ISPD

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

ISPD

V3.2

1. Introducción

1.1. Objetivo y alcance

Este documento recoge la Política General de Seguridad de la Información de ISPD con relación a las Entidades en su Alcance, entendida como los principios básicos de actuación y ordenación de ISPD en materia de Seguridad de la Información.

Se entenderá por "ISPD" el conjunto de Empresas constituido por las siguientes entidades:

- ISPD Network, S.A.
- Rebold Marketing, S.L.
- Rebold Communication, S.L.U.
- Mamvo Performance, S.L.U.
- Marketing Manager Servicios de Marketing, S.L.U.
- B2Marketplace Ecommerce Consulting Group, S.L.
- Antevenio Media, S.L

El resto de los documentos relacionados con la Seguridad de la Información de ISPD estarán alineados con las directrices contenidas en esta Política General de Seguridad de la Información.

1.2. Fecha de realización y vigencia

Esta Política de Seguridad de la Información es efectiva desde la Fecha de Aprobación de la versión y hasta que sea reemplazada por una nueva Política.

1.3. Antecedentes

La presente Política se aplica a todos los recursos, procesos de ISPD y a todos los servicios relacionados con terceros que impliquen uso y/o acceso a los datos, recursos, administración y cualquier función de control de sistemas de información.

1.4. Publicación

La presente Política de Seguridad está disponible en el Library de ISPD y para su versión reducida y pública, en la página web principal de Rebold.

2. Política

2.1. Ámbito

ISPD protege los recursos involucrados en la gestión de la información relacionada con el normal desarrollo de sus funciones, dando cumplimiento a la legislación vigente, preservando la confidencialidad y privacidad de la información y asegurando la disponibilidad, acceso, integridad, calidad, trazabilidad, autenticidad y conservación. Estos objetivos se trasladan también a los sistemas de información utilizados para el desarrollo de su actividad.

Es voluntad de ISPD establecer condiciones de confianza en el uso de los medios electrónicos y la prestación continua de sus servicios, adoptando las medidas necesarias destinadas a proteger los sistemas de información de la Organización de aquellas amenazas a los que se estén expuestos, con la finalidad de garantizar la seguridad de los sistemas de información, minimizar los riesgos y consolidar así las bases para prevenir, detectar, reaccionar y recuperarse de los posibles incidentes que puedan acaecer.

La presente Política General de Seguridad de la Información se aplica en todo el ámbito de actuación de ISPD, es decir:

a) Todos los recursos, servicios y procesos de ISPD. De esta manera se aplicará a todos los sistemas de información que intervienen en la prestación de los servicios y a todos aquellos sistemas de soporte a las diferentes funciones y responsabilidades de ISPD.
b) A todos los usuarios, ya sean internos o externos vinculados, directa o indirectamente, a ISPD que hacen uso de los sistemas descritos en el punto a) anterior.

2.2. Objetivos de Seguridad de la Información

ISPD ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en directrices claras y alineadas a las necesidades del negocio, y a los requerimientos regulatorios. Los objetivos del Sistema de Gestión de Seguridad de la Información son:

a) Garantizar, asegurar e implementar las medidas de seguridad adecuadas y necesarias sobre todos los recursos, procesos, funciones y servicios relacionados directa e indirectamente con usuarios internos y externos, y con clientes, proveedores, partners u otros terceros, con la finalidad de asegurar la disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad de la información y la conformidad con la legislación aplicable.

b) Garantizar la continuidad, seguridad y calidad de los servicios ofrecidos.

c) Implementar y mantener los procesos de mejora continua para favorecer la eficiencia y eficacia de las medidas de seguridad de la información.

d) Reducir al máximo las posibilidades que produzcan incidentes de seguridad y minimizar el impacto de estos en caso de que se produjeran.
e) Disponer de los medios por los que los diferentes usuarios de los servicios y procesos de ISPD hacen buen uso de la información, sistemas de la información y recursos utilizados en el desarrollo de sus funciones, obligaciones y responsabilidades, así como los que no comprometan la seguridad de la información de ISPD.

De acuerdo con los objetivos citados, la presente Política General de Seguridad de la Información busca la adopción de premisas de seguridad, garantizando:

a) Disponibilidad: la información y sistemas de información pueden ser utilizados en los tiempos y forma requerida.

b) Confidencialidad: los datos y sistemas de información solamente se accederán por las personas debidamente autorizadas.

c) Integridad: exactitud de la información y de los sistemas de información contra la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

d) Autenticidad: inequívoco al asegurar que una persona o entidad es quién dice ser, o bien que garantiza la fuente de la que proceden los datos.

e) Trazabilidad: cualquier acción o transacción puede ser relacionada inequívocamente al sujeto que lo ha llevado a cabo.

f) Legalidad: la información se trata de acuerdo con el marco normativo.

g) Formación: de acuerdo con el principio de seguridad integral, garantizar un adecuado nivel de concienciación y capacitación en materia de seguridad de la información a todo el personal de la Organización.

h) Gestión de incidentes: el análisis y gestión de los riesgos como parte esencial del proceso de seguridad de la Organización, manteniendo el entorno controlado y minimizando los riesgos, de acuerdo con las medidas de prevención, detección, reacción y recuperación y estableciendo protocolos para el intercambio de información relacionada con los incidentes.

2.3. Cumplimiento Normativo

La presente Política General de Seguridad de la Información y el resto de documentación asociada está alineada con el ámbito jurídico actual de leyes, reglamentos y normativas que sean de aplicación a ISPD, respecto a cualquier alcance material (Privacidad y Protección de datos, Comunicaciones comerciales, Publicidad, Marketing, Cookies, Propiedad Intelectual, etc.) o territorial (País, Unión Europea, etc.).

2.4. Aplicación de recursos

La Dirección de ISPD manifiesta su compromiso de hacer todo lo necesario por garantizar, dentro de su ámbito de funciones y responsabilidades, la provisión de recursos necesarios para implementar y mantener los procesos relacionados con la seguridad de la información de ISPD y la mejora continua de estos. Todo ello con el fin de conseguir los objetivos estratégicos, la difusión, consolidación y cumplimiento de la presente Política General de Seguridad de la Información, así como también implementar los mecanismos de distribución y publicación adecuados con el objetivo de que esta pueda ser conocida por los diferentes usuarios a los que afecte.

3. Responsabilidades

3.1. Roles y responsabilidades

Todo usuario afectado por la presente Política, de acuerdo con el apartado 2.1, tendrá la obligación de:

a) Cumplir en todo momento con la Política General de Seguridad de la Información, normas, procedimientos e instrucciones de seguridad de la información de la Organización.

b) Tener un papel activo en la protección de la información.

c) Mantener el secreto profesional y la confidencialidad respecto de la información de la Organización.

d) Informar, de acuerdo con el correspondiente procedimiento, de situaciones sospechosas, incidencias de seguridad, insuficiencias o anomalías de seguridad de los sistemas de información y/o activos de la Organización.

La responsabilidad general de la Seguridad de la Información recae en la persona a la que se le asignen las funciones de Responsable de Seguridad de la Información.

La coordinación de la Seguridad de la Información se canalizará a través del Comité de Seguridad de la Información, que es responsable de la implementación de esta Política de Seguridad y de aquellas normas, procedimientos e instrucciones de seguridad que se deriven.

En cuanto al incumplimiento de la Política General de Seguridad de la Información de ISPD, y el resto de los documentos relacionados con la seguridad de la información, por parte de cualquiera al que le sean de aplicación y que ponga en riesgo la seguridad de la información en cualesquiera de sus dimensiones, la Dirección de ISPD en conjunto con el área de People Development, se reserva el derecho de iniciar las acciones correspondientes según los códigos y normas internas de comportamiento y el marco legal vigente.

3.2. Oficial de Seguridad de la Información.

El rol del Oficial de Seguridad de la Información es de aseguramiento de que la Política de Seguridad de la Información, la Política del SGSI y sus políticas asociadas sean establecidas e implementadas para proteger los activos de información de la organización.

El Oficial de Seguridad de la Información también cumple un rol de asesor en lo concerniente a la gestión de la seguridad de la información, con el fin de facilitar el cumplimiento de las políticas y objetivos de seguridad de la información de la organización, de sus requisitos de negocio y de la estrategia de riesgo.

3.3. Responsable del Servicio.

El rol del responsable del servicio tiene un papel operativo y estratégico en la gestión y supervisión de la seguridad de los servicios de la organización, asegurando el cumplimiento de los requisitos normativos en vigor en cada momento y colaborando con otras áreas para mantener la seguridad y resiliencia de los sistemas de información.

Entre otras tareas, el responsable del servicio se responsabiliza de la definición y supervisión del servicio, de la gestión de la seguridad, del cumplimiento normativo, colabora con el oficial se seguridad de la información (responsable de seguridad), estable y supervisa planes de evaluación continua y, por último, se responsabiliza del proceso de gestión de incidentes.

3.4. Responsable de la Información.

El responsable de la información tiene el deber de garantizar la protección adecuada de los datos e información gestionada por los sistemas de ISPD, definiendo, supervisando y actualizando las medidas de seguridad necesarias conforme a la normativa en vigor en cada momento. Este rol se centra en la gestión de la seguridad de los datos y la protección de su integridad y confidencialidad dentro del ciclo de vida de la información.

Entre otras tareas, el responsable de la información se responsabiliza de la protección de la información, de la clasificación de esta, define los requisitos de seguridad, supervisa la seguridad de la información y el cumplimiento normativo, supervisa la gestión de riesgos y, finalmente, colabora con otros responsables y con las tareas de concienciación y formación.

3.5. Responsable del Sistema.

El responsable del sistema tiene un rol operativo y técnico, asegurando que los sistemas de información de la organización cumplen con los requisitos de seguridad establecidos. Este rol se enfoca en la correcta gestión, protección y mantenimiento de los sistemas, colaborando con otros roles claves como el responsable de seguridad y el responsable de la información para proteger la infraestructura tecnológica y la información que estos sistemas manejan.

Entre otras tareas, el responsable del sistema es responsable de la gestión del sistema de información, de la implantación de medidas de seguridad, de la supervisión técnica de la seguridad, del cumplimiento de requisitos de seguridad, de la evaluación y gestión de riesgos, de la coordinación con otros responsables, del mantenimiento de la seguridad del sistema, de la gestión de incidencias de seguridad y, finalmente, de la documentación y control de los cambios sobre esta.

3.6. Comité de Seguridad.

ISPD dispondrá de un Comité de Seguridad encargado de alinear todas las actividades de la Organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones),

seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.

El Comité de Seguridad estará compuesto por:

- Miembros permanentes:
    - Chief Financial Officer (CFO)
    - Chief Technology Officer (CTO)
    - Chief Legal & Privacy Officer
    - General Counsel
    - Chief Information Security Officer (CISO)
    - Chief Operation Officer (COO)
- Miembros temporales:
    - Country Manager Spain
    - Country Manager Italy
    - VP LatAm

3.7. Control de cumplimiento

El grado de aplicación de esta política será medido periódicamente (como mínimo, anualmente) mediante autoevaluaciones coordinadas por el Comité de Seguridad de la Información y mediante auditorías internas o externas (como mínimo, anualmente), y siempre que se produzcan cambios sustanciales en los sistemas de información del ISPD.

3.8. Aprobación y revisión

La Política General de Seguridad de la Información es aprobada formalmente por parte el Comité de Seguridad de la Información de ISPD, que lo reflejará en el correspondiente Acta y estará vigente hasta que sea reemplazada por una nueva versión.

Así mismo, se revisará anualmente y siempre que se produzcan cambios significativos que lo requieran, con el fin de adaptarla a las nuevas circunstancias, técnicas y/o organizativas, evitando que quede obsoleta.

Para estos efectos, regularmente se revisará su idoneidad, oportunidad y precisión. Las modificaciones que puedan derivarse serán propuestas al Comité de Seguridad de la Información para su validación, quien aprobará formalmente, en su caso, la nueva versión de la Política General de Seguridad de la Información.

4. Referencias

ISO/IEC 27002:2013 "Information technology – Security techniques – Code of practice for information security management".

ISO/IEC 27001:2013 "Information technology – Security techniques – Information security management systems – Requirements".

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

ISO/IEC 27001:2022 AMD 1:2024: que vincula la gestión de la seguridad de las organizaciones con el cambio climático.

SGSI.FOR.14_Formato Matriz de Requisitos Legales