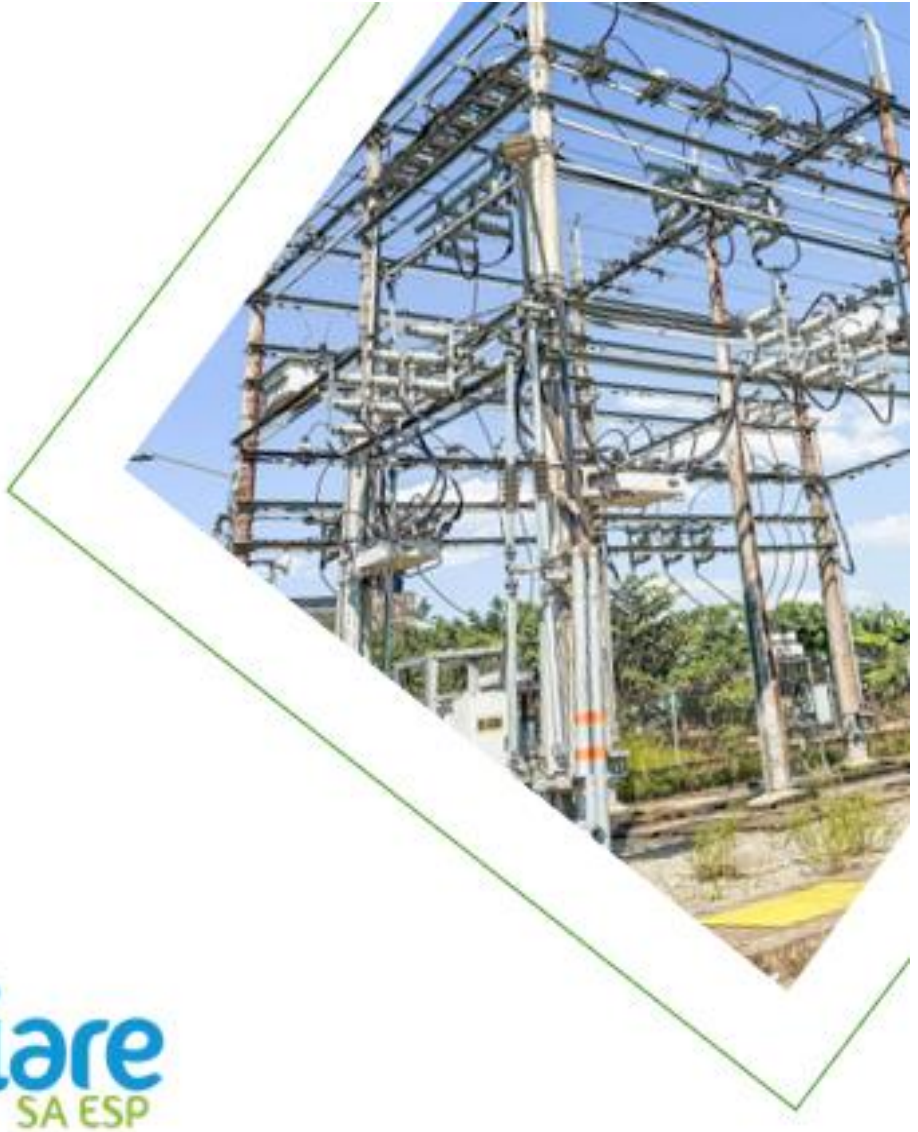

Energuaviare SA ESP

PROGRAMA DE CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO: A-GI-PG-001
Versión:
Fecha de Aprobación: 26/12/2024

San José del Guaviare

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento establece el programa de concienciación de seguridad de la información para ENERGUAVIARE S.A E.S.P. Este programa surge en respuesta a la creciente necesidad de sensibilizar y capacitar a todos los trabajadores sobre la importancia de mejorar las prácticas y medidas de seguridad de la información.

La seguridad de la información es un aspecto fundamental en la operación de cualquier empresa, especialmente en un entorno donde las amenazas cibernéticas son cada vez más sofisticadas y persistentes. En este sentido, el objetivo principal del programa es crear una fuerza laboral consciente y capacitada que contribuya activamente a proteger los activos de información crítica de la empresa contra posibles amenazas.

Este programa no solo busca reducir los riesgos de seguridad mediante la educación de los trabajadores sobre las amenazas y cómo prevenirlas, sino que también aspira a promover una mentalidad de seguridad donde todos los trabajadores comprendan que la seguridad es responsabilidad de todos y se sientan empoderados para reportar incidentes de seguridad o cualquier otro posible problema.

A lo largo de este documento, se detallan los objetivos del programa, así como las estrategias y actividades específicas que se llevarán a cabo para lograrlos. Se abordan aspectos como la concienciación, educación y capacitación en seguridad de la información, la responsabilidad de los trabajadores, los procedimientos y controles básicos de seguridad, entre otros.

Además, se establecen métodos de evaluación y seguimiento para medir la efectividad del programa, se asignan recursos y responsabilidades, se describen estrategias de comunicación y divulgación, y se delinean procesos de mejora continua para asegurar que el programa evolucione de manera adaptativa según las necesidades de la empresa y las nuevas amenazas de seguridad.

En resumen, el Programa de Concienciación de Seguridad de la Información de ENERGUAVIARE S.A E.S.P. es una iniciativa integral diseñada para proteger los activos de información de la empresa y fortalecer su postura de seguridad en un entorno cada vez más digital y dinámico.

2. OBJETIVOS

El objetivo del programa de concienciación de la seguridad de la información es sensibilizar y capacitar a todos los trabajadores de ENERGUAVIARE S.A E.S.P. sobre la importancia de mejorar las prácticas y medidas de seguridad de la información, para que así con su comportamiento, logren aportar a proteger los activos de información de la empresa. Mediante la implementación de este programa se pretende:

- Crear una fuerza laboral consciente y capacitada que pueda ayudar a proteger los activos de información crítica de ENERGUAVIARE S.A E.S.P. contra amenazas de seguridad de la información.
- Reducir los riesgos de seguridad mediante la educación de los trabajadores sobre las amenazas y cómo prevenirlas.
- Ayudar a los trabajadores a comprender la importancia de proteger la información confidencial de la empresa.
- Promover una mentalidad de seguridad de la información donde todos los trabajadores comprendan que la seguridad es responsabilidad de todos y se sientan empoderados para reportar incidentes de seguridad o cualquier otro posible problema.
- Lograr la capacidad en los trabajadores para reconocer y evitar caer en ataques de ingeniería social.

3. CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

3.1. Compromiso

En ENERGUAVIARE S.A E.S.P., priorizamos la seguridad de la información de la empresa en todo momento. Estamos comprometidos a implementar y mantener rigurosos estándares y protocolos de seguridad, así como a fomentar una cultura organizacional que valore la protección y confidencialidad de los datos. Conscientes de la importancia estratégica de la información, dedicamos recursos significativos para fortalecer continuamente las defensas cibernéticas y salvaguardar la integridad de los activos de la compañía. Este compromiso se refleja en cada nivel de la empresa, desde la alta dirección hasta cada trabajador, quienes asumen la responsabilidad compartida de preservar la seguridad de los sistemas y datos.

3.2. Necesidad de conocer y cumplir la normatividad de seguridad de la información

3.2.1. Contexto

En el último año en San José del Guaviare se han intensificado los ataques phishing y de ingeniería social, afectando varias empresas e instituciones estructural y económicamente, dejando en evidencia que las medidas de seguridad, así como el nivel de conciencia de los ciudadanos actualmente son insuficientes, y dichos ciudadanos son parte del plantel de trabajadores de esta empresa.

En tan solo un día, el sistema de firewall de ENERGUAVIARE S.A E.S.P. ha bloqueado más de 5.150.130 amenazas de las cuales alrededor de 300 eran de alta criticidad, lo cual es bueno para la empresa, pero actuando bajo el pensamiento de incertidumbre como es esperado por el sistema de calidad de la empresa, hay que pensar siempre bajo el criterio de la posibilidad en que los atacantes encuentren el modo de pasar estas defensas. Por ende, es requerido que los trabajadores de ENERGUAVIARE S.A E.S.P. se encuentren en capacidad de discernir cuando aquellos activos de información con los que interactúan en sus respectivas actividades se encuentran en riesgo.

Además, el anterior caso solo está tomando un tipo entre las muchas posibles amenazas externas. Hay que tener en cuenta que una de las amenazas más grandes que pueden tener los activos de información es

interna y esta es la falta de capacidad y conocimiento de los trabajadores con respecto a la seguridad de la información.

3.2.2. Marco legal y normativo

Dentro del enfoque legal y normativo encontramos fundamental la protección y la privacidad de los datos, construir la confianza del cliente, prevenir ciberataques, gestionar riesgos y evitar consecuencias legales y de reputación adversas para la empresa.

Estos criterios atienden a lo establecido según la normatividad y política a nivel nacional e internacional como lo es el caso de la ley 1582 del 2012 a nivel nacional o el GDRP a nivel internacional, las cuales dictan las regulaciones para la protección de datos personales, la norma ISO IEC 27001 que proporciona a nivel internacional el marco normativo para los sistemas de gestión de seguridad de la información, etc.

Cuando los trabajadores de la empresa son plenamente conscientes sobre el marco legal y normativo respectivo a sus actividades y puestos de trabajo estos gestionan con mayor eficiencia los activos de información con los que interactúan, y esto se refleja en menores posibilidades de caer en incidentes de seguridad de la información, lo cual a su vez reduce posibles problemas legales con clientes y terceros, además de mantener resguardada la economía de la empresa desde otros ámbitos.

El incumplimiento de las normativas de seguridad de la información puede resultar en sanciones legales y daños a la reputación de la empresa a nivel nacional como internacional.

3.3. Responsabilidad

Cada trabajador es responsable del/los activos de información vinculados a sus respectivas actividades y puestos de trabajo, así como de una adecuada gestión de los mismos. Debemos ser conscientes que cada acción u omisión ejercida sobre dichos activos no solo va a repercutir sobre el activo en cuestión, sino también sobre toda la empresa por ende cada trabajador está en la obligación de actuar de manera ética, profesional y conforme a las políticas y procedimientos establecidos.

Cada uno en su puesto de trabajo es responsable de salvaguardar la información confidencial de la empresa, así como de terceros, con los que se vea involucrado, implementando para ello medidas de seguridad adecuadas para prevenir accesos no autorizados, pérdidas, robos o

filtraciones de información. Los trabajadores deben entender la importancia de proteger esta información y cumplir con las políticas de seguridad establecidas por la empresa, incluyendo el manejo adecuado de contraseñas, la protección de dispositivos y redes, y la sensibilización sobre posibles amenazas cibernéticas.

3.4. Procedimientos y controles básicos de seguridad de la información

Responde a aquellos procedimientos y controles del SGSI que requieren ser conocidos por todos o la mayoría de los trabajadores en la empresa.

- Reconocimiento de amenazas y vulnerabilidades.
- Políticas de seguridad de la información.
- Roles y responsabilidades del SGSI.
- Uso adecuado de activos de información.
- Escritorio limpio, pantalla limpia.
- Transferencia de información.
- Dispositivos móviles y teletrabajo.
- Restricción y uso de software.
- Copias de seguridad.
- Transferencia de información.
- Reconocimiento de correos maliciosos.
- Protección de software malicioso.
- Privacidad de credenciales.
- Privacidad y protección de la información.
- Reporte de incidentes de seguridad de la información.
- Control de medios transitorios
- Concienciación y capacitación
- Identificación de activos de información

3.5. Formación especifica

- **Identificación y clasificación de activos de información:** Capacitar a los miembros del equipo de Gestión Informática, para que sean personas competentes en la identificación de activos de información críticos de la empresa, así como clasificarlos adecuadamente según su importancia y sensibilidad.
- **Evaluación de riesgos:** Capacitación en técnicas para identificar, evaluar y gestionar los riesgos de seguridad de la información,

incluyendo la realización de análisis de riesgos y la selección de controles adecuados.

- **Principios de la ISO 27001:** Entender los requisitos y principios de la norma ISO 27001, incluyendo el contexto de la organización, el liderazgo, la planificación, el soporte, la operación, la evaluación del desempeño y la mejora continua.
- **Conciencia en cumplimiento normativo:** Entender las leyes y regulaciones relevantes relacionadas con la seguridad de la información, así como los requisitos contractuales y de clientes en materia de seguridad de datos.
- **Políticas y procedimientos de seguridad:** Conocimiento de las políticas y procedimientos de seguridad de la información de la empresa, incluyendo el acceso a los sistemas, el manejo de datos sensibles, la protección contra malware, entre otros.
- **Gestión de incidentes de seguridad:** Capacitación sobre cómo detectar, reportar y responder a incidentes de seguridad de la información de manera adecuada, incluyendo la comunicación con el equipo de respuesta a incidentes y la documentación de las acciones tomadas.
- **Conciencia en seguridad física:** Capacitación sobre la importancia de proteger físicamente los activos de información, incluyendo el acceso a las instalaciones y la protección de equipos y dispositivos.
- **Conciencia en seguridad en la cadena de suministro:** Entender los riesgos asociados con los proveedores y socios comerciales, así como las medidas para mitigar estos riesgos en la seguridad de la cadena de suministro.
- **Controles de SOA/Estado de Disponibilidad:** Socializar con los miembros del equipo de gestión informática, para que estén en la capacidad de identificar los controles aplicables según el contexto de la empresa
- **Auditorías internas:** Capacitación sobre cómo realizar auditorías internas para evaluar el cumplimiento del SGSI con los requisitos de la norma ISO 27001 y detectar áreas de mejora.

4. CRONOGRAMA DE CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Este cronograma detalla las actividades programadas para la concienciación y capacitación en seguridad de la información a lo largo del año. Las actividades se programan semestral y anualmente; se ajustan según las necesidades de los diferentes procesos de la empresa. El objetivo es asegurar una capacitación continua y adaptativa que aborde las necesidades emergentes y los cambios en el panorama de la seguridad de la información.

CRONOGRAMA DE CONCIENTIZACIÓN DE SEGURIDAD DE LA INFORMACION					
N.	**CONCIENCIACIÓN**	**TIPO DE ACTIVIDAD**	**METODOLOGIA**	**A QUIEN VA DIRIGIDO**	**FECHA**
1	Roles y responsabilidades del SGSI	Capitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se dará a conocer el instructivo de roles y responsabilidades del SGSI	Todo el personal de la empresa/Por área	24-05-2024
2	Reconocimiento de correos maliciosos.	Capacitación virtual	Por medio de una charla con apoyo visual de presentaciones PowerPoint se les indicara como reconocer los correos maliciosos	A todo el personal de la empresa	24-05-2024
3	Privacidad de credenciales.	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint dentro de una charla virtual se les socializara la privacidad de credenciales para la seguridad de la información de la empresa	A todo el personal de la empresa	24-05-2024
4	Identificación de activos de información	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les concienciara sobre los activos de información de sus puestos de trabajo.	Personal de planta	24-05-2024
5	Identificación y clasificación de activos de información	Charla/Capacitación	Se realizará una capacitación al equipo de gestión informática, sobre identificación y clasificación de activos de información, con base a la metodología maguerit.	Gestión Informática	24-05-2024
6	Principios de la ISO 27001	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les dará a conocer los principios de la ISO 27001 S.G.S.I.	Por área/Por proceso	24-05-2024
7	Conciencia en cumplimiento normativo	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les indicara la importancia de tomar conciencia en el cumplimiento normativo del S.G.S.I.	Por área/Por proceso	24-05-2024

8	Conciencia en seguridad física	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les indicara la importancia de tomar conciencia en seguridad física de la información	Por área/Por proceso	24-05-2024
9	Participación, concienciación y capacitación	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les indicara la importancia de participar en los programas de concienciación y capacitación del S.G.S.I.	Todo el personal de la empresa/Por área	24-05-2024
10	Reconocimiento de amenazas y vulnerabilidades.	Capitación virtual	Mediante una charla virtual con apoyo visual de presentaciones PowerPoint, se indicará como reconocer las posibles vulnerabilidades y cuales amenazas afectan los activos de información y finalizando se realizará una actividad reforzando lo anteriormente visto	A todo el personal de la empresa	25-06-2024
11	Uso adecuado de activos de información (Política de uso aceptable y responsable de recursos TI)	Capitación virtual	Mediante una charla virtual con apoyo visual de presentaciones PowerPoint, se indicará como realizar un buen uso de los activos de información	Por área/Por proceso	19-12-2024
12	Restricción y uso de software y hardware.	Capitación virtual	Mediante una charla virtual con apoyo visual de presentaciones PowerPoint, se les indicara que software es permitido en las instalaciones y equipos de la empresa y cuáles deben ser evitados.	Por área/Por proceso	19-12-2024
13	Transferencia de información.	Capitación virtual	Mediante una charla virtual con apoyo visual de presentaciones PowerPoint, se les advertirá como llevar a cabo la transferencia de información de forma segura	A todo el personal de la empresa	19-12-2024
14	Reporte de incidentes de seguridad de la información.	Charla y actividad lúdica	Mediante una charla virtual con apoyo visual de presentaciones PowerPoint, se les informara como reportar alguna incidencia de S.I. que se presente y finalizando se desarrollara una actividad donde se evidencia lo anteriormente mencionado	A todo el personal de la empresa	19-12-2024
15	Copias de seguridad.	Socialización	Con la ayuda de folletos se socializará como generar copias de seguridad en sus dispositivos de trabajo, así como su importancia.	Por área/Por proceso	19-12-2024
16	Escritorio limpio, pantalla limpia.	Socialización	A través de infografías se socializará como el buen manejo y limpieza del sitio de trabajo puede agilizar las actividades, a su vez el tener la pantalla limpia genera una mayor visibilidad del equipo de trabajo, con el fin de evitar abrumarse en caso de incidencias	A todo el personal de la empresa	19-12-2024
17	Dispositivos móviles y teletrabajo	Socialización	A través de infografías se socializará las regulaciones del uso de dispositivos móviles y teletrabajo en la empresa.	A todo el personal de la empresa	19-12-2024

18	Control de medios transitorios	Socialización	A través de infografías se socializará la política mediante la cual se anula los medios transitorios para evitar riesgos de S.I.	A todo el personal de la empresa	19-12-2024
19	Políticas y procedimientos de seguridad de la información	Socialización	Con la ayuda de folletos se socializará las políticas y procedimientos de S.I.	Por área/Por proceso	19-12-2024
20	Protección de software malicioso.	Simulacro	Se llevará a cabo un Simulacro de ciberseguridad	A todo el personal de la empresa	19-12-2024
21	Privacidad y protección de la información	Simulacro	Se llevará a cabo un Simulacro de ciberseguridad	A todo el personal de la empresa	19-12-2024
22	Evaluación de riesgos	Charla/Capacitación metodología del diamante	Se realizará una capacitación al equipo de gestión informática, sobre evaluación de riesgos, con base a la metodología del diamante	Gestión Informática	20-12-2024
23	Controles de SOA-Estado de disponibilidad	Charla y publicación	Se realizará una socialización al equipo de gestión informática, sobre los Controles de SOA aplicable en el S.G.S.I. de la empresa definidos en el **Anexo A** de la Norma ISO 27001-2013.	Gestión Informática	20-12-2024
24	Gestión de incidentes de seguridad	Capacitación virtual	Se realizará una charla virtual con apoyo visual de presentaciones PowerPoint, donde se les informará cómo reaccionar ante un incidente de seguridad informática.	Gestión Informática / Propietarios de activos	20-03-2025
25	Conciencia en seguridad en la cadena de suministro	Capacitación virtual	Se realizará una charla virtual con apoyo visual de presentaciones PowerPoint, se les socializará la importancia de tomar conciencia en seguridad en la cadena de suministros	Subgerencias	24-04-2025
26	Auditorías internas	Capacitación virtual	Por medio de una charla virtual con apoyo visual de presentaciones PowerPoint se les socializara la realización de auditorías internas del S.G.S.I. y su responsabilidad, según su Rol.	Por área / Por proceso	20-06-2025

Cronograma de Concienciación de Seguridad de la Información

4.1. Revisión y Ajuste del Cronograma

El cronograma se revisará periódicamente para asegurar que las actividades de capacitación se mantengan relevantes y efectivas. Se podrán realizar ajustes según los comentarios de los trabajadores, cambios en el entorno de amenazas y nuevos requisitos legales o normativos. La evaluación continua y la retroalimentación son fundamentales para mantener un programa de concienciación en seguridad de la información que evolucione con las necesidades de la empresa.

4.2. Almacenamiento y Acceso del Documento

El cronograma de concienciación de seguridad de la información se encuentra almacenado en la unidad de Google Drive del dominio de la oficina de gestión informática de ENERGUAVIARE S.A E.S.P. Este documento está organizado y tratado por el equipo de gestión informática, asegurando que se mantengan actualizados y accesibles para los trabajadores autorizados.

5. MÉTODOS DE EVALUACIÓN Y SEGUIMIENTO

Para asegurar la efectividad del programa de concienciación de seguridad de la información de ENERGUAVIARE S.A E.S.P., se implementarán los siguientes métodos de evaluación y seguimiento. Estos métodos permitirán medir el impacto de las actividades de concienciación, identificar áreas de mejora y ajustar el programa según sea necesario para una efectiva protección continua de los activos de información de la empresa.

5.1. Encuestas

Realizar encuestas periódicas es una de las estrategias clave para medir el nivel de comprensión y concienciación de los trabajadores sobre la seguridad de la información. Estas encuestas se diseñarán de manera que cubran los diversos aspectos del programa de concienciación, incluyendo la identificación de amenazas, políticas de seguridad, y procedimientos específicos.

5.2. Pruebas de conocimiento

Implementar pruebas de conocimiento es crucial para evaluar la retención de la información impartida durante las sesiones de capacitación. Estas pruebas permitirán medir no solo la comprensión inmediata de los trabajadores, sino también su capacidad para aplicar los conceptos aprendidos en su trabajo diario.

5.3. Análisis de incidentes

El análisis de los incidentes de seguridad reportados es una herramienta fundamental para identificar áreas de mejora en el programa de concienciación. Este proceso incluye la revisión detallada de los incidentes para comprender sus causas y determinar cómo se puede mejorar la formación para prevenir futuros eventos similares.

6. RECURSOS Y RESPONSABILIDADES

6.1. Recursos necesarios

Para llevar a cabo el programa de concienciación en seguridad de la información, se requiere una inversión significativa en los siguientes recursos:

- Trabajadores
- Presupuesto
- materiales de capacitación
- infraestructura tecnológica

6.2. Responsabilidades

6.2.1. Equipo de Gestión Informática

- **Desarrollo del Programa:** Creación y estructuración del contenido del programa de concienciación, incluyendo el diseño de las actividades formativas y materiales didácticos.
- **Ejecución del Programa:** Implementación de las actividades de capacitación y concienciación, asegurando que todos los trabajadores participen en las sesiones programadas.
- **Actualización Continua:** Revisión y actualización regular del contenido del programa para mantener su relevancia frente a nuevas amenazas y tecnologías emergentes.

6.2.2. Equipo de Seguridad de la Información

- **Supervisión del Programa:** Monitoreo continuo de la implementación del programa para asegurar que se cumplan los objetivos establecidos.
- **Evaluación de la Efectividad:** Análisis de los resultados de encuestas, pruebas de conocimiento y reportes de incidentes para evaluar la efectividad del programa.
- **Ajustes y Mejoras:** Propuesta e implementación de mejoras en el programa basadas en los datos de evaluación y las necesidades emergentes de la empresa.

6.2.3. Alta Dirección

- **Aprobación del Programa:** Revisión y aprobación del programa de concienciación, asegurando que esté alineado con los objetivos estratégicos de la empresa.

- **Apoyo Continuo:** Provisión de los recursos necesarios (financieros, tecnológicos y humanos) para la implementación efectiva del programa.
- **Fomento de la Cultura de Seguridad:** Promoción de la importancia de la seguridad de la información dentro de la empresa, incentivando la participación de todos los trabajadores.

6.2.4. Todos los Trabajadores

- **Participación en el Programa:** Asistencia y participación en todas las actividades de capacitación y concienciación programadas.
- **Cumplimiento de Políticas:** Adopción y cumplimiento de las políticas y procedimientos de seguridad de la información establecidos por la empresa.
- **Reporte de Incidentes:** Notificación inmediata de cualquier incidente de seguridad o actividad sospechosa al equipo de seguridad de la información.
- **Promoción de Buenas Prácticas:** Aplicación de los conocimientos adquiridos en su trabajo diario y promoción de buenas prácticas de seguridad entre compañeros.

7. COMUNICACIÓN Y DIVULGACIÓN

La comunicación efectiva es fundamental para el éxito del programa de concienciación en seguridad de la información. Se deben utilizar diversas estrategias para difundir los mensajes clave y mantener a los trabajadores informados sobre los avances y resultados del programa. A continuación, se mencionan las estrategias de comunicación y divulgación que se implementarán:

7.1. Estrategias de comunicación

Utilización de correos electrónicos, intranet corporativa, reuniones y boletines informativos para comunicar los mensajes de concienciación.

7.2. Divulgación de resultados

Informar periódicamente a los trabajadores sobre los avances y resultados del programa de concienciación.

8. PROCESO DE MEJORA CONTINUA

8.1. Recopilación de comentarios

Se recopilarán activamente los comentarios y sugerencias de los trabajadores para identificar áreas de mejora, lo que incluye tanto aspectos positivos como posibles deficiencias. Estos comentarios serán analizados de manera exhaustiva para comprender mejor las necesidades y preocupaciones del trabajador en relación con la seguridad de la información.

8.2. Actualización del programa

Basándose en los resultados de estas evaluaciones y comentarios, se realizarán ajustes y mejoras continuas al programa. Esto implica una revisión constante de las estrategias, métodos de capacitación y comunicación, así como de cualquier otro aspecto del programa que pueda beneficiarse de mejoras. El objetivo es adaptar el programa según las necesidades cambiantes del entorno empresarial y las nuevas amenazas de seguridad de la información, procurando una eficacia a largo plazo.

8.3. Periodicidad

Las actividades de capacitación del programa de concienciación en seguridad de la información, referentes a charlas y capacitaciones tendrán una periodicidad semestral, acomodándose estas dentro del calendario según las necesidades, de los diferentes procesos de la empresa. Para actividades de concienciación el equipo de gestión informática y el equipo de seguridad de la información de ENERGUAVIARE S.A E.S.P. se reserva el derecho de implementar estas en cualquier momento dentro de los periodos de implementación del SGSI según vea necesario.

Además de lo anterior Ha de incluirse un resumen con los puntos más indispensables para ser expuestos de forma rápida e inmediata ante los nuevos ingresos de trabajadores a la empresa.

9. CONCLUSIONES

La implementación del Programa de Concienciación de Seguridad de la Información en ENERGUAVIARE S.A E.S.P. es esencial para fortalecer la protección de los activos de la empresa frente a las amenazas cibernéticas. Este programa establece objetivos claros, asigna recursos y responsabilidades, y promueve una cultura de seguridad. Su éxito dependerá del compromiso de todos los trabajadores y del apoyo continuo de la alta dirección. En resumen, el programa es una herramienta crucial para la seguridad y la confianza de la información en la empresa en un entorno digital en constante evolución.

10. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
VERSIÓN N°	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**	**FUENTE DE VERIFICACIÓN**
1			
2	26/12/2024	Se modifico la tabla del cronograma de concienciación de seguridad de la información.	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