Política de seguridad de la información

Objetivo

El objeto de esta política es establecer los principios básicos de actuación que deben regir a las personas, entidades, instituciones o unidades, tanto internas como externas, que tengan acceso a nuestros activos de información (TIC), o al entorno y/o los activos de operación (OT), para asegurar la protección efectiva de los recursos de información y la sostenibilidad de los servicios proporcionados, a través de la implementación de medidas preventivas, de detección, reacción y recuperación apropiadas frente a posibles incidentes de seguridad, garantizando la integridad, la confidencialidad y la disponibilidad de los activos y procesos digitales de la organización.

Esta Política ha sido elaborada considerando las principales referencias normativas en materia de seguridad de la información y mejores prácticas nacionales e internacionales.

Principios

La presente Política se fundamenta en principios esenciales de protección diseñados para asegurar que Zelestra pueda lograr sus metas mediante el uso seguro de sus sistemas de información/operación.

Estos pilares fundamentales, que deben ser tenidos en cuenta en todo momento al tomar decisiones en materia de seguridad de la información/ciberseguridad, se describen a continuación:

- Definir una estrategia de seguridad integral con un enfoque tanto preventivo como proactivo para garantizar un nivel razonable de riesgo.
- Asegurar que la seguridad de la información, incluyendo la confidencialidad, disponibilidad e integridad de los datos, se ajuste a la estrategia empresarial, así como a los requisitos contractuales y legales vigentes.
- Promover la integración de la seguridad en la cultura organizacional y en el marco de gestión de la entidad.
- Garantizar el derecho a la protección de los datos personales de todas las personas físicas que se relacionan con las sociedades pertenecientes al Grupo, de conformidad con lo dispuesto en la Política de Privacidad y Protección de datos personales (o norma que la sustituya en el futuro).
- Priorizar el análisis y gestión de riesgos como parte central de las operaciones.
- Mantener los niveles de riesgo dentro de límites mínimos aceptables mediante la aplicación continua de medidas de seguridad adecuadas y actualizadas.
- Salvaguardar los recursos de información y la tecnología empleada por Zelestra contra amenazas tanto internas como externas, sean intencionadas o accidentales.
- Adoptar las medidas necesarias para prevenir, neutralizar, minimizar o restaurar el daño causado por amenazas de seguridad para el normal desarrollo de las actividades, con base en criterios de proporcionalidad a los potenciales riesgos y a la criticidad y al valor de los activos y servicios afectados.
- Establecer una protección compuesta por múltiples capas de seguridad al objeto de minimizar el impacto resultante, en caso de fallo o incidencia.
- Utilizar de manera eficaz y eficiente el conocimiento y la infraestructura de seguridad disponibles.
- Establecer procedimientos de monitorización y reporte para garantizar el cumplimiento de los objetivos establecidos.
- Cualquier tercero que tenga acceso a nuestros sistemas de información deberá cumplir con lo establecido en esta política, así como con los procedimientos que emanen de ella.
- Garantizar y promover programas adecuados de formación, tanto presencial como online o por cualquier otro método que resulte apropiado en los deberes que impone la normativa aplicable con una periodicidad suficiente para garantizar la actualización de sus conocimientos en esta materia. Asimismo, requerir a proveedores y contratistas formación en la materia, previo al comienzo de la relación contractual efectiva.
- Optimizar las inversiones en seguridad para respaldar los objetivos empresariales de manera eficiente.
- Revisar y actualizar de forma continua los procedimientos y medidas de seguridad implementadas para asegurar que sigan siendo efectivas en respuesta a la evolución constante de los riesgos y los sistemas de protección.

La presente Política fue actualizada por el Consejo de Administración el 21 de noviembre de 2024 y es efectiva desde su aprobación.

- Aplicar las medidas disciplinarias correspondientes por el órgano responsable, de acuerdo con nuestros procedimientos internos, los convenios colectivos de aplicación y la normativa legalmente aplicable en cada momento.

La responsabilidad de Zelestra es asegurar que la seguridad de las Tecnologías de la Información y Comunicación (TIC), así como de los activos en operación (OT), esté integrada en todas las etapas del ciclo de vida de los sistemas de información, desde la concepción hasta la retirada del servicio, incluyendo las decisiones de desarrollo o adquisición, así como las actividades operativas.

Sistema de monitoreo

El comité de seguridad de la información o, en su defecto, el área de Digitalización y Ciberseguridad de Zelestra (o las figuras que en cada momento asuman sus funciones), supervisará la definición, revisión continua e implantación de esta Política, de los planes que se desarrollen y concreten en los territorios y para los negocios específicos del Grupo.

Comunicación y participación de los grupos de interés

Esta Política es comunicada y entendida en el ámbito de la organización, y está disponible a través de los canales de información y comunicación que la compañía pone a disposición de todos sus grupos de interés.

La Política está disponible públicamente en el sitio web de Zelestra.

Con el fin de facilitar que cualquier persona pueda comunicar de manera confidencial y/o anónima cualquier incumplimiento de los principios descritos en la presente Política, se facilita el Canal Ético de Zelestra (https://zelestra.integrityline.com/) que garantiza la independencia, la imparcialidad y la ausencia de conflictos de intereses durante todo el proceso de recepción, tramitación y resolución de estas.

Alcance

La presente Política es de aplicación a todas las sociedades que integran el Grupo Zelestra, a ZELESTRA CORPORACIÓN, S.A.U. y aquellas sociedades de las que se disponga, de forma directa o indirecta, de la mayoría de las acciones, participaciones o derechos de voto, o en cuyo órgano de gobierno o administración se haya designado o se tenga la facultad de designar a la mayoría de sus miembros, de tal manera que controle la sociedad de forma efectiva.

En aquellas sociedades participadas en las que las sociedades del Grupo Zelestra no tengan control efectivo, Zelestra promoverá principios y directrices coherentes con los establecidos en esta Política.

Definiciones

Confidencialidad: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Únicamente accede a la información las personas que cuentan con la debida autorización.

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas. Garantiza la exactitud de la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Disponibilidad: Característica, cualidad o condición de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Comité de seguridad de la información: Órgano responsable del gobierno de la seguridad de la información.