POLÍTICAS N.º 001-0309025-DPDP

LA AGENCIA DE CIBERSEGURIDAD DEL ESTADO,

CONSIDERANDO:

I. Que en cumplimiento de lo establecido en la Ley para la Protección de Datos Personales, resulta necesario contar con lineamientos claros que orienten las actuaciones de la institución en el tratamiento, resguardo y protección de los datos personales, garantizando así la transparencia, la seguridad jurídica y el respeto a los derechos fundamentales de las personas titulares de los datos.

II. Que el artículo 50 literal i), de la Ley para la Protección de Datos Personales, confiere a la Agencia de Ciberseguridad del Estado (ACE) la atribución de dictar políticas de actuación sobre el manejo y mantenimiento de los datos personales, así como de definir las medidas de seguridad y protección correspondientes; lo cual implica la obligación de esta entidad de establecer lineamientos claros, consistentes con estándares internacionales y buenas prácticas, que garanticen tanto la integridad, confidencialidad y disponibilidad de la información, como la prevención de riesgos asociados a su tratamiento.

POR TANTO,

en uso de sus facultades legales, el Director General de la Agencia de Ciberseguridad del Estado,

EMITE las siguientes:

POLÍTICAS DE ACTUACIÓN Y MANEJO DE DATOS PERSONALES DE LA "LEY PARA LA PROTECCIÓN DE DATOS PERSONALES"

CAPÍTULO I

DISPOSICIONES GENERALES

Objeto

Art. 1.- El presente documento establece las políticas de actuación sobre el manejo y mantenimiento de los datos personales, así como las medidas de seguridad y protección de los mismos, conforme a la Ley para la Protección de Datos Personales (LPDP) y la ISO 27001. Se

procura la implementación, en lo que fuera aplicable, de las mejores prácticas internacionales en la materia. ISO 27001: A.5.1.1 (Política de Seguridad de la Información).

Ámbito de Aplicación

Art. 2.- Estas políticas son de cumplimiento obligatorio para todas las entidades públicas y privadas que recolecten, almacenen, procesen o transfieran datos personales en El Salvador. También aplican a operaciones internacionales vinculadas a ciudadanos salvadoreños. ISO 27001:A.6.1.1 (Roles y Responsabilidades de Seguridad de la Información).

Principios Rectores

Art. 3.- Toda actuación sobre datos personales se regirá por los siguientes principios:

a) **Exactitud:** Mantener los datos actualizados y corregir inexactitudes sin demora. (Art. 5 literal a) LPDP)
b) **Lealtad y Legalidad**: Recopilar y tratar datos de forma lícita y transparente. (Art. 5 literal b) LPDP)
c) **Consentimiento y Finalidad:** Obtener autorización explícita del titular para la recolección y tratamiento de sus datos. (Art. 5 literal c) LPDP)
d) **Minimización:** Recopilar únicamente los datos necesarios para la finalidad declarada. (Art. 5 literal d) LPDP)
e) **Transparencia:** Informar claramente a los titulares sobre el uso, almacenamiento y derechos sobre sus datos. (Art. 5 literal e) LPDP)
f) **Seguridad y Confidencialidad:** Proteger los datos contra accesos no autorizados mediante medidas técnicas y organizativas. (Art. 5 literal f) LPDP)
g) **Temporalidad y Derecho al Olvido:** Conservar los datos solo mientras sean necesarios y eliminarlos cuando no se requieran. (Art. 5 literal h) LPDP)
h) **Responsabilidad y Supervisión:** Las entidades responsables deben garantizar cumplimiento y someterse a auditorías. (Art. 5 literal i) LPDP)
i) **Cumplimiento de Normas Internacionales:** Se promoverá la adopción de estándares globales en protección de datos de la ISO27001 y actualizaciones. (ISO 27001: A.8.2.1 (Clasificación de la Información)

CAPÍTULO II

SEGURIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES

Medidas de Seguridad en el Tratamiento de Datos Personales

Art. 4.- Según la Ley para la Protección de Datos Personales de El Salvador, las medidas de seguridad buscan garantizar la integridad, disponibilidad y confidencialidad de la información. Estas medidas deben ser implementadas por los responsables y encargados del tratamiento de datos, y su incumplimiento puede llevar a sanciones.

Medidas Organizativas:

a) **Política de Protección de Datos:** Establecer normas internas que regulen el manejo de los datos personales.
b) **Delegado de Protección de Datos Personales (DPDP):** Nombramiento de un responsable encargado de garantizar el cumplimiento de la normativa.
c) **Capacitación del Personal:** Formación continua sobre seguridad de datos.
d) Registro de Actividades de Tratamiento: Mantener un registro detallado de cómo se recopilan, almacenan y utilizan los datos personales.
e) **Evaluaciones de Impacto en la Privacidad (EIPD**): Identificación y mitigación de riesgos.
f) **Auditorías de Cumplimiento:** Verificación periódica del cumplimiento de las medidas de seguridad.

Medidas Técnicas:

a) **Control de Acceso:** Implementación de contraseñas seguras, autenticación en dos pasos (2FA) y acceso restringido.
b) **Cifrado de Datos:** Protección de la información tanto en almacenamiento como en tránsito.
c) **Gestión de Identidades y Perfiles:** Definición de roles y niveles de acceso según la necesidad del usuario.
d) **Copias de Seguridad y Recuperación:** Mecanismos de respaldo periódico para garantizar disponibilidad.
e) **Protección de Infraestructura:** Uso de firewalls, antivirus y sistemas de detección de intrusos (IDS/IPS).
f) **Análisis de Vulnerabilidades y Pruebas de Penetración:** Evaluaciones regulares de seguridad en sistemas.

g) **Digitalización:** Usar sistemas especializados que permitan gestionar y documentar el tratamiento de datos.

Medidas Físicas:

a) **Control de Acceso a Instalaciones:** Restricción en áreas con documentos físicos o servidores con datos personales.
b) **Monitoreo y Vigilancia:** Uso de cámaras de seguridad y registros de ingreso.
c) **Almacenamiento Seguro:** Protección de archivos físicos en cajas fuertes o gabinetes con llave.
d) **Protección ante Desastres Naturales:** Medidas contra incendios, inundaciones o terremotos.
e) **Eliminación Segura de Documentos:** Uso de trituradoras de papel y borrado seguro de dispositivos electrónicos.

Medidas de Seguridad en Transferencias de Datos:

a) **Protocolos de Comunicación Segura:** Uso de SSL/TLS para cifrar comunicaciones.
b) **Contratos de Confidencialidad y Contratos para la Transferencia de Datos:** Acuerdos legales con terceros que tratan datos.
c) **Transferencias Internacionales Seguras:** Solo compartir datos con países que garanticen protección equivalente.
d) **Notificación de Brechas de Seguridad:** Reporte a la Agencia de Ciberseguridad del Estado, Fiscalía General de la República y titulares en un máximo de 72 horas.

ISO 27001:
A.9.1.1 (Control de Acceso a Sistemas y Datos)
A.10.1.1 (Cifrado de Datos)
A.12.1.1 (Seguridad en la Infraestructura Tecnológica)

Cumplimiento y Supervisión

Art. 5.- Con el fin de garantizar la eficacia de la presente Política, se establecen los siguientes mecanismos de cumplimiento y supervisión:

a) **Auditorías Periódicas:** Para verificar el cumplimiento de las medidas de seguridad.
b) **Actualización de Políticas:** Adaptación a nuevas amenazas y regulaciones.

c) **Mecanismos de Denuncia:** Vías para que los titulares reporten incumplimientos o violaciones de seguridad.

ISO 27001: A.18.2.2 (Auditorías de Seguridad de la Información)

Resumen de Medidas

Art. 6.- Las medidas de seguridad en el tratamiento de datos personales incluyen:

a) **Organizativas:** Delegado de Protección de Datos Personales, auditorías, políticas internas.
b) **Técnicas:** Cifrado, control de acceso, copias de seguridad.
c) **Físicas:** Restricción de acceso, almacenamiento seguro, destrucción adecuada.
d) **Transferencias de datos:** Comunicación cifrada, contratos de confidencialidad, notificación de brechas.

El objetivo es proteger la privacidad de los ciudadanos, evitar accesos no autorizados y garantizar el uso adecuado de los datos personales.

ISO 27001: A.17.1.1 (Plan de Continuidad del Negocio)

CAPÍTULO III

INFRACCIONES Y SANCIONES

Art. 7.- Tipificación de Infracciones

Las infracciones al manejo de datos personales se clasifican en leves, graves y muy graves, con sanciones que varían desde advertencias hasta multas económicas significativas (Art. 56 y 57 LPDP).
ISO 27001: A.16.1.5 (Respuestas a Incidentes de Seguridad)

CAPÍTULO IV

IMPLEMENTACIÓN Y SUPERVISIÓN

Art. 8.- Supervisión y Monitoreo

Todas las entidades obligadas deben actualizar sus procedimientos internos para cumplir con esta normativa (Art. 60 LPDP)

a) El Delegado de Protección de Datos Personales será responsable de la supervisión interna. (Art. 15 y 16 LPDP)
b) Se realizarán auditorías anuales para evaluar el cumplimiento de estas políticas. (Art. 50 literal l) LPDP)
c) Se fomentará la certificación en normas internacionales de privacidad y seguridad de datos.

ISO 27001: A.18.1.3 (Protección de Datos Personales y Privacidad)

Entrada en Vigencia y Actualización

Artículo 9.- Estas políticas entrarán en vigencia a partir de su publicación y serán actualizadas periódicamente para garantizar su adecuación a nuevas regulaciones (Art. 24 literal g) LPDP).

ISO 27001: A.5.1.2 (Revisión de Políticas de Seguridad)