POLÍTICA DE CONCIENCIACIÓN Y FORMACIÓN EN SEGURIDAD

CÓDIGO: A-GI-POL-003
Versión: 1.0
Fecha de aprobación: 26/12/2024

San José del Guaviare

TABLA DE CONTENIDO

1. INTRODUCCION

En ENERGUAVIARE S.A. E.S.P. como empresa dedicada a la distribución y comercialización de energía, entendemos que la seguridad es un aspecto esencial para el éxito y la sostenibilidad de nuestras operaciones. En un sector que enfrenta desafíos significativos en cuanto a la protección de infraestructuras críticas, la seguridad de nuestros datos y el cumplimiento de normativas resulta indispensable que todos los integrantes de nuestra organización participen activamente en el fortalecimiento de una cultura de seguridad sólida.

La Política de Concienciación y Formación en Seguridad, busca promover la sensibilización y el conocimiento a nuestros trabajadores, proveedores y demás involucrados sobre los riesgos asociados a nuestras actividades y establecer medidas preventivas que minimicen dichos riesgos. La concienciación y la formación continua les permite comprender la importancia de sus roles individuales en la protección de la empresa, adoptando medidas de seguridad que van desde el uso adecuado de contraseñas hasta la identificación de correos electrónicos sospechosos y la protección de la información sensible, para evitar conductas que puedan comprometer la seguridad y confiabilidad de la empresa.

2. OBJETIVO

Esta política tiene como objetivo asegurar que todo trabajador, proveedor, terceros y demás involucrados conozcan, entiendan y cumplan las normas y controles de seguridad implementados en el SGSI de ENERGUAVIARE S.A E.S.P. y respondan ante posibles amenazas y vulnerabilidades presentes en su entorno de trabajo, sino también la información y el servicio que brindamos a nuestros clientes.

Para ello, esta política se enfoca en:

- **Capacitar a los trabajadores** para que identifiquen, comprendan y respondan adecuadamente a posibles amenazas y riesgos asociados a las actividades de Energuaviare S.A. E.S.P.
- **Fomentar el cumplimiento** de las normas de seguridad y los protocolos de respuesta ante incidentes, garantizando la integridad y la continuidad de nuestro servicio.
- **Reducir el riesgo de incidentes de seguridad** a través de prácticas preventivas y correctivas, minimizando el impacto de posibles amenazas para nuestros colaboradores, clientes y comunidades.

- **Fortalecer el compromiso con el cumplimiento normativo** y las mejores prácticas de seguridad en el sector energético, alineándonos con los estándares nacionales e internacionales aplicables.

3. ALCANCE

La **Política de Concienciación y Formación en Seguridad** de **Energuaviare S.A. E.S.P.** aplica a todos los niveles de la empresa, incluyendo a trabajadores, contratistas, proveedores y terceros que interactúan con los sistemas, instalaciones y datos de la empresa. Su propósito es brindarle a todos los involucrados que conozcan, comprendan y apliquen los principios y prácticas de seguridad necesarios para proteger a la empresa, sus activos y el servicio continuo.

Este alcance incluye:

- **Empleados de Energuaviare:** Todo el personal debe participar en los programas de formación y concienciación en seguridad, independientemente de su cargo o responsabilidad. Esto garantiza que todos los colaboradores estén capacitados para identificar y responder a riesgos de seguridad física y cibernética.
- **Contratistas y Proveedores**: Todo contratista o proveedor que tenga acceso a las instalaciones, sistemas o datos de Energuaviare está sujeto a esta política y debe cumplir con las directrices de seguridad establecidas, para la protección y la integridad de la infraestructura energética.
- **Sistemas y Procesos Críticos**: La política abarca todos los sistemas de información, activos y procesos operativos esenciales para la distribución y comercialización de energía, con el fin de minimizar riesgos y mantener la continuidad del servicio.
- **Toda la Infraestructura Operativa y Digital**: Incluye los entornos físicos y digitales que sostienen las operaciones de Energuaviare, desde redes informáticas hasta instalaciones energéticas. Se establecen controles de seguridad para proteger estos activos y prevenir accesos no autorizados o incidentes.
- **Actividades de Formación Continua**: La política abarca todos los programas de capacitación, simulacros y campañas de concienciación en seguridad, garantizando que todos los actores conozcan las amenazas actuales y las prácticas de mitigación.

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.
- **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.

5. DECLARACIÓN DE COMPROMISO

ENERGUAVIARE S.A. E.S.P. se compromete a proporcionar los medios y recursos para realizar las actividades de concienciación a fin de mantener informados y consientes a todo individuo que se involucre en las actividades y procesos de la empresa, interactuando con sus activos de información o con información y datos de sus clientes y usuarios.

Este compromiso se extiende a los trabajadores, terceros, proveedores y demás involucrados, para ser partícipes en cada una de las actividades de concienciación que la oficina de gestión informática estará llevando a cabo con el objetivo de seguridad de la información.

6. RESPONSABILIDADES

6.1. Alta Dirección

- Respaldar con compromiso la política de concienciación y formación en seguridad de la información.
- Proveer los recursos necesarios para el desarrollo de programas de concienciación y capacitación.
- Fomentar una cultura de seguridad de la información desde los niveles más altos de la organización.

6.2. Director de Seguridad de la Información

- Diseñar, implementar y mantener el programa de concienciación y formación en seguridad de la información.
- Identificar las necesidades de formación en seguridad para todos los empleados y ajustando los programas a estas necesidades.
- Coordinar las actividades de concienciación y formación, procurando una periodicidad y actualización constante.

6.3. Recursos Humanos

- Integrar la sensibilización en seguridad de la información en los programas de inducción y capacitación continua.
- Colaborar con el Director de seguridad de la información para registrar y verificar la participación de los empleados en las actividades de formación.
- Incorporar los requisitos de concienciación en las evaluaciones de desempeño, cuando corresponda.

6.4. Líderes de proceso

- Procurar e incentivar que los trabajadores bajo su supervisión participen en los programas de concienciación y formación.
- Actuar como modelos de buenas prácticas en seguridad de la información y motivar a sus equipos a seguir estas prácticas.
- Colaborar en la detección de brechas de conocimiento en seguridad y sugerir temas para futuras capacitaciones.

6.5. Usuario informado

- Participar activamente en las actividades de formación y concienciación en seguridad de la información.

- Cumplir con las prácticas de seguridad establecidas y reportar cualquier incidente o anomalía detectada.
- Mantenerse informado sobre las políticas, procedimientos y prácticas de seguridad de la información aplicables a sus funciones.

6.6. Equipo de gestión informática

- Apoyar en la difusión de las políticas y buenas prácticas de seguridad de la información a través de la infraestructura tecnológica.
- Colaborar con el Oficial de Seguridad de la Información en el diseño y distribución de contenidos formativos (como simulaciones de ataques, phishing, etc.).
- Monitorear y reportar el cumplimiento de las prácticas de seguridad en el uso de sistemas y aplicaciones de la organización.

7. DESARROLLO DE LA POLÍTICA

- El equipo de gestión informática de ENERGUAVIARE S.A. E.S.P., con el aval de la alta dirección, determina el **programa de concienciación en seguridad de la información,** a fin de generar, adquirir, divulgar y fortalecer continuamente una cultura de seguridad y privacidad de la información en todas los trabajadores, proveedores y demás involucrados.
- La charlas y concienciaciones se llevarán a cabo con una periodicidad mensual, dividiendo los temas en ciclos de seis meses, evitando saturar a los usuarios en una sola charla.
- Los nuevos trabajadores deberán recibir sensibilización de seguridad de la información como parte del proceso de inducción dentro de los primeros 30 días de su incorporación. Esta se brindará a través de material didáctico, y una evaluación que tendrá el fin de medir y conocer las necesidades y áreas de refuerzo del trabajador que ingresa.
- El personal que opera activos críticos e información sensible de la empresa debe recibir capacitación adicional específica.
- Se realizarán evaluaciones al término de cada actividad de concienciación y él programas de concienciación y adaptar los contenidos según las necesidades detectadas.
- Implementar un recurso de comunicación a través del cual se debe dar a conocer toda información relacionada con ciberseguridad, y el SGSI. A través de este sistema se deben publicar todas las políticas, procedimientos, protocolos y demás concerniente a dar cumplimiento a la normatividad para todos los trabajadores.
- Se promoverán campañas periódicas de concienciación mediante emails, boletines, posters, y presentaciones sobre temas de actualidad en seguridad de la información.
- Los usuarios recibirán alertas y recordatorios sobre buenas prácticas en seguridad y cualquier amenaza emergente, como campañas de phishing, de manera oportuna.
- Mantener informados a todos los trabajadores y proveedores que presten sus servicios dentro de las instalaciones de la empresa, sobre cambios y actualizaciones relacionados con controles de seguridad y políticas del SGSI.
- Realizar actividades de revisión, gestión y auditorias de forma periódica a fin de medir resultados de la implementación del programa de concienciación de seguridad de la información
- Se llevarán a cabo simulaciones como pruebas de phishing, falso hackeo, etc. para evaluar la respuesta de los empleados ante posibles amenazas.
- Los resultados de estas simulaciones serán anónimos y utilizados para identificar áreas de mejora en la concienciación y sensibilización.

- La participación en las actividades de formación y cumplimiento de esta política es obligatoria para todos los usuarios.
- El incumplimiento de esta política, o la participación en prácticas inseguras, podrá ser sujeto a medidas disciplinarias conforme a las políticas de recursos humanos y las leyes aplicables.

8. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

Esta política será revisada y actualizada anualmente o cuando se identifiquen cambios significativos en el entorno de amenazas y/o leyes y normatividad aplicables. Todos los cambios serán comunicados a los trabajadores y se reflejarán en los materiales de formación y concienciación.

9. 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	ORIGNAL FIRMADO ORIGINAL FIRMADO	ORIGINAL FIRMADO
NOMBRE	José Luis Rojas Bohórquez	Marlon Yohan López Sanches Eidi Yuliana Peña León	Ing. Cristian Andrey Pinto Lozano
CARGO	Profesional 01 de Sistemas	Director de Planeación Profesional 01 Gestión de Calidad	Gerente