



Política de Seguridad Digital

Rotorr-Motor de Innovación



Introducción

En un mundo cada vez más interconectado y dependiente de la tecnología, Rotorr reconoce la importancia crítica de proteger sus activos digitales. Como líderes en la vanguardia de la innovación y el progreso, nuestra capacidad para salvaguardar la confidencialidad, integridad y disponibilidad de la información es fundamental para el éxito continuo de nuestra misión.

La digitalización de nuestros procesos y la gestión de datos nos han permitido alcanzar nuevas alturas de eficiencia y colaboración, pero también han ampliado la superficie de ataque para amenazas cibernéticas. Desde la propiedad intelectual hasta la información de nuestros clientes y socios, la seguridad de la información es un pilar sobre el cual se construye nuestra reputación y credibilidad.

La Política de Seguridad Digital de Rotorr establece un marco integral para proteger nuestros activos digitales contra amenazas internas y externas, al tiempo que fomenta una cultura de seguridad cibernética en toda la organización. Al enfocarnos en la prevención, detección y respuesta proactiva a las amenazas, estamos comprometidos a mantener la confianza de nuestros stakeholders y salvaguardar la continuidad de nuestras operaciones.

En esta introducción, exploraremos los principios rectores de nuestra Política de Seguridad Digital, los objetivos estratégicos que buscamos alcanzar y las medidas concretas que implementaremos para mitigar los riesgos cibernéticos y promover la resiliencia digital en todos los aspectos de nuestra operación.

Objetivo General

El objetivo primordial de la Política de Seguridad Digital de Rotorr es garantizar la protección integral de los activos digitales de la organización, incluyendo información confidencial, sistemas críticos y recursos tecnológicos, frente a amenazas cibernéticas.

Objetivos Específicos

- Garantizar la seguridad de la propiedad intelectual de Rotorr, incluidas las ideas innovadoras, diseños, patentes y otros activos digitales relacionados, mediante la implementación de controles de acceso adecuados y medidas de cifrado.
- Integrar prácticas de seguridad en todas las etapas del ciclo de vida del desarrollo de software, desde el diseño hasta la implementación, para garantizar la seguridad y confiabilidad de las aplicaciones desarrolladas internamente.
- Facilitar la colaboración segura con socios, clientes y terceros, estableciendo políticas y procedimientos para el intercambio seguro de información confidencial y la protección de los datos compartidos.
- Salvaguardar la información personal y confidencial de los clientes de Rotorr, cumpliendo con las regulaciones de protección de datos aplicables y aplicando medidas de seguridad bien estructuradas para prevenir el acceso no autorizado o la divulgación de datos sensibles.

- Proteger los activos digitales relacionados con la investigación y el desarrollo de productos, garantizando la confidencialidad de los datos experimentales, resultados de pruebas y otros hallazgos críticos.
- Asegurar la seguridad de los dispositivos IoT (Internet de las cosas) y otros dispositivos conectados utilizados en proyectos de innovación, mediante la implementación de controles de seguridad y la segmentación de redes para mitigar riesgos de ciberataques.
- Fomentar una cultura de seguridad cibernética entre los empleados y contratistas de Rotorr, mediante la realización de sesiones de formación, simulacros de seguridad y programas de sensibilización que destaquen la importancia de la seguridad digital en el entorno de innovación y desarrollo.
- Realizar evaluaciones de riesgos específicas para proyectos de innovación y desarrollo, identificando posibles amenazas y vulnerabilidades asociadas con nuevas tecnologías y procesos, y aplicando medidas de seguridad adecuadas para mitigar dichos riesgos.

Alcance

La finalidad de la Política de Seguridad Digital consiste en identificar, gestionar, abordar y disminuir los riesgos de seguridad digital que se encuentren presentes en las actividades operativas de Rotorr.

Marco Legal

- Constitución Política.
- Artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre.
- Artículo 20 en donde se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
- Artículo 76 que establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado.
- Artículo 101 que incluye el espectro electromagnético como parte del territorio colombiano.
- **Ley 57 de 1985:** Publicidad de los actos y documentos oficiales.
- **Decreto Ley 2150 de 9885:** Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la administración pública.
- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Decreto 1747 de 2000:** Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- **Ley 594 de 2000:** Por medio de la cual se dicta la Ley General de Archivos.
- **CONPES 3292 de 2004:** Proyecto de racionalización y automatización de trámites que tiene por objetivo establecer un marco de política para que las relaciones del gobierno con los ciudadanos y empresarios sean más transparentes, directas y eficientes, utilizando estrategias de simplificación, racionalización, normalización y automatización de los trámites ante la administración pública.
- **Ley 962 de 2005:** Facilitar las relaciones de los particulares con la Administración Pública, de tal forma que las actuaciones que deban surtirse ante ella para el ejercicio de actividades, derechos o cumplimiento de obligaciones se desarrollen de conformidad con los principios establecidos en los artículos 83, 84, 209 y 333 de la Carta Política. En tal virtud, serán de obligatoria observancia los siguientes principios como rectores de la política de racionalización, estandarización y automatización de trámites, a fin de evitar exigencias injustificadas a los administrados.
- **Decreto 1151 de 2008:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Lineamientos generales de la Estrategia de Gobierno en Línea.

- **Decreto 1273 de 2009:** "De la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009:** La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.
- **Decreto 235 de 2010:** "La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones" y que "las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado".
- **Decreto 2609 de 2012:** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

- **Ley Estatutaria 1581 de 2012:** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
- **Decreto 019 de 2012:** Los trámites, los procedimientos y las regulaciones administrativas tienen por finalidad proteger y garantizar la efectividad de los derechos de las personas naturales y jurídicas ante las autoridades y facilitar las relaciones de los particulares con estas como usuarios o destinatarios de sus servicios de conformidad con los principios y reglas previstos en la Constitución Política y en la ley.
- **Decreto 2693 de 2012:** Definir los lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad.
- **Ley 1712 de 2014:** Transparencia y acceso a la información pública.
- **Decreto 20573 de 2014:** Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un

Estado abierto, eficiente, transparente, participativo y que preste mejores servicios con la colaboración de toda la sociedad.

- **Decreto 103 de 2015:** El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea, expedirá los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 de 2014, con el objeto de que sean dispuestos de manera estandarizada.
- **Ley Estatutaria 1757 de 2015:** La presente ley está encargada de promover, proteger y garantizar modalidades del derecho a participar en la vida política, administrativa, económica, social y cultural, y asimismo de controlar el poder político.
- **Decreto 1166 de 2016:** El presente capítulo regula la presentación, radicación y constancia de todas aquellas peticiones presentadas verbalmente en forma presencial, por vía telefónica, por medios electrónicos o tecnológicos o a través de cualquier otro medio idóneo para la comunicación o transferencia de la voz.
- **Decretos 415 de 2016:** La definición de estrategias, políticas, planes, objetivos, metas, estándares y lineamientos en materia de Tecnologías de la Información y las Comunicaciones que adopte cada sector, organismo o entidad, deberán estar articuladas con el Plan Nacional de Desarrollo, los planes de desarrollo sectorial y con la estrategias, políticas, planes, estándares, programas y lineamientos que para el efecto establezca el Ministerio de Tecnologías de la Información y las Comunicaciones.

- **Decreto 704 de 2018:** Por el cual se crea la Comisión Intersectorial para el Desarrollo de la Economía Digital y se adiciona un artículo en el título 2 de la parte 1 del libro 1 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015.
- **Decreto 108 de 2018:** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones.
- **Ley 1978 de 2018:** Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.
- **Directiva Presidencial 02 de 2019:** Simplificación de la interacción digital entre los ciudadanos y el Estado.
- **Decreto 2106 de 2019:** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Ley 2080 de 2021.** Establece los lineamientos de uso de medios electrónicos en los procedimientos administrativos de las entidades públicas.

Componentes

- **Declaración de Propósito y Alcance:** Establece el propósito de la política y define claramente los activos digitales cubiertos, así como las áreas de la organización a las que se aplica la política.
- **Gestión de Riesgos:** Identifica y evalúa los riesgos asociados con los activos digitales y las operaciones de Rotorr. Esta evaluación ayuda a priorizar los esfuerzos de seguridad y determinar los controles necesarios.
- **Controles de Acceso:** Políticas y procedimientos para gestionar el acceso a los sistemas y datos digitales. Esto incluye la autenticación de usuarios, autorización de acceso basada en roles y gestión de contraseñas.
- **Protección de Datos y Privacidad:** Determina medidas para proteger la confidencialidad, integridad y disponibilidad de los datos. Esto implica políticas de cifrado, gestión de acceso a datos sensibles y cumplimiento de regulaciones de privacidad.
- **Gestión de Incidentes:** Respuesta a incidentes que describa los pasos a seguir en caso de una violación de seguridad. Esto incluye la detección, contención, mitigación y recuperación de incidentes de seguridad.
- **Seguridad del Desarrollo de Software:** Implementa prácticas seguras de desarrollo de software para prevenir vulnerabilidades y garantizar

la seguridad de las aplicaciones desarrolladas internamente o adquiridas externamente.

- **Seguridad de la Infraestructura:** Establece medidas para proteger la infraestructura digital, incluyendo redes, servidores, sistemas de almacenamiento y dispositivos finales. Esto implica la configuración segura de sistemas, parcheo de vulnerabilidades y protección contra malware.
- **Concientización y Formación en Seguridad:** Proporciona programas de formación y concienciación en seguridad digital para todos los empleados, contratistas y colaboradores externos. Esto ayuda a promover una cultura de seguridad dentro de Rotorr.
- **Cumplimiento Legal y Normativo:** Asegura que la Política de Seguridad Digital cumpla con todas las leyes y regulaciones aplicables, como GDPR, HIPAA, PCI DSS, entre otras.
- **Revisión y Mejora Continua:** Establece procesos para revisar periódicamente la eficacia de la política de seguridad digital y realizar mejoras en función de las nuevas amenazas, tecnologías y cambios organizativos.

Recursos Financieros

La Gerencia Financiera y Administrativa de Rotorr apropiará anualmente, en su respectivo presupuesto, los recursos necesarios para el efectivo cumplimiento de las obligaciones emanadas de la Política de Seguridad Digital.



Los recursos presupuestales se ejecutarán de conformidad con los programas y proyectos diseñados.