POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de esta política es establecer las directrices y principios para proteger la integridad, confidencialidad y disponibilidad de la información de la organización contra amenazas asegurando a su vez el cumplimiento de los requisitos legales y regulatorios.

Esta política se aplica a toda la información manejada por la organización, independientemente del formato o medio, y es de obligado cumplimiento para todos los empleados, contratistas, proveedores y cualquier otra persona con acceso a la información de la organización.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Proteger la confidencialidad de la información y evitar su divulgación no autorizada.
- Garantizar la integridad de la información y prevenir su modificación no autorizada.
- Asegurar la disponibilidad de la información y los sistemas que la procesan.
- Cumplir con las leyes, regulaciones y requisitos contractuales aplicables.
- Promover una cultura de seguridad de la información entre todos los empleados y partes interesadas.

Para alcanzar estos objetivos, la organización establecerá indicadores apropiados que faciliten el seguimiento del progreso.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Gestión de Riesgos:** Identificar, evaluar y tratar los riesgos de seguridad de la información mediante un enfoque basado en riesgos.
- **Control de Acceso:** Asegurar que el acceso a la información esté restringido a personas autorizadas y según el principio de mínimo privilegio.
- **Gestión de Activos:** Inventariar y clasificar todos los activos de información y asegurar su protección adecuada.
- **Segregación de funciones**: Dividir las responsabilidades y tareas críticas entre distintos roles para reducir el riesgo de errores o acciones malintencionadas.
- **Seguridad de Recursos Humanos:** Asegurar que los empleados, contratistas y terceros sean conscientes de sus responsabilidades de seguridad y reciban la formación adecuada.
- **Seguridad Física y Ambiental:** Proteger las instalaciones y equipos contra accesos no autorizados, daños y fallos ambientales.
- **Seguridad de las Operaciones:** Implementar y mantener procedimientos para la gestión segura de las operaciones de TI.
- **Seguridad de las Comunicaciones:** Asegurar la protección de la información en tránsito y la integridad de las comunicaciones.
- **Adquisición, Desarrollo y Mantenimiento de Sistemas:** Asegurar que la seguridad sea una parte integral del ciclo de vida del desarrollo de sistemas.

- **Gestión de Incidentes:** Establecer y mantener procedimientos para la gestión de incidentes de seguridad de la información.
- **Cumplimiento:** Asegurar el cumplimiento de las leyes, regulaciones y requisitos contractuales aplicables.

EVALUACIÓN Y TRATAMIENTO DE RIESGOS

- Realizar evaluaciones de riesgos periódicas para identificar amenazas y vulnerabilidades.
- Establecer planes de tratamiento de riesgos para mitigar los riesgos identificados, priorizando las medidas de seguridad según su impacto y probabilidad.

CONTROL DE ACCESO

- Implementar controles de acceso físico y lógico para proteger la información, proporcionales a la criticidad del sistema y de la información.
- Revisar y actualizar regularmente los permisos de acceso.

GESTIÓN DE INCIDENTES DE SEGURIDAD

- Establecer un proceso formal para la notificación y gestión de incidentes de seguridad de la información.
- Investigar y documentar todos los incidentes de seguridad, y tomar medidas correctivas y preventivas adecuadas.
- Realizar simulacros y ejercicios de respuesta a incidentes para mejorar la preparación y la capacidad de respuesta.

CAPACITACIÓN Y CONCIENTIZACIÓN

- Proveer capacitación inicial y continua en seguridad de la información para todos los empleados.
- Realizar campañas de concientización para promover la cultura de seguridad de la información.

CUMPLIMIENTO Y AUDITORÍA

- Realizar auditorías internas y revisiones periódicas para asegurar el cumplimiento de la política de seguridad de la información y la efectividad del SGSI.
- Mantener registros de todas las auditorías, revisiones y acciones correctivas.

SISTEMA DE GESTIÓN

- Mantener un listado de toda la documentación, políticas, normativas, procedimientos, etc. que compongan el sistema de gestión de seguridad de la información.
- Realizar las revisiones periódicas correspondientes de esta documentación.

REVISIÓN Y ACTUALIZACIÓN

- Revisar y actualizar esta política al menos una vez al año o cuando sea necesario debido a cambios en los requisitos legales, regulatorios o del entorno tecnológico.
- Asegurar que todos los cambios sean aprobados por la alta dirección y comunicados a todos los empleados.

Esta política ha sido aprobada por la dirección de la organización y es de cumplimiento obligatorio para todos los usuarios con acceso a los sistemas y recursos de la organización.

En Madrid a 13 de octubre de 2025

Fernando Cifuentes de Frutos

Presidente del Comité de Seguridad del Sistema de Gestión de Seguridad de la Información conforme al reglamento UE 2022/2554 (Reglamento DORA).