29 de Junio de 2026

Política de Seguridad de la Información (v1)

Misión y Compromiso de la Dirección

En RAINDANCE, la seguridad de la información es un pilar estratégico fundamental para nuestra operativa en el desarrollo de soluciones de software. La Dirección asume el compromiso inequívoco de garantizar la **Confidencialidad, Integridad y Disponibilidad** de todos los activos de información, tanto propios como de nuestros clientes.

Para lograrlo, la Dirección proporciona el liderazgo y los recursos técnicos, humanos y financieros necesarios para establecer, implementar, mantener y mejorar continuamente nuestro Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO 27001.

Alcance y Aplicabilidad

Esta política es de **obligado cumplimiento** para todos los empleados, directivos, contratistas, proveedores externos con acceso a nuestros sistemas y cualquier otra parte interesada que participe en el ciclo de vida de los servicios de RAINDANCE. Aplica a todos los sistemas TIC, infraestructuras en la nube y procesos de negocio de la compañía.

Objetivos de Seguridad

Nuestro SGSI se rige por los siguientes objetivos medibles y revisables anualmente:

- **Resiliencia Operativa:** Garantizar la continuidad del negocio y la rápida recuperación de los servicios (RTO/RPO) frente a contingencias técnicas o ciberataques.
- **Cumplimiento Estricto:** Asegurar el cumplimiento al 100% de los requisitos legales y las cláusulas de seguridad contractuales con nuestros clientes.
- **Seguridad por Diseño**: Integrar controles técnicos desde el código hasta la infraestructura Cloud.
- **Cultura de Ciberseguridad:** Mantener a nuestro equipo capacitado y concienciado frente a las amenazas actuales (ingeniería social, fraude, vulnerabilidades).

Organización y Responsabilidades

Dado el tamaño y la estructura ágil de RAINDANCE, la gestión de la seguridad se articula a través del **Comité de Seguridad de la Información** como órgano ejecutivo supremo. Se aseguran así todas las funciones requeridas por el estándar ISO 27001 bajo la siguiente distribución de roles:

- **Dirección General (Alta Dirección):** Ejerce el máximo liderazgo del SGSI. Es responsable de aprobar esta política, garantizar los recursos necesarios, asegurar que la seguridad se integre en el negocio y asumir la aceptación de los riesgos residuales.
- **Comité de Seguridad de la Información:** Órgano corporativo encargado de coordinar la seguridad, gestionar la disponibilidad de recursos y ratificar las decisiones estratégicas y roles del sistema.
- **Responsable de Seguridad de la Información (RSGSI / Dirección Técnica):** Asume la responsabilidad operativa y de cumplimiento. Se encarga de asegurar que el SGSI conforme con la norma, implementar y monitorizar los controles técnicos, gestionar las auditorías y reportar el desempeño al Comité. Asimismo, asume el rol de **Propietario de los Activos** tecnológicos centrales.
- **Todo el Personal y Colaboradores:** Tienen la responsabilidad directa de aplicar las directrices de esta política, proteger la confidencialidad de la información y notificar inmediatamente cualquier posible incidente, vulnerabilidad o sospecha de fraude.

Marco Operativo de Seguridad

RAINDANCE fundamenta su seguridad en los siguientes pilares operativos, cuyo detalle se desarrolla en los procedimientos técnicos específicos:

- **Gestión de Riesgos:** El análisis de riesgos se revisará formalmente al menos una vez al año, o de manera inmediata cuando cambie la información manejada, los servicios prestados, ocurra un incidente grave o se detecten vulnerabilidades críticas.

- **Concienciación y Formación:** Todo el personal atenderá a sesiones de concienciación al menos una vez al año. La formación técnica específica será obligatoria antes de asumir responsabilidades críticas o ante un cambio de puesto de trabajo.
- **Gestión de Identidad y Accesos:** Todos los accesos se rigen por el principio de "mínimo privilegio". El acceso a sistemas críticos requiere Autenticación de Doble Factor (MFA) obligatoria y el uso del gestor de contraseñas corporativo. Se prohíbe el uso de cuentas compartidas.
- **Desarrollo Seguro:** La seguridad se integra en cada etapa del desarrollo (DevSecOps). Se prohíben los pases a producción directos sin revisión de código (Pull Requests aprobadas) y análisis de vulnerabilidades automatizado. Existe una separación lógica y funcional estricta entre los entornos de Desarrollo, Staging/Demo y Producción.
- **Puesto de Trabajo y Movilidad:** Todo equipo corporativo debe contar con cifrado de disco completo, software de protección EDR y bloqueo automático de pantalla. Es obligatorio aplicar la política de "Mesa y Pantalla Limpia" tanto en la oficina como en situación de teletrabajo.
- **Resiliencia y Continuidad:** Los sistemas de producción y repositorios de código están sujetos a políticas de copias de seguridad automatizadas, redundantes y probadas anualmente mediante simulacros de recuperación.
- **Proveedores y Cadena de Suministro:** Solo se operará con proveedores críticos de infraestructura Cloud y SaaS que demuestren un nivel de seguridad adecuado (ej. certificaciones ISO 27001 o SOC 2 vigentes).

Estructura Documental de Seguridad

La documentación de seguridad de la compañía se encuentra estructurada dentro del repositorio restringido (Google Drive) en cuatro niveles organizados:

- **Política de Seguridad:** El presente documento marco que define las directrices estratégicas.

- **Normativa de Seguridad:** Documentos que describen el uso correcto de equipos, servicios e instalaciones, detallando deberes y derechos del personal.
- **Documentos Específicos:** Documentación técnica y guías de seguridad aplicables a los sistemas.
- **Procedimientos de Seguridad:** Documentos operativos que detallan cómo explotar y administrar los elementos del sistema de información.

Clasificación y Tratamiento de la Información

Toda la información tratada en RAINDANCE debe ser protegida de acuerdo a su clasificación:

1. **Confidencial:** Datos cuyo compromiso causaría impacto legal, financiero o reputacional grave (ej. Código fuente de la IA, datos personales/PII de clientes, contraseñas, datos financieros). Acceso estrictamente limitado.
2. **Uso Interno:** Información operativa que no debe ser pública (ej. Planes estratégicos, manuales internos, organigramas). Acceso permitido a la plantilla.
3. **Público:** Información aprobada para su divulgación externa (ej. Web comercial, notas de prensa).

Gestión de Incidentes

Cualquier empleado o colaborador que detecte o sospeche de una brecha de seguridad, intento de fraude o anomalía técnica, tiene la obligación ineludible de reportarlo inmediatamente a través de los canales internos designados. RAINDANCE se compromete a no tomar represalias por reportes de buena fe e investigará la causa raíz para aplicar mejoras estructurales.

Régimen Disciplinario y Cumplimiento Legal

El incumplimiento intencionado o por negligencia grave de esta Política de Seguridad y de la Normativa de Uso Aceptable anexa podrá dar lugar a la aplicación del régimen disciplinario, de acuerdo con el Estatuto de los Trabajadores y la

legislación vigente, independientemente de las acciones civiles o penales que pudieran derivarse.

RAINDANCE garantiza el cumplimiento del marco legal aplicable, incluyendo de forma destacada:

- Reglamento General de Protección de Datos (RGPD) y LOPDGDD.
- Ley de Servicios de la Sociedad de la Información (LSSI).
- Normativa vigente en materia de Propiedad Intelectual.