POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En **iDISC INFORMATION TECHNOLOGIES, S.L.**, la información debe estar siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada.

Introducción

La información puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.

iDISC depende de los sistemas TIC para alcanzar sus objetivos.
Estos sistemas deben ser administrados para protegerlos frente amenazas y vulnerabilidades que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales, y maximizar el retorno de las inversiones y oportunidades de negocio.

Alcance

Esta política apoya la Política general del Sistema de Gestión Integrado de la organización, se aplica a todos los sistemas TIC de iDISC y debe ser considerada por todas las personas que trabajan o colaboran con la empresa, sin excepciones.

Objetivos de seguridad de la información

- Evitar o prevenir los incidentes de seguridad mediante la evaluación y tratamiento de riesgos.
- Detectar anomalías en la prestación de servicios mediante mecanismos de monitorización y análisis.
- Responder eficazmente a los incidentes de seguridad.
- Garantizar la disponibilidad de los servicios críticos mediante planes de continuidad y recuperación.
- Proteger la confidencialidad los datos personales de acuerdo con el RGPD 2016/679.

Principios de seguridad de la información

- Esta organización evalúa los riesgos y tolera o trata aquellos que, en base a la evaluación, deben ser controlados o tratados.
- Todo el personal será informado acerca de las políticas de seguridad de la información relevantes para el desempeño de su trabajo.
- Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información.
- Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
- Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
- Los criterios para la clasificación y la aceptación del riesgo se encuentran referenciados en la documentación del SGSI.
- Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.

Marco normativo

- Esquema Nacional de Seguridad (ENS) – *Disposición 7191 del* ***Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.***
- Reglamento General de Protección de Datos personales (RGPD - UE*) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.*
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) *– Ley 3/2018, de 5 de diciembre*.

Responsabilidades

- El equipo directivo es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
- El equipo directivo nombra a los Responsables que forman el Comité de Seguridad, según el procedimiento establecido en cumplimiento del Esquema Nacional de Seguridad.
- Cada director de departamento es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.
- El responsable de seguridad asesora al equipo directivo, proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

Políticas y normas relacionadas

- Política del Sistema de Gestión Integrado (SGI)
- Política de uso aceptable
- Política de dispositivos móviles y teletrabajo
- Política BYOD – Trae tu propio dispositivo
- Política de clasificación de la información
- Política de copias de seguridad
- Declaración del personal interno sobre la protección de datos personales – RGPD
- Acuerdo de confidencialidad - NDA

Estas políticas/normas/procedimientos deben ser comunicadas a los empleados y partes externas interesadas.

Olesa de Montserrat, 22 de mayo de 2023

La Dirección