice de Figuras

Índice de Tablas

Índice de Anexos

1. Introducción

"El sector de energía y servicios públicos está constantemente en la mira de adversarios, debido a grupos de actores patrocinados por estados que constantemente se enfocan en organizaciones en este sector para proyectar fuerza geopolítica, realizar reconocimientos, efectuar ataques destructivos o impulsar sus propios objetivos estratégicos. Las redes eléctricas son responsables de proporcionar electricidad a los productores y consumidores, lo que permite que continúe la vida tal como la conocemos. El sector de servicios públicos proporciona los servicios esenciales para que la sociedad prospere, tales como electricidad, agua, alcantarillado, recolección de basura y gas natural. Las amenazas cibernéticas y los adversarios continúan adaptándose y evolucionando, demostrando un cambio en su enfoque para centrarse más en las cadenas de suministro (*supply chain*) y también en comprometer sistemas de control industrial (ICS).

Con la integración continua de Internet de las cosas (*Internet of Things* - IoT) y una creciente conectividad de dispositivos, los actores de amenazas continúan enfocando sus esfuerzos contra las redes de tecnología de la información (TI) para usarlas como punto pivote al intentar lograr el compromiso de las redes de tecnología operativa (OT)". (Deloitte, 2020, pág. 1).

2. Desarrollo del proyecto de titulación.

2.1. Caso de negocio

El modelo de empresa eléctrica provincial seleccionada se encarga de la comercialización, distribución, transmisión y generación del servicio de energía eléctrica, siendo la única empresa con permiso de concesión para la comercialización de energía de toda la provincia; cuenta con una oficina matriz y 2 agencias. La empresa eléctrica posee un único accionista.

Actualmente cuenta con un total de 14004 clientes distribuidos en 6 sectores en un área de concesión de 6.638 km^2.

La información relevante para el estudio del caso de negocio de la empresa de estudio puede ser revisado en el Anexo 1: Caso de negocio.

De acuerdo con los objetivos estratégicos de la Empresa y siendo un servicio básico y crítico la electricidad, la falta de seguridad de la información podría impactar notablemente a los siguientes parámetros:

- Multas y sanciones de los Organismos de Control.
- Interrupción de operaciones parciales o totales.
- Pérdidas financieras.

Como parte del análisis realizado se elaboró un modulador de apetito de riesgo empresarial con sus niveles de impacto que pueden ser revisados en el Anexo 2: Modulador del Apetito y Anexo 3: Niveles de Impacto.

2.2. Objetivo General del Proyecto

- Desarrollar el programa del sistema de Seguridad de la Información para una Empresa Eléctrica.

2.3. Objetivos Específicos

- Minimizar, asumir y mitigar las amenazas que puedan encontrarse en los distintos sistemas de información, por medio de planes y estrategias que se encuentran definidas y documentadas, los cuales podrán ser actualizados.
- Proporcionar a la Empresa Eléctrica documentación importante y vital que permita: medir, informar y revelar los factores sensibles. Siendo herramientas que contribuirán a la Continuidad del Negocio.

2.4. Metodología

Para el proyecto del desarrollo del programa del sistema de gestión de seguridad de la información para una Empresa Eléctrica Provincial se utilizaron los marcos de referencia NIST y COBIT 2019 que permitirán fortalecer los procedimientos para la gestión, uso y tratamiento de la información.

2.4.1. NIST

NIST (National Institute of Standards & technology) es un marco de referencia que se adapta a las necesidades de distintos tipos de empresas cuyo objetivo es servir de guía para incorporar estándares de seguridad en las organizaciones.

Figura 1. Marco de Referencia NIST, adaptada de Mahn, Marron, Quinn, y Top, 2021, p. 1.

Los elementos del núcleo del marco de referencia trabajan con las siguientes 5 funciones:

Identificar: Entender a la organización para gestionar los riesgos de ciberseguridad de los sistemas, personas, activos, datos y capacidades.

Dentro de esta función el objetivo principal es entender el contexto del negocio, conocer los recursos que este posee para apoyar sus funciones críticas, priorizando los esfuerzos siendo consistente con la gestión de riesgos y las necesidades de este. Para ello se analizan los activos, el negocio, el gobierno y los riesgos.

Proteger: Desarrollar e implementar salvaguardas para servicios críticos. En esta función las actividades son orientadas a limitar y contener el impacto de eventos potenciales de ciberseguridad, las categorías que se incluyen son la gestión de accesos y activos de la información, capacitación y educación a los funcionarios y usuarios, proteger dispositivos y datos sensibles, realizar respaldos periódicos, entre otros.

Detectar: Desarrollar e implementar las acciones adecuadas para identificar eventos de ciberseguridad. Esta función gestiona las actividades relacionadas a los procesos de detección de eventos, para ello prueba y actualiza procesos de

detección, capacitación del personal, comprensión de flujos de datos, comunicación oportuna de eventos y se encarga de determinar sus efectos.

Responder: Desarrollar e implementar las actividades necesarias a efectuarse ante un evento de ciberseguridad detectado. Estas actividades están enmarcadas en desarrollar, probar y actualizar planes de respuesta, así como coordinar a las partes interesadas tanto internas como externas.

Recuperar: Desarrollar e implementar las acciones oportunas para sostener la resiliencia y restablecer los servicios o capacitades afectados ante un evento de seguridad, para ello se desarrollan, prueban y actualizan planes de contingencia y comunicación a las partes interesadas, además de la gestión de las relaciones públicas y la reputación de la empresa. (Mahn, Marron, Quinn, & Top, 2021, págs. 1-3).

2.4.2. COBIT

COBIT es un marco de referencia para Gobierno y Gestión de los sistemas de información y tecnología, no solo para el área de IT, sino que abarca a toda la organización.

COBIT se fundamenta en 3 principios que todo marco de gobierno debe tener: basarse en un modelo conceptual, ser abierto y flexible; finalmente alinearse con las normativas.

Este marco de referencia posee objetivos de gobierno y gestión, los cuales están relacionados con procesos y se encuentran divididos en 5 dominios.

Los objetivos de gobierno se encuentran contenidos en el dominio Evaluar, Dirigir y Monitorizar (EDM), en el cual los consejos administrativos y la dirección ejecutiva se encargan de evaluar la estrategia, dirigir a la alta gerencia con respecto a la estrategia y monitorea su resultado.

Los objetivos de gestión guardan relación con los procesos de gestión. Son dirigidos por la alta y media Gerencia y se encuentran incluidos en los 4 dominios restantes, ver *Figura 2. Modelo Core de COBIT, tomada de ISACA, 2018, p. 21.*

- Alinear, Planificar y Organizar (**APO**) forman parte de este dominio la estrategia, la organización general y las actividades de apoyo para IT.

- Construir, Adquirir e Implementar (**BAI**), en este dominio se define, adquiere e implementan soluciones de Tecnologías de la Información (TI), así como la integración en los procesos de negocio.
- Entregar, dar Servicio y Soporte (**DSS**) este dominio se encarga de las labores operativas, así como del soporte para los servicios de TI incluyendo su seguridad.
- Monitorizar, Evaluar y Valorar (**MEA**), integran a este dominio el monitoreo y la correlación entre los objetivos de desempeño, los de control interno con los requerimientos externos. (ISACA, 2018, págs. 20-21)

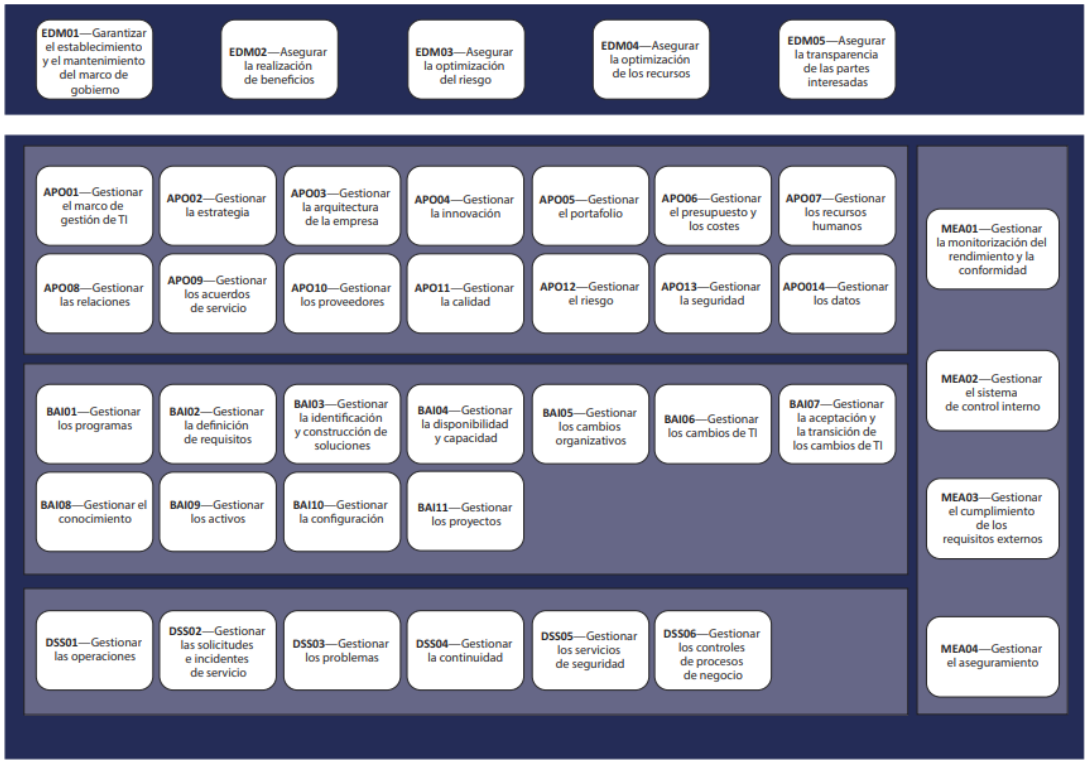


Figura 2. Modelo Core de COBIT, tomada de ISACA, 2018, p. 21.

Para el proyecto desarrollado se utilizó la última versión del marco de referencia es decir COBIT 2019. (ISACA, 2018).

2.4.3. MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que permite estudiar los riesgos que soporta un sistema de información y su entorno asociado.

La metodología permite realizar un análisis de riesgos a través, de la evaluación del impacto que una violación de seguridad tiene sobre la organización. Ver Figura 3.

La metodología cuenta con objetivos directos e indirectos.

"Objetivos directos:

1. Hacer que los responsables de las organizaciones entiendan que los riesgos existen y es necesario que estos sean gestionados.
2. Brindar un método que permita analizar los riesgos a los que se encuentran expuestos debido a tecnologías de la información y comunicación.
3. Busca descubrir y planificar oportunamente el tratamiento de los riesgos (mantenerlos bajo control).

Objetivos indirectos:

1. Entrenar a la organización para auditorias, evaluaciones, certificaciones o acreditaciones." (Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 8).

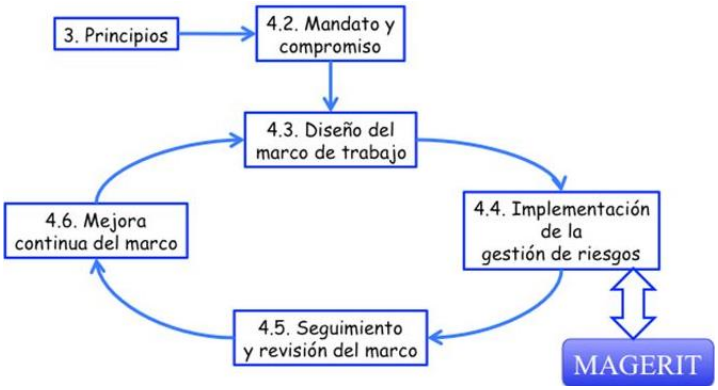


Figura 3. ISO 31000 - Marco de trabajo para la gestión de riesgos. Tomado de Ministerio de Hacienda y Administraciones Públicas, 2012, p. 7.

2.4.4. ISO 27001

El objetivo principal de la norma es ayudar a las organizaciones a proteger los activos de la organización, garantizando su confidencialidad, integridad y disponibilidad, y reducir riesgos e incidencias.

Otro de los principales objetivos de la norma, es el enfoque del sistema de gestión de manera alineada con la estrategia de negocio de la organización.
Por otro lado, ISO 27001 busca la integración de esta norma con los demás sistemas de gestión para que sean accesibles a todo tipo de organizaciones. Esto se consigue con una estructura de alto nivel, común a todas las normas de gestión.
Gracias a esta estructura de alto nivel, es fácil la integración con otros sistemas de gestión como IDP 9001, ISO 14001, ISO 45001, ISO 22000, IDP 26000, ISO 20000-1, ISO 31000; lo cual facilita y simplifica enormemente su gestión e integración real en la organización y aplicación efectiva.
La norma ha sido diseñada para “proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información”.

La norma “puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización a fin de cumplir con sus propios requisitos de seguridad de la información”.

La norma también incluye “requisitos para la evaluación y el tratamiento de los riesgos en la seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza”. (Global Trust Association, 2022, pág. 14), ver Figura 4.

Figura 4. Estructura de la Norma ISO 27001. Tomada de Global Trust Association, 2022, p. 16.

2.4.4.1. ISO 27002

"La norma 27002 de la Organización Internacional para la Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) es un reglamento reconocido a escala internacional que establece buenas prácticas para la seguridad de la información. Cumplir esta norma reconocida en todo el mundo ayuda a las organizaciones a cumplir sus obligaciones contractuales con sus clientes y socios comerciales. Las licencias de operación exigen cada vez más a los proveedores de servicios (desde centros de datos en la nube hasta bufetes de abogados) que demuestren que administran de forma responsable la información confidencial de una cartera de clientes globales. Los auditores de todo el mundo también toman la seguridad de la norma ISO 27002 como referencia para evaluar los controles o verificar el cumplimiento de distintos reglamentos y normas." (Cyberark, 2022)

2.5. Alcance - Fases

Las fases que fueron aplicadas para el proyecto de desarrollo del programa del sistema de gestión de seguridad de la información para una Empresa Eléctrica Provincial son las siguientes:

2.5.1. Fase 1: Diagnóstico/Evaluación del SGSI

La primera fase permite dar a conocer el diagnóstico del estado actual de la Empresa Eléctrica, mediante la aplicación del marco de referencia NIST y COBIT 2019.

2.5.1.1. Metodología

La metodología de la evaluación del estado actual del SGSI para la Empresa Eléctrica, de acuerdo con el marco de referencia NIST agrupa cada una de las funciones: Identificar, Proteger, Detectar, Responder y Recuperar; relacionando la categoría y subcategoría con los controles de COBIT 2019 para determinar el diagnóstico inicial de la Empresa Eléctrica, su situación y el plan de acción para mejorar su respuesta en temas de seguridad de la información.

Tabla 1. Informe de diagnóstico del SGSI

Función	SITUACION ACTUAL	TOTAL %
1. IDENTIFICAR (ID)	La empresa eléctrica no ha implementado un programa de seguridad de la información, por ello no se encuentran definidos los principios, políticas, requisitos. No se ha realizado una evaluación de riesgos interna ni externa(terceros), sin embargo, se cuenta con el apoyo de la presidencia ejecutiva para desarrollar el programa de seguridad, la organización ha implementado controles básicos de seguridad de la información los cuales incluyen charlas sobre phishing, uso de correo electrónico y credenciales de acceso.	**23,33%**
2. PROTEGER (PR)	La empresa no cuenta con un programa de seguridad de la información, sin embargo, si existe la gestión de accesos y realiza inducción de seguridad sobre uso de correo electrónico. No se encuentra definido un plan de capacitación de seguridad de la información ya que no existe un área de seguridad de la información o un responsable	**28,84%**

3. DETECTAR (DE)	La empresa no cuenta con un programa de seguridad de la información, tampoco se ha clasificado la información ni su tratamiento ni protección. No se ha realizado un análisis de riesgos por ello no hay una evaluación de impactos, sin embargo, la empresa ha implementado medidas como redundancia para mitigar el impacto a la disponibilidad.	**28,08%**
4. RESPONDER (RS)	La empresa eléctrica, no ha diseñado ni implementado un programa de seguridad de la información, por ello no ha realizado una evaluación de riesgos, tampoco se han definido prácticas y controles formales para la mitigación de riesgos, sin embargo, en función de sus recursos ha implementado la gestión de accesos y privilegios para sus colaboradores.	**21,25%**
5. RECUPERAR (RC)	La empresa no cuenta con un programa de seguridad de la información, no se ha implementado aún un plan de continuidad de negocios, tampoco se ha hecho una evaluación de riesgos interna y externa.	**35,00%**
	TOTAL	**27,30%**

A continuación, se muestra la Figura 5. Promedio de valoración % de cumplimiento, la cual muestra el porcentaje de cumplimiento con respecto a las funciones de la metodología, con base en el análisis realizado se confirma el bajo porcentaje de cumplimiento de las funciones, verificando que las que poseen los valores más preocupantes son identificar (23,33%) y responder (21,24%).

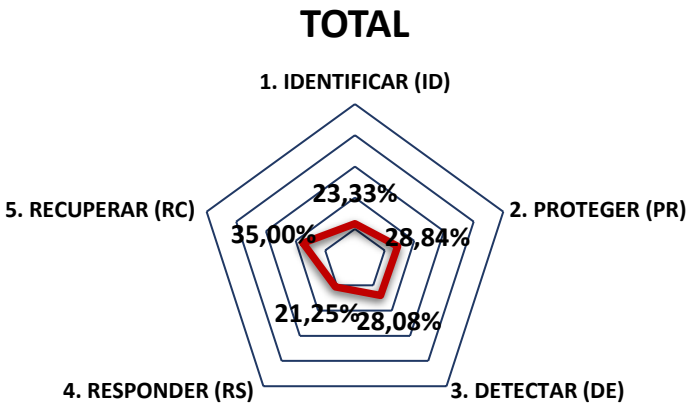


Figura 5. Promedio de valoración % cumplimiento.

2.5.1.2. Resultados (Análisis)

Con el apoyo de los marcos de referencia NIST y COBIT 2019 para la evaluación del estado actual de la organización, se obtuvieron los siguientes resultados:

En la Tabla 1. Informe de diagnóstico del SGSI, se evidencia que la Empresa Eléctrica no ha incluido a la seguridad de la información dentro de su perfil de Riesgo Empresarial, ya que presenta porcentajes bajos de cumplimiento en cada función evaluada, confirmando así la falta de un programa de seguridad de la información, un plan de continuidad del negocio y un análisis de riesgos de seguridad, por lo que es necesario diseñar e implementar el programa del Gestión de Seguridad de la Información para la Empresa Eléctrica.

Para mayor detalle sobre el análisis realizado por favor referirse al Anexo 4: Metodología.

2.5.2. Fase 2: Clasificación de la Información

La fase de Clasificación de la Información permite realizar un inventario de los activos de información de la Empresa Eléctrica de acuerdo con su giro de negocio.

2.5.2.1. Metodología

Para realizar la clasificación de las entidades de información de la Empresa Eléctrica y calificarlas en términos de Disponibilidad, Integridad, Confidencialidad y Cumplimiento. Para ello es necesario investigar el tipo de información y su definición por cada una de las entidades con el objetivo de determinar su grado de criticidad.

Tabla 2: Clasificación de Entidades

Entidad	Descripción	Tipo de información	Definición tipo de información
Cliente Persona Natural	Cliente Persona Natural que adquiere el servicio de la empresa.	Personal	Nombres, Apellidos, Cédula de identidad o pasaporte, certificado de votación del solicitante cuando corresponda
		Contacto	Información de contacto (número de teléfono celular, convencional y correo electrónico)
		Ubicación	Copia de escritura o documento legal que acredite la propiedad, posesión legítima, arrendamiento o anticresis sobre el inmueble donde se instalará el servicio; o, acreditar

			disponer, croquis de la casa, ubicación exacta de la casa (georreferencial)
		Financiera	Número de cuenta, Banco
		Servicio	Número de contrato, código del suministro, número del medidor
		Autorización ocasional	Autorización o permiso otorgado por: el Gobierno Autónomo Descentralizado del cantón o la autoridad competente, en caso de que el servicio se otorgue en espacios públicos.
Empleado	Un empleado que da servicios a la empresa.	Personal	Cédula de identidad o pasaporte, cargas familiares, sexo, edad, orientación sexual, raza/etnia, declaración juramentada de bienes, declaración del impuesto a la renta, Copia de la licencia de Conducir
		Contacto	Información de contacto (nombres completos, teléfonos, correo electrónico)
		Ubicación	Dirección, referencia domiciliaria
		Financiera	cuenta bancaria, banco
		Salud	Discapacidad, historial médico, enfermedad catastrófica, resultados de laboratorio, enfermedades, historial de atención, contacto de emergencia, seguro de vida, afiliación al IESS
		Protocolo de Seguridad	Se define normas, reglas y parámetros para que el empleado pueda ingresar y operar adecuadamente para brindar el servicio eléctrico
		Ingresos	Sueldos, préstamos, beneficios, bonos, comisiones, horas extras
		Educación	Nivel de estudios (básico, pregrado, posgrado), capacitaciones, certificación en riesgos eléctricos, experiencia laboral
		Contrato	Tipo de contrato firmado (fijo, ocasional, servicios profesionales)
		Legal	Demandas, juicio de alimentos

Información detallada se encuentra disponible en el Anexo 5: Clasificación de Entidades.

2.5.2.2. Resultados (Análisis)

De acuerdo con la evaluación a la clasificación de las Entidades identificadas que posee la Empresa Eléctrica, se determinaron las siguientes entidades críticas: cliente persona natural, empleado y proveedor ya que dichas entidades cuentan con datos personales como: datos sensibles, datos de salud, crediticios, entre otros.

En cumplimiento con la Ley Orgánica de Protección de Datos Personales del Ecuador que rige desde mayo 2021 y cuyo régimen sancionatorio comienza desde mayo 2023, es necesario que esta información sea protegida de manera

especial y se asegure su tratamiento por parte del responsable de la información que en este caso es la Empresa Eléctrica.

2.5.3. Fase 3: Inventario de activos de información

La fase de inventario de activos de información permite identificar los activos que gestionan información crítica de la Empresa Eléctrica.

2.5.3.1. Metodología

De acuerdo con la fase de inventario de activos de información, la cual guarda estrecha relación con la fase 2 de clasificación de la información en la que se determina su criticidad. En la fase 3 se investigan los activos de información vitales para la organización, para ello es necesario identificar y listar los activos, sus propietarios, el formato en el que se encuentre almacenada la información, el proceso al que pertenece, área responsable de dicho proceso. En este análisis se consideran como pieza fundamental las entidades de información que fue analizada en la fase anterior; ya que es necesario conocer en que activos se encuentran almacenadas. Factor que será determinante para la calificación del activo en función de la disponibilidad, integridad, confidencialidad y cumplimiento, determinando así su calificación de criticidad.

Tabla 3: Inventario de Activos de Información

Tipo del Activo	Nombre de Activo	Proceso	Criticidad del activo de información
BDD	Base de datos Comercial (SAP CIS/CRM)	Proceso Comercialización	Catastrófico
SRVR	Servidor-Compras	Todos los procesos	Catastrófico
BDD	Base de Datos ERP	Procesos de Talento Humano	
SRVR	Carpetas compartidas	Información de Departamentos	

BDD	Base de Datos COD (ADMS)	Procesos Operativos	Catastrófico
BDD	Base de Datos GIS	Procesos Sistema de información Geográfica	Moderado
SRVR	Servidor Correo Electrónico	Procesos Administrativos	Moderado
SRVR	Servidor central telefonía IP	Procesos Administrativos	Moderado

2.5.3.2. Resultados (Análisis)

Conforme al inventario de activos de información evaluado, se priorizaron dos activos críticos en función de la clasificación de la información, la cual se encuentra almacenada en bases de datos como: información personal, información de contacto, ubicación georreferenciada, ordenes de trabajo, plan de maniobras, documento de seguridad. Su evaluación fue realizada en términos de disponibilidad, integridad, confidencialidad y cumplimiento de acuerdo con el giro del negocio de la Empresa.

Cada una de las bases de datos almacenan información crítica con relación directa a la continuidad del negocio. Las bases de datos seleccionadas son:

- Base de Datos Comercial (SAP [1]CIS/[2]CRM), en esta base se almacenan todos los datos referentes a los clientes, así como la información de cobro por los servicios que brinda la empresa.
- Base de Datos Distribución (ADMS[3]), permite la gestión operativa de toda la Empresa, ya que se encarga del control y monitoreo de la generación, subtransmisión, distribución y atención a emergencias eléctricas a nivel provincial.

[1] Customer Information System(CIS),(MEER,2013)
[2] Customer Relationship Management (CRM), (MEER,2013)
[3] Advanced Distribution Management System (ADMS)

Tabla 4. Priorización de activos de información

Código	Activo de Información	Criticidad del activo de información
EE-01	BASE DE DATOS COMERCIAL	Crítico
EE-05	BASE DATOS SCADA-ADMS	Crítico

Los objetivos principales de las bases de datos seleccionadas son los siguientes:

- Mejorar la Eficiencia Operativa.
- Mejorar la Confiabilidad y Calidad del Servicio Eléctrico.
- Impulsar la eficiencia energética en armonía con el ambiente.

Para más detalle revisar el Anexo 6: Inventario de Activos Fijos.

2.5.4. Fase 4: Análisis de amenazas y vulnerabilidades de activos de información

En la fase de análisis de amenazas y vulnerabilidades para los activos de información, se consideró el uso de algunas herramientas de apoyo como: la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y el Marco de Referencia ISO 27005:2018, para la gestión de riesgos de Seguridad de la información.

Tomando en consideración las particularidades de cada activo de información crítico seleccionado, ya que no se encuentran ubicados en el mismo servidor ni en el mismo centro de datos; las herramientas mencionadas fueron aplicadas para identificar las amenazas y vulnerabilidades de acuerdo con las condiciones de riesgo reales de cada activo crítico.

2.5.4.1. Metodología

A fin de facilitar el proceso de análisis y la valoración de riesgos se definen los siguientes conceptos:

“**Riesgo**: Efecto de la incertidumbre sobre la consecución de objetivos. Es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una

cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus.

Amenaza: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.” (Global Trust Association, 2022, pág. 31 y 34)

“**Impacto**: es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Riesgo inherente: Es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo” (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020, pág. 4)

Riesgo Objetivo (Target): Es el riesgo al que se quiere llegar.

Se elaboraron escenarios por cada activo de información, donde se listan las amenazas de acuerdo con la metodología MAGERIT y se determina la vulnerabilidad con respecto a la ISO 27005. A continuación, se identificó su impacto de seguridad de acuerdo con la integridad, disponibilidad y confidencialidad, así como el impacto organizacional. Ver la Tabla 5: Muestra Escenario ADMS y Tabla 6: Muestra Escenario CRM.

Tabla 5: Muestra Escenario ADMS

ESCENARIO BASE DATOS ADMS					
Cod.	**Amenazas**	**Cod.**	**Vulnerabilidades**	**Impacto de Seguridad**	**Impacto Organizacional**
AME I.5	**[I.5] Avería de origen físico o lógico**	VUL I.5.1	Falta de un control de cambios de configuración eficiente	Disponibilidad	Interrupción de operaciones parciales y/o totales
		VUL I.5.2	Susceptibilidad a las variaciones de tensión		
		VUL I.5.3	Susceptibilidad a las variaciones de temperatura		
		VUL I.5.4	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento		
		VUL I.5.5	Susceptibilidad a la humedad, polvo, suciedad		

Tabla 6: Muestra Escenario CRM

ESCENARIO BASE DE DATOS COMERCIAL					
Cod.	**Amenazas**	**Cod.**	**Vulnerabilidades**	**Impacto de Seguridad**	**Impacto Organizacional**
AME I.5	**[I.5] Avería de origen físico o lógico**	VUL I.5.1	Falta de un control de cambios de configuración eficiente	Disponibilidad	-Interrupción de operaciones parciales y/o totales -Pérdidas financieras
		VUL I.5.2	Susceptibilidad a las variaciones de tensión		
		VUL I.5.3	Susceptibilidad a las variaciones de temperatura		
		VUL I.5.4	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento		
		VUL I.5.5	Susceptibilidad a la humedad, polvo, suciedad		
AME I.6	**[I.6 Corte de suministro**	VUL I.6.1	Red eléctrica inestable	Disponibilidad	Interrupción de operaciones parciales y/o totales -Pérdidas financieras -Multas y sanciones de los Organismos de Control

Una vez definidas las amenazas y vulnerabilidades de los dos activos críticos de información, se elabora la matriz de riesgo en función de la probabilidad e impacto del riesgo.

Por cada vulnerabilidad se determina el riesgo, se califica su impacto y probabilidad en caso de que este llegara a materializarse.

A continuación, se calculan los riesgos: inherente, residual y objetivo (Target). Los riesgos residual y objetivo dependerán de los controles existentes y controles a implementar, los cuales son analizados a detalle en la fase 6.

Para calcular el riesgo inherente se multiplica la probabilidad de ocurrencia por su impacto al negocio (Tabla 7), obteniendo como resultado la severidad del riesgo tal como se presenta en la tabla 8.

Tabla 7. Riesgo Inherente.

Riesgo Inherente = Probabilidad x Impacto

Tabla 8. Severidad del riesgo

		Impacto				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Probabilidad	**Raro**	Bajo	Bajo	Moderado	Moderado	Moderado
	Poco probable	Bajo	Moderado	Moderado	Alto	Alto
	Posible	Moderado	Moderado	Alto	Alto	Crítico
	Probable	Moderado	Alto	Alto	Crítico	Crítico
	Casi certeza	Moderado	Alto	Crítico	Crítico	Crítico

Posteriormente se definen los controles que ejecuta la Empresa de forma intrínseca, a fin de evaluar la mitigación del impacto, probabilidad y la calificación del control con el objetivo de obtener el riesgo residual.

Para calificar el control existente se asignaron valores a la mitigación del impacto y a la probabilidad con el fin de determinar el riesgo residual, para obtener su calificación es necesario disminuir del riesgo inherente la mitigación que ejercen los controles existentes como se puede observar en la Tabla 9: Riesgo Residual.

Tabla 9: Riesgo Residual.

Riesgo Residual = Riesgo Inherente-Mitigación de controles existentes

Una vez evaluados los controles existentes, se identifica oportunidades de mejora y se proponen controles por implementar, los cuales permitirán mitigar el riesgo residual y proyectarse a alcanzar el riesgo objetivo (target).

Con el objetivo de implementar mejoras, a los controles propuestos se les asignaron valores para calificar la mitigación de impacto y probabilidad esperada con el fin de determinar el riesgo objetivo (target), tal como se puede observar en la *Tabla 10. Riesgo Target*.

Tabla 10. Riesgo Target

Riesgo Target = Riesgo Residual-Mitigación de controles por implementar

2.5.4.2. Resultados (Análisis).

Del análisis de escenarios para los activos críticos se concluye, que los activos analizados poseen amenazas que los afectan individualmente, sin embargo, algunas de ellas son compartidas por ambas bases de datos como: averías de origen físico o lógico, errores del administrador y del usuario, vulnerabilidades propias de los programas, suplantación de identidad y abuso de privilegios.

De igual manera comparten vulnerabilidades y por ende riesgos asociados, estos factores impactan sustancialmente a la seguridad y organización. El análisis detallado de estos escenarios se puede encontrar en el Anexo 7: Escenario Base de Datos ADMS y Anexo 8: Escenario Base de Datos Comercial.
Con base en las amenazas y vulnerabilidades detectadas para los activos en estudio, se definieron los riesgos a los que estos se encuentran expuestos; los cuales pueden ser revisados en el Anexo 9: Matriz de Riesgos

A través del análisis de la matriz de riesgos, se calificaron los riesgos inherentes, residuales y objetivo (target) para los dos activos de información catalogados como críticos de la Empresa Eléctrica. Como resultado se determinó que existen amenazas con alto riesgo de materializarse y podrían traer consecuencias que comprometerían la disponibilidad, integridad y confidencialidad, provocando en algunos casos daños irreversibles hasta posibles pérdidas económicas que pueden ser minimizadas gracias a los controles a implementar, que han sido propuestos durante el desarrollo del programa de gestión de seguridad de la información.

Para las vulnerabilidades se realizaron diferentes análisis de riesgo: riesgo inherente, riesgo residual (luego de controles existentes) y objetivo (evaluado asumiendo controles por implementar).
Como se puede observar en la Tabla 11, se extrajo una muestra de los riesgos inherentes con impacto catastrófico y probabilidad probable dando como

resultado una severidad crítica. Estos riesgos son los que tendrían un impacto importante en la seguridad y en la organización. Entre los riesgos que fueron calificados con severidad crítica para la organización tenemos lo que corresponden a las siguientes amenazas:

- Avería de origen físico o lógico.
- Falla de servicios de comunicaciones.
- Errores de los usuarios y administradores.
- Errores de monitorización.
- Fugas de información.
- Suplantación de la identidad del usuario.
- Abuso de privilegio de acceso.
- Corte de suministro eléctrico.
- Manipulación de la configuración.
- Modificación deliberada de la información.

Tabla 11. Muestra Matriz de Riesgo Inherente

No.	Activo	Riesgo	Factor de Riesgo	Impacto de Seguridad	Impacto Organizacional	ANÁLISIS DE RIESGO INHERENTE		
						Impacto	Probabilidad	Severidad
1	Base de Datos ADMS (EE-05)	Falta de un control de cambios de configuración eficiente	Personas Tecnología de la Información	Disponibilidad	Interrupción de operaciones parciales y/o totales	Mayor	Posible	Alto
		Instalaciones eléctricas deficientes	Personas Tecnología de la Información			Catastrófico	Probable	Crítico

	Sistema de climatización defectuoso o sin mantenimiento / falta de limpieza y mantenimiento	Personas Tecnología de la Información		Catastrófico	Probable	Crítico
	Fallas en el mantenimiento de medios de almacenamiento	Personas		Catastrófico	Probable	Crítico
	Sistema de climatización defectuoso o sin mantenimiento/falta de limpieza y mantenimiento	Personas Tecnología de la Información		Catastrófico	Probable	Crítico

Luego de calcular el riesgo inherente, se procede a revisar los controles existentes para calificar su fortaleza de mitigación de probabilidad e impacto (el análisis y calificación de controles será revisada a detalle en la siguiente fase), los cuales pueden ser revisados en el Anexo 9: Matriz de Riesgos.

Como se puede observar en la Tabla 12. Muestra Matriz de Riesgo Residual, se indican los riesgos residuales con severidad crítica, esto se debe a que la mitigación de impacto y probabilidad que ejercen los controles son débiles para las siguientes amenazas:

- Avería de origen físico o lógico.
- Falla de servicios de comunicaciones.
- Errores de los usuarios y administradores.
- Fugas de información.
- Suplantación de la identidad del usuario.
- Abuso de privilegio de acceso.
- Corte de suministro eléctrico.
- Modificación deliberada de la información.

Dada la criticidad del riesgo residual es urgente diseñar controles nuevos y mejorar los existentes, seguidos de la creación de planes de acción con el objetivo de mitigar la criticidad del riesgo a los que se encuentran expuestos los activos vitales para la operación de la Empresa Eléctrica.

Tabla 12. Muestra Matriz de Riesgo Residual

No.	Activo	Riesgo	Factor de Riesgo	EVALUACIÓN DE CONTROLES ACTUALES				RIESGO RESIDUAL
				Control Actual	Mitigación del Impacto	Mitigación de la Calificación del Control		Severidad
1	Base de Datos ADMS (EE-05)	Falta de un control de cambios de configuración eficiente	Personas Tecnología de la Información	Aprobación de cambios	Fuerte	Fuerte	Fuerte	Bajo
		Instalaciones eléctricas deficientes	Personas Tecnología de la Información	Informe de mantenimiento de instalaciones eléctricas	Neutro	Débil	Débil	Crítico
		Sistema de climatización defectuoso o sin mantenimiento/ falta de limpieza y mantenimiento	Personas Tecnología de la Información	Informe de mantenimiento de aires de precisión	Neutro	Débil	Débil	Crítico
		Fallas en el mantenimiento de medios de almacenamiento	Personas	Ordenes de trabajo de mantenimiento de medios de almacenamiento.	Neutro	Fuerte	Neutro	Alto

	Sistema de climatización defectuoso o sin mantenimiento/ falta de limpieza y mantenimiento	Personas Tecnología de la Información	Informe de mantenimiento de sistemas de control de humedad.	Neutro	Débil	Débil	Crítico

Con el objetivo de minimizar el riesgo residual se han diseñado y mejorado los controles existentes a fin de llegar a un riesgo objetivo o target. Estos controles buscan reducir el impacto y la probabilidad, por ello fueron calificados bajo los mismos criterios de los controles existentes para simular su acción. Para más detalle revisar el Anexo 12: controles por implementar.

Como se puede observar en la Tabla 13: Muestra de Riesgo Target, los controles por implementar se esperan ayuden a reducir la severidad del riesgo residual de un valor crítico a un valor alto e incluso en algunos casos a un valor moderado. Particularidad que se ve reflejada en el riesgo objetivo (target) simulado, lo que permite demostrar que los controles en conjunto con los planes de acción ayudan a mitigar los riesgos a lo que se encuentran expuestos actualmente los activos críticos de la Empresa Eléctrica.

Tabla 13: Muestra de Riesgo Target

No. Activo	Riesgo	PLAN DE MEJORAMIENTO CONTROLES POR IMPLEMENTAR					RIESGO OBJETIVO
		Cod.	Control por Implementar	Descripción Control por Implementar	Mitigación del Impacto	Mitigación de la Probabilidad	Severidad
1 Base de Datos ADMS (EE-05)	Falta de un control de cambios de configuración eficiente	CON-I I.5.1	- Repositorio de control de cambios - Informes de control de cambios	- Revisar el repositorio de los controles de cambio y la automatización de los flujos de aprobación -Revisiones aleatorias de solicitudes de cambio. - Verificación de las autorizaciones y aprobaciones de control de cambios. - Validar la adecuada segregación de funciones en el control de cambios.	Fuerte	Fuerte	Bajo
	Instalaciones eléctricas deficientes	CON-I I.5.2	Informe de mantenimiento de instalaciones eléctricas	- Revisar el procedimiento de mantenimiento preventivo periódico a las instalaciones eléctricas. - Revisar el cronograma de mantenimiento a las instalaciones eléctricas. - Revisar el cumplimiento de plan anual de mantenimiento (Revisión de ordenes de trabajo).	Neutro	Fuerte	Alto

	Sistema de climatización defectuoso o sin mantenimiento/ falta de limpieza y mantenimiento	CON-I I.5.3	Informe de mantenimiento de aires de precisión	- Revisar el procedimiento de mantenimiento preventivo periódico de sistemas de climatización. - Revisar el cronograma de mantenimiento preventivo. - Revisar de cumplimiento de plan anual de mantenimiento preventivo (Revisión de Informes).	Neutro	Fuerte	Alto
	Sistema de climatización defectuoso o sin mantenimiento/ falta de limpieza y mantenimiento	CON-I I.5.5	Informe de mantenimiento de sistemas de control de humedad.	Evaluar el estado del sistema de control de humedad.	Neutro	Fuerte	Alto

De la evaluación realizada se evidencia la necesidad de que los controles se evalúen periódicamente con el objetivo de realizar una mejora continua. Es primordial definir nuevos controles en conjunto con planes de acción, ya que a pesar de que los controles por implementar reducen el riesgo (target), este sigue siendo alto para las siguientes amenazas:

- Avería de origen físico o lógico.
- Errores de los usuarios.
- Fugas de información
- Suplantación de la identidad del usuario
- Abuso de privilegio de acceso.
- Modificación deliberada de la información.

2.5.5. Fase 5: Programa del SGSI

Como parte del programa del SGSI se han definido políticas de alto nivel para que la Empresa Eléctrica defina y mantenga los controles necesarios, a fin de gestionar la seguridad de la información.

2.5.5.1. Metodología

Para definir las políticas de alto nivel, la Empresa Eléctrica requiere expresar su compromiso con la seguridad de la información a través de una política general de la Seguridad de la Información y las diferentes políticas de apoyo de acuerdo con el estándar ISO 27002:2013 con el fin de garantizar que la seguridad de la información se implemente y opere.

Las políticas que se definieron y elaboraron para la Empresa Eléctrica son:

- Política de Seguridad de la Información
- Política de transferencia de información
- Política de protección contra software malicioso
- Política de control de acceso
- Política de clasificación y manejo de información.
- Política de seguridad física y ambiental
- Política de gestión de activos
- Política de gestión de contraseñas
- Política de escritorio y pantallas limpios
- Política de dispositivos móviles y teletrabajo.
- Política de gestión de vulnerabilidades.
- Política de restricciones a las instalaciones y uso de software.
- Política de copia de seguridad.
- Política de controles criptográficos.
- Política de seguridad de las comunicaciones.
- Política de privacidad y protección de la información personal identificable.
- Política de relación con terceros.

Cada documento plasma los lineamientos y controles de seguridad que debe tener la Empresa Eléctrica, se definen objetivos, alcance, definiciones, responsables y políticas; para mayor detalle sobre las políticas por implementar revisar el Anexo 10: Políticas del Sistema de Gestión de Seguridad de la Información.

De acuerdo con el organigrama actual de la Empresa se definieron responsables, los cuales serán nombrados en las políticas, así como al responsable de Seguridad de la Información, como se muestra en la siguiente Figura 6 Organigrama de Tecnologías de la información y comunicación (TICS).

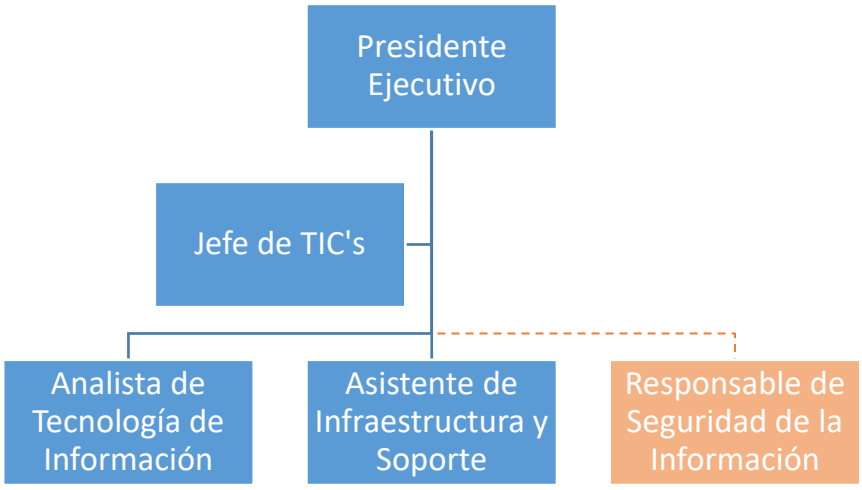


Figura 6 Organigrama de TICS.

2.5.5.2. Resultados (Análisis)

Con la elaboración de las Políticas se definieron las directrices de apoyo para la gestión de la seguridad de la información en la Empresa Eléctrica desde el área de Tecnología de la Información y la Comunicación (TIC's).

Se determinó la necesidad de contar con un responsable de Seguridad de Información, quien estará a cargo de la gestión de la seguridad de la información en la organización y entre sus funciones tendrá las siguientes: coordinar la elaboración, revisión e implementación de las políticas.

Posteriormente las políticas deberán ser aprobadas y difundidas en la intranet para todo el personal de la Empresa independientemente de su contrato.

Las políticas podrán ser revisadas y actualizadas de acuerdo con las necesidades y requerimientos que nazcan durante la implementación del programa.

2.5.6. Fase 6: Implementación y mejora de componentes SGSI/medidas de seguridad

En la fase de implementación y mejora de componentes de SGSI/medidas de seguridad, se valora cada uno de los controles existentes con respecto a los riesgos identificados en los dos activos críticos seleccionados a fin de definir los controles que se deben implementar.

2.5.6.1. Metodología

Para desarrollar está fase se evalúan los controles existentes asociados a cada riesgo y se describe la periodicidad con la que se aplicará el control. A continuación, se califica si los controles en el procesamiento de la información resultan efectivos. El método de calificación diseñado fue el siguiente:

Primero se clasifica la tipología del control en tres categorías: preventivo, detectivo y correctivo.

Preventivo: Este tipo de control permite descubrir problemas antes de que ocurran y hacer ajustes para impedir errores, omisiones o actos malicioso.

Detectivo: Se identifica si se utilizan controles para detectar y reportar si ha ocurrido un error, omisión o acto malicioso.

Correctivo: Este control permite remediar problemas que fueron descubiertos con el apoyo de los controles detectivos, identificar la causa raíz del problema y corregir los errores determinados de un problema.

Segundo a cada control existente se califica el tipo de automatización, manual, automático y mixto.

Manual: Corresponde al control que debe ser ejecutado por una persona para que este se desarrolle.

Automático: Este control se realiza por sí solo sin necesidad de la intervención directa de una persona y es ejecutado a través de un procesamiento definido dentro de un sistema.

Mixto: Es aquel control en el que los dos controles anteriores son ejecutados a la vez.

Finalmente, a cada control existente se califica el CAVR de acuerdo con las siguientes consideraciones:

Integridad: Garantiza que todas las transacciones que se ingresen sean registradas y aceptadas para su procesamiento, las cuales se actualizan en un archivo permitiendo que los datos sigan siendo correctos y vigentes.

Valor Correcto: Se garantiza que los datos identificados como claves son registrados e ingresados de forma correcta, así como sus cambios.

Validez: Se garantiza que las transacciones son autorizadas y no son ficticias, y que sus cambios sean validados.

Acceso Restringido: Garantizan que exista confidencialidad y protección de los datos.

Una vez que se realiza una valoración de acuerdo con cada tipo de control indicado previamente, se determina si el control aplicado permite reducir el impacto, probabilidad o ambos.

Como se muestra en la Tabla 14: Muestra de Controles existentes, se califica el control para determinar su impacto y probabilidad, para mayor detalle sobre los controles existentes en la organización referirse al Anexo 11: Controles Existentes.

Tabla 14: Muestra de Controles existentes

CONTROLES EXISTENTES

		Riesgo/Control						Tipo			Automatización			CAVR							
No.	Activo	Riesgo	Cod.	Control	Descripción del control	Periodicidad	Preventivo	Detectivo	Correctivo	Calificación Control	Manual (1)	Automático (2)	Mixto (3)	Calificación Control	Completitud(1)	Exactitud(1)	Validez(1)	Acceso Restringido(3)	Calificación Control	Resultado	Calificación del Control (Cualitativa)	Calificación del Control Impacto	Calificación del Control Probabilidad
1	Base de Datos ADMS (EE-05)	Deficiente control de cambios de configuración	CON-E I.5.1	Aprobación de cambios	Cuando se requiere realizar cambios de configuraciones, se pasa a una instancia de aprobación para que se revise al cambio y se apruebe en la misma aplicación, se sincroniza y se distribuye en el ambiente de producción, sin embargo, no existe documentación y los permisos para la aprobación no se encuentran segregados.	Periódico	3	2	1	6			3	3	1	1	1	3	6	Ambos	Fuerte	Fuerte	Fuerte
2		Instalaciones eléctricas deficientes	CON-E I.5.2	Informe de mantenimiento de instalaciones eléctricas	Actualmente los centros de datos para protección de equipos cuentan con las siguientes características: - Aire de precisión para control de temperatura y humedad. - Sistemas de alimentación ininterrumpida (UPS) con una capacidad de 10KVA con una duración 1 hora. -El Centro de datos más grande cuenta con un generador de servicios auxiliares. -Mantenimientos correctivos	Semestral			1	1	1			1	1		1		2	Impacto	Débil	Neutro	Débil
3		Sistema de climatización defectuoso o sin mantenimiento/falta de limpieza y mantenimiento	CON-E I.5.3	Informe de mantenimiento de aires de precisión	Los centros de datos para protección de equipos cuentan con Aire de precisión para control de temperatura y humedad. -Mantenimiento preventivo anual.	Anual			1	1	1			1	1		1		2	Impacto	Débil	Neutro	Débil

1	CONTROLES EXISTENTES				
	Riesgo/Control				
No.	**Activo**	**Riesgo**	**Cod.**	**Control**	**Descripción del control**
1	**Base de Datos ADMS (EE-05)**	Deficiente control de cambios de configuración	CON-E I.5.1	Aprobación de cambios	Cuando se requiere realizar cambios de configuraciones, se pasa a una instancia de aprobación para que se revise al cambio y se apruebe en la misma aplicación, se sincroniza y se distribuye en el ambiente de producción, sin embargo, no existe documentación y los permisos para la aprobación no se encuentran segregados.
2		Instalaciones eléctricas deficientes	CON-E I.5.2	Informe de mantenimiento de instalaciones eléctricas	Actualmente los centros de datos para protección de equipos cuentan con las siguientes características: - Aire de precisión para control de temperatura y humedad. - Sistemas de alimentación ininterrumpida (UPS) con una capacidad de 10KVA con una duración 1 hora. -El Centro de datos más grande cuenta con un generador de servicios auxiliares. -Mantenimientos correctivos
3		Sistema de climatización defectuoso o sin mantenimiento/falta de limpieza y mantenimiento	CON-E I.5.3	Informe de mantenimiento de aires de ...	Los centros de datos para protección de equipos cuentan con Aire de precisión para control de temperatura y humedad. -Mantenimiento preventivo anual.

2	CONTROLES EXISTENTES													
	Tipo			Automatización				CAVR						
Periodicidad	**Preventivo**	**Detectivo**	**Correctivo**	**Calificación Control**	**Manual (1)**	**Automático (2)**	**Mixto (3)**	**Calificación Control**	**Completitud (1)**	**Exactitud (1)**	**Validez (1)**	**Acceso Restringido (3)**	**Calificación Control**	**Reduce**
Periódico	3	2	1	6			3	3	1	1	1	3	6	Ambos
Semestral			1	1	1			1	1		1		2	Impacto
Anual			1	1	1			1	1		1		2	Impacto

3	CONTROLES EXISTENTES		
Calificación del Control (Cualitativa)	**Calificación del Control Impacto**	**Calificación del Control Probabilidad**	
Fuerte	Fuerte	Fuerte	
Débil	Neutro	Débil	
Débil	Neutro	Débil	

A continuación, se definen los controles por implementar asociados a cada riesgo, se describe la periodicidad con la que se ejecuta el control, se procede a realizar la calificación de los controles para evaluar su efectividad.

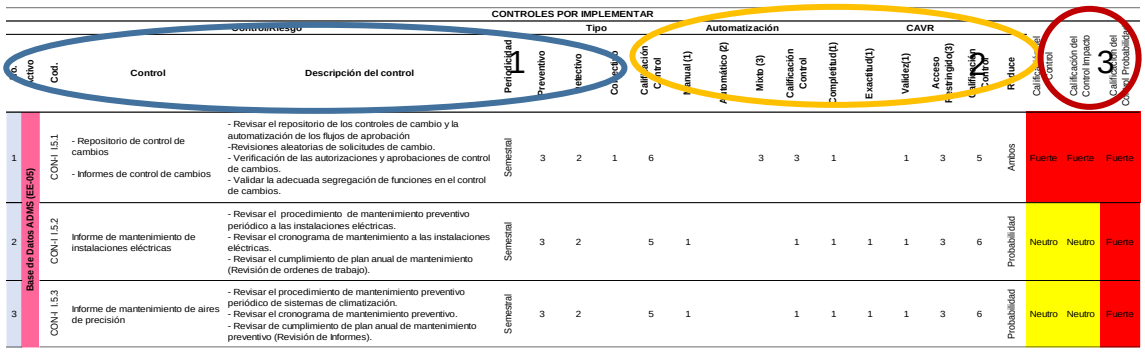
Primero se clasifica la tipología del control en tres categorías: preventivo, detectivo y correctivo.

Segundo cada control existente se califica por tipo de automatización, manual, automático y mixto.

Finalmente, a cada control existe se califica el CAVR.

Una vez que se realiza una valoración de acuerdo con cada tipo de control indicado previamente, se determina si el control aplicado permite reducir el impacto, probabilidad o ambos, tal como se muestra en la Tabla 15: Muestra de Controles por Implementar.

Tabla 15: Muestra de Controles por Implementar



CONTROLES POR IMPLEMENTAR

No.	Activo	Cod.	Control	Descripción del control	Periodicidad	Tipo: Preventivo	Tipo: Detectivo	Tipo: Correctivo	Tipo: Calificación Control	Automatización: Manual (1)	Automatización: Automático (2)	Automatización: Mixto (3)	Automatización: Calificación Control	CAVR: Completitud(1)	CAVR: Exactitud(1)	CAVR: Validez(1)	CAVR: Acceso Restringido(3)	CAVR: Calificación Control	Reduce	Calificación Control	Calificación del Control Impacto	Calificación del Control Probabilidad
1	Base de Datos ADMS (EE-05)	CON-I I.5.1	- Repositorio de control de cambios - Informes de control de cambios	- Revisar el repositorio de los controles de cambio y la automatización de los flujos de aprobación -Revisiones aleatorias de solicitudes de cambio. - Verificación de las autorizaciones y aprobaciones de control de cambios. - Validar la adecuada segregación de funciones en el control de cambios.	Semestral	3	2	1	6			3	3	1		1	3	5	Ambos	Fuerte	Fuerte	Fuerte
2		CON-I I.5.2	Informe de mantenimiento de instalaciones eléctricas	- Revisar el procedimiento de mantenimiento preventivo periódico a las instalaciones eléctricas. - Revisar el cronograma de mantenimiento a las instalaciones eléctricas. - Revisar el cumplimiento de plan anual de mantenimiento (Revisión de ordenes de trabajo).	Semestral	3	2		5	1			1	1	1	1	3	6	Probabilidad	Neutro	Neutro	Fuerte
3		CON-I I.5.3	Informe de mantenimiento de aires de precisión	- Revisar el procedimiento de mantenimiento preventivo periódico de sistemas de climatización. - Revisar el cronograma de mantenimiento preventivo. - Revisar de cumplimiento de plan anual de mantenimiento preventivo (Revisión de Informes).	Semestral	3	2		5	1			1	1	1	1	3	6	Probabilidad	Neutro	Neutro	Fuerte

1

CONTROLES POR IMPLEMENTAR

Control/Riesgo

No.	Activo	Cod.	Control	Descripción del control
1	**Base de Datos ADMS (EE-05)**	CON-I I.5.1	- Repositorio de control de cambios - Informes de control de cambios	- Revisar el repositorio de los controles de cambio y la automatización de los flujos de aprobación -Revisiones aleatorias de solicitudes de cambio. - Verificación de las autorizaciones y aprobaciones de control de cambios. - Validar la adecuada segregación de funciones en el control de cambios.
2		CON-I I.5.2	Informe de mantenimiento de instalaciones eléctricas	- Revisar el procedimiento de mantenimiento preventivo periódico a las instalaciones eléctricas. - Revisar el cronograma de mantenimiento a las instalaciones eléctricas. - Revisar el cumplimiento de plan anual de mantenimiento (Revisión de ordenes de trabajo).
		CON-I I.5.3	Informe de mantenimiento de aires de precisión	- Revisar el procedimiento de mantenimiento preventivo periódico de sistemas de climatización. - Revisar el cronograma de mantenimiento preventivo. - Revisar de cumplimiento de plan anual de mantenimiento preventivo (Revisión de Informes).

2 CONTROLES POR IMPLEMENTAR														
	Tipo				Automatización				CAVR					
Periodicidad	Preventivo	Detectivo	Correctivo	Calificación Control	Manual (1)	Automático (2)	Mixto (3)	Calificación Control	Completitud (1)	Exactitud (1)	Validez (1)	Acceso Restringido (3)	Calificación Control	Reduce
Semestral	3	2	1	6			3	3	1		1	3	5	Ambos
Semestral	3	2		5	1			1	1	1	1	3	6	Probabilidad
Semestral	3	2		5	1			1	1	1	1	3	6	Probabilidad

3 CONTROLES POR IMPLEMENTAR		
Calificación del Control	Calificación del Control Impacto	Calificación del Control Probabilidad
Fuerte	Fuerte	Fuerte
Neutro	Neutro	Fuerte
Neutro	Neutro	Fuerte

2.5.6.2. Resultados (Análisis)

Como resultado de esta fase se evalúan los controles existentes, así como los controles por implementar, confirmando la necesidad de realizar mejoras en varios campos dentro de la Empresa Eléctrica, por ejemplo: en Auditoría Interna (no existe un Auditor Interno y no se desarrollan auditorías de sistemas), Seguridad de la Información (no se tiene definido un responsable de la Seguridad de la Información); tampoco se han elaborado, aprobado y difundido políticas de seguridad de la información.

A través de la evaluación se detecta que no existe una clasificación de la información ni sus procedimientos de tratamiento asociados. Además, se confirma lo detectado en la fase de diagnóstico inicial, la inexistencia de una evaluación de riesgos asociada a seguridad de la información.

Existe una notable oportunidad de mejora en la ejecución del mantenimiento preventivo que permita incrementar la confiabilidad en la infraestructura física de los centros de datos a nivel provincial, así como en los enlaces de comunicaciones, la estabilidad del sistema eléctrico y de climatización, entre otros.

Tabla 16: Muestra de controles existentes débiles

CONTROLES EXISTENTES

	Activo	Riesgo/Control: Riesgo	Cod.	Control	1 Descripción del control	Tipo / Automatización / CAYR		
21	Base de Datos ADMS (EE-05)	Inexistencia de definición y clasificación de información.	CON-E E.19.1	No existe el control		Nada	Débil	Débil	Débil
22		Inexistencia de procedimientos para tratamiento de información clasificada.	CON-E E.19.2	No existe el control		Nada	Débil	Débil	Débil
32		Deficiencia de procedimiento de seguimiento de las instalaciones de procesamiento de información	CON-E A.6.4	No existe el control	No existe un control sobre el seguimiento de las instalación de procesamiento de información	0 Nada	Débil	Débil	Débil
33		Deficiente planificación para auditorías periódicas.	CON-E A.6.5	No existe el control	Al momento la empresa no cuenta con un auditor interno	0 Nada	Débil	Débil	Débil
34		Insuficiente evaluación de riesgos periódica.	CON-E A.6.6	No existe el control	No existe un control para la evaluación de riesgos	0 Nada	Débil	Débil	Débil

2

		CONTROLES EXISTENTES (1)			
No.	Activo	Riesgo	Cod.	Control	Descripción del control
21	Base de Datos ADMS (EE-05)	Inexistencia de definición y clasificación de información.	CON-E E.19.1	No existe el control	
32		Deficiencia de procedimiento de seguimiento de las instalaciones de procesamiento de información	CON-E A.6.4	No existe el control	No existe un control sobre el seguimiento de las instalaciones de procesamiento de información
33		Deficiente planificación para auditorías periódicas.	CON-E A.6.5	No existe el control	Al momento la empresa no cuenta con un auditor interno
34		Insuficiente evaluación de riesgos periódica.	CON-E A.6.6	No existe el control	No existe un control para la evaluación de riesgos

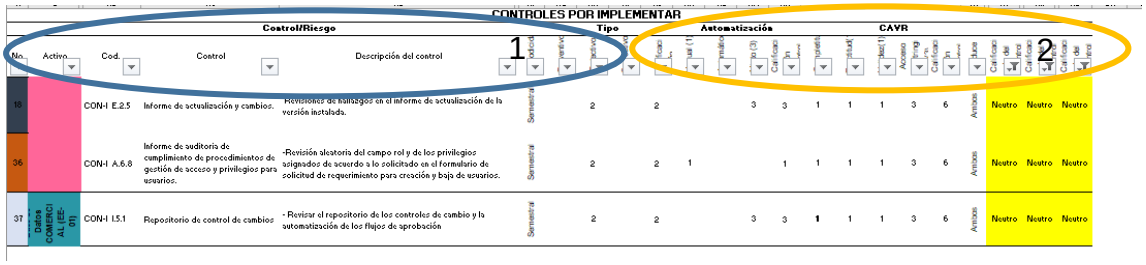
CONTROLES EXISTENTES (2)																	
Preventivo	Detectivo	Correctivo	Calificación Control Manual (1)	Automático (2)	Mixto (3)	Calificación Control Completitud (1)	Exactitud (1)	Validez (1)	Acceso Restringido (3)	Calificación Control Reduce	Preventivo	Calificación del Control (Cualitativa)	Calificación del Control	Calificación del Control Probabilidad
											Nada	Débil	Débil	Débil
										0	Nada	Débil	Débil	Débil
										0	Nada	Débil	Débil	Débil
										0	Nada	Débil	Débil	Débil

Como se indica en la Tabla 16: Muestra de controles existentes débiles, se definieron medidas para mitigar los riesgos asociados, y con ello disminuir el riesgo residual con el objetivo de minimizar la exposición al riesgo al que se

encuentran sujetos los dos activos críticos analizados. Para mayor detalle referirse al Anexo 11: Controles Existentes.

Con los controles propuestos se ha calificado el resultado que se esperaría luego de su implementación, como se observa en Tabla 17: Muestra controles por implementar, se evidencia una notable mejora en la fortaleza de los controles, permitiendo así la mejora continua gracias a la implementación del programa de seguridad de la información.

Tabla 17: Muestra controles por implementar



	1	CONTROLES POR IMPLEMENTAR		
No.	**Activo**	**Cod.**	**Control**	**Periodicidad**
18	**Base de Datos ADMS (EE-05)**	**CON-I E.2.5**	Informe de actualización y cambios.	Revisiones de hallazgos en el informe de actualización de la versión instalada.	Semestral
36		**CON-I A.6.8**	Informe de auditoría de cumplimiento de procedimientos de gestión de acceso y privilegios para usuarios.	-Revisión aleatoria del campo rol y de los privilegios asignados de acuerdo con lo solicitado en el formulario de solicitud de requerimiento para creación y baja de usuarios.	Semestral
37	**Base de Datos COMERCIAL (EE-01)**	**CON-I I.5.1**	Repositorio de control de cambios	- Revisar el repositorio de los controles de cambio y la automatización de los flujos de aprobación	Semestral

2

CONTROLES POR IMPLEMENTAR

Preventivo	Detectivo	Correctivo	Calificación Control	Manual (1)	Automático (2)	Mixto (3)	Calificación Control	Completitud (1)	Exactitud (1)	Validez (1)	Acceso Restringido (3)	Calificación Control	Reduce	Calificación del Control	Calificación del Control Impacto	Calificación del Control Probabilidad
	2		2			3	3	1	1	1	3	6	Ambos	Neutro	Neutro	Neutro
	2		2	1			1	1	1	1	3	6	Ambos	Neutro	Neutro	Neutro
	2		2			3	3	1	1	1	3	6	Ambos	Neutro	Neutro	Neutro

Mayor detalle sobre la tabla anterior puede ser encontrado en el Anexo 12: Controles por implementar.

2.5.7. Fase 7: Operación

La fase 7 o fase de operación comprende el diseño e implementación de las acciones y planes necesarios (*Road Map*) por implementarse en la empresa eléctrica con el objetivo de cumplir de manera eficaz los controles propuestos.

2.5.7.1. Metodología

Con base en los controles propuestos, se diseñó un plan para la mejora continua que describe actividades, las cuales se asocian de acuerdo con el cumplimiento de cada control propuesto, en dicho plan se designa un responsable para ejecutar las acciones por implementarse y el plazo para su ejecución. Además, se determina si el tipo de control es nuevo o una mejora, se selecciona el alcance (Organizacional o Autónomo) que dicha actividad tendrá dentro de la Organización. Para más detalle revisar el Anexo 13: Planes por implementar.

Tabla 18: Muestra Planes por implementar

No.	Activo	PLANES				
		Plan por implementar	**Capacidad de Ejecución**	**Tipo**	**Alcance**	**Responsable**
1	**Base de Datos ADMS (EE-05)**	- Adquirir un repositorio para almacenar los controles de cambios que permitan manejar un flujo de aprobación, permitiendo la creación de la solicitud, ingreso de documentación para su posterior seguimiento y control.	Mediano Plazo (1 año)	Nuevo Control	Organizacional	Jefe de Sección SCADA
2		- Establecer un procedimiento de mantenimiento preventivo periódico a las instalaciones eléctricas.	Corto Plazo (6 meses)	Nuevo control	Autónomo	Jefe de Mantenimiento .
3		- Elaborar un cronograma anual de mantenimiento para las instalaciones eléctricas.	Corto Plazo (6 meses)	Nuevo control	Autónomo	Jefe de Mantenimiento .
4		- Definir un repositorio donde se almacene los informes de mantenimiento para su respectivo control y seguimiento.	Mediano Plazo (1 año)	Nuevo control	Organizacional	Jefe de Mantenimiento .
5		- Elaborar un cronograma anual de mantenimiento de sistemas de climatización.	Corto Plazo (6 meses)	Mejora	Autónomo	Jefe de Infraestructura .

2.5.7.2. Resultados (Análisis)

Como resultado de esta fase se determinaron los planes de acción por implementar, su capacidad de ejecución, tipo, alcance y responsable como, se muestra a continuación:

- Diseñar un plan anual de capacitaciones sobre instalación y mantenimiento de medios de almacenamiento. Corto Plazo (6 meses), nuevo control, alcance autónomo, responsable jefe de Sección SCADA/Jefe de Talento Humano.
- Elaborar un cronograma anual de mantenimiento de medios de almacenamiento. Corto Plazo (6 meses), nuevo control, alcance autónomo, responsable jefe de sección SCADA.
- Elaborar la política de clasificación de la información, Corto Plazo (6 meses), Nuevo Control, alcance Autónomo, Responsable de Seguridad de la Información.
- Elaborar la política de clasificación de la información, Corto Plazo (6 meses), Nuevo Control, alcance Autónomo, Responsable de Seguridad de la Información.
- Contratar enlaces redundantes, Mediano Plazo (1 año), nuevo control, alcance Organizacional, Jefe de Tecnologías de la información.
- Elaborar guion de pruebas para verificar el correcto funcionamiento de los enlaces redundantes, Corto Plazo (6 meses), Nuevo control, alcance Autónomo, Jefe de Tecnologías de la información.
- Elaborar el plan anual de capacitación especializada en temas de seguridad para los responsables de seguridad de la información, Mediano Plazo (1 año), alcance Nuevo Control, Autónomo, Jefe de Talento Humano/Responsable de Seguridad de la Información.
- Elaborar el plan para enviar campañas en temas de seguridad, Mediano Plazo (1 año), Nuevo Control, alcance Autónomo, responsable de Seguridad de la Información.
- Definir el contenido de las campañas a ser enviadas, Mediano Plazo (1 año), Nuevo Control, alcance Autónomo, Responsable de Seguridad de la Información.
- Configuración de encriptación de contraseñas en tablas críticas, Mediano Plazo (1 año), Nuevo control, alcance Autónomo, Jefe de Sección SCADA

- Cambios de contraseña periódicos no mayor a 45 días, Corto Plazo (6 meses), Nuevo control, alcance Autónomo, Responsable de Seguridad de la Información.
- Definir e implementar logs de auditoría, Mediano Plazo (1 año), Nuevo control, alcance Autónomo, Responsable de Seguridad de la Información/Jefe de Sección SCADA. Para más detalle revisar el Anexo 13: Planes por implementar.

3. CONCLUSIONES

- Con el apoyo de los distintos marcos de referencia NIST, COBIT, ISO27001, ISO 27002, ISO 27005 y con la metodología MAGERIT se puede realizar un análisis completo de la realidad de la Empresa en términos de Seguridad de la Información, confirmando que es necesario mejorar los controles existentes y diseñar controles, así como planes de acción que permitan minimizar el riesgo a los que se encuentran expuestos.

- El estado actual en temas de seguridad de la Empresa Eléctrica indica que necesita una atención prioritaria ya que existen controles básicos con una mitigación muy débil, lo que facilitaría que los activos críticos se encuentren expuestos a varios riesgos que se traduzcan a pérdidas financieras, multas, afectación a su imagen corporativa.

- La clasificación de entidades y de activos de información permite priorizar los elementos indispensables para este giro de negocio con el objetivo de proteger y conservar el activo más importante en la organización que es la información.

- Con el apoyo de la matriz de riesgos, se evidencia como va mejorando la calificación en términos de impacto y probabilidad, de acuerdo con los controles existentes en la Empresa y los propuestos para su mejora, los mismos que fueron simulados por propósito educativos.

- A partir de la evaluación de riesgos se determinó los planes de acción a ser implementados: acciones, responsables y plazos (*Road Map*) establecidos para poderles hacer su seguimiento para mejorar de esta manera su estado actual del SGSI.

4. RECOMENDACIONES

- Dado que la Empresa Eléctrica forma parte de un sector estratégico (infraestructura crítica), se recomienda que la metodología para el desarrollo del programa del sistema de gestión de seguridad de la información, así como su plan de mejora continua se basen en marcos de referencia y metodologías homologadas con estándares internacionales reconocidos de seguridad de la información para incorporar buenas prácticas en su operación y con ello mitigar riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información

- Implementar en un corto plazo el presente programa de SGSI en la Empresa Eléctrica, a partir de los planes de acción identificados con el fin de proteger el activo más importante de la Empresa, la información. Esos planes abarcan aspectos importantes como el tratamiento de datos personales, capacitación al personal y terceros, creación de políticas y controles, así como implementar diversas acciones con el objetivo de mitigar los riesgos a los que se encuentra expuesta la empresa.

- Mantener actualizada la clasificación de la información de la Empresa Eléctrica permitirá realizar una adecuada gestión, ya que se identificará cuáles son los activos críticos para determinar los controles apropiados.

- Mantener la herramienta de matriz de riesgos actualizada para realizar evaluaciones de los demás activos de información, identificando nuevos riesgos y controles por implementar a fin de completar la evaluación de los riesgos de la Empresa Eléctrica, dicha evaluación también deberá incluir la evaluación de riesgos a terceros incluso proveedores.

- Se recomienda mejorar los controles existentes e incrementar nuevos controles para proteger todos los activos de información que posee la Empresa Eléctrica y realizar evaluaciones de riesgo periódicas

(trimestrales y una anual) para analizar el riesgo residual y mejorar los controles implementados para alcanzar un riesgo objetivo cada vez menor con el objetivo de minimizar los riesgos a los que se encuentra expuesta la Empresa Eléctrica.

- Es importante la creación del puesto de responsable de seguridad de la información que se encuentre en el área de TI, con proyección a crear un área independiente de seguridad de la información ya que junto con el avance tecnológico del sector energético y su transformación digital, los entornos industriales y redes OT se encuentran en constante exposición a nuevas amenazas y ataques, particular que ha sido evidenciado en los últimos eventos internacionales como en la guerra entre Rusia y Ucrania. Demostrando de esta manera, la importancia de la mitigación de riesgos y la inversión en seguridad de la información que todas las empresas del sector deben realizar.

- Es necesario que la Empresa Eléctrica incremente los controles para el tratamiento de los datos personales de clientes, empleados, exempleados y proveedores, en cumplimiento de la Ley Orgánica de Protección de Datos Personales y a las disposiciones de la Autoridad de Datos Personales. De igual manera se deberá dar un tratamiento especial a la categoría de datos sensibles estipulada en la ley.

- Para el cumplimiento de la Ley Orgánica de Protección de Datos Personales es necesario que la Empresa Eléctrica contrate un Delegado de Protección de Datos Personales, quien deberá cumplir con el perfil profesional y obligaciones dispuestas por la LOPDP.

5. REFERENCIAS

Asamblea Nacional. (2021). Ley Orgánica de Protección de Datos Personales. Quito, Ecuador: Asamblea Nacional.

CEDIA. (2020). ¿Qué es un incidente? Obtenido de https://csirt.cedia.edu.ec/que-es-un-incidente/

CEDIA. (2020). Criptografía. Obtenido de https://csirt.cedia.edu.ec/glossary/criptografia/

Comité Técnico CTN 71 Tecnología de la Información. (2017). Tecnología de la Información Técnicas de Seguridad Código de Prácticas para los controles de seguridad de la Información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015). Cataluña, España.

Consultoría, t. T. (2013). Gestión de Riesgos. Obtenido de https://www.tithink.com/publicacion/MAGERIT.pdf

Cyberark. (2022). ISO/IEC 27002. Obtenido de https://www.cyberark.com/es/solutions/audit-compliance/iso-iec/

Deloitte. (Diciembre de 2020). Deloitte. (Deloitte, Ed.) Lima, Perú. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/cl-ciberseguridad-en-el-sector-electrico-diciembre-2020.pdf

Global Trust Association. (2022). Information Security Management Professional ISO 27001. Madrid, España: GTA Iberoamerica.

ISACA. (2018). Introducción y Metodología. Schaumburg, Estados Unidos: ISACA.

Kaspersky. (2022). ¿Qué es le cifrado de datos? Defínción y explicación. Obtenido de https://latam.kaspersky.com/resource-center/definitions/encryption

Mahn, A., Marron, J., Quinn, S., & Top, D. (2021). Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. Estados Unidos: NIST. doi:https://doi.org/10.6028/NIST.SP.1271

Meza, R. C. (s.f.). Unidad IV.- Seguridad Lógica. Obtenido de Administración de Centro de Computo: https://www.fcca.umich.mx/descargas/apuntes/academia%20de%20infor

matica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20IV.pdf

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Vol. II Catálogo de Elementos). (M. d. Públicas, Ed.) Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). Guía para la Gestión de Riesgos de Seguridad de la Información. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Ministerio de Trabajo. (s.f.). Teletrabajo. Obtenido de https://www.trabajo.gob.ec/teletrabajo/

Red Hat. (2018). ¿Qué es el malware? Obtenido de https://www.redhat.com/es/topics/security/what-is-malware

techopedia. (2022). Obtenido de ¿Qué es el acceso? - definición de techopedia: https://es.theastrologypage.com/access

Veritas. (2022). Copias de seguridad y recuperación de datos: la guía esencial para las empresas. Obtenido de https://www.veritas.com/es/es/information-center/data-backup-and-recovery

ANEXOS

Anexo 1: Caso de negocio.

Ver el archivo: 1_Caso de Negocio.pdf

Anexo 2: Modulador del Apetito

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Modulador del Apetito.

Anexo 3: Niveles de Impacto.

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Tipología del impacto.

Anexo 4: Metodología

Ver el archivo: 2_Metodologia.xls.

Anexo 5: Clasificación de Entidades.

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Dominios.

Anexo 6: Inventario de Activos Fijos.

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Inventario.

Anexo 7: Escenario Base de Datos ADMS

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Escenario_ADMS

Anexo 8: Escenario Base de Datos Comercial.

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Escenario_CRM

Anexo 9: Matriz de Riesgos

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Matriz Riesgos.

Anexo 10: Políticas del Sistema de Gestión de Seguridad de la Información.

Ver el archivo: 4_Políticas del Sistema de Gestión de Seguridad de la Información.pdf

Anexo 11: Controles Existentes

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Control Existente.

Anexo 12: Controles por implementar

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Controles Implementar.

Anexo 13: Planes por implementar.

Ver el archivo: 3_DominiosRiesgos.xls, en la pestaña Planes.