



Plan para la implementación del Sistema de Gestión de Seguridad de la Información

CÓDIGO: A-GI-PN-001

Versión: 2.0

Fecha de Aprobación: 09/04/2025

San José del Guaviare

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	2 de 19

1. TABLA DE CONTENIDO

2.	INTRODUCCIÓN	3
3.	OBJETIVO	4
4.	ALCANCE	4
5.	DESARROLLO	4
5.1.	DEFINICION DEL SISTEMA.....	4
5.1.1.	DEFINICIONES GENERALES.....	4
5.1.2.	MARCO REGULATORIO.....	5
5.2.	ACTIVIDADES PRELIMINARES.....	6
5.2.1.	TECNICAS.....	6
5.2.2.	DOCUMENTALES	7
5.3.	ACTIVIDADES DE IMPLEMENTACIÓN	8
5.3.1.	TÉCNICAS.....	8
5.3.2.	DOCUMENTALES	9
5.4.	UBICACIONES DE IMPLEMENTACIÓN	10
5.4.1.	UBICACIONES DONDE REGIRÁ EL SISTEMA.....	10
5.4.2.	UBICACIONES QUE SERAN AFECTADAS ESTRUCTURALMENTE	11
	Modificaciones Propuestas:	11
	Modificaciones Propuestas:	12
5.5.	ANÁLISIS DE COSTOS ASOCIADOS.....	13
5.5.1.	TALENTO HUMANO.....	13
5.5.2.	RECURSOS TECNOLÓGICOS	13
5.5.3.	MODIFICACIONES A LA INFRAESTRUCTURA FÍSICA.....	14
5.5.4.	CAPACITACIÓN	14
6.	CRONOGRAMA.....	15
6.1.	PLANEAR	15
6.2.	HACER	17
6.3.	VERIFICAR.....	17
6.4.	ACTUAR	18
7.	SEGUIMIENTO Y CONTROL.....	18
8.	CONTROL DE CAMBIOS	19

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	3 de 19

2. INTRODUCCIÓN

Con la finalidad de fortalecer la seguridad de nuestra información y asegurar el cumplimiento con las regulaciones pertinentes en nuestro sector de distribución y comercialización eléctrica, este documento detalla un plan de implementación meticuloso para nuestro Sistema de Gestión de Seguridad de la Información – SGSI. Siguiendo un enfoque estructurado y coherente, se empieza con una definición del sistema y un marco regulatorio bien establecido, adaptado a las exigencias regulatorias y las particularidades del sector eléctrico. Este plan no solo traza las actividades preliminares, tanto técnicas como documentales, que preparan el terreno para una infraestructura de seguridad informática robusta, sino que también establece las fases críticas de implementación necesarias para construir y mantener el Sistema de Gestión de Seguridad de la Información (SGSI).

De manera crucial, después de abordar el análisis de costos, donde se evalúan los recursos necesarios en términos de talento humano, tecnología y modificaciones infraestructurales, el documento se adentra en el cronograma de implementación. Este cronograma, derivado directamente de la planificación inicial, articula las fechas claves, los hitos y la secuencia de actividades necesarias, garantizando un despliegue eficiente y oportuno del Sistema de Gestión de Seguridad de la Información – SGSI. Este esquema temporal no solo facilita la gestión y asignación de recursos, sino que también establece expectativas claras para todas las partes involucradas, asegurando una visión compartida y un compromiso hacia los objetivos de seguridad de la información.

Siguiendo el cronograma, se detalla la metodología de seguimiento y control, esencial para la gestión efectiva del proyecto de implementación del Sistema de Gestión de Seguridad de la Información – SGSI. Aquí se definen los mecanismos para monitorear el avance, evaluar la efectividad de los controles de seguridad y hacer ajustes proactivos. Este enfoque garantiza que el Sistema de Gestión de Seguridad de la Información – SGSI no solo sea implementado de acuerdo con los estándares internacionales y las regulaciones específicas del sector, sino que también permanezca relevante y robusto frente a las evoluciones en el panorama de amenazas y las necesidades organizacionales.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	4 de 19

3. OBJETIVO

El objetivo principal de este documento es establecer un plan detallado y estructurado para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI en nuestra empresa. Se busca no solo reforzar la seguridad de nuestra información crítica y gestionar la conformidad con las regulaciones aplicables, sino también crear una infraestructura informática que sea resiliente ante las amenazas emergentes y adaptable a las cambiantes necesidades del negocio y el entorno regulatorio.

4. ALCANCE

Aplica para toda la actividad informática de la empresa

5. DESARROLLO

5.1. DEFINICION DEL SISTEMA

5.1.1. DEFINICIONES GENERALES

- **Sistema de Gestión de Seguridad Informática SGSI:** Es un enfoque sistemático para gestionar información sensible de la empresa con el fin de asegurar su confidencialidad, integridad y disponibilidad, mediante la aplicación de procesos de gestión de riesgos.
- **VPN (virtual private network) o red privada virtual,** es una herramienta técnica de control **que** forma parte de las medidas de seguridad para **garantizar la confidencialidad, integridad y disponibilidad** de la información durante su transmisión por redes públicas o no seguras.
- **El Acuerdo 1502 del Consejo Nacional de Operación (CNO),** Es la **guía de Ciberseguridad** para el sector eléctrico colombiano. Este acuerdo establece lineamientos y plazos para que los agentes del Sistema Interconectado Nacional (SIN) implementen medidas de ciberseguridad que protejan la infraestructura crítica del sector eléctrico, y están alineadas con estándares internacionales, como la norma ISO/IEC 27001.
- El documento **SOA (statement of applicability) o declaración de aplicabilidad,** es un registro formal y obligatorio que enumera todos los controles del Anexo A de la ISO/IEC 27001, e indica cuáles han sido seleccionados para gestionar los riesgos de seguridad de la información, justificando su inclusión o exclusión, y señalando su estado de implementación.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	5 de 19

5.1.2. MARCO REGULATORIO

Para desarrollar un marco regulatorio específico para la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI en el sector eléctrico colombiano, incluyendo el acuerdo del Consejo Nacional de Operación (CNO), consideraremos la siguiente lista de normativas y leyes relevantes, así como el acuerdo específico:

1. **Norma técnica colombiana NTC-ISO/IEC 27001:2022:** Establece los requisitos para un Sistema de Gestión de Seguridad de la Información – SGSI, proporcionando un marco para asegurar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de riesgos de gestión de procesos.
2. **Ley 23 de 1982, sobre derechos de autor:** Regula los derechos de autor y los derechos conexos, incluyendo la protección de las obras y los derechos de los autores y otros titulares de derechos sobre obras y prestaciones protegidas.
3. **Ley 594 de 2000 (Ley general de archivo):** Establece las normas para la gestión de archivos, lo cual es esencial para asegurar la adecuada organización, almacenamiento, conservación y recuperación de la documentación, incluidas las informaciones digitales.
4. **Decreto 1747 de 2000:** Reglamenta parcialmente la Ley 527 de 1999 respecto a las entidades de certificación, los certificados y las firmas digitales, elementos clave para asegurar la autenticidad, integridad y no repudio de la información digital.
5. **Ley 1221 de 2008 (Teletrabajo):** Fomenta y regula el teletrabajo, una modalidad laboral que implica consideraciones especiales para la seguridad de la información y la comunicación.
6. **Ley 1341 de 2009:** Define principios y conceptos sobre la sociedad de la información y la organización de las TIC, estableciendo el marco para el desarrollo, la protección y el uso de las TIC en Colombia.
7. **Ley 1273 de 2009 (Delitos informáticos):** Crea un bien jurídico tutelado denominado "de la protección de la información y de los datos", fundamental para la protección contra actos delictivos que afecten los sistemas de información.
8. **Ley 1581 de 2012 (Protección de datos personales):** Dicta disposiciones generales para la protección de datos personales, estableciendo los derechos de los titulares de los datos y las obligaciones de los responsables y encargados del tratamiento de datos personales.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	6 de 19

9. **Ley 1928 de 2018 (Convenio sobre la ciberdelincuencia):** Aprueba el Convenio sobre la ciberdelincuencia, promoviendo medidas y cooperación internacional para combatir delitos informáticos.
10. **Documento CONPES 3854:** Establece la Política Nacional de Seguridad Digital, orientando sobre la protección de la infraestructura crítica de información y la gestión de riesgos cibernéticos.
11. **Acuerdo 1502 del Consejo Nacional de Operación (CNO):** Este acuerdo es específico del sector eléctrico y establece criterios para la operación del sistema interconectado nacional, incluyendo aspectos que pueden influir en la seguridad de la información relacionada con la operación eléctrica.

Este marco regulatorio debe ser utilizado como base para asegurar que la implementación del Sistema de Gestión de Seguridad de la Información – SGSI en el sector eléctrico no solo cumpla con los estándares internacionales de seguridad de la información, sino también con los requisitos legales y regulatorios específicos de Colombia, garantizando así la protección de la infraestructura crítica y la información sensible en el sector eléctrico.

5.2. ACTIVIDADES PRELIMINARES

5.2.1. TECNICAS

- **Implementación de un sistema de firewall fortigate 200F:** La instalación del FortiGate 200F como solución de firewall proporciona una barrera robusta contra ataques externos, filtrando el tráfico de red y protegiendo los recursos de la empresa. Esta tecnología avanzada de seguridad de red permite establecer controles detallados de acceso, detección de intrusos y prevención, así como funciones avanzadas de VPN.
- **Creación de túneles VPN seguros para conexión de externos:** El desarrollo de túneles VPN seguros facilita la conexión remota de empleados y colaboradores externos, garantizando que el intercambio de información se realice de manera segura y cifrada. Esto es esencial para mantener la integridad y confidencialidad de los datos corporativos, incluso en comunicaciones a través de Internet.
- **Depuración de usuarios inactivos de todas las bases de datos empresariales:** Esta actividad consiste en revisar y eliminar las cuentas de usuarios que ya no están activas en las bases de datos de la empresa. Reducir el número de cuentas inactivas disminuye el riesgo de accesos no autorizados y potenciales brechas de seguridad, asegurando que solo los usuarios actuales tengan acceso a los sistemas y datos relevantes.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	7 de 19

- **Dibujo de toda la topología de red y comunicaciones:** Elaborar un esquema detallado de la topología de red permite tener una visión clara de la infraestructura de red y comunicaciones de la organización. Identificar todos los componentes de la red, como routers, switches, dispositivos de seguridad, y conexiones de comunicación, es fundamental para la gestión de la seguridad y la planificación de mejoras.
- **Definición de plan de trabajo para implementación de un directorio activo:** Establecer un plan de trabajo detallado para la implementación de un directorio activo facilita la gestión centralizada de usuarios, grupos, dispositivos y políticas de seguridad. Este sistema es esencial para el control de acceso y la administración de políticas de seguridad a nivel empresarial.

5.2.2. DOCUMENTALES

- **Aproximaciones documentales al acuerdo 1502 del CNO entregadas como informe anexo:** La elaboración de un informe que detalle cómo la organización se alinea o planea alinearse con los requisitos del Acuerdo 1502 del CNO es crucial. Este documento sirve como base para asegurar que las prácticas de seguridad de la información estén en conformidad con las regulaciones específicas del sector eléctrico colombiano.
- **Creación de la política de credenciales:** Desarrollar una política de credenciales establece las directrices para la creación, distribución, uso y gestión de credenciales de usuario. Esto incluye contraseñas, certificados digitales y otros mecanismos de autenticación, asegurando que se apliquen prácticas de seguridad robustas para el acceso a los sistemas y datos.
- **Documentación preliminar del formato de seguimiento de incidencias de red:** Preparar un formato estandarizado para el seguimiento de incidencias de red permite documentar y gestionar eficazmente cualquier evento de seguridad o falla técnica. Esto facilita la resolución rápida de incidentes y contribuye a la mejora continua de la seguridad de la red.
- **Reestructuración del proceso de gestión informática con enfoque en seguridad:** Revisar y modificar el proceso de gestión informática para incorporar un enfoque centrado en la seguridad mejora la capacidad de la organización para proteger sus activos de información. Esto implica integrar consideraciones de seguridad en todas las fases de gestión de TI, desde la planificación y la implementación de sistemas hasta el mantenimiento y la gestión de cambios.

Estas actividades preliminares, tanto técnicas como documentales, son pasos esenciales para fortalecer la infraestructura de seguridad de la información de la empresa y

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	8 de 19

establecer las bases para la implementación exitosa de un Sistema de Gestión de Seguridad de la Información – SGSI alineado con los estándares NTC-ISO/IEC 27001:2022 y los requisitos regulatorios específicos del sector eléctrico colombiano.

5.3. ACTIVIDADES DE IMPLEMENTACIÓN

5.3.1. TÉCNICAS

- **Análisis de contexto de la organización:** Esta actividad implica comprender tanto el entorno interno como el externo de la organización que influye en el Sistema de Gestión de Seguridad de la Información – SGSI. Esto incluye identificar las partes interesadas relevantes, entender las necesidades y expectativas de estas partes, y evaluar los factores externos e internos que pueden afectar los objetivos y la planificación del Sistema. Este análisis ayuda a asegurar que el sistema esté alineado con la estrategia global de la organización.
- **Evaluación de la seguridad de la información:** Consiste en realizar un análisis detallado de la seguridad actual de la información, identificando las vulnerabilidades existentes en los sistemas, procesos y controles de la organización. Esta evaluación también incluye la identificación de amenazas potenciales que podrían explotar estas vulnerabilidades y afectar la confidencialidad, integridad o disponibilidad de la información.
- **Evaluación del riesgo:** Involucra la identificación sistemática de riesgos de seguridad de la información específicos para la empresa, evaluando tanto la probabilidad de que ocurran como el impacto que tendrían en la organización. Este proceso es fundamental para entender los riesgos a los que se enfrenta la organización y para priorizar las acciones de mitigación.
- **Planificación del tratamiento del riesgo:** Después de identificar y evaluar los riesgos, esta actividad se centra en desarrollar estrategias para gestionar esos riesgos a un nivel aceptable. Esto puede incluir la aplicación de controles específicos, la transferencia del riesgo, su aceptación o la evitación del mismo. La selección de controles se documenta en el documento de aplicación de controles (SOA).
- **Implementación de controles:** Esta fase implica la aplicación física y lógica de los controles de seguridad seleccionados para mitigar los riesgos identificados. Puede incluir la implementación de tecnologías de seguridad, la realización de cambios organizativos, la formación de personal y la modificación de procesos y procedimientos.
- **Creación de equipos de ciberseguridad y respuesta a incidentes:** Consiste en formar equipos especializados responsables de gestionar la seguridad de la

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	9 de 19

información y responder ante incidentes de seguridad. Esto incluye la definición de roles y responsabilidades, la formación en gestión de incidentes y la creación de procedimientos para la detección, análisis, contención, erradicación y recuperación de incidentes.

- **Implementación y reestructuración de la oficina de gestión informática:** Esta actividad implica revisar y ajustar la estructura organizativa y los procesos internos para apoyar la implementación y operación efectiva del Sistema de Gestión de Seguridad de la Información – SGSI. Puede incluir la creación de nuevas posiciones, la definición de nuevas responsabilidades y la integración del sistema en las operaciones diarias de la organización.

5.3.2. DOCUMENTALES

- **Documento integrado del alcance del sistema de gestión de seguridad de la información – SGSI:** Define con precisión el alcance del Sistema de Gestión de Seguridad de la Información – SGSI, detallando los límites organizacionales, de TIC y físicos que este abarcará. Este documento es fundamental para delimitar el área de aplicación del sistema, asegurando que todos los involucrados comprendan las áreas cubiertas y las exclusiones justificadas.
- **Instructivo de roles y responsabilidades:** Este documento esencial establece las responsabilidades específicas de la dirección, el administrador del Sistema de Gestión de Seguridad de la Información – SGSI y otros roles claves dentro de la organización. Con el fin de involucrar a cada trabajador en el sistema y que comprendan como su trabajo contribuye a la seguridad de la información.
- **Plan de reestructuración y manual de funciones modificado:** Documenta los cambios organizacionales necesarios para implementar y sostener el Sistema de Gestión de Seguridad de la Información – SGSI. El cual incluye modificaciones en el manual de funciones y la descripción de los procesos de reestructuración que se llevarán a cabo para alinear la organización con los requisitos del sistema.
- **Programa de concienciación de seguridad:** Desarrolla y documenta un programa comprensivo destinado a educar a los empleados sobre la importancia de la seguridad de la información, los riesgos asociados y su papel en la protección de los activos informativos. Este programa busca cambiar comportamientos y fomentar una cultura de seguridad en toda la organización.
- **Documento de requerimientos de seguridad:** Especifica los requerimientos de seguridad de la información para la organización, basándose en el análisis de riesgos y la evaluación de las necesidades de seguridad. Este documento sirve como una guía para la selección e implementación de controles de seguridad apropiados.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	10 de 19

- **Inventario de activos informáticos y diagrama de árbol de dependencia de activos:** Lista todos los activos informáticos relevantes para el Sistema de Gestión de Seguridad de la Información – SGSI, proporcionando detalles como ubicación, importancia y responsables. El diagrama de árbol de dependencia visualiza las interrelaciones entre los activos, ayudando en la identificación de dependencias críticas y puntos de vulnerabilidad.
- **Informe de evaluación de la seguridad y documento de caracterización de riesgos:** Presenta los hallazgos de las evaluaciones de seguridad realizadas y detalla los riesgos identificados, su nivel de criticidad y las recomendaciones para su tratamiento. Estos documentos son claves para el proceso de toma de decisiones en la gestión de riesgos.
- **Documentos de gestión de controles SOA, políticas de seguridad, y planes:** Incluyen la documentación detallada de los controles seleccionados para mitigar los riesgos (SOA), las políticas de seguridad establecidas para la organización, y los planes de acción para la implementación de controles y la mitigación de riesgos.
- **Cuadro de mando de indicadores y plan de continuidad del negocio:** Desarrolla indicadores para medir la efectividad del Sistema de Gestión de Seguridad de la Información – SGSI y documenta un plan para asegurar la continuidad del negocio ante incidentes de seguridad. Estos documentos son fundamentales para el monitoreo continuo y la mejora del sistema.
- **Procedimiento de mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI:** Establece un proceso sistemático para revisar y mejorar continuamente el sistema basado en auditorías internas, revisiones de la dirección y el análisis de incidentes de seguridad. Este documento garantiza que el sistema se mantenga efectivo y alineado con los objetivos de la organización a lo largo del tiempo.

5.4. UBICACIONES DE IMPLEMENTACIÓN

5.4.1. UBICACIONES DONDE REGIRÁ EL SISTEMA

- **Sede principal:** La implementación del Sistema de Gestión de Seguridad de la Información – SGSI en la sede principal es fundamental, dado que esta ubicación suele albergar la mayor parte de las operaciones centrales de la empresa, incluyendo la gestión administrativa, la planificación estratégica y los centros de control de operaciones. Aquí se concentran los sistemas críticos de gestión de la información y la toma de decisiones, lo que la convierte en una ubicación

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	11 de 19

prioritaria para asegurar la protección de la información.

- **Oficinas de la subestación:** Las oficinas ubicadas en las subestaciones son esenciales para la operación y mantenimiento de la infraestructura eléctrica. Estas ubicaciones contienen sistemas operativos importantes, incluyendo aquellos relacionados con el control de la red eléctrica, monitoreo y respuesta ante incidentes. La implementación del Sistema de Gestión de Seguridad de la Información – SGSI en estas oficinas es crucial para garantizar la seguridad de la información relacionada con las operaciones críticas y la infraestructura.
- **Miembros de la red operativa:** Todos los individuos que forman parte de la red operativa, incluyendo aquellos involucrados en la generación, transmisión y distribución de energía eléctrica, estarán sujetos al Sistema de Gestión de Seguridad de la Información – SGSI. Esto abarca a empleados que trabajan directamente en la infraestructura física, así como aquellos que realizan tareas de supervisión, mantenimiento y gestión de operaciones a través de sistemas de control.
- **Usuarios de VPN (Red Privada Virtual):** Los miembros de la organización que acceden a los sistemas y redes de la empresa a través de VPN, incluyendo empleados remotos, consultores y socios, también estarán cubiertos por el Sistema de Gestión de Seguridad de la Información – SGSI. Esto asegura que el acceso remoto a la red de la empresa se realice de manera segura, protegiendo la transmisión de datos críticos y sensibles contra accesos no autorizados y amenazas cibernéticas.

5.4.2. UBICACIONES QUE SERAN AFECTADAS ESTRUCTURALMENTE

AGREGAR CONTROLES DE ACCESO BIOMETRICOS AL CENTRO DE CONTROL

Ubicación: Oficinas de Subestación – Centro de Control

Modificaciones Propuestas:

- **Instalación de sistemas biométricos:** Implementar controles de acceso biométricos, como lectores de huellas dactilares o reconocimiento facial, en las entradas del centro de control. Estos sistemas aseguran que solo el personal autorizado pueda acceder al centro, limitando el riesgo de acceso no autorizado a áreas críticas.
- **Actualización de protocolos de seguridad:** Revisar y actualizar los protocolos de seguridad para incorporar el uso de la biometría como método de autenticación. Esto incluye la creación de políticas para el registro de características biométricas del personal autorizado y procedimientos de acceso.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	12 de 19

- **Capacitación del personal:** Organizar sesiones de capacitación para el personal sobre el funcionamiento de los nuevos sistemas de acceso biométrico y la importancia de la seguridad física en la protección de la información crítica de la empresa.
- **Integración con sistemas de seguridad existentes:** Asegurar que los nuevos controles de acceso biométrico estén integrados con los sistemas de seguridad existentes, como cámaras de vigilancia y alarmas, para proporcionar una solución de seguridad completa.

CREACIÓN DE UNA SALA PARA TRASLADAR EL DATA CENTER DE LA EMPRESA

Ubicación: Oficinas de Subestación – Nueva Sala de Data Center

Modificaciones Propuestas:

- **Diseño y construcción de la sala:** Diseñar y construir una sala específicamente para albergar el data center, siguiendo las normas de seguridad y de infraestructura crítica. Esto incluye consideraciones sobre el control climático, resistencia al fuego, y redundancia de energía y conectividad.
- **Controles de acceso biométricos:** Instalar sistemas de acceso biométrico en las entradas de la sala del data center para garantizar que solo el personal autorizado con roles específicos pueda entrar. Esto protege la integridad y disponibilidad de los sistemas y datos críticos.
- **Cumplimiento de normas de seguridad:** Asegurar que la sala cumpla con las normas de seguridad para data centers, incluyendo la segregación física de redes, la protección contra inundaciones y otros desastres naturales, así como la seguridad contra intrusiones físicas y cibernéticas.
- **Sistemas de vigilancia y monitorización:** Implementar sistemas avanzados de vigilancia y monitorización en y alrededor de la sala del data center. Esto incluye cámaras de seguridad, sensores de movimiento y sistemas de detección de intrusos para monitorizar la actividad las 24 horas del día.

Estas modificaciones no solo mejoran la seguridad física y de la información en las oficinas de subestación, sino que también son fundamentales para cumplir con los estándares de seguridad requeridos por un Sistema de Gestión de Seguridad de la Información – SGSI eficaz, protegiendo los activos de información críticos contra riesgos y amenazas tanto internos como externos.

La implementación de estas actualizaciones deberá planificarse cuidadosamente para minimizar la interrupción de las operaciones y garantizar que todos los cambios se realicen de acuerdo con las mejores prácticas de seguridad y los requisitos reglamentarios.

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	13 de 19

5.5. ANÁLISIS DE COSTOS ASOCIADOS

5.5.1. TALENTO HUMANO

ÍTEM	CANTIDAD	DESCRIPCIÓN	COSTO	COSTO TOTAL
INGENIERO INDUSTRIAL (10 MESES)	1	Esta nueva OPS corresponde a la necesidad de la implementación bajo una mirada estrictamente normativa, este tipo de actividades son desarrolladas bajo las competencias de un ingeniero industrial.	\$ 3.525.251	\$ 35.252.510

5.5.2. RECURSOS TECNOLÓGICOS

5.5.2.1. HARDWARE

ÍTEM	CANTIDAD	DESCRIPCIÓN	COSTO	COSTO TOTAL
FORTIGATE 200F (LIC 30 MESES)	1	Este dispositivo se propone como medida de redundancia respecto a la administración de la red y de protección de la misma.	\$60.078.357	\$60.078.357
SERVIDOR DELL R350 SCADA	2	Estos dos servidores se establecen como requerimiento a partir del proyecto que responde a la necesidad de independización y alta disponibilidad por redundancia del sistema SCADA	\$ 23.000.000	\$46.000.000
RACK PARA SERVIDORES CERRADO CON CHAPA CAMBIABLE	2	De acuerdo a las necesidades y observaciones de la norma, se requiere de este elemento para garantizar la seguridad final previa al acceso directo a los dispositivos.	\$2.800.000	\$ 5.600.000

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	14 de 19

5.5.2.2. OTROS

ÍTEM	CANTIDAD	DESCRIPCIÓN	COSTO	COSTO TOTAL
CORREOS LICENCIA PARA 3 AÑOS	150	Como uno de los requisitos principales para la seguridad de la información, se requiere la compra de esta cantidad aproximada de correos adicionales.	\$8.643.000 TRM 14/02/2024	17.286.000 TRM 14/02/2024
DOCUMENTO - NTC 27001	1	Documento guía para la implementación donde se establece la normatividad asociada	\$ 178.000	\$ 178.000
DOCUMENTO - NTC 27003	1	Documento guía para la implementación donde se establecen las actividades a seguir para la implementación.	\$ 178.000	\$ 178.000

5.5.3. MODIFICACIONES A LA INFRAESTRUCTURA FÍSICA

ÍTEM	CANTIDAD	DESCRIPCIÓN	COSTO	COSTO TOTAL
ADECUACIONES CENTRO DE CONTROL	2	Se requiere como una medida básica para normalizar el control de acceso al centro de control	\$ 5.000.000	\$ 5.000.000

5.5.4. CAPACITACIÓN

ÍTEM	CANTIDAD	DESCRIPCIÓN	COSTO	COSTO TOTAL
CAPACITACION PARA AUDITORIA INTERNA EN ISO 27001	4	Corresponde a la necesidad de capacitación de por lo menos cuatro miembros del área, con el fin de realizar las auditorías internas respecto al sistema SGSI	\$ 2.000.000	\$ 8.000.000
Diplomado en Ciberseguridad - ISO 27001	4	Corresponde a la necesidad de capacitación de por lo menos cuatro miembros del área, con el fin de implementar correctamente todas las medidas normativas del estándar ISO 27001	\$ 4.000.000	\$ 16.000.000
			TOTAL	\$193.572.867

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	15 de 19

6. CRONOGRAMA

6.1. PLANEAR

Categoría	Actividad	Sub actividad	Entregable	Fecha de Entrega
Definir el alcance del SGSI, límites y políticas del SGSI	Análisis de Contexto de la Organización:	N/A	Documento Integrado de Alcance SGSI	31/03/2024
	Definir el alcance y límites organizacionales	N/A		
	Definir el alcance y límites de las Tecnologías de la Información y Comunicación (TIC)	N/A		
	Definir el alcance y límites físicos	N/A		
	Integrar cada alcance y límites para obtener el alcance y límites del SGSI	N/A		
Establecimiento de las responsabilidades del SGSI	Identificación del rol de la dirección.	N/A	Modificación de Instructivo de roles y responsabilidades asociados al SGSI	28/04/2025
	Identificación del rol administrador de SGSI	N/A		
	Identificación de los roles asociados al uso del SGSI	N/A		
	Implementación reestructuración de la oficina de gestión informática	N/A	Plan de Reestructuración aprobado y manual de funciones modificado	25/11/2025
	Creación del equipo de ciberseguridad	N/A	Instructivo de roles y responsabilidades del equipo de gestión de ciberseguridad, y de respuesta a incidentes de ciberseguridad	25/11/2025
	Creación del equipo de respuesta a incidentes de ciberseguridad	N/A		
	Creación del comité de emergencia de ciberseguridad.	N/A	Comité de Emergencia de Ciberseguridad Constituido	25/11/2025
Creación del programa de formación y concientización "Cultura de la Seguridad Informática"	Gestionar las capacitaciones posibles respecto a la norma ISO 27001	N/A	Programa de Concienciación de Seguridad	26/12/2024
	Generar cronograma de charlas de conciencia de seguridad de la información 2025	N/A		30/04/2025

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	16 de 19

Realizar el análisis de los requerimientos de seguridad de la información	Definir los requerimientos de seguridad de la información para el proceso del SGSI	N/A	Documento de Requerimientos de Seguridad	19/05/2025
	Identificar los activos dentro del alcance del SGSI	Creación del inventario de activos informáticos de la empresa	Inventario de Activos Informáticos	
		Árbol de dependencia de activos	Diagrama de Árbol de Dependencia de Activos	
Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo	Realizar una evaluación de la seguridad de la información	N/A	Informe de Evaluación de la Seguridad	25/04/2025
	Realizar la evaluación del riesgo	Caracterización e identificación de los riesgos de seguridad de la información por cada proceso	Documento de Caracterización de Riesgos	30/05/2025
	Determinación del margen de riesgo aceptable en la empresa	N/A	Margen de Riesgo Aceptable Definido	30/05/2025
	Seleccionar los objetivos de control y los controles	Desarrollo del documento de gestión de controles SOA	Documento de Gestión de Controles SOA 2025	26/12/2025
		Diseño y aprobación del plan de mitigación de riesgos de seguridad de la información	Plan de Mitigación de Riesgos Aprobado	30/05/2025
Diseño del SGSI	Diseñar la seguridad de la información organizacional	N/A	Política de Seguridad Organizacional	26/12/2024
	Diseñar la seguridad de la información de las Tecnologías de la Información y Comunicación (TIC) y física	N/A	Políticas de Seguridad TIC y Física.	26/12/2024
	Diseñar la seguridad de la información específica del SGSI	Creación de la política de seguridad informática	Política de seguridad Informática Específica	26/12/2024
	Crear del plan final del proyecto del SGSI	N/A	Plan Final del Proyecto SGSI	30/06/2025

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	17 de 19

	Creación del cuadro de mando de indicadores de seguridad de la información	N/A	Cuadro de Mando de Indicadores	18/07/2025
	Creación del plan de continuidad del negocio	N/A	Plan de Continuidad del Negocio	31/07/2025
	Desarrollo del documento de estimación de escenarios de posible incidencia en la empresa	N/A	Documento de Estimación de Escenarios	22/08/2025
	Crear el procedimiento de mejora continua del SGSI	N/A	Procedimiento de Mejora Continua del SGSI	29/08/2025
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección	N/A	Política del SGSI Aprobada	26/12/2024
	Diseñar la estrategia de implementación del SGSI	N/A	Estrategia de implementación del SGSI	21/07/2025
	Obtener autorización de la Dirección para implementar y operar un SGSI	N/A	Autorización de Dirección Obtenida	26/12/2024
	Diseñar la estrategia de verificación del SGSI	N/A	Estrategia de verificación del SGSI	31/07/2025

6.2. HACER

Ejecución de la estrategia para la implementación del SGSI	Ejecutar las actividades programadas en el plan de implementación	N/A	Informe de ejecución de la estrategia para la implementación del SGSI	28/11/2025
	Replantear actividades con restricciones o con retroalimentación negativa	N/A		

6.3. VERIFICAR

Ejecución de la estrategia para la verificación del SGSI	Ejecutar las actividades programadas en el plan de verificación	N/A	Informe de ejecución de la estrategia para la Implementación del SGSI	26/12/2025
	Realizar primera auditoría interna de gestión de seguridad de la información	N/A		

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	18 de 19

6.4. ACTUAR

Ejecución del procedimiento de mejora continua	Desarrollar informe general de SGSI implementación del	N/A	Informe de ejecución de la estrategia para la implementación del SGSI	26/12/2025
	Desarrollar informe informe general de sugerencias para el siguiente año del SGSI	N/A	Informe de sugerencias para la próxima vigencia del SGSI	26/12/2025

7. SEGUIMIENTO Y CONTROL

Con el propósito de garantizar la efectiva implementación del Sistema de Gestión de la Seguridad de la Información en nuestra empresa, conforme a los estándares establecidos por la norma ISO/IEC 27001:2022, se adoptará una estrategia de seguimiento integral basada en la metodología ágil Scrum, respaldada por la versátil plataforma Jira. Esta iniciativa tiene como objetivo principal proporcionar un marco de trabajo que permita una gestión eficiente, transparente y adaptable durante todas las fases del proyecto.

En consonancia con los principios de Scrum, cada componente significativo del proyecto será identificado y gestionado como una Épica. Esta abstracción facilitará una visión macro del proyecto, permitiendo una planificación estratégica y una asignación de recursos más efectiva. A su vez, las actividades se desglosan en historias de usuario, proporcionando una comprensión detallada de los requisitos específicos y metas intermedias. La especificidad de estas historias de usuario permitirá un seguimiento preciso y una adaptabilidad ágil a medida que avanzamos en la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.

La plataforma Jira ha sido seleccionada como herramienta central para este seguimiento gracias a su capacidad para ofrecer una trazabilidad completa del proceso. Desde las Épicas hasta las tareas más específicas, Jira facilitará la asignación de responsabilidades, el monitoreo continuo del progreso y la identificación de posibles áreas de mejora. La elección de esta herramienta se fundamenta en la convicción de que una implementación exitosa requiere no sólo la adhesión a estándares rigurosos, sino también una gestión eficiente respaldada por tecnologías que faciliten la ejecución efectiva del proyecto.

Cabe destacar que nuestro enfoque integral también se verá enriquecido por la utilización de la norma ISO/IEC 27003:2018 – Guía para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los requisitos establecidos en la norma ISO/IEC 27001. La ISO/IEC 27003:2018

	GESTIÓN INFORMÁTICA	Código:	A-GI-PN-001
		Fecha de aprobación:	09/04/2025
	Plan para la implementación del SGSI	Versión:	2.0
		Página:	19 de 19

proporcionará directrices detalladas que respaldan cada fase del proyecto, asegurando coherencia con los estándares internacionales de seguridad de la información. Además, mantenemos una estrecha relación con lo dispuesto en la guía de ciberseguridad del Acuerdo 1502:2021 del Consejo Nacional de Operación del Sistema Eléctrico de Colombia (CNO), alineando el sistema con prácticas de seguridad de información, expuestas en los requisitos específicos del sector eléctrico.

8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
VERSIÓN N°	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO	FUENTE DE VERIFICACIÓN
1	22/02/2024	CREACIÓN DEL DOCUMENTO	Acta N°03 del comité de CGC del 22/02/2024
2	09/04/2025	Modificación del cronograma y el formato del documento	Acta N°05 del comité de CGC del 09/04/2025.

	ELABORÓ	REVISÓ	APROBÓ
FIRMA	ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
	ORIGINAL FIRMADO	ORIGINAL FIRMADO	
NOMBRE	Jose Luis Rojas Bohórquez	Marlon Yohan López Sánchez	Ing. Cristian Andrey Pinto Lozano
	Caroll Johana Muñoz Cortes	Eidi Yuliana Peña León	
	Jenifer Karina Quevedo Velasquez		
CARGO	Profesional 01 sistemas	Director de Planeación	Gerente
	Técnico 04 sistemas	Profesional 01 Gestión de Calidad	
	Profesional de apoyo de sistemas		