Política del sistema de gestión de la información

REVISIONES			
FECHA	**REALIZADO**	**APROBADO**	**Descripción del cambio**
15/10/2022	CISO	CISO	**v0. Edición Inicial**
5/3/2025	CISO	Dirección	**v1.0. Versión oficial. Revisión integral con alineación a normativas. v2022**

Política de Seguridad de la información

Up-Spain es una organización comprometida con la prestación de servicios de calidad, orientada a satisfacer las expectativas de sus clientes y partes interesadas, asegurando la protección, confidencialidad, integridad, disponibilidad y resiliencia de la información que gestiona.

La Dirección de Up-Spain establece, implementa y mantiene esta Política de Seguridad de la Información como marco estratégico para garantizar la protección de los activos de información y el cumplimiento de los requisitos legales, reglamentarios, contractuales y de negocio aplicables.

Con este propósito, la Dirección asume los siguientes compromisos:

1. Integración estratégica y liderazgo

Garantizar que la gestión de la seguridad de la información forme parte integral de la estrategia y procesos de negocio de CHEQUE, asignando los recursos necesarios y demostrando liderazgo y compromiso en la protección de la información.

2. Conocimiento del contexto y partes interesadas

Analizar y considerar el contexto interno y externo de la organización, así como las necesidades y expectativas de las partes interesadas relevantes, asegurando que las decisiones en materia de seguridad de la información estén alineadas con dichos factores.

3. Protección integral de la información

Proteger la información frente a cualquier amenaza, interna o externa, deliberada o accidental, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, mediante la implementación de controles técnicos, organizativos y físicos adecuados.

4. Gestión de activos y clasificación

Mantener un inventario actualizado de activos de información, clasificados en función de su criticidad, sensibilidad y relevancia para el negocio, aplicando medidas de protección proporcionales a dichos niveles.

5. Continuidad, resiliencia y recuperación

Establecer planes y procedimientos que aseguren la continuidad de las operaciones, la resiliencia operativa y la capacidad de recuperación ante incidentes, interrupciones o desastres, minimizando el impacto en los servicios prestados.

6. Gestión de riesgos

Adoptar un enfoque basado en la gestión del riesgo, identificando, evaluando y tratando los riesgos de seguridad de la información de manera sistemática, con especial atención a los riesgos relacionados con proveedores, terceros y la cadena de suministro.

7. Gestión de incidentes

Implantar procedimientos eficaces para la detección, gestión, notificación y aprendizaje derivado de los incidentes de seguridad de la información, garantizando una respuesta oportuna y adecuada, y asegurando la comunicación a las partes interesadas según corresponda.

8. Protección de datos personales y privacidad

Asegurar el tratamiento lícito, leal y transparente de los datos personales, garantizando la privacidad y protección de los mismos en conformidad con los requisitos legales y reglamentarios aplicables.

9. Protección de información sensible

Adoptar controles específicos para la protección de información sensible, financiera o confidencial, incluyendo la información relacionada con transacciones electrónicas y medios de pago, mediante técnicas de cifrado, segmentación de redes y controles de acceso robustos.

10. Formación y concienciación

Promover la concienciación y formación continua de todo el personal en materia de seguridad de la información, asegurando que comprendan sus responsabilidades y actúen conforme a esta política y los procedimientos establecidos.

11. Mejora continua

Establecer mecanismos de seguimiento, medición y revisión periódica del sistema de gestión de la seguridad de la información, asegurando su mejora continua y adaptación a los cambios del entorno tecnológico, normativo y de negocio.

Esta Política es revisada y aprobada por la Dirección y comunicada a todo el personal, proveedores y partes interesadas relevantes. Su cumplimiento es obligatorio para todos los integrantes de Up-Spain y sus colaboradores externos.

Firmado: Dirección / CISO