POLITICA DE SEGURIDAD DE LA INFORMACIÓN

VERSION:	FECHA DE VIGENCIA:
1.0/2022	JUNIO 2022

1. OBJETO

La presente Política establece las directrices y líneas de actuación en materia de Seguridad de la Información que regirán el modo en que la Dirección General de Seguridad Privada y Custodia de Bienes gestionará y protegerá su información y sus servicios.

Una adecuada gestión de la seguridad de la información permite proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. ÁMBITO DE APLICACIÓN

La presente política, así como toda la normativa y procedimientos vigentes y/o derivados de ésta, son de carácter obligatorio para todo el ámbito de la Dirección General de Seguridad Privada y Custodia de Bienes e involucra a la totalidad de los recursos, sean internos o externos.

3. ALCANCE

Los recursos de información y toda información de cualquier naturaleza o especie que administre o gestione la Dirección General de Seguridad Privada y Custodia de Bienes, sean internos o externos.

4. PRINCIPIOS BÁSICOS

4.1 La política está alineada con la política del Gobierno de la Ciudad y con el concepto de Gobernanza de la Seguridad Privada; y se complementa con el resto

de la normativa de la Dirección General de Seguridad Privada y Custodia de Bienes.

4.2 La Dirección comprende la importancia de gestionar eficazmente la seguridad de la información. En consecuencia, declara su compromiso y total apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos organizacionales y se involucra en la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia.

4.3 Las personas alcanzadas por esta política recibirán una capacitación acorde a su función, en particular sobre el compromiso que asumen para cumplir con esta política.

4.4 El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa aplicable.

4.5 La presente Política es de revisión obligatoria anualmente, debiendo asentarse el Control de Cambios y su aprobación. Su revisión es obligatoria cuando la normativa, las tecnologías de la información o los procedimientos de tratamiento de información cambien.

4.6 Debe estar disponible para todos los involucrados.

4.7 La Dirección General de Seguridad Privada y Custodia de Bienes se compromete a cumplir con los requisitos de seguridad de la información:

- ✓ Organización de la Seguridad de la Información: establecer un marco organizativo de referencia definiendo roles y responsabilidades de Seguridad de la Información que permitan la definición e implementación de un Plan de

Tratamiento del Riesgo y la evaluación de su efectividad para reducir los riesgos identificados.

- ✓ Seguridad en Recursos Humanos: informar y concienciar al personal desde su incorporación y de forma continua, cualquiera que sea su situación de actividad y modalidad de contratación, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
- ✓ Gestión de Activos: proteger adecuadamente los activos de la organización de acuerdo con su sensibilidad. Entre los activos se incluyen tanto el hardware como el software y los dispositivos de comunicación, los elementos de apoyo y la información y los datos en sí mismos, cualquiera sea el soporte y formato en el que se encuentren.
- ✓ Control de Acceso: asegurar el acceso a los sistemas de información únicamente al personal autorizado.
- ✓ Criptografía: utilizar sistemas y técnicas criptográficas para la protección de la información en base a la realización de análisis de riesgo, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.
- ✓ Seguridad física y ambiental: proteger los activos físicos del organismo y la información sensible que gestionan mediante el establecimiento de perímetros de seguridad y áreas protegidas.
- ✓ Gestión de las operaciones: garantizar la administración y gestión de las plataformas y servicios vinculados al tratamiento de información.
- ✓ Seguridad de las comunicaciones: asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

- ✓ Adquisición de sistemas, desarrollo y mantenimiento: garantizar la seguridad por defecto y desde el diseño en aplicaciones y durante la etapa de desarrollo o implementación del software.
- ✓ Relación con proveedores: implementar, mantener y monitorear el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.
- ✓ Gestión de la continuidad: asegurar que los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales contemplen todos los aspectos de seguridad de la información involucrada.
- ✓ Gestión de los incidentes de seguridad: garantizar que los eventos de seguridad de la información y las vulnerabilidades asociadas a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.
- ✓ Cumplimiento: garantizar el cumplimiento de los requerimientos legales y contractuales de seguridad que se aplican al diseño, operación, uso y gestión de los sistemas de información. Atender y dar cumplimiento de las observaciones de las auditorías.

5. HISTORIA DE CAMBIOS

Versión	Fecha	Descripción
1.0	Junio 2022	Primera versión Política de Seguridad de la Información.