Política de Seguridad de la información

Política de Seguridad de la Información

Ciberseguridad

1. Introducción

RSI fundamenta su misión y estrategia empresarial en el desarrollo de soluciones bancarias adaptadas a las necesidades del cliente, abarcando desde servicios digitales y de conectividad, hasta soluciones de Core Banking y pagos por lo que, dada la dependencia directa de nuestros sistemas de información para alcanzar objetivos y garantizar así como la excelencia en la prestación de servicios, la seguridad de la información orientada a proteger la confidencialidad, integridad, disponibilidad y autenticidad de los datos, así como a asegurar la continuidad operativa, se establece como un pilar estratégico con el objetivo último de mantener y fortalecer la calidad y seguridad de los servicios TI, tanto para clientes del Grupo Caja Rural como para clientes externos.

Este compromiso se materializa a través de la Política de Seguridad de la Información, que define los principios, directrices y responsabilidades necesarias para proteger los activos de información de RSI y sus clientes, los cuales se desarrollan mediante normativa y procedimientos específicos que forman parte del marco documental de seguridad de la entidad y que podrán consultarse, tanto en la base de procedimientos a través de la intranet, como en los repositorios oficiales de los Departamentos.

2. Ámbito de aplicación

Esta política se aplica a todos los sistemas de información, servicios, personal, proveedores y terceros que manejen o accedan a información o infraestructuras TIC de RSI, quienes están en la obligación de conocer y cumplir esta política, así como la normativa de seguridad complementaria. En este sentido, RSI garantizará formación y concienciación periódica en materia de seguridad de la información.

Adicionalmente, los proveedores y terceros que presten servicios a RSI deberán cumplir con esta política y con la normativa complementaria aplicable, debiendo aportar evidencias periódicas de cumplimiento.

3. Principios rectores

Compromiso estratégico de la Dirección

El Comité de Dirección asume la seguridad de la información como un pilar estratégico y transversal para el cumplimiento de los objetivos institucionales, garantizando la dotación de recursos humanos, técnicos y financieros adecuados, liderando con el ejemplo en la promoción de la cultura de seguridad en toda la organización.

Asimismo, velará por la implantación de un proceso de mejora continua que permita revisar, evaluar y optimizar de manera permanente las medidas y controles de seguridad en función de la evolución de los riesgos y las necesidades de la entidad.

Seguridad integral, por defecto y desde el diseño

La seguridad se integra de forma transversal en todos los procesos, servicios y sistemas de la entidad, mediante medidas de protección en las dimensiones tecnológica, organizativa, legal y humana. Todo sistema o servicio se diseña considerando la seguridad desde su origen (security by design) y con el nivel más alto posible por defecto (security by default), minimizando la exposición a riesgos innecesarios.

En este marco, RSI garantiza el cumplimiento de los estándares de seguridad aplicables a categorías específicas de datos, aplicando controles como cifrado, segmentación de redes, control de accesos, monitorización continua y pruebas de seguridad periódicas, conforme a las mejores prácticas y requisitos regulatorios.

Gestión basada en riesgos

RSI aplica un enfoque sistemático para identificar, evaluar y tratar los riesgos relacionados con la información y los servicios, realizando análisis de riesgos periódicos y siempre que se introduzcan cambios significativos, priorizando la inversión en seguridad en función del nivel de riesgo, y adoptando medidas proporcionales y justificadas, equilibrando protección y operatividad.

Prevención, detección, respuesta y mejora continua

El ciclo de seguridad será proactivo y dinámico, estableciendo controles preventivos para reducir vulnerabilidades y evitar incidentes, implantando mecanismos de monitorización y detección temprana de amenazas, definiendo procedimientos de respuesta que aseguren

contención, erradicación y recuperación efectiva ante incidentes y fomentando la mejora continua a través de revisiones, auditorías y lecciones aprendidas.

A tal efecto, la gestión de incidentes se llevará a cabo de forma estructurada y documentada, conforme a los procedimientos internos aprobados garantizando la adecuada identificación, registro, tratamiento y reporte de los incidentes, asegurando la coordinación de los equipos implicados y la adopción de medidas correctivas que eviten su reiteración.

4. Marco regulatorio

RSI, como entidad del ámbito financiero y tecnológico, está sujeta a diversas normativas nacionales e internacionales que regulan la seguridad de la información, la resiliencia operativa y el cumplimiento normativo, en función del tipo de datos tratados, los servicios prestados y el rol que desempeña como proveedor tecnológico, razón por la que dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) que sirve como marco para establecer objetivos, aplicar controles, gestionar riesgos, supervisar el desempeño y garantizar la mejora continua en la protección de la información y los servicios.

Entre los principales marcos regulatorios y normativos que aplican, destacan:

- **DORA (Digital Operational Resilience Act)**: Reglamento europeo específico para el sector financiero, que exige a las entidades y sus proveedores tecnológicos garantizar la resiliencia operativa digital, incluyendo la gestión de riesgos TIC, pruebas de resiliencia y control de terceros.
- **EBA Guidelines**: Las directrices de la Autoridad Bancaria Europea (EBA) complementan el marco regulatorio europeo, especialmente en materia de gobernanza TIC, subcontratación, gestión de riesgos y continuidad de negocio.
- **PCI-DSS (Payment Card Industry Data Security Standard)**: Estándar de seguridad para organizaciones que almacenan, procesan o transmiten datos de tarjetas de pago. RSI lo aplica en los servicios relacionados con medios de pago.
- **SWIFT Customer Security Programme (CSP)**: Conjunto de controles obligatorios y recomendados para entidades que utilizan la red SWIFT. RSI aplica estos controles en los entornos donde se gestionan transacciones SWIFT.
- **ISO/IEC 27001**: Norma internacional para la gestión de la seguridad de la información que aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI) de RSI.
- **RD 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad**: Marco normativo español que establece los principios y requisitos mínimos para la protección de la información en el sector público y entidades que prestan servicios a este.

5. Gobierno

La Dirección de Ciberseguridad, encabezada por el Director de Seguridad de la Información (CISO), tiene la responsabilidad de la implementación de la Política de Seguridad a través de los equipos operativos especializados, los cuales trabajan de forma coordinada para asegurar que las medidas de seguridad se implementan de manera homogénea, eficaz y alineada con los objetivos estratégicos de la entidad y del Grupo.

5.1. Órganos de gobierno

Los principales órganos de gobiernos a través de los cuales se articula la gobernanza de la seguridad de la información son:

- **Comité de Dirección:** órgano principal de gobierno y responsable de la supervisión de la Política de Seguridad, delegando en la Dirección de Ciberseguridad la implementación de esta.

- **Comité de Ciberseguridad, Tecnología y Riesgos (CCTR)**: El Comité es el órgano decisor de referencia en ciberseguridad y tecnología para el Grupo, donde se adoptan decisiones obligatorias para las Entidades (políticas, requisitos mínimos y medidas), con el objetivo de homogeneizar y acelerar despliegues. Sus funciones incluyen evaluar el perfil de riesgo tecnológico y de ciberseguridad, revisar indicadores y alertas, y asegurar el cumplimiento regulatorio (ISO, DORA, EBA ICT, etc.) tanto en RSI como en las Entidades. Además, coordina la implantación de medidas en todas las entidades del Grupo, gestiona planes de acción y auditorías, garantizando una respuesta alineada y eficaz.

- **Foro de Tecnología, Ciber y RRTT:** El Foro está conformado por todas las entidades del Grupo Caja Rural, incluidas las participadas, y tiene como misión la difusión de las decisiones adoptadas en el Comité de Ciberseguridad, Tecnología y RRTT, así como el seguimiento y actualización de las distintas iniciativas en curso para el Grupo en materia tecnológica, de ciberseguridad y riesgos tecnológicos. Entre sus funciones se incluyen el seguimiento de proyectos con impacto en el ámbito del Foro, la compartición de buenas prácticas y la conexión con el Comité cuando sea necesario escalar cuestiones que requieran una decisión.

- **Comité de Riesgos, Seguridad y Control Interno**: Órgano con representación de la Dirección, cuya función incluye la presentación de objetivos estratégicos y la revisión de riesgos por encima del umbral de apetito y el seguimiento del mapa de riesgos, entre otras funciones.

- **Comité de Continuidad y Contingencia**: actúa como órgano de apoyo en la gestión de incidentes de seguridad, especialmente aquellos que requerir la activación de planes de contingencia.

6. Aprobación, revisión y vigencia

Esta Política de Seguridad de la Información entrará en vigor el día de su aprobación, estando disponible tanto en la Intranet oficial, como en la página web, de forma que sea accesible por todas las partes interesadas hasta su sustitución.

La presente política será revisada, al menos, una vez al año o cuando se produzcan cambios significativos en el entorno normativo, tecnológico u organizativo que lo hagan necesario.

****