POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO: A-GI-POL-004
Versión: 1.0
Fecha de aprobación: 26/12/2024

San José del Guaviare

TABLA DE CONTENIDO

1. INTRODUCCION

Esta política establece las pautas generales que rigen la seguridad de la información dentro de la organización, alineándose con los marcos regulatorios aplicables. Asimismo, busca definir roles y responsabilidades claras para todos los trabajadores y proveedores de la empresa en la protección de los activos de información de la empresa. A través de la implementación de controles de seguridad efectivos, se promueve un entorno seguro que protege la confidencialidad, integridad y disponibilidad de la información, contribuyendo a la confianza de los clientes y al cumplimiento normativo.

ENERGUAVIARE S.A. E.S.P. reconoce que una gestión adecuada de la seguridad de la información es esencial no solo para la protección de sus activos, sino también para respaldar la resiliencia operativa frente a las crecientes amenazas del entorno digital.

2. OBJETIVO

El objetivo de esta política es establecer el marco y lineamientos para la protección de la información y datos de ENERGUAVIARE S.A. E.S.P. y la información de los clientes y usuarios que se encuentra en su poder, mediante la implementación de medidas que ayudan a mantener su **confidencialidad**, **integridad** y **disponibilidad**. Se busca cumplir con las normativas aplicables, gestionar los riesgos de seguridad de la información, y promover la concienciación en todos los niveles de la empresa. Se establece también un enfoque de mejora continua para que el sistema de gestión de seguridad de la información (SGSI) se adapte a los cambios tecnológicos y operacionales, facilitando la confianza y la continuidad de las operaciones.

3. ALCANCE

La política general de seguridad de la Información de ENERGUAVIARE S.A. E.S.P. Se aplica a todos los sistemas, activos de información, procesos y personas que, en el desarrollo de sus actividades, acceden, generan, gestionan y/o almacenan información de la empresa. Esto incluye cualquier formato de información y abarca todos los procesos de la empresa. El alcance de esta política cubre los siguientes aspectos:

- **Usuarios:** Todos los trabajadores de ENERGUAVIARE S.A. E.S.P., proveedores, consultores y terceros que tengan acceso a sistemas y/o activos de información de la empresa.

- **Sistemas de información:** Cualquier software, hardware, aplicaciones, y redes que procesan, transmiten o almacenan información sensible de la empresa.

- **Datos:** Toda la información relacionada con clientes, usuarios, y la propia empresa, independientemente del formato o medio en que se encuentre.

- **Ubicación:** Tanto las instalaciones físicas donde se almacena, gestiona o genera información, como los entornos virtuales utilizados para almacenar y procesar datos.

- **Equipos:** Todo dispositivo, ya sea móvil o de escritorio, que tenga acceso a las redes y sistemas de la empresa o gestione activos de información de la misma. Esto incluye equipos tanto de propiedad de la empresa como de terceros.

- **Normatividad:** Cualquier norma, estándar o requisito legal relacionado con la protección de datos y seguridad de la información, así como todos los planes, procesos, políticas y documentación derivados del Sistema de Gestión de Seguridad de la Información (SGSI).

- **Proveedores y terceros:** Todos los servicios externos y sus proveedores que manejen o tengan acceso a la información de ENERGUAVIARE S.A. E.S.P. en el marco del cumplimiento de sus contratos. Estos actores deben cumplir con los requisitos establecidos en las políticas de seguridad de la información y el SGSI.

4. DEFINICIONES

- **Seguridad de la Información**: Es el conjunto de políticas, procesos y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de la información, minimizando los riesgos de acceso no autorizado, alteraciones y pérdidas.

- **Confidencialidad:** Pretende que la información solo sea accesible para las personas, sistemas o procesos debidamente autorizados. Esto implica la implementación de mecanismos de control de acceso, autenticación y cifrado, entre otros, para evitar que individuos no autorizados accedan a datos sensibles.

- **Integridad:** Se refiere a la protección de la exactitud, coherencia y completitud de la información a lo largo de su ciclo de vida. Es decir, ayuda a que los datos no sean alterados de manera no autorizada, accidental o maliciosa.

- **Disponibilidad:** Tiene por meta que la información esté accesible y utilizable cuando las personas o sistemas autorizados la necesiten. Para facilitar la disponibilidad, se implementan medidas como la redundancia, copias de seguridad, planes de recuperación ante desastres y monitoreo continuo de los sistemas, con estos se pretende evitar interrupciones en el acceso a la información debido a fallos técnicos, ataques o cualquier otro incidente.

- **Tecnologías de la Información (TI)**: Abarcan el conjunto de herramientas, sistemas, hardware y software que facilitan la gestión, procesamiento, almacenamiento y transmisión de la información en un margen aceptable de seguridad, dentro y fuera de la empresa.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Es un marco de políticas y procedimientos que permite gestionar y proteger los activos de información. Se basa en la identificación, evaluación y mitigación de riesgos, y está diseñado para reforzar la **confidencialidad**, **integridad** y **disponibilidad** de la información. El **SGSI** constituye una parte importante de la norma ISO/IEC 27001, la cual establece el marco para su implementación adecuada.

5. DECLARACIÓN DE COMPROMISO

Toda la dirección de ENERGUAVIARE S.A E.S.P. reconoce la importancia de la seguridad de la información como un factor clave para el éxito continuo del negocio, y En consecuencia a esto se compromete a:

- Facilitar los recursos necesarios para el desarrollo, implementación, mantenimiento y mejora continua del SGSI en toda la empresa, brindando el apoyo adecuado para alcanzar los objetivos establecidos.

- Fomentar una cultura organizacional donde la seguridad de la información sea una prioridad, para que todos los trabajadores comprendan su papel y responsabilidad en la protección de los activos de información. Para ello, se llevarán a cabo charlas de concienciación y sensibilización dirigidas a todos los trabajadores, proveedores, terceros y demás partes interesadas, se colaborará para que comprendan las políticas, procedimientos y prácticas de seguridad de la información aplicables a sus funciones.

- Procurar que todas las prácticas de seguridad de la información cumplan con las normativas legales, regulatorias y los estándares internacionales aplicables, como la ISO/IEC 27001 y otras regulaciones sectoriales relevantes, minimizando el riesgo legal y reputacional.
- Establecer y mantener un proceso efectivo para la identificación, evaluación, y tratamiento de riesgos de seguridad de la información, con el objetivo de reducir los riesgos a niveles aceptables para la empresa.

- Participar activamente en la revisión y actualización periódica de la política y del SGSI para que estas sigan siendo eficaces frente a los cambios en el entorno de la empresa, la tecnología y las amenazas a la seguridad.

- Establecer claramente la responsabilidad y rendición de cuentas en todos los niveles de la empresa, desde la alta dirección hasta los trabajadores y terceros, en cuanto a la protección de la información.

6. RESPONSABILIDADES

- **Alta dirección:** Responsable de la revisión y aprobación de las políticas de seguridad de la información. Debe proporcionar los recursos necesarios para su implementación y promover una cultura de seguridad de la información en toda la empresa.

- **Director de seguridad de la información:** Responsable de implementar y supervisar el Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa. Evalúa riesgos de seguridad, propone medidas de mitigación, supervisa su ejecución y coordina la respuesta ante incidentes. Además, mantiene vigilancia sobre amenazas emergentes y promueve la cultura de seguridad mediante sensibilizaciones adecuadas.

- **Usuarios:** Responsables de dar cumplimiento a las políticas implementadas, proteger los activos de información con los que interactúan directamente en sus respectivos puestos de trabajo, reportar cualquier incidente de seguridad en el que se vean implicados y/o aquellos que presencian en su entorno.

- **Terceros:** Proveedores y consultores deben cumplir con las normativas y políticas de la empresa en cuanto a seguridad de la información, proteger los activos de información de ENERGUAVIARE S.A E.S.P. a los que tenga acceso, según contrato, dar aviso de los incidentes de seguridad que ocurran dentro de sus respectivas entidades, que puedan afectar a ENERGUAVIARE S.A E.S.P.

- **Toda la empresa:** La seguridad de la información es una responsabilidad compartida. Los cargos y roles establecidos dentro del marco del SGSI actúan como facilitadores, proporcionando lineamientos claros a los que todos deben adherirse para lograr un estándar de seguridad aceptable.

7. PRINCIPIOS GENERALES

ENERGUAVIARE S.A. E.S.P. Establece como principio fundamental de ciberseguridad la preservación de la confidencialidad, integridad y disponibilidad de sus datos e información. Esto implica:

- **Confidencialidad:** La información sensible será accesible únicamente a las personas autorizadas. Se implementarán controles de acceso, como autenticación multifactor y políticas de clasificación de datos, para proteger la privacidad de la información.

- **Integridad:** La precisión y completitud de la información son esenciales. Para mantener la integridad de los datos, se llevarán a cabo auditorías regulares y se utilizarán herramientas de detección para identificar y prevenir alteraciones no autorizadas.

- **Disponibilidad:** Se procurará que los sistemas y datos estén disponibles para los usuarios autorizados en todo momento. Esto incluye la implementación de soluciones de respaldo y recuperación ante desastres, así como la realización de pruebas periódicas de continuidad del negocio.

- **Actualización y Mantenimiento:** La ciberseguridad requiere una revisión constante. Se realizarán evaluaciones periódicas de vulnerabilidades y se mantendrá la infraestructura de TI actualizada con los últimos parches de seguridad.

- **Cumplimiento Normativo:** ENERGUAVIARE S.A. E.S.P. se compromete a cumplir las leyes y regulaciones aplicables en materia de ciberseguridad, así como a alinearse con estándares internacionales como la ISO/IEC 27001. Se llevarán a cabo auditorías para evaluar esta conformidad.

- **Conciencia y Responsabilidad Compartida:** La seguridad de la información es responsabilidad de todos en la empresa. Se fomentará una cultura de seguridad mediante capacitaciones y campañas de concienciación, estableciendo roles claros y promoviendo la participación activa en la identificación y reporte de incidentes de seguridad.

A través de estos principios, ENERGUAVIARE S.A. E.S.P. busca implementar la protección de su información y la continuidad de sus operaciones, enfrentando proactivamente los desafíos en el ámbito de la ciberseguridad.

8. DESARROLLO DE LA POLÍTICA

La política general de seguridad de la información de ENERGUAVIARE S.A E.S.P. Está integrada por el compromiso de la alta dirección, los principios de seguridad de la

información, el compendio de demás políticas complementarias, planes, procedimiento y demás documentación derivados de estas.

La política general de seguridad de la información de ENERGUAVIARE S.A E.S.P. tendrá como principio los tres pilares de la seguridad de la información (Integridad, confidencialidad, disponibilidad), procurando el cumplimiento de estos para mantener la seguridad de sus activos de información, para ello implementándose de la siguiente manera:

- Monitorear el uso y la vida útil de los activos de información, procurando que se utilicen de manera adecuada y responsable, de acuerdo con los lineamientos establecidos para las actividades de los respectivos procesos.

- Se establecen niveles de criticidad a la información y acorde a estos se implementan controles de seguridad para proteger toda información generada, gestionada, almacenada y/o transferida en los procesos de negocio e infraestructura tecnológica, de cualquier posible riesgo.

- Implementar y mantener controles de acceso físico a instalaciones donde se llevan a cabo procesos críticos y/o que resguardan en su interior activos críticos de la empresa.

- Implementar otras medidas y controles de seguridad física con las cuales controlar el entorno de información.

- Implementar controles sobre los procesos para procurar la seguridad de los recursos de la empresa, así como sus redes de datos.

- Establecer y mantener programas de concienciación de seguridad de la información, repitiéndolos cíclicamente, procurando que llegue a cada uno de los trabajadores, proveedores que prestan sus servicios en las instalaciones, terceros, colaboradores y demás interesados.

- Promover buenas prácticas de seguridad de la información, y aplicar políticas y análisis de seguridad con las cuales integrar la seguridad como parte de los procesos empresariales.

- Establecer procedimientos de copias de seguridad, aplicarlos, y validar el proceso de restauración.

- Mantener una mejora continua en el modelo de seguridad mediante la Gestión adecuada de vulnerabilidades, riesgos e incidentes, revisando las posibles actualizaciones que puedan tener estos al día.

- Diseñar e implementar planes y/o procesos que establezcan la continuidad y disponibilidad operativa del negocio basándose en el impacto de los posibles eventos e incidentes de seguridad.

- Poner a prueba los controles y políticas establecidas de forma periódica. Este junto a los dos puntos anteriores ayudarán a establecer, mantener y fortalecer la resiliencia de la empresa ante situaciones adversas.

- Elaborar planes de respuesta organizados que definan claramente los diferentes roles y sus respectivas responsabilidades frente a posibles incidentes de seguridad de la información.

- Dar cumplimiento a toda obligación legal, regulatoria, normativa y contractual establecida.

8.1. POLÍTICAS DERIVADAS DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

- **Política sobre el uso de controles criptográficos:** Esta política establece el uso de controles criptográficos para proteger la información sensible de la empresa.

- **Política de escritorio limpio y pantalla limpia:** Esta política promueve el mantener un escritorio libre de papeles y unidades extraíbles.

- **Políticas y procedimientos de transferencia de información:** Establece un marco de seguridad y controles formales para la transferencia de información a través de cualquier medio y/o instalación de comunicaciones.

- **Políticas de desarrollo seguro:** Establece reglas para el desarrollo de software y sistemas para los desarrollos internos de la empresa.

- **Política de seguridad de la información para las relaciones con proveedores:** Establece un marco y requisitos de seguridad de la información pertinentes a las elaciones y accesos de proveedores y los riesgos que esto conlleva.

- **Política de gestión de vulnerabilidades, riesgo de seguridad y gestión de incidentes de seguridad de la información:** Esta política define el proceso para identificar, evaluar y elaborar planes para mitigar los riesgos de seguridad de la información.

- **Política de seguridad para la gestión de credenciales:** Establece un marco para la creación, distribución, uso y gestión de credenciales, como lo son usuarios, contraseñas, certificados, etc.

- **Política de continuidad del negocio y plan de contingencia:** Esta política establece lineamientos para que la empresa pueda mantener sus operaciones incluso en caso de interrupciones graves, como desastres naturales, ciberataques o fallos de sistemas.

- **Política de concienciación y formación en seguridad:** Esta política promueve la educación y la concienciación sobre seguridad de la información entre los trabajadores.

- **Política de cumplimiento legal y normativo:** Esta política procura que la empresa cumpla con todas las leyes, regulaciones y estándares relacionados con la seguridad de la información.

- **Política de gestión de activos de la información**: Esta política establece cómo se identifican, clasifican, protegen y gestionan los activos de información de la empresa.

- **Política de seguridad física, electrónica y control de accesos:** Esta política define quién tiene acceso a qué información y bajo qué condiciones. Incluye la autenticación de usuarios, y control de acceso lógico, las medidas de seguridad

física y otros controles que deben implementarse para proteger los activos de información de la empresa.

- **Política de respaldo y recuperación de datos:** Establece lineamientos para realizar y almacenar las copias de seguridad de datos críticos de la empresa.
- **Política de uso aceptable y responsable de recursos de TI:** Establece las pautas para el uso apropiado de los recursos de TI.

9. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

El cumplimiento y la eficacia de esta política se evaluarán periódicamente a través de auditorías internas y revisiones por la alta dirección. Se realizarán ajustes, cuando sea necesario, para adaptarse a los cambios tecnológicos, regulatorios o de amenaza.

Adicionalmente, a final de año se llevará a cabo una revisión de la política y el SGSI verificar su efectividad y su vigencia, con respecto a la normatividad y legal establecida, además de los controles internos pertinentes

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
VERSIÓN N°	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**	**FUENTE DE VERIFICACIÓN**
1	26/12/2024	Creación del documento	Acta N°14 del Comité de CGC del 26/12/2024

	ELABORÓ	**REVISÓ**	**APROBÓ**
FIRMA	ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
		ORIGINAL FIRMADO	
		ORIGINAL FIRMADO	
NOMBRE	José Luis Rojas Bohórquez	Marlon Yohan López Sanches	Ing. Cristian Andrey Pinto Lozano
		Finia Janeth Useche Niño	
		Eidi Yuliana Peña León	
CARGO	Profesional 01 de Sistemas	Director de Planeación	Gerente
		Subgerente Administrativa	
		Profesional 01 Gestión de Calidad	