	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 1 de 20

1

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

EMPRESA FÉRREA REGIONAL S.A.S


BOGOTÁ, NOVIEMBRE 2020



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

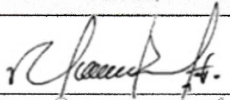
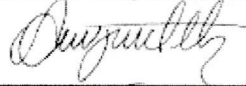
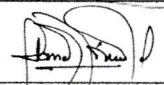

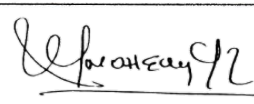
www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 2 de 20

2




Control de Cambios		
VERSIÓN	FECHA	NATURALEZA DEL CAMBIO
1	03/11/2020	Creación del documento.


Responsable	Cargo	Nombre	Firma
APROBÓ	Gerente General	Jeimmy Villamil Buitrago	
REVISÓ	Jefe oficina asesora de Planeación Institucional	Ana Judith Torres Zorro	
	Director Administrativo y Financiero	Iván Javier Gómez	
ELABORÓ	Contratista Dirección Administrativa y Financiera	Giovanny Quecan	
	Contratista Dirección Administrativa y Financiera	María Nohemí Gonzalez	



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 3 de 20

1. INTRODUCCIÓN

La información junto a los procesos y sistemas que hacen uso de ella, son activos muy significativos de una organización. La confidencialidad, integridad y disponibilidad de información sensible logran llegar a ser esenciales para amparar los niveles de competitividad, rentabilidad, conformidad legal e imagen precisos para lograr los objetivos de la entidad y afirmar el cumplimiento de objetivos misionales.

Las organizaciones y sus sistemas de información son sensibles a un número cada vez más elevado de amenazas que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son unos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad producidos voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. Es así como, estos tres términos constituyen la base sobre la que se funda todo el edificio de la seguridad de la información:


- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

De esta forma, y teniendo en cuenta la importancia de los proyectos que lidera la Empresa Férrea Regional SAS-EFR, es fundamental definir las necesidades de sus grupos de interés y la valoración de los controles precisos para mantener la seguridad de la información, para lo cual, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la Entidad, sus objetivos institucionales, sus procesos misionales y que este adaptada a las condiciones específicas y particulares de cada área de la Empresa según corresponda, y para que sea implementada y resguardada por la Dirección Administrativa y Financiera y acogida por todos los funcionarios y contratistas de la Empresa.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 4 de 20

De esta forma, la EFR define una política para la gestión y seguridad de su información, la cual tendrá los criterios de ser sucinta, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Esta Políticas le permite a la Empresa tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, permitiendo una gestión oportuna y efectiva aprovechando de la mejor forma los activos con que cuenta,

Finalmente es de señalar que la Política de Seguridad de la Información de la Empresa se fundamentara y utilizara, como marco de referencia a la futura implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), la norma IS027001.

2. OBJETIVO

Establecer los lineamientos para proteger, preservar y administrar correctamente la información de la Empresa Férrea Regional SAS., junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el desempeño de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no rechazo de la información.


3. ALCANCE

Esta política aplica a todas las áreas que componen la Empresa Férrea Regional SAS, a todos los activos de información, a la totalidad de los procesos internos o externos vinculados a la misma a través de contratos o acuerdos con terceros y a todo el personal que labora en ella cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe que tengan acceso a los servicios de red, aplicaciones y sistemas de información y a las grupos de interés que accedan o hagan uso de cualquier activo de información independientemente de su ubicación, medio o formato.

4. DEFINICIONES

Para efectos de la aplicación de las políticas se adoptan las siguientes definiciones:

- **Activos de Información:** cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 5 de 20

5


- **Activos de Información críticos:** activo de información cuya afectación o alteración puede generar un impacto negativo de carácter económico, legal o al buen nombre de la institución.
- **Archivo:** colección de datos e información del mismo tipo, almacenada en forma organizada como una unidad, que puede emplearse y tratarse como soporte material de la información contenida en éstos.
- **Aplicación:** programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.
- **Base de Datos:** conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.
- **Backups o Copias de respaldo:** copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.
- **Categorías de información:** toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formato o estructura). Decreto 103/2015
- **CIO:** Chief Information Officer
- **Clasificar:** Acto de asignar a la información alguna de las categorías definidas por la Entidad: Reservada, clasificada, Documento en construcción, Pública.
- **Confidencialidad:** Propiedad de la información que determina que esté disponible a personas autorizadas.
- **Código fuente:** Conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.
- **Credenciales de acceso:** Privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.
- **Criptografía:** es una de las disciplinas más relevantes dentro del campo de la seguridad de la información. A la hora de proteger los datos y la información que manejan las organizaciones, tanto física como digital, las técnicas criptográficas están



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 6 de 20

6

ganando mucho peso en la actualidad. Por ello, todo profesional que aspire a ocupar puestos especializados en **Ciberseguridad y Riesgos Digitales**, debe saber **qué es la criptografía** y cuáles son sus principales aplicaciones.


- **Custodio:** Es el encargado de gestionar y administrar la adecuada operación del activo y la información relacionada con éste. En ocasiones el responsable y el custodio son la misma persona.
- **Datacenter, centro de datos o sala de servidores:** área dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).
- **Dispositivo biométrico:** dispositivo de seguridad utilizado en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.
- **Dispositivo móvil:** aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).
- **Información:** todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.
- **Información sensible o vulnerable:** también llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, datos personales, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria.
- **Niveles de backup:** se refiere a la cantidad de copias o respaldos que se tiene de datos determinados. Si se cuenta con una sola copia, se está hablando de un backup de 1er. Nivel; si se tienen dos copias, de un backup de 2do. Nivel. Cuanto mayor sea el número de niveles de backup, menor será el riesgo de perder los datos.
- **Propietario:** En la estructura administrativa de la institución, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 7 de 20

7

- **Reportes básicos académicos (RBA):** son aquellos informes generados por el sistema de información institucional que soportan o sirven de base para la toma de decisiones en la gestión académica y el reporte a los organismos de inspección, control y vigilancia, tanto en el ámbito interno como externo.
- **Responsable:** el jefe de área o gerente de cada una de dichas áreas, será el responsable ante la Institución, de los activos de información registrados como de su propiedad.
- **SAN (Storage Área Network) O Red de Área de Almacenamiento:** recurso compartido, empleado como repositorio de información institucional tanto de funcionarios, docentes y/o contratistas como de grupos y unidades funcionales, donde se definen permisos de acceso de acuerdo a los roles al interior de la organización.
- **Seguridad de la Información:** son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.
- **Servidor:** equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.
- **Servidor de Almacenamiento:** equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.
- **Sistema Operativo (SO) u Operating System (OS):** programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la EFR, se compromete tanto con el desarrollo y la implementación de las políticas de Seguridad de la Información, como de la ejecución de las estrategias e instrumentos para su mejora continua, para lo cual, mantendrá un actuar permanente respecto a:


- Apoyar la implementación de la política de Seguridad de la Información en todas las áreas de la EFR
- Acompañar la revisión y aprobación de las políticas de Seguridad de la Información.
- Garantizar los recursos humanos, técnico y financieros necesarios para la correcta implementación de la política.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 8 de 20

8

- Garantizar que la política se incorpore en la implementación del Sistema de Gestión de Seguridad de la Información.
- Garantizar una adecuada divulgación frente al cumplimiento de la política de Seguridad de la Información, así como su evaluación, monitoreo y control.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Empresa Férrea Regional SAS, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Empresa Férrea Regional, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Empresa Férrea Regional SAS.
- Garantizar la continuidad del negocio frente a incidentes.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1. POLÍTICA PARA DISPOSITIVOS MÓVILES


- Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de la Empresa Férrea Regional SAS. únicamente para desarrollar y cumplir con los objetivos laborales y/o contractuales del personal, procurando que no



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 9 de 20

9

se almacene en estos dispositivos información institucional y siempre en cumplimiento del Reglamento para el uso de las TICS de la entidad.


- En el caso de asignar dispositivos móviles a administrativos o contratistas, estos son de propiedad de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.
- Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por la Dirección Administrativa Financiera (Área de Tecnologías), con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.
- El funcionario asumirá los riesgos y costos asociados a la pérdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados, además del cumplimiento de las políticas y regulaciones vigentes por parte de la Dirección Administrativa y Financiera, concernientes a los costos del activo físico.
- La solicitud de conexión de dichos dispositivos a la red inalámbrica de la Empresa se realizará por intermedio de la mesa de ayuda de tecnología o por los funcionarios debidamente autorizados por el Área de Tecnologías de la Dirección Administrativa y Financiera.
- La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por las regulaciones emitidas por el Área de Tecnologías de la Dirección Administrativa y Financiera, en lo concerniente a autorización de salida de elementos.
- Se prohíbe conectar a los perfiles de red institucionales dispositivos móviles de uso personal, salvo que exista autorización explícita emitida el Área de Tecnologías.
- Se prohíbe la entrada de teléfonos celulares y otros dispositivos móviles a los centros de datos y centros de cableado de la empresa, salvo que exista una autorización explícita emitida por el Área de Tecnologías
- La alta dirección de la empresa podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.
- Para los visitantes y personal de apoyo que ingrese a la empresa y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de la empresa para esta visita, con el fin de evitar usos indebidos de las tecnologías.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca


	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 10 de 20

7.2. POLÍTICA DE CONTROL DE ACCESO LÓGICO

- Es responsabilidad del Área de Talento Humano, informar a la Oficina de Comunicaciones sobre los nuevos empleados de planta que ingresan a la empresa y respecto de los contratistas será competencia de la Oficina Asesora Jurídica, con el fin de poder asignar desde el Área de Tecnologías, los respectivos permisos para el acceso a los recursos tecnológicos de la empresa.
- La Dirección Administrativa y Financiera (Área de Tecnologías) es la responsable de definir y suministrar los mecanismos de acceso lógico para la asignación de permisos y privilegios a los usuarios de acuerdo a sus funciones, términos contractuales y/o roles definidos al interior de la Empresa, así como la modificación los permisos y privilegios de los usuarios en los mecanismos y/o sistemas de autenticación definidos.
- El Área de Talento Humano es la encargada de notificar y dar los lineamientos para la creación, modificación y supresión de permisos y privilegios de usuarios.
- Se prohíbe el uso de las cuentas de usuario administrador local en la empresa, salvo en aquellos casos que estén debidamente justificados y autorizados.
- Los propietarios, responsables y/o custodios de los activos de información de la institución deben revisar periódicamente los derechos de acceso de los usuarios.
- Los propietarios y/o responsables de los activos deben informar inmediatamente sobre las novedades de los derechos de acceso lógico de los usuarios.
- Para la creación y administración de las credenciales de acceso institucionales, para empleados y contratistas, se deben adoptar los lineamientos establecidos por la Dirección Administrativa y Financiera (Área de Tecnologías).
- Los empleados y contratistas son los únicos responsables por la seguridad de sus credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

7.3. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS


- La Empresa Férrea Regional SAS. a través de la Dirección Administrativa (Área de Tecnologías) establecerá la implementación de los sistemas y técnicas criptográficas para la protección de la información, con base en los análisis de riesgos efectuados y con el fin de mantener la confidencialidad, integridad y autenticidad de la información.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 11 de 20

- Cada dependencia de la Empresa Férrea Regional SAS., debe velar por tener una óptima administración de la información y debe implementar sistemas y técnicas criptográficas a la información catalogada como reservada o controlada, acorde a los lineamientos institucionales, con el fin de prevenir riesgos relacionados con la fuga de información durante su transmisión o almacenamiento teniendo en cuenta su nivel privada o simétrica dependiendo el caso.
- Se deben definir custodios o responsables de la información de carácter reservado en cada dependencia de la entidad.
- La Dirección Administrativa y Financiera (Área de Tecnologías) debe brindar el apoyo necesario a los funcionarios y contratistas, en el uso de las herramientas tecnológicas para protección de la información sensible, que debe ser cifrada.
- La Dirección Administrativa y Financiera (Área de Tecnologías), debe definir las herramientas necesarias para el cifrado de datos, de tal forma que preserve la confidencialidad, la integridad y el no-repudio en la transmisión de información sensible entre la comunidad y la Empresa Férrea Regional SAS.
- La Dirección Administrativa y Financiera (Área de Tecnologías), debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.
- El procedimiento de gestión de claves debe tener en cuenta la fecha de finalización de contratos o de retiro de cada responsable del activo de información; de esta manera podrán desactivar, bloquear o eliminar los accesos no autorizados durante el periodo no laboral para que la información no corra ningún riesgo que afecte la continuidad de los procesos de la Empresa Férrea Regional SAS.
- Es responsabilidad del Área de Talento Humano y de la Oficina Asesora Jurídica informar al Área de Tecnologías sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

7.4. POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

- La Dirección Administrativa y Financiera (Área de Tecnologías) debe cumplir acciones de mejoramiento respecto a la seguridad de la información, principalmente respecto al uso de protocolos para realizar transferencia de información digital y/o física entre unidades, usuarios y terceras partes de la entidad.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 12 de 20

12


- Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y estos deben ser conocidos solo por el emisor y por el receptor(es), del mensaje.
- Cada dependencia y/o supervisor de los contratos firmados con terceros, está en la necesidad de verificar la firma de los acuerdos de confidencialidad previo a la transferencia de información entre la Empresa Férrea Regional SAS. y sus proveedores y/o contratistas, en los casos que aplique.
- Las terceras partes implicadas se verán obligadas a firmar los formatos de confidencialidad aplicables. Estos formatos serán entregado por el supervisor del contrato para el caso de proveedores y contratistas, y por el Área de Talento Humano para los funcionarios. El formato hará parte del Sistema Integral de Gestión.
- Toda la información que se reciba o envíe a través de impresoras, máquinas de fax u otros medios de reprografía y transmisión de datos, debe ser monitoreada por el funcionario o contratista que los esté utilizando y debe permanecer siempre sin ningún tipo de documentos o información clasificada como controlada o reservada.
- Toda la información verbal que sea intercambiada por conversaciones formales, atención de llamadas telefónicas y demás procesos que no dejen soportes físicos, debe cumplir con el protocolo de manejo y escalamiento de comunicaciones vigente para la Empresa.
- La Dirección Administrativa y Financiera (Área de Tecnologías) debe realizar capacitaciones y/o difundir los lineamientos institucionales para evitar que se traten temas de Empresa Férrea Regional SAS., en sitios públicos o escenarios no autorizados formalmente para la divulgación de información.
- Salvo casos de estricta necesidad y bajo previa autorización y/o recomendación de la Dirección Administrativa y Financiera (Área de Tecnologías), no se suscribirán o diligenciarán formularios electrónicos para uso personal o para medios de investigación a través de internet, igualmente se debe impedir el diligenciamiento de los datos de ubicación física, teléfonos móviles, teléfonos fijos, estructura organizacional, divulgación de cargos o información sensible de la Empresa Férrea regional SAS., cuando el personal se suscriba o diligencie formularios electrónicos para uso personal o para medios de investigación a través de internet.
- La Empresa Férrea Regional SAS. a través de la oficina Asesora de Planeación Institucional establecerá los propietarios, responsables y/o custodios de los reportes oficiales que serán utilizados para la certificación de totales, valores o listados, especialmente al reportar a entidades externas.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897


www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 13 de 20

13

- La descarga de reportes a herramientas ofimáticas tipo hoja de cálculo será autorizada, pero el archivo de salida será enteramente identificable como un reporte diferente a los que el sistema genere en salidas de solo lectura.
- Los reportes extraídos claramente de los sistemas de información de la Empresa contarán con las siguientes características mínimas:
 - ✓ Deberán ser generados, almacenados y codificados según una fecha de corte claramente estipulada.
 - ✓ Tienen asignado un propietario, responsable o custodio y un validador de la información contenida.
 - ✓ El propietario es el único autorizado para su generación, difusión al interior de la entidad y el subsecuente archivo o salvaguarda.
- Los reportes oficiales utilizados para la certificación de totales, valores o listados, especialmente los dirigidos a entidades externas, organismos de inspección, control y/o vigilancia, deberán ser validados y firmados física o digitalmente por el responsable de la información, para esto la Empresa establecerá en sus procesos y procedimientos los propietarios, responsables y/o custodios para cada caso.
- El director de cada dependencia y/o jefe de oficina serán los responsables de definir los permisos de acceso a los dispositivos de almacenamiento central o SAN, como repositorio de información de la entidad.
- La Dirección Administrativa y Financiera (Área de Tecnologías) será la encargada de definir los mecanismos y lineamientos de uso de la unidad de almacenamiento SAN.
- La recepción de correspondencia rotulada como "Información Confidencial" exclusivamente podrá ser revisada y visualizada por el destinatario de los documentos.
- El envío de correspondencia rotulada como "Información Confidencial" solo podrá salir de la Empresa en medio impreso o digital con la expresa autorización del emisor.
- Cada dependencia está encargada de solicitar a la Dirección Administrativa y Financiera, (Área de Gestión Documental) la correspondencia rotulada como "No Confidencial" que no sea abierta por parte del grupo de correspondencia.
- Toda información clasificada como sensible o vulnerable que sea enviada por medios electrónicos, debe usar algoritmos de cifrado según los lineamientos de la Dirección Administrativa y Financiera (Área de Tecnologías) y la herramienta con la que cuenta la entidad.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 14 de 20

14

- El funcionario encargado de la información de cada dependencia, es el responsable de velar por el cumplimiento de la clasificación, foliación y rotulación de los documentos, de conformidad con los términos ordenados por la Dirección Administrativa y Financiera (Área Gestión Documental) de la Empresa Férrea Regional SAS.

7.5. POLÍTICAS DE DESARROLLO SEGURO


- Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser tramitadas conforme a los procedimientos vigentes y estipulados para tal fin. De acuerdo al procedimiento, las solicitudes realizadas en el tiempo estipulado, serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La sola radicación no implica aceptación y estará sujeta a un cronograma de desarrollo con prioridades según los objetivos misionales de la Empresa Férrea Regional SAS.
- La Dirección Administrativa y Financiera (Área de Tecnologías) es la única dependencia encargada de la realizar desarrollos dentro de la Empresa Férrea Regional SAS. y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptadas para la Empresa.
- Todo desarrollado será puesto en producción según las presentes políticas, los términos y condiciones de privacidad y el reglamento para el uso adecuado de las TICs.
- La Empresa Férrea Regional SAS apoyará la debida aplicación de los lineamientos de desarrollo facilitando los recursos, elementos y lugares de trabajo adecuados para el equipo de desarrollo de la entidad.
- Se prohíbe el acceso y/o uso de los recursos físicos y/o tecnológicos a personal no autorizado y en general, a los recursos asignados al grupo de desarrollo de por la Dirección Administrativa y Financiera (Área de Tecnologías). El intento de uso total o parcial del código fuente de las aplicaciones administradas y/o adquiridas por la Empresa, por parte de personal no autorizado queda expresamente prohibido.
- Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben realizar de conformidad con el procedimiento aprobado para ello.
- Las direcciones o jefaturas de la Empresa solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de las pruebas.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 15 de 20


- Las solicitudes de desarrollo o modificación de aplicaciones que no pueden ser atendidas por la Dirección Administrativa y Financiera (Área de Tecnologías) se registrarán por el procedimiento de "Contratación de bienes y servicios" de la Empresa Férrea Regional SAS.

7.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

- El escritorio de trabajo de todos los funcionarios y contratistas la Empresa, debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.
- Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como "Información confidencial" debe permanecer guardados en un lugar seguro (archivadores con llaves), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.
- El escritorio o la pantalla de inicio del computador, tableta, escritorio virtual o cualquier dispositivo que admita el acceso a información, debe permanecer libre de documentos, carpetas e íconos de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.
- Todos los funcionarios y contratistas la Empresa son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.

7.7. POLÍTICA DE GESTIÓN DE CAMBIOS

- Los recursos que se encuentran administrados por la Dirección Administrativa y Financiera (Área de Tecnologías), que son deben estar incluidos por un procedimiento de gestión de cambios y despliegue del servicio son: las aplicaciones de software que han sido desarrolladas internamente o desarrolladas externamente y entregadas formalmente para su administración, los equipos de cómputo misionales (servidores), las redes de telecomunicaciones locales, extendidas y externas, los manejadores de bases de datos institucionales y la información documentada de los servicios gestionados por esta gerencia.
- Cualquier modificación a las condiciones actuales de funcionamiento de los recursos administrados por la Dirección Administrativa y Financiera (Área de Tecnologías) y que estén cobijados por el procedimiento de desarrollo de sistemas de información, serán


	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 16 de 20

considerados como cambios tecnológicos y por tanto, deben cumplir con los procedimientos y protocolos emitidos por el Área de Tecnología .

- La Dirección Administrativa y Financiera (Área de Tecnologías) determinará las fechas y responsables de efectuar la validación de condiciones y la correspondiente ejecución controlada del cambio.
- En casos de emergencia manifiesta, que estén afectando directamente la normal prestación de los servicios de la Empresa Férrea Regional SAS en cualquiera de sus dependencias, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica; sin que estos cambios sean susceptibles de revisión posterior por parte de la Dirección Administrativa y Financiera (Área de Tecnologías).
- La Empresa Férrea Regional SAS, propenderá porque los servicios tecnológicos que se encuentran tercerizados, cuenten con procedimientos y/o protocolos definidos para la gestión de cambios y despliegue del servicio sobre los servicios contratados.


7.8. POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD

- La responsabilidad de la gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos estará a cargo de la persona designada por el Director Administrativo y Financiero (Área de Tecnología); así el profesional (ingeniero de plataforma tecnológica) es el encargado de la administración de equipos de respaldo masivo de datos.
- El funcionario encargado de la administración de equipos de respaldo masivo de datos, velará por los backups y por la seguridad de los datos contenidos en ellos; asimismo como por su integridad, disponibilidad y confidencialidad y en su efecto el salva guarda de la información debe ser almacenados en un lugar que garantice su protección.
- Los medios de respaldo utilizados para efectuar las copias de seguridad en la Empresa Férrea Regional SAS, serán los definidos por el Director Administrativo y Financiero (Área de Tecnologías) en el procedimiento de copias de respaldo o aquel que lo supla.
- El responsable de la administración de equipos de respaldo masivo de datos, custodiará los respectivos medios de respaldo (y los datos contenidos en éstos) y serán quienes tengan acceso a ellos.
- Se hará respaldo a los archivos, aplicaciones, bases de datos y configuración de los sistemas operativos de los servidores calificados como críticos para la Empresa Férrea Regional SAS y contemplados en el Inventario de Servidores Críticos.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 17 de 20


17

- Se incluye como información a respaldar, las configuraciones completas de los servidores locales o externos que estén en el inventario de la Empresa Férrea Regional SAS.
- La Dirección Administrativa y Financiera (Área de Tecnologías) será la responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, etiquetado, lugar de archivo y el tiempo de retención de las copias.
- Para todos los casos de criticidad definidos en el Inventario de Servidores Críticos, será obligatorio contar con mínimo dos niveles de respaldo.
- La ejecución de las copias de seguridad debe realizarse en horas de poca o ninguna actividad laboral; por lo cual, la Dirección Administrativa y Financiera (Área de Tecnologías) será la responsable de precisar el horario de ejecución de éstas.
- En los casos en que el backup no finalice exitosamente en los tiempos establecidos, éste se relanzará después de evidenciado el fallo, en los tiempos determinados.
- Cuando sea preciso un respaldo por demanda de los servidores críticos, se debe requerir formalmente a través de correo electrónico por parte del personal autorizado, para informar mínimo con 24 horas de anterioridad sobre posibles interrupciones en el servicio a las personas afectadas.
- Todos los respaldos se revisarán con la periodicidad definida y se evidenciarán en la bitácora de backups.
- La comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en el formato para pruebas periódicas de restauración de backups.
- Los equipos para el respaldo de información de la Empresa Férrea Regional SAS, deben estar ubicados en centros de datos (Datacenters) con las medidas de seguridad pertinentes, y tener contratos de soporte y mantenimiento regular vigentes.
- Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la ocurrencia de daños físicos y por consiguiente la pérdida de la información.

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 18 de 20

7.9. POLÍTICA DE GESTIÓN, ADMINISTRACIÓN Y CONSERVACIÓN DOCUMENTAL

- La Empresa Férrea Regional SAS, está obligada a la creación, organización, preservación y control de los archivos, teniendo en cuenta los principios de procedencia, orden original, el ciclo vital de los documentos y la normatividad archivística.
- La Empresa Férrea Regional SAS, deberá garantizar los espacios y las instalaciones necesarias para la conservación de sus archivos. En los casos de construcción de edificios públicos, adecuación de espacios, adquisición o arrendamiento, deberán tenerse en cuenta las especificaciones técnicas existentes sobre áreas de archivos, como lo establece el Archivo General de la Nación.
- La documentación institucional es producto y propiedad de la Empresa Férrea Regional SAS, y ésta ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.
- La Empresa Férrea Regional SAS, podrá contratar con personas naturales o jurídicas, los servicios de custodia, organización, reprografía y conservación de documentos de archivo, esto teniendo en cuenta lo establecido por el Archivo General de la Nación.
- Los funcionarios y contratistas de la Empresa Férrea Regional SAS, al desvincularse de la Entidad, entregarán los documentos y archivos a su cargo debidamente organizados e inventariados, conforme a las normas y procedimientos que establezca la entidad, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.
- La Dirección Administrativa y Financiera tendrá la obligación de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, liderando a través del Área de Gestión Documental la planeación, control, dirección, organización, capacitación, inspección o vigilancia, promoción y otras actividades involucradas en la gestión del ciclo de vida de la información, incluyendo la creación, mantenimiento (uso, almacenamiento, recuperación), y disposición, independientemente de los medios o soportes., así como la prestación de los servicios archivísticos en el archivo de gestión, central e histórico.
- Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, y a lo dispuesto en la Constitución Política de Colombia y la Ley 594 del 2000 o Ley General de Archivos.
- La Dirección Administrativa y Financiera podrá incorporar tecnologías de avanzada en la administración, gestión, seguimiento, control y conservación de sus archivos,

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 19 de 20

19

empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumpla con los siguientes requisitos mínimos:


- ✓ Organización archivística de los documentos
- ✓ Realización de estudios técnicos para la adecuada toma de decisiones, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema a impactar en toda la Dirección Administrativa y Financiera.
- La Gestión Documental dentro del concepto de archivo total, comprende procesos tales como la producción o recepción, distribución, consulta, organización, recuperación y disposición final de los documentos.
- Será obligatorio para la Empresa Férrea Regional SAS, elaborar y adoptar las respectivas tablas de retención documental.
- Es obligación de la Dirección Administrativa y Financiera elaborar inventarios de los documentos que produzcan en ejercicio de las funciones de las diferentes direcciones y jefaturas, de manera que se asegure el control de los documentos en sus diferentes fases.
- Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley; el costo de su reproducción estará fijado por el Acto Administrativo que expida la Empresa.
- La Empresa Férrea Regional SAS., garantizará el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las Leyes.
- Sólo por motivos legales, la Dirección Administrativa y Financiera podrá autorizar la salida temporal de los documentos de archivo, previa autorización de la gerencia de la Empresa Férrea Regional SAS.
- La Dirección Administrativa y Financiera contará con instrumentos de planeación y control para la ejecución de las actividades del Sistema de Gestión Documental, mediante la elaboración de un Plan Institucional de Archivos, Programa de Gestión Documental Físico y/o Electrónico, Sistema Integrado de Conservación y demás instrumentos informacionales o de control.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	POLITICA GESTION Y SEGURIDAD DE LA INFORMACION	Versión: 01
		Fecha: 03-11-2020
	PO-EFR-SI-002	Página 20 de 20

20

- La Dirección Administrativa y Financiera establecerá los diferentes mecanismos, instrucciones o pasos a seguir en temas relacionados con la preservación y conservación a largo plazo de los archivos tanto físicos como electrónicos en cualquier soporte material.

8. APLICABILIDAD

El contenido de esta política aplica para todos los procesos y procedimientos de la Empresa Férrea Regional SAS, así como a todas las actuaciones administrativas que desarrollen las distintas direcciones y jefaturas de la Empresa, por intermedio de sus funcionarios o contratistas.

Se sancionará a todo funcionario o contratista que infrinja las disposiciones del presente documento de conformidad con lo establecido en las leyes y normas vigentes relacionadas.



Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897

www.efr-cundinamarca.gov.co

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca