Política de
Seguridad Digital

PL-004 V1

Introducción

En un mundo altamente interconectado, Rotorr-Motor de Innovación reconoce la importancia de proteger sus activos digitales para garantizar la confidencialidad, integridad y disponibilidad de la información, aspectos clave para su éxito. La digitalización ha mejorado la eficiencia y colaboración, pero también ha incrementado los riesgos cibernéticos, lo que pone en juego la reputación y credibilidad de la organización.

La Política de Seguridad Digital establece un marco integral para mitigar estas amenazas y fomenta una cultura de ciberseguridad enfocada en la prevención, detección y respuesta proactiva. Este documento detalla los principios, objetivos y medidas diseñados para proteger los activos digitales, asegurar la continuidad operativa y promover la resiliencia en toda la organización.

Objetivo General

Asegurar la defensa integral de los activos digitales de Rotorr-Motor de Innovación contra amenazas cibernéticas, que incluye datos confidenciales y sistemas esenciales.

Objetivos Específicos

- Proteger la propiedad intelectual y datos críticos mediante controles de acceso, cifrado y prácticas de seguridad integradas en el desarrollo de *software*.
- Establecer políticas para el intercambio seguro de información con terceros.
- Garantizar la confidencialidad de los datos personales de clientes.
- Promover una cultura de ciberseguridad con formación constante.

Alcance

La Política de Seguridad Digital tiene como finalidad gestionar y mitigar los riesgos de seguridad digital asociados a sus actividades operativas.

Marco Legal

- Constitución Política de Colombia,
    - Artículo 15.
    - Artículo 20.
    - Artículo 76.
    - Artículo 101.
- Ley 57 de 1985.
- Decreto Ley 2150 de 1995.
- Ley 527 de 1999.
- Decreto 1747 de 2000.
- Ley 594 de 2000.
- CONPES 3292 de 2004.
- Ley 962 de 2005.
- Decreto 1151 de 2008.
- Decreto 1273 de 2009.

- Ley 1341 de 2009.
- Decreto 235 de 2010.
- Decreto 2609 de 2012.
- Ley Estatutaria 1581 de 2012.
- Decreto 019 de 2012.
- Decreto 2693 de 2012.
- Ley 1712 de 2014.
- Decreto 2573 de 2014.
- Decreto 103 de 2015.
- Ley Estatutaria 1757 de 2015.
- Decreto 1166 de 2016.
- Decretos 415 de 2016.
- Decreto 704 de 2018.
- Decreto 108 de 2018.
- Ley 1978 de 2018.
- Directiva presidencial 02 de 2019.

- Decreto 2106 de 2019.
- Ley 2080 de 2021.

Componentes

- **Propósito y Alcance:** Define el objetivo de la política y especifica los activos digitales y áreas organizacionales a las que aplica.
- **Gestión de Riesgos:** Identifica y prioriza los riesgos asociados a los activos digitales y operaciones, al determinar los controles necesarios para mitigarlos.
- **Controles de Acceso:** Establece políticas para autenticar usuarios, autorizar accesos según roles y gestionar contraseñas.
- **Protección de Datos y Privacidad:** Implementa medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos, cumpliendo regulaciones de privacidad mediante cifrado y controles de acceso.
- **Gestión de Incidentes:** Define protocolos para detectar, contener, mitigar y recuperar incidentes de seguridad.
- **Seguridad del Desarrollo de *Software:*** Promueve prácticas seguras en el desarrollo de *software* para prevenir vulnerabilidades y proteger aplicaciones internas y externas.

- **Seguridad de la Infraestructura:** Establece medidas para proteger redes, servidores, almacenamiento y dispositivos contra amenazas mediante configuraciones seguras, actualizaciones y protección frente a *malware.*

- Concientización y Formación en Seguridad: Ofrece programas para sensibilizar a empleados y colaboradores externos sobre la importancia de la seguridad digital, al fomentar una cultura organizacional de seguridad.

- **Cumplimiento Legal y Normativo:** Garantiza que la política cumpla con las normativas legales aplicables, como GDPR, HIPAA y PCI DSS.

- Revisión y Mejora Continua: Define procesos para evaluar y actualizar periódicamente la política, adaptándola a nuevas amenazas, tecnologías y cambios en la organización.

Recursos Financieros

La Gerencia Financiera de Rotorr asignará cada año los recursos necesarios en el presupuesto para cumplir con las obligaciones de la Política de Seguridad Digital. Los recursos se ejecutan conforme a los programas y proyectos establecidos.