1. Objetivo

La Política de Seguridad de la Información de Red Instantic S.A.S. tiene como objetivo establecer las directrices y compromisos necesarios para proteger los activos de información utilizados en la prestación de servicios tecnológicos, Contact center, compra de activos improductivos y desarrollo de software. Esta política busca garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, alineándose con los requisitos normativos, contractuales y estándares internacionales como ISO/IEC 27001:2022.

2. Alcance

Esta política es de obligatorio cumplimiento para todos los colaboradores, proveedores, contratistas, desarrolladores internos y externos, aliados estratégicos y terceros que, en el ejercicio de sus actividades, accedan, manipulen o gestionen información o activos tecnológicos de Redinstantic S.A.S., independientemente de su ubicación o medio de acceso.

3. Normativa Aplicable

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 – Controles de Seguridad.
- ISO 22301 – Continuidad del Negocio.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1266 de 2008 – Habeas Data.
- Ley 1273 de 2009 – Delitos Informáticos.

4. Desarrollo

Red Instantic S.A.S. reconoce la importancia de salvaguardar la información como un activo estratégico para sus procesos de negocio, incluyendo tecnología, desarrollo de software, servicios de Contact center y actividades comerciales. La alta dirección se compromete a establecer, implementar y mantener controles de seguridad que garanticen la continuidad del negocio, gestión apropiada de riesgos y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

4.1 Principios Fundamentales

Los principios fundamentales de nuestra política de Seguridad de la Información los cuales están alineados con la norma ISO/IEC 27001:2022 son los siguientes:

- **Confidencialidad:** Nos comprometemos a garantizar que la información solo sea accesible a personas autorizadas, protegiendo así los datos sensibles contra accesos no autorizados y divulgaciones indebidas.
- **Integridad:** Nos aseguramos de que la información y los métodos de procesamiento se mantengan exactos y completos. Esto implica proteger la información contra modificaciones no autorizadas y garantizar la precisión de los datos a lo largo de su ciclo de vida.
- **Disponibilidad:** Nos esforzamos por asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran. Esto incluye la implementación de medidas para prevenir interrupciones en el acceso y garantizar la continuidad del negocio.

Al adherirnos a estos principios, buscamos proteger los activos de información de la organización, mitigar riesgos y asegurar la continuidad de nuestras operaciones.

5. Roles y Responsabilidades

Para garantizar la eficacia de nuestra política de seguridad de la información, es fundamental que cada miembro de Red Instantic S.A.S entienda y cumpla con sus responsabilidades específicas. A continuación, se detallan los roles clave, con el fin de asegurar una gestión integral y coordinada de la seguridad de la información:

Líder TIC:

- Diseña y ejecuta estrategias tecnológicas que alineen los recursos tecnológicos con los objetivos empresariales y los requisitos de seguridad.
- Administra y mantiene las infraestructuras tecnológicas, incluyendo servidores, redes y sistemas de almacenamiento, asegurando que estén configurados y actualizados de acuerdo con las mejores prácticas de seguridad.
- Evalúa y recomienda tecnologías y soluciones que refuercen la seguridad de la información, realizando análisis de riesgo para la implementación de nuevas herramientas y sistemas.

- Supervisa el rendimiento y la seguridad de los sistemas tecnológicos, implementa medidas para la detección y respuesta ante incidentes de seguridad y gestiona las actividades de soporte técnico relacionadas con la seguridad.

Responsable de Seguridad de la Información:

- Elabora, revisa y actualiza las políticas y procedimientos de seguridad de la información para asegurar su alineación con las normativas internacionales y locales.
- Supervisa las actividades de seguridad, realiza revisiones internas para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y coordina las actividades para remediar las no conformidades.
- Identifica, evalúa y gestiona los riesgos asociados a la seguridad de la información, registrándolos en la Matriz de Riesgos e implementando los controles establecidos para su mitigación.
- Desarrolla e implementa programas de formación y sensibilización sobre seguridad de la información para el personal, promoviendo una cultura de seguridad y asegurando que todos los colaboradores comprendan y cumplan con las políticas de seguridad.

Desarrolladores de Software:

- Siguen los lineamientos, políticas y procedimientos establecidos para el desarrollo seguro, garantizando que todas las actividades asociadas a la creación, modificación o mantenimiento de aplicaciones se realicen bajo prácticas que protejan la información y eviten vulnerabilidades.
- Utilizan de forma adecuada las herramientas, repositorios, ambientes y recursos tecnológicos asignados para el desarrollo, asegurando la confidencialidad, integridad y disponibilidad del código fuente y de la información tratada durante el ciclo de vida del software, y reportan al área TIC y/o al responsable de seguridad cualquier hallazgo, incidente o riesgo que identifiquen.
- Participan activamente en actividades de formación y concienciación relacionadas con desarrollo seguro y protección de la información, aplicando los conocimientos adquiridos para contribuir a la construcción de soluciones tecnológicas confiables y alineadas con las prácticas de seguridad definidas por la organización.

Coordinadores, conciliadores de cuenta y Otros:

Siguen las políticas y procedimientos establecidos para la seguridad de la información, asegurando que todas las prácticas y actividades relacionadas con el manejo de información sean seguras y conformes a las normativas.

Utilizan los recursos de información de manera adecuada, protegen la confidencialidad, integridad y disponibilidad de los datos, y reportan al área de TIC y/o al coordinador de seguridad de la información cualquier incidente o vulnerabilidad que detecten.

Participan en las actividades de formación y concienciación sobre seguridad de la información, aplicando el conocimiento adquirido para proteger los activos de información de la organización.

6. Controles de Seguridad

En Redinstantic S.A.S. implementamos controles de seguridad orientados a proteger la confidencialidad, integridad y disponibilidad de la información, asegurando que solo las personas autorizadas accedan a los sistemas conforme a los lineamientos internos de gestión de identidades. Estos controles incluyen medidas de acceso, protección física y ambiental de la infraestructura, así como mecanismos de monitoreo y mantenimiento que permiten identificar y mitigar incidentes o vulnerabilidades de manera oportuna. Asimismo, integramos prácticas de seguridad en el ciclo de vida de desarrollo de software, incorporando validaciones, protección del código, separación de ambientes y revisión continua de soluciones tecnológicas, garantizando que los desarrollos realizados por la organización se mantengan seguros, confiables y alineados con las políticas vigentes.

7. Educación y Cultura de Seguridad

Redinstantic S.A.S. promoverá programas permanentes de concientización y capacitación para todos los colaboradores y equipos técnicos, con el fin de fortalecer la cultura de seguridad dentro de la organización.

8. Cumplimiento

El incumplimiento de las disposiciones establecidas en esta política será considerado una falta grave y podrá acarrear sanciones disciplinarias según el reglamento interno de trabajo, sin perjuicio de acciones legales aplicables.

9. Revisión y Mejora Continua

Esta política será revisada anualmente o cuando existan cambios significativos en la operación, infraestructura tecnológica, procesos del negocio o requisitos legales. La Líder TIC y el responsable de Seguridad de la Información serán los encargados de su actualización y control documental.

Se firma en San José de Cúcuta el día 20 de diciembre de 2021

Yebrail Arévalo Álvarez
Director TIC

Laura Yamile Buendia Ramírez
Gerente