Fecha: abril 2025 | Código: POL-CGP-002 | Política de Seguridad de la información | Versión: 1.0

Política de Seguridad de la Información

Política de Seguridad de la Información

Objetivo

Establecer los lineamientos que se deben seguir para implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información en la organización, mediante el cual se desarrollarán los controles necesarios que permiten salvaguardar los principios de:

- Confidencialidad: asegurar que sólo quienes estén autorizados puedan acceder a la información.
- Integridad: asegurar que la información y sus métodos de proceso sean exactos y completos.
- Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.

Lineamientos

1. Evaluación y tratamiento de riesgos. La organización identifica, evalúa y trata los riesgos relacionados con la seguridad de la información, implementando controles adecuados para reducirlos a niveles aceptables.
2. La organización ha establecido, implementado y mantiene un proceso documentado de evaluación y tratamiento de riesgos de seguridad de la información, conforme a los requisitos establecidos en la cláusula 8 de la norma ISO/IEC 27001:2022. Como parte del proceso.

a) Se definen y aplican criterios de riesgo que permiten evaluar la probabilidad e impacto de los eventos relacionados con la seguridad de la información.
b) Se establecen criterios de aceptación del riesgo, con base en el contexto organizacional y el apetito de riesgo definido.
c) Se lleva a cabo una evaluación sistemática de los riesgos, identificando amenazas, vulnerabilidades, activos y sus impactos potenciales.

3. Gestión de incidentes de seguridad. Se debe reportar de inmediato cualquier incidente de seguridad de la información. La organización cuenta con procedimientos para gestionar, registrar, investigar y mitigar los incidentes.

La organización ha planificado, establecido y documentado un proceso de gestión de incidentes de seguridad de la información, con el objetivo de asegurar una respuesta eficaz y oportuna ante eventos que comprometan la confidencialidad, integridad o disponibilidad de la información.

El proceso incluye:

a) Capacidades claras y documentadas para la detección, reporte, evaluación, respuesta, mitigación y recuperación ante un incidente de seguridad.
b) Reporte inmediato de cualquier incidente o debilidad relacionada con la seguridad de la información por parte de todo el personal.
c) Procedimientos definidos, para el registro, análisis e investigación de incidentes, así como para la implementación de acciones correctivas y preventivas.
d) La prueba y revisión periódica de los procedimientos de Gestión de incidentes con el fin de garantizar su eficacia y mejora continua.

4. Objetivos estratégicos. La compañía establece objetivos estratégicos anuales (frecuencia de control establecida) con relación a la Seguridad de la Información, elabora y actualiza el plan de acción para la obtención de dichos objetivos.

5. Continuidad del negocio. Se establecerán y mantendrán planes de continuidad que aseguren la disponibilidad de los servicios críticos, protegiendo la información ante eventos disruptivos. Esto implica identificar los requisitos de continuidad, establecer objetivos, implementar y mantener planes y procedimientos, realizar pruebas y revisiones, y considerar la resiliencia de la seguridad de la información.

6. Clasificación y protección de la información. La información debe clasificarse según su nivel de sensibilidad y protegerse en función de dicha clasificación, mediante controles físicos, lógicos y administrativos. La organización ha definido e implementado un esquema formal de clasificación de la información, que permite identificar y categorizar los activos de información de acuerdo con su nivel de sensibilidad, valor, criticidad y riesgo asociado. Este esquema contempla:

    a. Criterios documentados de clasificación, que pueden incluir niveles como: Uso Interno, Confidencial, Restringida (o los que defina la organización) y Pública.

b. Lineamientos específicos de manejo, almacenamiento, transmisión y eliminación de la información para cada nivel de clasificación.

c. Consideración de obligaciones legales, regulatorias, contractuales y de las necesidades del negocio, garantizando que la protección de la información esté alineada con dichos requerimientos.

7. Implementación de controles físicos, lógicos y administrativos proporcionales al nivel de clasificación definido.

8. Capacitación del personal en el uso correcto del esquema de clasificación y en el cumplimiento de los procedimientos asociados

9. Concientización y formación. Todo el personal debe participar en programas de concientización y capacitación en seguridad de la información, para garantizar el cumplimiento de buenas prácticas. Teniendo como objetivo fomentar la comprensión y la importancia dentro del Sistema de Gestión de Seguridad de la información. Asegurar que los colaboradores conocen sus responsabilidades especificas en materia de seguridad incluyendo los impactos organizacionales y disciplinarios. Reforzar la capacidad del personal para identificar, reportar y responder adecuadamente ante incidentes de seguridad.

10. Gestión de proveedores. Los proveedores que manejen información de la organización deben cumplir con requisitos de seguridad acordados contractualmente y estar sujetos a revisiones periódicas. La organización establece y mantiene un proceso formal para la gestión de la seguridad de la información en las relaciones con proveedores, con el fin de proteger los activos. El proceso incluye: La identificación y evaluación de los riesgos asociados a cada proveedor, considerando el tipo de servicios prestados, el nivel de acceso a la información y la criticidad del proveedor para las operaciones del negocio. Así como la vigilancia y monitoreo continuo del cumplimiento de dichos requisitos, incluyendo revisiones periódicas, auditorías, indicadores de desempeño y mecanismos de reporte.

11. Sanciones por incumplimiento. El incumplimiento de esta política podrá derivar en acciones disciplinarias, incluyendo la terminación del contrato laboral o comercial, según la gravedad del caso.

12. Compromiso de la dirección. La Dirección se compromete a liderar, respaldar y revisar continuamente el SGSI, asegurando su alineación con los objetivos

estratégicos de la organización. La dirección demuestra su compromiso con la seguridad de la información mediante el liderazgo activo, respaldo continuo y participación directa en la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI). Este compromiso se manifiesta a través de la alineación del SGSI con los objetivos estratégicos del negocio y las prioridades de la organización. El aseguramiento de la disponibilidad de recursos adecuados (humanos, tecnológicos y financieros) para el funcionamiento eficaz del SGSI. La asignación de responsabilidades claras en todos los niveles organizacionales, fomentando una cultura de seguridad y cumplimiento. La comunicación de la importancia de una gestión eficaz de la seguridad de la información, tanto dentro como fuera de la organización. La revisión periódica del SGSI, con el objetivo de evaluar su desempeño, eficacia y oportunidades de mejora continua.

13. Revisión y mantenimiento de la política. Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos en el entorno de negocio, legal o tecnológico que afecten la seguridad de la información. Esta política será revisada de forma sistemática y documentada al menos una vez al año, o con mayor frecuencia si ocurren cambios significativos en el entorno organizacional, tecnológico, normativo o de amenazas que puedan afectar la seguridad de la información. La revisión considerará, entre otros elementos:

a) Retroalimentación interna y externa relacionada con la implementación y eficacia del SGSI.
b) Resultados de auditorías
c) Lecciones aprendidas de incidentes de seguridad o eventos relevantes.
d) Cambios en el contexto legal, regulatorio o contractual aplicable.
e) Cambios organizacionales, tecnológicos o de procesos.
f) Oportunidades de mejora identificadas como parte del ciclo de mejora continua del SGSI.

14. Mejora continua. La compañía se compromete a establecer en el SGSI un sistema de mejora continua. La organización mantiene un compromiso permanente con la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que este se mantenga eficaz, alineado con los objetivos estratégicos del negocio y adaptado a los cambios del entorno.

La ciberseguridad es concebida como un proceso transversal y evolutivo, que busca

proteger de forma integral la confidencialidad, integridad y disponibilidad de la información en todas las funciones, procesos y niveles de la organización. Mediante La evaluación constante del desempeño del SGSI, a través de auditorías, revisiones por la dirección, análisis de incidentes y monitoreo de controles.

La identificación y tratamiento de no conformidades y oportunidades de mejora, asegurando que se tomen acciones correctivas eficaces.

La incorporación de lecciones aprendidas, avances tecnológicos y mejores prácticas en seguridad de la información.

La adaptación a nuevas amenazas, requisitos legales y expectativas de las partes interesadas.

15. Cumplimiento de requisitos legales, reglamentarios y contractuales en materia de ciberseguridad La organización se compromete a cumplir con todos los requisitos aplicables en materia de seguridad de la información y ciberseguridad, incluyendo los requisitos del servicio, así como las obligaciones legales, reglamentarias y contractuales suscritas con clientes, proveedores, socios y otras partes interesadas.

16. La organización se compromete a que la información generada, almacenada y transferida sea tratada con fines alineados a los objetivos del negocio y en estricto apego a la confidencialidad e integridad; estableciendo y manteniendo controles en la creación de la información, almacenamiento seguro y transferencia de información.

Documentos de Referencia

Norma Anexo A de la norma ISO/IEC 27001:2022.

Fin