POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La misión principal de nuestra organización es proporcionar los servicios que abarcan el *diseño*, *instalación y mantenimiento de sistemas de seguridad privada y contraincendios; central receptora de alarmas, servicios de acuda, custodia de llaves y vigilancia de seguridad privada*, todo ello se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc. Esto constituye uno de los activos principales de la organización, de tal manera que el daño pérdida de los mismos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización.

Por ello, la Dirección ha apostado por el estableciendo un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) de acuerdo a la norma internacional **ISO/IEC 27001:2022** cuyo alcance se acota a la *"gestión de la seguridad de la información que da soporte al diseño, instalación y mantenimiento de sistemas de seguridad privada, circuito cerrado de televisión, central receptora de alarmas, servicio de vigilancia y acuda, y a la instalación y mantenimiento de sistemas contra incendios"*.

El objeto de esta política es alcanzar una protección adecuada de la información de la organización, dentro del alcance definido, preservándolos siguientes principios de la seguridad:

- **Confidencialidad:** garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.
- **Integridad:** garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de la organización o fuera de ellas.

Así mismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física:** comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información.
- **Lógica:** incluyendo los aspectos de protección de aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos.
- **Político-corporativa:** formada por los aspectos de seguridad relativos a la propia compañía, a las normas internas, regulaciones y normativa legal.

Con el propósito de alcanzar sus objetivos estratégicos, la Dirección diseña esta política de seguridad de la información cuyos fines principales son:

- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
- **Definir la responsabilidad** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a las partes interesadas (dirección, empleados, socios, proveedores de servicios externos, etc.).

- **Especificar** los efectos que conlleva el **incumplimiento** de la política de seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicación o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de la organización.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.

Por todo ello, la Dirección de la organización quiere dejar constancia y expresa de sus conocimiento y aprobación de las políticas desarrolladas de este documento, de forma que todo el personal la debe conocer y asumir como una parte de sus funciones laborales.

El incumplimiento de estas obligaciones por parte del personal podrá dar lugar a responsabilidad disciplinaria, y al ejercicio de los procedimientos legales por la empresa.

Para que sea posible, se asignarán los recursos necesarios para el buen desarrollo de lo aquí establecido, tanto en el inicio del proyecto como en su mantenimiento futuro.

En Santa Cruz de Tenerife, a 21 de marzo de 2024.

Fdo. Director General
José Luis García Hurtado