

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 1 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

Contenido

1. OBJETIVO	5
2. ALCANCE	5
3. DEFINICIONES	5
4. DESARROLLO	9
4.2. POLITICA GENERAL	10
4.3. REVISIÓN DEL MANUAL.....	10
4.4. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	11
4.4.1. Roles y responsabilidades.....	11
4.4.2. Separación de Deberes	12
4.4.3. Contacto con las autoridades	12
4.4.4. Contactos con grupos de interés.....	12
4.4.5. Seguridad de la información en la gestión de proyectos	13
4.5. DISPOSITIVOS MÓVILES	13
4.5.1. Política de Dispositivos Móviles Corporativos.....	13
4.5.2. Política de uso de dispositivos móviles no corporativos.....	14
4.6. TELETRABAJO.....	15
4.6.1. Lineamientos para RMS SAS	15
4.6.2. Lineamientos para el Teletrabajador	16
4.6.3. Lineamientos para la Oficina de Tecnologías e Información.....	17
4.6.4. Directrices y acuerdos por incluir	18
4.6.5. Método de conexión de la modalidad de acceso remoto en RMS SAS.....	18
4.7. SEGURIDAD DE LOS RECURSOS HUMANOS.....	19
4.7.1. Previa vinculación de un funcionario es importante considerar	19
4.7.2. Previa vinculación de un contratista es importante considerar	19
4.7.3. Inicio de Ejecución del contrato.....	20
4.7.4. Durante la Ejecución del empleo de funcionario o contratista.....	20
4.7.5. Terminación o cambio de responsabilidades de empleo.....	21
4.7.6. Procesos Disciplinarios.....	21
4.7.7. Intercambio de Información	21
4.8. GESTIÓN DE ACTIVOS	22
4.8.1. Inventario de activos.....	22
4.8.2. Uso aceptable de los activos.....	22
4.8.3. Uso de equipos de cómputo de propiedad de RMS SAS.....	22
4.8.4. Uso de Internet	23

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 2 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

4.8.5.	Uso del Correo Institucional	24
4.8.6.	Clasificación de la Información	25
4.8.7.	Gestión de Medios Removibles	25
4.8.8.	Disposición de los Medios	26
4.8.9.	Transferencia de Medios Físicos	26
4.9.	CONTROL DE ACCESO	27
4.9.1.	Lineamientos Control de Acceso	27
4.9.2.	Acceso a Redes y Servicios en Red	27
4.9.3.	Solicitud o Inicio de Acceso	28
4.9.4.	Suspensión o Terminación de Acceso	29
4.9.5.	Revisión o Validación de Accesos	30
4.9.6.	Identificación de los Usuarios	30
4.9.7.	Normas para la Creación de Contraseñas	30
4.9.8.	Segregación de Funciones	31
4.9.9.	Requerimientos de negocio para el acceso lógico	32
4.9.9.1.	Control de Acceso a las Aplicaciones y Recursos Tecnológicos	32
4.9.9.2.	Restricción del Acceso a la Información	33
4.9.9.3.	Uso de las Utilidades del Sistema	34
4.9.9.4.	Control de Acceso a la Red	34
4.9.9.5.	Acceso a datos de producción	35
4.9.9.6.	Conexiones remotas	35
4.10.	CONTROLES CRIPTOGRÁFICOS	36
4.10.1.	La Oficina de Tecnología e Información debe:	36
4.10.2.	Los funcionarios y Colaboradores de RMS SAS deben:	37
4.10.3.	Firma Digital	38
4.10.4.	Firma Electrónica	39
4.10.5.	Cifrado de la Información	39
4.10.6.	Llaves Criptográficas	40
4.10.7.	Certificados Digitales	41
4.11.	SEGURIDAD FÍSICA Y DEL ENTORNO	41
4.11.1.	Áreas Seguras	42
4.11.2.	Ubicación y Protección de los Equipos	43
4.11.3.	Servicios de Suministro	43
4.11.4.	Seguridad del Cableado	43
4.11.5.	Mantenimiento de Equipos	43

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 3 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

4.11.6.	Seguridad de Equipos y Activos Fuera de las Instalaciones	43
4.11.7.	Disposición Segura o Reutilización de Equipos.....	44
4.11.8.	Política de Equipo Desatendido, Escritorio Limpio y Pantalla Limpia	44
4.12.	SEGURIDAD DE LAS OPERACIONES	45
4.12.1.	Documentación de Procedimientos Operativos	45
4.12.2.	Control de Cambios	45
4.12.3.	Gestión de Capacidad	45
4.12.4.	Separación de los Ambientes	45
4.13.	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.....	45
4.14.	COPIAS DE RESPALDO.....	46
4.15.	REGISTRO Y SUPERVISIÓN DE EVENTOS	46
4.15.1.	Registro de Eventos.....	46
4.15.2.	Protección de la Información de Registro	47
4.15.3.	Sincronización de Relojes	47
4.16.	CONTROL DE SOFTWARE OPERACIONAL	47
4.16.1.	Instalación de Software en Sistemas Operativos	47
4.17.	GESTIÓN DE LA VULNERABILIDAD TÉCNICA.....	48
4.17.1.	Gestión de las Vulnerabilidades Técnicas	48
4.18.	AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	49
4.18.1.	Controles sobre auditorías de sistemas de información	49
4.19.	SEGURIDAD EN LAS COMUNICACIONES.....	49
4.19.1.	Gestión de la Seguridad en las Redes.....	49
4.19.2.	Transferencia de Información.....	50
4.20.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	50
4.20.1.	Requisitos de Seguridad de los Sistemas de Información.	51
4.20.2.	Seguridad en los Procesos de Desarrollo y Soporte	51
4.20.3.	Ambiente de Desarrollo Seguro	52
4.20.4.	Desarrollo Contratado Externamente.....	52
4.20.5.	Pruebas de Seguridad de Sistemas	53
4.20.6.	Pruebas de Aceptación de Sistemas	53
4.20.7.	Datos de Prueba	53
4.21.	RELACIÓN CON LOS PROVEEDORES	53
4.21.1.	Seguridad de la Información en las Relaciones con los Proveedores.	53
4.21.2.	Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores.....	53
4.22.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 4 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

b.	Acceso no autorizado:	54
c.	Ataque:	55
d.	Código dañino:	55
e.	Denegación de servicio:	55
f.	Robo o pérdida:	55
g.	Alarmas de sistemas de monitoreo:	55
h.	Usos inadecuados:	55
4.23.	NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	55
4.24.	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL RIESGO.....	56
4.24.1.	La Gestión del Riesgos para la Confidencialidad	56
4.24.2.	La Gestión del Riesgos para la Integridad	56
4.24.3.	La Gestión del Riesgos para la Disponibilidad.....	56
4.25.	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.....	56
4.25.1.	Continuidad de la Seguridad de la Información	56
4.25.2.	Redundancias	57
4.26.	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	57
4.26.1.	Identificación Legislación Aplicable y Requisitos Contractuales	57
4.26.2.	Derechos de Propiedad Intelectual	57
4.26.3.	Protección de Registros.....	58
4.26.4.	Privacidad y Protección de Información de Datos Personales	58
4.26.5.	Reglamentación de Controles Criptográficos.....	58
4.27.	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.....	58
4.27.1.	Revisión de la Seguridad de la Información.....	58
4.27.2.	Revisión Cumplimiento Técnico	58
4.28.	CUMPLIMIENTO.....	58
4.29.	BIBLIOGRAFÍA	58

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 5 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

1. OBJETIVO

Establecer las políticas de seguridad de la información, mediante el uso y la apropiación de los lineamientos de seguridad que permitan preservar la confidencialidad, integridad y disponibilidad de los activos de información de RMS SAS.

2. ALCANCE

El manual de políticas de seguridad de la información inicia estableciendo los lineamientos de seguridad desde cada una de sus políticas definidas, para que toda la información creada, procesada, almacenada y utilizada para gestión y soporte en RMS SAS sea accedida por todos los funcionarios, contratistas, proveedores, terceros y demás ciudadanos de forma interna o externa, logrando así el uso y cumplimiento de cada uno de los lineamientos en toda la Entidad.

3. DEFINICIONES

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.
- **Acuerdos de Niveles de servicio:** El modelo de Acuerdo de Nivel de Servicios (ANS) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc. En esta parte del contrato se describe y obliga a un nivel específico de calidad en el suministro. Los puntos que debe cubrir un acuerdo de niveles de servicio son: servicio, soporte y asistencia, provisiones para seguridad y datos, Garantías del sistema y tiempos de respuesta, disponibilidad entre otros.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema de información o la Entidad.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Análisis de vulnerabilidad:** Es la medida o grado de debilidad de ser afectado por amenazas o riesgo según la frecuencia y severidad de estos. La vulnerabilidad depende de varios factores, entre otros: La posibilidad de ocurrencia del evento, la frecuencia de ocurrencia de este, los planes y programas preventivos existentes, la posibilidad de programación anual entre otros.
- **ARL:** Administradora de Riesgos Laborales.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **CCTV:** Circuito Cerrado de Televisión.
- **Ciberamenaza o amenaza cibernética:** Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- **Ciberataque o ataque cibernético:** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- **Ciber-riesgo o riesgo cibernético:** Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 6 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.
- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **CNSC:** Comisión Nacional del Servicio Civil.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.
- **Contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso. Forma parte del PCN.
- **Control de acceso:** El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC).
- **Criptografía:** El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad.
- **CSIRT (Computer Security Incident Response Team):** Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.
- **DBA:** Esta palabra define el administrador de base de datos.
- **Disponibilidad:** Propiedad de ser accesible y utilizable sobre demanda por una Entidad autorizada.²²
- **DRP:** Disaster Recovery Plan - Plan de Recuperación de Desastres.
- **Encriptación (Cifrado, codificación):** La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.
- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
- **Evaluación de Riesgos:** Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de RMS SAS.
- **Evidencia Digital:** También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos.
- **Firewall (Muro de Fuego - Cortafuego):** Herramienta de seguridad que controla el tráfico de entrada/salida de una red.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Hacking - Hackear:** Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.
- **Hacking Ético:** Es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de “pentester”. A la actividad que realizan se le conoce como “hacking ético” o “pruebas de penetración”.
- **Hardware:** Es un término genérico para todos los componentes de Tecnología físicos (Redes, servidores, computadores, Portátiles, etc.).

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 7 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- **HIDS:** Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina. Puede tomar medidas protectoras.
- **IMAC:** Instalación, Movimiento, Actualización y Cambio.
- **Impacto:** El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros Eje: pérdida de reputación, implicaciones legales, etc.
- **Incidente de Seguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Ley 1712 de 2014).
- **Información:** Datos relacionados que tienen significado para la Entidad. Además, es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada.
- **Infraestructura de TI:** Todo el hardware, software, redes, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar aplicaciones y servicios de TI.
- **Integridad:** Propiedad de la información que hace referencia a su exactitud y completitud.
- **Internet:** Es un sistema mundial de redes de computadores, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computador puede, en caso de contar con los permisos apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.
- **Intranet:** Red de una Entidad que utiliza tecnologías y protocolos de Internet, pero que sólo está disponible para determinadas personas, por ejemplo, para los funcionarios o terceros autorizados de una Entidad. Una Intranet también recibe el nombre de red privada.
- **IP:** Es un número que identifica de manera lógica y jerárquica a un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP (parte de la capa de Internet).
- **Keylogger (registrador de teclas):** Es una herramienta que se encarga de registrar las pulsaciones que se hacen sobre el teclado, para guardarlas en un archivo o enviarlas a través de Internet.
- **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el sistema de información.
- **Mitigación:** Acciones desarrolladas antes, durante y después de un siniestro, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto se efectúe la recuperación.
- **MSPI:** Modelo de seguridad y privacidad de la información.
- **Navegador:** Es un programa que, a través de la Web, permite visualizar hipertextos de datos o imágenes que estén en algún computador o en dispositivos conectados a la misma. La función primordial es la de poder acceder a páginas que se encuentran como hipervínculo en algún archivo. A esta acción de traslado de ubicación entre portales o sitios Web se le denomina Navegación. Los navegadores más utilizados son Internet Explorer y Mozilla Firefox.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 8 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- **No repudio:** El no repudio es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
- **Ofuscación:** En computación, la ofuscación se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático o código máquina cuando el programa está en forma compilada o binaria, con el fin de que no sea fácil de entender o leer.
- **OTI:** Oficina de Tecnología e Información.
- **Password:** Significa contraseña, clave, key o llave.
- **PCN:** Plan de Continuidad de Negocio.
- **PILA:** Planilla Integrada de Liquidación de Aportes.
- **Planes de contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.
- **PN:** En informática, acrónimo del Inglés Virtual Private Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo, Internet manteniendo y garantizando la protección de la información.
- **Política:** Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos, que representa los objetivos sobre los que se sustenta el Modelo de Seguridad de los Activos de Información. Debe cumplir con una directriz de la Entidad en general, debe revisarse y estar sujeta a modificaciones ante cambios estructurales.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar.
- **Propietario de Información:** Unidad organizacional o proceso donde se crean los activos de información.
- **Redundancia:** Cuando la opción de las copias de respaldo no satisfaga el RPO (Recovery Point Objective, se refiere al volumen de datos en riesgo de pérdida que una Entidad considera tolerable) y RTO (Recovery Time Objective, expresa el tiempo durante el cual una Entidad puede tolerar la falta de funcionamiento de sus aplicaciones y / o nivel de servicio, sin afectar a la continuidad del negocio) se debe contar con un esquema de redundancia para los componentes de hardware y/o software involucrados.
- **Requerimiento:** Es una característica que el sistema debe tener o es una restricción que el sistema debe cumplir para satisfacer las necesidades del solicitante.
- **Responsable de Seguridad de la Información:** Es la persona con la función de supervisar el cumplimiento de la presente Política.
- **Responsable por el activo de Información:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Riesgo de Seguridad de la Información:** Es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad.
- **Riesgo:** Es el potencial de exposición a pérdidas. Los riesgos, ya sean naturales o provocados por el hombre, son constantes a lo largo de nuestra vida diaria. El potencial es medido normalmente por su probabilidad de ocurrencia en un periodo determinado.
- **Rol:** Es un conjunto de permisos que puede asignarse a un usuario que se registra en un administrador de sistemas. Normalmente, los roles se definen de modo que incluyan permisos para acceder a la información.
- **RPO:** Recovery Point Objective - Punto de recuperación objetivo.
- **Seguridad de la Información:** Son todas aquellas medidas preventivas de los sistemas de información que permitan resguardar y proteger la información.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 9 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- **SG SST:** Sistema de Gestión de Seguridad y Salud en el Trabajo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de Información:** El sistema de información es el sistema que se encarga de recopilar los datos necesarios para que el director del proyecto sepa si el proyecto lleva la dirección prevista. Sin embargo, esa información debe ser puntual, y uno de los problemas que tienen algunas organizaciones es que los datos sobre el proyecto son recogidos, introducidos en un ordenador central, procesados y distribuidos a intervalos tan largos de tiempo que la información resulta inútil a efectos de control.
- **Software de Borrado Seguro:** Software que borra de forma segura, definitiva e irreversible todos los datos almacenados en los discos duros de un equipo informático, incluido el disco de sistema, permitiendo su reciclaje o reutilización con total garantía de seguridad.
- **Teletrabajo:** Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo (Artículo 2, Ley 1221 de 2008).
Tecnología de la Información y Comunicación: Se refiere al Hardware y Software que interviene en el procesamiento de la información.
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo funcionarios, contratistas, terceros, entre otros inequívoco a un individuo o Entidad.
- **Troyano:** Es un programa malicioso capaz de alojarse en un computador y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de apoderarse de la información.
- **UPS:** Uninterruptible Power Supply - Sistema de alimentación eléctrica ininterrumpida.
- **Validación:** Se realiza al comparar si el resultado de las pruebas de usuario es correcto.
- **Verificación:** Comprobación de la correcta funcionalidad de un producto o servicio o de la salida congruente e íntegra de la información.
- **Vulnerabilidad:** Debilidad de un activo o control que pone en riesgo la seguridad de la información y/o sus activos asociados, y que puede ser explotada por una o más amenazas.
- **Vulnerabilidad Día Cero:** Es un tipo de vulnerabilidad que acaba de ser descubierta y que aún no tiene un parche que la solucione.
- **Wireless:** Referido a las telecomunicaciones, se aplica el término inalámbrico (inglés Wireless - sin cables) al tipo de comunicación en la que no se utiliza un medio de propagación físico, sino que utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.
- **WPA2-PSK:** WPA2 (Wi-Fi Protected Access 2), en español «Acceso Wi-Fi protegido 2», es un sistema para proteger las redes inalámbricas (Wi-Fi).

4. DESARROLLO

4.1. GENERALIDADES

La posibilidad de interconectarse a través de redes, la utilización de aplicaciones, y el manejo de la información por parte de los funcionarios, contratistas, proveedores, terceros, ha abierto nuevos horizontes a las instituciones para mejorar su productividad y ofrecer sus servicios, más allá de las fronteras institucionales e incluso nacionales, lo cual, lógicamente ha traído la aparición de nuevas amenazas para los sistemas de

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 10 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

información, como son:

- Ataques cibernéticos internos y externos.
- Pérdida de información ante la migración de datos.
- Navegación imprudente por parte de los funcionarios y contratistas.
- Correos electrónicos maliciosos.
- Explotación automática de vulnerabilidades conocidas.
- Manipulación inadecuada de la información por parte de funcionarios y contratistas.
- Fuga de información por parte de funcionarios y contratistas.

Es así que estas políticas, están orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, a través de los lineamientos y controles que se adoptan en cumplimiento a los requisitos exigidos por la norma técnica Internacional ISO/IEC 27001:2013 y que, con su adopción desde la Alta Dirección de RMS SAS, se establece el cumplimiento a éstas para la seguridad y privacidad de sus activos de información, con el propósito de minimizar posibles impactos no deseados que puedan comprometer los principios esenciales del Sistema de Gestión de Seguridad de la Información.

4.2. POLITICA GENERAL

RMS SAS, Entidad aliada del desarrollo sostenible del país a través de la generación de valor, con una gestión moderna, transparente y eficiente de los recursos minerales de los colombianos, está comprometida con el cuidado y gestión adecuado de la información propia, de los titulares mineros y ciudadanos mediante la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a mantener y preservar los principios fundamentales de Confidencialidad, Integridad y Disponibilidad de la información, al igual que identificar y mitigar sus riesgos asociados.

La Presidencia de RMS SAS mediante la aprobación de esta Política declara su posición y compromiso con el cumplimiento de los requisitos definidos en el marco del SGSI, aspectos en los cuales se involucra directamente la función de seguridad de la información, que tiene como propósito principal mantener un ambiente razonablemente seguro, alineado a la misión, objetivos estratégicos de RMS SAS y requerimientos regulatorios aplicables, definiendo e implementando buenas prácticas que permitan minimizar posibles impactos no deseados que puedan comprometer los principios esenciales de Seguridad de la Información.

4.3. REVISIÓN DEL MANUAL

El manual de políticas de seguridad de la información debe ser revisado al menos una vez al año o cuando surjan cambios relevantes de mejora y de cumplimiento al Sistema de Gestión de Seguridad de la Información en RMS SAS.

La documentación a la que hace llamado cada una de las políticas relacionadas en este manual, hacen parte de la caracterización del proceso de Tecnologías de la Información y de su operación, tales como; (procedimientos, instructivos, formatos, etc.) la cual, se ha venido fortaleciendo a través de actualizaciones o creando algunos de éstos, fundamentales para el cumplimiento de los lineamientos establecidos en este manual, entre éstos están:

- Procedimiento Gestión de Incidentes de Seguridad de la Información.
- Procedimiento Gestión de Cambios Tecnológicos.
- Procedimiento Gestión de Vulnerabilidades Técnicas.
- Procedimiento Gestión de Activos de Información.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 11 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- Procedimiento Gestión con Proveedores.
- Procedimiento Gestión Control de Accesos.
- Procedimiento Derechos Propiedad Intelectual.
- Procedimiento Copias de Respaldo.
- Procedimiento Recolección Evidencia Digital.
- Formato Dar de Baja un Software.
- Formato Acuerdo Intercambio Información.
- Instructivo Seguridad Cifrado.
- Instructivo Copias de Respaldo.

4.4. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.4.1. Roles y responsabilidades

- Todo el personal que tenga acceso a la información de RMS SAS**, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este manual; entre ellos están: servidores públicos, contratistas, proveedores, terceros, convenios entre instituciones y visitantes.
- El Oficial de Seguridad de la Información**, debe asumir la responsabilidad en el desarrollo e implementación del SGSI, debe velar por el cumplimiento de las políticas, debe orientar a todo el personal que tenga acceso a la información de la Entidad, debe coordinar actividades de gestión de riesgos de seguridad y ciberseguridad, debe apoyar la identificación de controles y debe poner en contexto al Comité Institucional de Gestión y Desempeño, de toda la Gestión del Sistema de Seguridad de la Información.
- El Comité Institucional de Gestión y Desempeño**, Este comité asumiera el rol recomendado por la norma ISO 27001:2013, denominado Comité de Seguridad de la información.
- La Alta Dirección**, es el ente máximo en RMS SAS y se encuentra representado por los miembros del Comité Institucional de Gestión y Desempeño de RMS SAS, es responsable de revisar y aprobar la política de Seguridad de la Información y Ciberseguridad; revisar la eficacia de la implementación de la política de Seguridad; proporcionar y avalar los recursos necesarios para el desarrollo e implementación de iniciativas de Seguridad; comunicar la importancia de una gestión eficaz de la Seguridad de la Información y Ciberseguridad; promover el cumplimiento de las políticas y normas definidas en el SGSI.
- El Comité Institucional de Gestión y Desempeño**, es un grupo interdisciplinario conformado al interior de RMS SAS, es responsable de revisar y aprobar las políticas de Seguridad de la Información y Ciberseguridad, revisar los lineamientos definidos por Seguridad de la Información; revisar la implementación del SGSI en Entidad; realizar el seguimiento a la gestión de Seguridad de la Información y Ciberseguridad; apoyar la implementación de los lineamientos en la Entidad en temas de Seguridad de la Información y Ciberseguridad; promover la sensibilización y comunicación al interior de la Entidad del Sistema de Gestión de Seguridad de Información.
- La Oficina de Tecnologías de Información**, la OTI es la líder de la implementación y gestión de los controles de ciberseguridad que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad que se encuentre bajo administración de la Jefatura de la OTI, es responsable definir políticas, procedimientos de gestión de accesos lógicos y esquema, metodología de construcción de roles y perfiles para los accesos a plataformas e infraestructura de la Entidad; definir procedimientos de gestión de logs; definir líneas base, guías de aseguramiento, etc. para

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 12 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

aseguramiento de los sistemas; definir la metodología y procedimientos del ciclo de vida de desarrollo de software incluyendo requerimientos de seguridad en cada etapa; definir la estrategia de respaldo de información; definir políticas y procedimientos de gestión de cambios; definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la Entidad Implementación de planes de remediación de vulnerabilidades; adquirir e implementar herramientas de gestión de logs y correlación; adquirir e implementar tecnologías de seguridad; adquirir, implementar y configurar la red y las plataformas tecnológicas de acuerdo con el diseño propuesto; realizar los ajustes/mejoras necesarias en el proceso de desarrollo de software; ajustes o mejoras a la estrategia de respaldo de información.

- g. **Los Propietarios de los Activos de Información**, es el líder de proceso que tiene la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el modelo de clasificación de la información en RMS SAS, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad; realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida; mantener actualizada la matriz de activos de información definida por el Oficial de Seguridad de la Información y Ciberseguridad, validando los controles de acceso asignado a los activos; identificar riesgos asociados con la Seguridad de la Información en los procesos de los cuales son responsables o tienen participación; reportar oportunamente eventos o incidentes de Seguridad de la Información.
- h. Para mayor nivel de detalle se recomienda consultar el Manual de Organización de la Seguridad de la Información, documento que hace parte del SGSI, en donde se definen todos los roles y responsabilidades para la implementación y gestión de la operación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

4.4.2. Separación de Deberes

- a. Todo el personal que tenga acceso a la información de RMS SAS debe tener claramente definidos sus deberes frente a la gestión de la Seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.
- b. En todos los sistemas de información de la Entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

4.4.3. Contacto con las autoridades

RMS SAS, debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control pertinentes tanto del orden local como el nacional.

La Oficina Administrativa de RMS SAS debe definir, actualizar y publicar el listado de autoridades a contactar en caso de que se sospeche de la violación de la Ley, para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultar el marco legal aplicable.

4.4.4. Contactos con grupos de interés

RMS SAS, a través de la Oficina de Tecnología e Información debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 13 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y amenazas nuevas.

4.4.5. Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar al procedimiento de gestión de proyectos de RMS SAS, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas de la OTI, asegurar que se sigan las siguientes directrices:

- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

4.5. DISPOSITIVOS MÓVILES

Los dispositivos móviles corporativos (teléfonos inteligentes, tablet, portátiles), son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la Entidad.

4.5.1. Política de Dispositivos Móviles Corporativos

- Conexión a redes de RMS SAS:** Con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles la Oficina de Tecnología e Información debe controlar la conexión de dispositivos móviles tales como Smartphone, tablets y computadores personales de los contratistas a la red corporativa, a excepción de los dispositivos que sean propiedad de RMS SAS.
- Software y protección:** Las estaciones de trabajo y equipos portátiles que son propiedad de RMS SAS cuentan con software licenciado y protección contra código malicioso. Solo el personal de soporte de la OTI está autorizado a instalar software específico en los dispositivos móviles propiedad de RMS SAS.
- Auditoría:** RMS SAS se reserva el derecho de revisar cuando se requiera el software instalado y utilizado en equipos de cómputo y servidores, además para los portátiles de los contratistas que se conecten a la red corporativa, se deben validar algunos aspectos de seguridad, entre éstos: antimalware activo y actualizado, sistema operativo actualizado, no permitir que se conecte a internet desde la red de los funcionarios, etc.
- Registro de equipos:** El grupo de servicios administrativos encargado de inventarios debe mantener un registro de los dispositivos móviles asignados (qué dispositivo y a quién se le asigna).
- Mantenimiento de dispositivos:** El mantenimiento de dispositivos que son propiedad de RMS SAS queda restringido al área responsable de su mantenimiento. Por tanto, debe controlar que el usuario no haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización de la OTI.
- Almacenamiento de la información:** La información de RMS SAS que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos, esta tiene que estar sincronizada para evitar duplicidades y errores en las

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 14 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

versiones. Los funcionarios autorizados por su respectivo jefe deben solicitar a la OTI la creación de los almacenamientos de datos para el intercambio de información al interior de la Entidad.

- g. **Conexión a redes:** Todas las conexiones de redes ajenas a la Entidad, deben seguir los lineamientos establecidos en la sección 4.9.2. de este manual denominado Acceso a Redes y a Servicios en Red.
- h. **Notificación en caso de infección:** Si un funcionario o contratista sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal de soporte de la OTI.
- i. **Transporte y custodia:** El computador de RMS SAS, no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo.

En ningún caso se debe descuidar el portátil, celular o tablet si se viaja en transporte público. También debe estar protegidos físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al personal de servicios administrativos grupo de inventarios.

Los dispositivos que contienen información sensible o crítica para RMS SAS no se deben dejar sin supervisión, y donde sea posible, debe estar protegidos bajo llave o se debe usar guayas para asegurarlos, adicionalmente, los computadores portátiles que salgan de RMS SAS y, de surgir un robo a éste, se debe comunicar inmediatamente a la Oficial de Seguridad de la Información, para seguir los pasos de reporte del incidente y comunicarlo a los entes tales como Policía Nacional, el CAI, la Fiscalía, etc.

La información sensible o crítica para RMS SAS no se debe reposar o ser almacenada en los equipos personales de los contratistas.

- j. **Uso del puesto de trabajo:** El usuario debe aplicar las buenas prácticas de uso del puesto de trabajo que sean relativas al uso de un equipo móvil (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, entre otras).
- k. **Responsabilidades:** El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones de RMS SAS. Por tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene. Esta normativa es de obligatorio cumplimiento y debe ser objeto a los acuerdos que se firmen al aceptar el uso de estos dispositivos.
- l. **Viajes de trabajo:** Los funcionarios que viajan por asuntos de la Entidad son responsables de la seguridad de la información propiedad de la Entidad.

4.5.2. Política de uso de dispositivos móviles no corporativos

- a. **Acceso a contratistas:** El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato debe:
 - Tener y usar solo software legal instalado en su equipo.
 - Contar con software antivirus licenciado.
 - Adjuntar a los ingenieros de soporte de la Mesa de Ayuda, el listado del software que va a utilizar y

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 15 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones), se debe entregar al supervisor del contrato con copia a la OTI.

- b. **Información en dispositivos propios:** Los contratistas que tienen información corporativa en sus dispositivos móviles personales son responsables de la seguridad de la información en su poder.
- c. **Antivirus en Dispositivo Móvil:** Es recomendable contar con un software antivirus en su dispositivo móvil.
- d. **Apps en Dispositivos Móviles:** Se recomienda solo descargar apps de sitios oficiales.
- e. **Almacenamiento de información:** En lo posible se debe evitar almacenar información de RMS SAS en los dispositivos móviles personales.

4.6. TELETRABAJO

La implementación del teletrabajo en RMS SAS supone una transformación organizacional, desde sus formas de planear y hacer, hasta sus formas de realizar seguimiento y evaluación. La adopción de esta modalidad y organización laboral requiere del liderazgo del equipo directivo y la participación de un equipo de trabajo coordinado, la utilización de recursos y la movilización hacia un cambio cultural y de procedimientos, que son posibles de alcanzar con el apoyo de las directivas que respalden las iniciativas de aplicar el teletrabajo. El Grupo de Gestión Talento Humano, viene liderando las alternativas que buscan un compromiso institucional y realizando acciones para la adopción e implementación del teletrabajo buscando que se genere beneficios para sus funcionarios, estos lineamientos tanto de seguridad de la Información, Seguridad en el Trabajo se establecen en el **“Procedimiento Implementación Teletrabajo ANM”** liderado por el Grupo de Talento Humano.

4.6.1. Lineamientos para RMS SAS

Afiliar al Teletrabajador al Sistema de Seguridad Social Integral. Debe especificar la clase de riesgo del centro de trabajo del que depende el Teletrabajador, conforme a la clasificación de actividades económicas establecidas en el Decreto 1607 de 2002, o las normas que lo modifiquen, adicionen o sustituyan. De igual forma;

- a. Debe especificar el lugar en el que se presta el servicio. El pago de los aportes se debe efectuar a través de la Planilla Integrada de Liquidación de Aportes (PILA).
- b. El empleador debe realizar la verificación de las condiciones del lugar destinado al Teletrabajo, para el cumplimiento de las condiciones de seguridad y salud en el trabajo con la asesoría de su Administradora de Riesgos Laborales.
- c. Asegurar que el Teletrabajador realice el Auto reporte de condiciones de trabajo, para lograr la identificación de condiciones de trabajo, antes del inicio de una modalidad de trabajo.
- d. Incorporar en el reglamento interno de trabajo o mediante resolución, las condiciones especiales para que opere el teletrabajo en la Entidad.
- e. La jornada laboral del Teletrabajador es la establecida para todos los servidores públicos de la entidad, el Teletrabajador asume con responsabilidad y capacidad de autogestión su modalidad de desempeño laboral, estableciendo sus propias metas y objetivos, que dando a conocer previamente a su jefe inmediato.
- f. Implementar los correctivos necesarios en el lugar de trabajo del Teletrabajador, con la Asesoría de la

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 16 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

Administradora de Riesgos Laborales.

- g. Garantizar que los equipos de trabajo en caso de ser suministrados a los teletrabajadores tengan los medios de protección adecuados para la tarea a realizar.
- h. Informar y dar una copia al Teletrabajador de la política de la empresa en materia de seguridad y salud en el trabajo.
- i. Definir el perfil para el teletrabajo, es decir establecer un conjunto de características personales y de competencias profesionales que permitan que el Teletrabajador se adapte con éxito a la nueva modalidad de trabajo.
- j. Cumplir con todas las obligaciones establecidas en el artículo 21 del Decreto 1295 de 1994.
- k. Reportar todo accidente de trabajo de conformidad con la legislación vigente.
- l. Facilitar los espacios y tiempos para la capacitación de los trabajadores a su cargo en materia de seguridad y salud en el trabajo, para participar en las actividades de asesoría técnica brindados por la Administradora de Riesgos Laborales.
- m. Mantener la motivación de los funcionarios a través de encuentros presenciales, actividades de grupo y una serie de encuentros físicos o virtuales que permitan la participación de opinión respecto al proceso.

4.6.2. Lineamientos para el Teletrabajador

El Teletrabajador debe autorizar a la Administradora de Riesgos Laborales (ARL) y al funcionario que designe el Grupo de Gestión del Talento Humano y Seguridad y Salud en el Trabajo de la Entidad, a realizar visitas periódicas a su domicilio que permitan comprobar si el lugar de trabajo es seguro y está libre de riesgos, debe autorizar también para realizar las visitas de asistencia para actividades de Seguridad y Salud en el Trabajo. Estas visitas deberán ser programas junto con el Teletrabajador y no se pueden realizar de manera arbitraria y sin consentimiento de éste.

- a. El Teletrabajador debe consultar las normas, reglamentos, instrucciones, lineamientos y condiciones de trabajo en la documentación del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) de la Entidad.
- b. Utilizar los equipos y herramientas en caso de ser suministrados en forma adecuada.
- c. Cumplir en la medida, que la información procesada y almacenada se consolide en la infraestructura tecnológica de la Entidad.
- d. En lo posible verifique que sus dispositivos, incluido el enrutador de Internet estén actualizados.
- e. Evitar acceder a redes Wifi-públicas, es importante que como funcionario trabaje en redes de conexiones a internet seguras y protegidas con contraseña.
- f. Asegurar la comunicación a través de herramientas seguras de mensajes de texto, de modo que, si los sistemas de información no funcionan y el correo electrónico no se encuentra disponible no se pierda la

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 17 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

comunicación.

- g. Cumplir con las políticas definidas por la entidad respecto al uso de equipos, aplicaciones y programas informáticos, protección de datos personales, propiedad intelectual y seguridad de la información, que se encuentren señaladas en la Ley.
- h. Utilizar los datos de carácter personal, privado o sensible a los que tenga acceso, única y exclusivamente, para cumplir con las funciones propias en RMS SAS, así como, garantizar que ningún tercero tenga acceso por cualquier medio a los datos de carácter personal, privado o sensible de la Entidad.
- i. Informar a la Oficina de Tecnologías de la Información, según la ruta establecida, sobre conflictos de red o problemas tecnológicos o del equipo que requieran ser solucionados para el cumplimiento de las funciones.
- j. El Teletrabajador se compromete a guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle. Se considera información confidencial la información de propiedad de la entidad y la información que genere el Teletrabajador en virtud de su vinculación laboral.
- k. En general, cumplir con todas las obligaciones establecidas en el artículo 22 del Decreto 1295 de 1994.

4.6.3. Lineamientos para la Oficina de Tecnologías e Información

- a. Fortalecer las capacidades de monitoreo para la operación remota, con el fin de detectar accesos indebidos o situaciones anormales.
- b. Contar con las capacidades y disponibilidad de los servicios de VPN, seguridad en los servicios de correo electrónico y el acceso a la información de la Entidad, realizando un análisis de riesgos.
- c. Fortalecer el monitoreo en el uso de los datos personales e información confidencial.
- d. Realizar oportunamente copias de seguridad de los datos en las plataformas físicas como en la nube.
- e. Disponer de protocolos para contar con una clara identificación de roles y responsabilidades del personal de la OTI.
- f. Contemplar herramientas para la gestión remota en la Entidad.
- g. Preparar a los funcionarios que prestan el soporte para la instalación y la configuración de los equipos para trabajo remoto.
- h. Contemplar las políticas y procedimientos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada de los funcionarios.
- i. Verificar el uso de software licenciado, de tal forma que RMS SAS quede eximida de responsabilidades por el no licenciamiento de software en las estaciones de trabajo propiedad de los funcionarios.
- j. Determinar requisitos de seguridad sobre el firewall y de protección contra software malicioso.
- k. El correo electrónico personal no debe utilizarse para ningún proceso de la Entidad.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 18 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

4.6.4. Directrices y acuerdos por incluir

- RMS SAS podrá eventualmente suministrar un equipo adecuado para las actividades de teletrabajo.
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el Teletrabajador está autorizado a acceder.
- RMS SAS podrá eventualmente suministrar equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto.
- La seguridad física y eléctrica debe ser evaluada por responsables del sistema de SG-SST de RMS SAS.
- El equipo de RMS SAS en el hogar del Teletrabajador debe ser utilizado solo por el funcionario de RMS SAS.
- RMS SAS debe suministrar soporte y mantenimiento del hardware y el software a los equipos de su propiedad asignados al Teletrabajador.
- Se debe realizar ocasionalmente auditoría y seguimiento de la seguridad en los sitios de teletrabajo.
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos de propiedad de ANM asignados al Teletrabajador, cuando las actividades del teletrabajo finalicen.

4.6.5. Método de conexión de la modalidad de acceso remoto en RMS SAS

Actualmente RMS SAS aplica trabajo en casa (Circular 041 del 2020) tanto para funcionarios como contratistas, se están estableciendo los lineamientos para cumplir con el marco regulatorio de Teletrabajo únicamente para los funcionarios.

La siguiente es la forma de conectarse a las plataformas de RMS SAS en la modalidad de acceso remoto y Trabajo en Casa:

- Cuando se requiera realizar labores de trabajo en casa (Circular 041 del 2020) el líder del proceso debe solicitar a la Oficina de Tecnología e Información la creación de una VPN de acceso en los recursos tecnológicos que se hayan definido para trabajo fuera de oficina, indicando el tiempo de acceso por el cual se requiere la conexión.
- El funcionario o contratista debe haber instalado el cliente de VPN en el computador personal de su hogar, con el fin de conectarse vía remota a los servicios tecnológicos de RMS SAS.
- Una vez ejecute el cliente de VPN en el equipo de su casa debe autenticarse con las credenciales otorgadas por la OTI de manera individual y personal.
- Establecida la conectividad a través de la IP del computador de escritorio en las oficinas de RMS SAS el usuario debe autenticarse con las credenciales normales de acceso brindada por el Directorio Activo. Esto permite que el usuario ingrese a los sistemas de información y recursos compartidos como si estuviera dentro de las oficinas de RMS SAS.
- Es muy importante que el usuario no copie archivos desde su sistema de archivos del computador de la casa hacia el computador al cual está conectado por la VPN y que es propiedad de RMS SAS.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 19 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- f. De igual manera es importante que todos los archivos que gestione el usuario mientras estén conectados por VPN en la estación de trabajo propiedad de RMS SAS no sean descargados a las unidades locales o escritorio del computador de la casa.
- g. Es importante que el usuario no se conecte a internet a páginas como YouTube, streaming, redes sociales, entre otras a través de la VPN y desde la estación de trabajo de RMS SAS.
- h. Es importante de igual manera adquirir la rutina de desconexión y conexión continua mientras se realizan labores que no requieren de conectividad.
- i. Es importante que el usuario identifique la forma adecuada de desconexión de su estación de trabajo de RMS SAS para no cometer el error de apagar esta estación de trabajo. De apagar esta estación de trabajo de RMS SAS en forma remota no le permitirá establecer conexiones futuras y deberá acudir a la línea de soporte de la OTI.
- j. El usuario de dispositivos móviles debe usar su carpeta virtual de office 365 (One Drive) para garantizar copias de respaldo de su información a través de esquemas de backup automáticos.
- k. La OTI debe asegurarse de incorporar en la póliza de seguro de equipos de cómputos, los dispositivos móviles de RMS SAS.

4.7. SEGURIDAD DE LOS RECURSOS HUMANOS

4.7.1. Previa vinculación de un funcionario es importante considerar

Aunque la vinculación al sector público se rige por la Comisión Nacional del Servicio Civil (CNSC) por méritos y validación de algunos soportes académicos y laborales. Es importante que el Grupo de Gestión de Talento Humano proporcional a las responsabilidades o al manejo de información sensible de la Entidad, establezca un proceso de verificación de los antecedentes de los candidatos que aspiran a un cargo, el cual se debe llevar a cabo de acuerdo con las leyes y reglamentos, siendo proporcionales a los requisitos dentro de RMS SAS, a la clasificación de la información que va a tener acceso y, a los riesgos percibidos.

La modalidad de Teletrabajo en RMS SAS, únicamente aplica a funcionarios nombrados en carrera administrativa el Grupo de Gestión de Talento Humano formaliza un acuerdo de voluntad, válida que el funcionario cumpla con las competencias, cumpla con las condiciones aprobadas por SST y por ARL y cumpla con las herramientas tecnologías aprobadas por la OTI para formalizar el Teletrabajo a través de un acto administrativo.

4.7.2. Previa vinculación de un contratista es importante considerar

La verificación está a cargo del Grupo de Contratación, la cual debe tener en cuenta toda la privacidad pertinente, la protección de la información de datos personales y legislación laboral, y cuando se permita, debe incluir lo siguiente:

- La disponibilidad de referencias satisfactorias, por ejemplo, una comercial y una personal;
- Una verificación (completa y precisa) de la hoja de vida del solicitante;
- Confirmación de las certificaciones y títulos brindados.
- Una verificación de identidad independiente (pasaporte o documento similar);
- Una verificación más detallada, como la información de antecedentes penales.
- Establecer acuerdos o compromisos contractuales con el personal contratista donde se indiquen las

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 20 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

responsabilidades en cuanto a la seguridad de la información.

- Firma formato de autorización de tratamiento de datos personales por parte del contratista.

4.7.3. Inicio de Ejecución del contrato

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedor o terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información de RMS SAS debe ser informado en el momento que inicie sus actividades contractuales, desde Talento Humano para los funcionarios de planta y para los demás colaboradores de la Entidad, desde el supervisor del contrato, con apoyo del Oficial de Seguridad de la Información, además:

- Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información ejemplo (Websafi, SGD, ANNA Minería, CMC, Trámites en Línea, etc.) o a la red corporativa de RMS SAS, debe hacer la solicitud a través del formato IMAC y, éste debe estar autorizado por el líder del grupo o supervisor del contrato.
- La solicitud a través del IMAC debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información.
- Desde la Oficina de Tecnología e Información se debe gestionar el requerimiento descrito desde el formato IMAC dando alcance a cada solicitud del IMAC, con el especialista del sistema de información o componente tecnológico que corresponda.
- Desde la Oficina de Tecnología e Información se debe notificar el alcance dado desde la solicitud del formato IMAC, con el fin de que el funcionario, contratista, proveedor o tercero, sea notificado y de inicio a sus labores o actividades contractuales.

4.7.4. Durante la Ejecución del empleo de funcionario o contratista

Todos los funcionarios o contratistas a los que se brinde acceso a información confidencial deben firmar un acuerdo de confidencialidad y no divulgación de información, antes de tener acceso a las instalaciones de procesamiento de información. Para los contratistas se maneja el contrato de prestación de servicios de apoyo a la gestión, además:

- Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades y derechos legales con relación a leyes sobre derecho de autor o legislación sobre protección de datos personales.
- Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.
- Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades del funcionario o contratista para el manejo de la información recibida de otras Entidades o partes externas.
- El Grupo de Gestión de Talento Humano y el Grupo de Contratación deben asegurar que los funcionarios

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 21 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

y contratistas respectivamente conozcan y acepten la política de seguridad de la información, para esto deben informar a la Oficial de Seguridad de la Información para que les indique las medidas a seguir para el acceso a esta política.

- e. Para los contratistas dentro del contrato se establecen responsabilidades de seguridad de la información y existe cláusula de confidencialidad.
- f. El Grupo de Gestión de Talento Humano debe establecer los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización en seguridad de la información brindadas por la OTI. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.
- g. El Grupo de Contratación debe establecer los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización en seguridad de la información brindadas por la OTI. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.
- h. El Grupo de Gestión de Talento Humano o el Supervisor del Contrato para los contratistas y/o terceros, deben comunicar a la Oficina de Tecnología e Información (OTI) los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados. Especialmente actualizaciones sobre los accesos a carpetas compartidas y sistemas de información.

4.7.5. Terminación o cambio de responsabilidades de empleo

Se debe informar al personal los deberes y responsabilidades después de la terminación del empleo. Previa emisión de paz y salvo para funcionario o contratista se debe considerar:

- a. Tener formato de paz y salvo firmado por la OTI, el cual asegura que se retiraron los accesos lógicos y físicos de acuerdo con el procedimiento de control de acceso.
- b. Tener formato de paz y salvo igualmente firmado por jefe inmediato o coordinador de grupo donde se aseguró de la transferencia apropiada de información al sucesor del cargo e informe de gestión que indica el estado de las actividades realizadas (en desarrollo, finalizadas o pendientes) y la aceptación del jefe inmediato o coordinador del grupo.

4.7.6. Procesos Disciplinarios

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 734 de 2002 (Código Único Disciplinario), y demás legislación aplicable con relación a los procesos disciplinarios, RMS SAS sigue los lineamientos de los procedimientos establecidos en RMS SAS.

4.7.7. Intercambio de Información

RMS SAS debe firmar acuerdos de confidencialidad o compromisos de confidencialidad con los servidores públicos, intercambio de información entre Entidades Públicas u otros Entes Externos, y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 22 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

En el formato Acuerdo Intercambio Información, deben quedar especificadas las responsabilidades para el intercambio de la información de cada una de las partes y se debe firmar antes de permitir el acceso o uso de dicha información, teniendo presente los siguientes lineamientos:

- a. El intercambio de información con organismos de control y autoridades de supervisión debe seguir el Procedimiento Intercambio Seguro de Información con los que se intercambie todo tipo de información.
- b. Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar el grado de sensibilidad de la información de RMS SAS según procedimiento de Gestión de Activos de Información código APO4-P-009 y las consideraciones de seguridad sobre la misma, así como, los controles a implementar.
- c. Es importante gestionar la firma de un acuerdo de intercambio de información por parte de los representantes legales de las partes involucradas.

4.8. GESTIÓN DE ACTIVOS

Si bien es cierto que los sistemas de información y la misma información digital están sujetos a amenazas graves desde el ciberespacio y, que pueden tener impactos adversos a la operación, comprometiendo los activos de información, tales impactos adversos, también pueden llegar a comprometer la Confidencialidad, Integridad y Disponibilidad de la información procesada, almacenada y transmitida.

Es así como, se deben proporcionar niveles de protección a todos los activos de información de la Entidad. Todas estas medidas o lineamientos son basadas para mitigar los posibles riesgos.

4.8.1. Inventario de activos

Cada área debe ser responsable de mantener actualizado el inventario de activos de seguridad de la información con el acompañamiento del Oficial de Seguridad de la Información de acuerdo con las directrices del Procedimiento de Gestión de Activos.

4.8.2. Uso aceptable de los activos

- a. La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de RMS SAS, son activos de la Entidad y se proporcionan a los funcionarios, contratistas y proveedores o terceros autorizados, para cumplir con los propósitos del negocio.
- b. Todos los funcionarios y contratistas deben etiquetar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices de Etiquetado de la Información que están dentro del procedimiento de Gestión de Activos de Información código APO4-P-009.
- c. Los funcionarios, contratistas, proveedores o terceros y, todo aquel que cuente con acceso a la información de RMS SAS debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes.

4.8.3. Uso de equipos de cómputo de propiedad de RMS SAS

- a. Está prohibido que personal ajeno a la Oficina de Tecnología e Información destape o retire partes de los

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 23 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

equipos de cómputo propiedad de RMS SAS.

- b. La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del proceso de Administración de Tecnología e Información y, por tanto, se debe solicitar soporte a la Oficina de Tecnología e Información para la realización de estas labores.
- c. Los equipos de cómputo no deben ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado, sin previo aviso a la Oficina de Tecnología e Información.
- d. Debe respetarse y no modificarse la configuración de hardware y software establecido por la Oficina de Tecnología e Información.
- e. No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, Celulares, Memory Card etc.) en las estaciones de trabajo de la Entidad, con excepción para aquellos funcionarios que, por sus funciones y actividades propias institucionales, sean autorizados por vicepresidentes/Gerentes, Jefes de Oficina o Coordinadores Regionales, mediante formato IMAC debidamente diligenciado. Las Tablets institucionales no requieren autorización y se hará uso sin restricción alguna.
- f. Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de RMS SAS, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.
- g. Durante la permanencia en las instalaciones de RMS SAS, los equipos de cómputo externos deben estar conectados únicamente a la red de datos corporativos configurada por el proceso de Administración de Tecnología e Información.
- h. Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.
- i. Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, debe conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar picos alto que puedan dañar el componente tecnológico. Estos puntos de corriente regulada se usan para regular la energía y que bien están soportados igualmente por las UPS en dado caso que se vaya la luz y no se apague abruptamente.
- j. La conexión eléctrica de equipos personales debe hacerse a través de los puntos eléctricos no regulados. RMS SAS no se responsabiliza por daños que puedan sufrir estos dispositivos.
- k. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de RMS SAS y que no son propiedad de la Entidad, es responsabilidad única y exclusiva de sus propietarios. RMS SAS, no es la responsable por estos equipos en ningún caso.

4.8.4. Uso de Internet

- a. No se autoriza conectar módems o celulares para acceder a Internet, dentro de las redes (WAN, LAN, WLAN) de la Entidad.
- b. No se autoriza a los funcionarios y contratistas acceder a cualquier página o dirección que contenga

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 24 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la Entidad como violencia, terrorismo, grupos al margen de la Ley, discriminación, entre otras.

- c. No se autoriza el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.
- d. Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de RMS SAS, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.
- e. Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.
- f. Todas las actividades realizadas en los sistemas de información de RMS SAS deben ser monitoreadas con el fin de preservar la seguridad informática de la Entidad.
- g. Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la Entidad. Esto es competencia de la Oficina de Tecnología e Información.
- h. Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la Entidad.

4.8.5. Uso del Correo Institucional

- a. La Entidad debe proveer a los usuarios un correo electrónico institucional con el dominio anm.gov.co.
- b. El estándar para la creación de buzón del correo es “primer nombre + punto (.) + primer apellido” ejemplo: Pedro.González, en caso de que exista un homónimo, se debe crear de la siguiente manera “primer nombre + punto (.) + primer apellido + primera letra del segundo apellido” ejemplo: pedro.gonzálezd, en dado caso continúe la igualdad, la Oficina de Tecnología e Información debe asignar un correo basado en el nombre completo del colaborador.
- c. La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la Entidad.
- d. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la Entidad; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.
- e. El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.
- f. Para el envío de información masiva a los grupos generados para Divulgación como ANM Nacional y ANM Central, es limitado y es de uso exclusivo del grupo de Talento Humano, el grupo de comunicaciones y El

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 25 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

Presidente.

- g. Cuando se reciban correos desde una cuenta de divulgación como ANM Nacional y ANM Central evite dar una respuesta utilizando la opción responder a todos.
- h. El servidor de correo debe bloquear archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.
- i. Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atacar contra los sistemas, programas y datos de la Entidad.
- j. No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia, sin embargo, es responsabilidad de cada usuario mantener sus sesiones atendidas, entiéndase no dejar los equipos sin cerrar sesión al alcance de cualquier intruso.
- k. El usuario debe notificar cualquier recibo de correo sospechoso, a la cuenta servicios.tecnologia@rmsltda.com, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

4.8.6. Clasificación de la Información

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 1712 de 2014 y sus decretos reglamentarios y la Ley 1581 de 2012 de protección de datos personales RMS SAS clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el Procedimiento de Gestión de Activos, además:

- a. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la Matriz de Activos de Información o informar al Oficial de Seguridad de la Información para su debido registro.
- b. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente.
- c. El funcionario, contratista, proveedor y/o tercero responsable del activo de información, debe definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.
- d. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

4.8.7. Gestión de Medios Removibles

Los medios removibles en los que se almacene información clasificada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento de gestión de activos (tabla controles según clasificación de información). La Oficina de Tecnología e Información (OTI) debe establecer herramientas tecnológicas para el cifrado de la información, además:

- a. La OTI debe proveer el uso de carpetas compartidas en lugar de medios removibles para el intercambio de

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 26 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

información al interior de la Entidad.

- b. Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se deben bloquear mediante directorio activo y quien requiera hacer uso de estas unidades debe solicitar la activación a la Oficina de Tecnología e Información, previa autorización del Gerente, indicando el tiempo por el cual se requiere la activación.
- c. Los funcionarios o contratistas que requieran los medios removibles habilitados de forma permanente deben tener una autorización firmada por el Gerente.
- d. Se debe hacer seguimiento a la transferencia de información de los medios removibles mediante herramientas tecnológicas que permita realizar la trazabilidad de la información transmitida a estos medios.
- e. El Gerente y jefes de oficina, deben controlar el ingreso y salida de los equipos de cómputo y medios extraíbles de almacenamiento de información de las instalaciones de RMS SAS, mediante el AP02-P-001-F-006 Formato Único de Retiro de Elementos.
- f. Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la Entidad se debe remover y formatear el dispositivo.
- g. Los medios removibles no deben ser utilizados en sitios públicos como un café internet, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

4.8.8. Disposición de los Medios

- a. Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.
- b. La información en las cintas de backups que contienen información pública clasificada o información pública reservada se debe cifrar, además deben estar protegidas en un lugar seguro y bajo llave, el lugar que disponga la OTI.
- c. La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.
- d. Se debe guardar varias copias de datos valiosos para RMS SAS en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.
- e. Las cintas de backups se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones, para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios etc.
- f. Se debe realizar pruebas a las copias de datos para validar la integridad de la información.

4.8.9. Transferencia de Medios Físicos

- a. Para la transferencia de medios físicos (Información en carpetas selladas, computadores, dispositivos móviles, tablets, etc.) se debe seguir las directrices del Procedimiento de Gestión de Activos y sus documentos relacionados (mensajería externa o interna - tabla controles según clasificación de

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 27 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

información).

- b. El embalaje de la información debe ser apropiada que mitigue los daños físicos que se puedan presentar en el transporte de la misma, protegiendo la exposición al calor, humedad o campos electromagnéticos.
- c. Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

4.9. CONTROL DE ACCESO

4.9.1. Lineamientos Control de Acceso

El Proceso de Administración de Tecnologías e Información debe controlar el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

- a. **Lo que necesita conocer:** solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
- b. **Lo que necesita usar:** solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

4.9.2. Acceso a Redes y Servicios en Red

- a. El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.
- b. La Oficina de Tecnología e Información provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado por usuario mediante la autorización previa de la Gerencia o el Coordinador de Tecnología.
- c. Para los usuarios que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, mediante formato IMAC dirigido a la Oficina de Tecnología de la Información, justificando la necesidad del acceso.
- d. La conexión remota a la red de área local de RMS SAS debe ser realizada a través de una conexión VPN segura, suministrada por la Oficina de Tecnología e Información, la cual debe ser aprobada por Gerencia mediante formato IMAC dirigido al jefe de la Oficina de Tecnología e Información.
- e. La conexión a servicios en red se controla mediante el directorio activo, a excepción del control de acceso físico mediante acceso biométrico y el servicio de impresión.
- f. La conexión a redes públicas abiertas está prohibida, así como la conexión a redes Wi-Fi públicas.
- g. Todo acceso o privilegio a sistemas, redes, aplicaciones o información de RMS SAS debe estar aprobado por los líderes de las áreas y los propietarios de información según aplique.
- h. El acceso a la red Wi-Fi de RMS SAS para los visitantes debe realizarse por la red destinada para estos accesos a visitantes, de no conocer este acceso se debe solicitar a la Mesa de Ayuda para su debida

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 28 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

activación.

- i. Es responsabilidad del Oficial de Seguridad de la Información definir los lineamientos a seguir para garantizar accesos seguros y confiables a los sistemas y plataformas de RMS SAS.

4.9.3. Solicitud o Inicio de Acceso

Los procedimientos definidos por RMS SAS para administrar los privilegios de acceso de los usuarios a la información de RMS SAS deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta por lo menos, que:

- a. Los líderes de grupo son los únicos funcionarios autorizados para realizar las solicitudes de acceso a los sistemas de información o delegados formalmente por el líder para ejecutar esta actividad, que se realiza mediante el formato IMAC.
- b. Ningún colaborador autorizado puede realizar solicitudes de acceso para sí mismo, excepto para el Gerente y Jefes de Oficina.
- c. Los jefes o delegados deben realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo en las herramientas establecidas por RMS SAS para tal fin, para lo que debe tener en cuenta las matrices de accesos previamente definidas y gestionadas por cada especialista funcional de la OTI.
- d. La OTI, asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada grupo y/o proceso.
- e. La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro. Esta entrega debe estar controlada por un proceso de administración formal que permita, informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios / contraseña) otorgados.
- f. El re-uso de nombres de cuentas no está permitido, aun cuando la cuenta de usuario ya se encuentre eliminada/inactiva. Para lo cual la OTI debe aplicar el procedimiento definido para la creación de cuentas de usuario y correo electrónico.
- g. Asignar identificaciones únicas a todos los funcionarios y colaboradores, es decir, que no debe existir cuentas genéricas para el acceso o gestión sobre los sistemas tecnológicos de la Entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). Cuando por razones del negocio u operación deben ser creadas únicamente como cuentas de servicio y no deben ser utilizadas por ningún funcionario o contratista. En el Directorio Activo se debe detallar el responsable de cada cuenta.
- h. La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir el uso de las claves de usuarios administradoras, tales como: "root", "adm" y "system", entre otros, debe ser controlado por la OTI quienes son los responsables de dichos accesos, de esta gestión existirá un registro que permita identificar la trazabilidad es decir conocer el funcionario o colaborador que está haciendo uso de estos accesos.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 29 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- i. Todo usuario del sistema debe tener un mecanismo de autenticación privado.
- j. En caso de ser necesario se debe utilizar métodos de autenticación fuerte como sensores biométricos, huellas dactilares o “tokens” de hardware.
- k. El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.
- l. Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.
- m. La utilización de información compartida por ejemplo unidades de red debe estar restringida mediante controles ejecutados por la OTI. El responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.
- n. Todos los usuarios creados en ambiente de producción de los sistemas de información o servicio de RMS SAS deben ser solicitados según el procedimiento establecido en el formato IMAC, con el fin de mantener un registro formal o la trazabilidad de los privilegios otorgados a los colaboradores autorizados para cumplir con las labores asignadas, utilizando algún servicio tecnológico.
- o. Los accesos a la información o sistemas de información no deben otorgarse por los administradores de Base de Datos y de Aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización.
- p. Se debe considerar la inclusión en los contratos del personal y contratos de servicio con terceros, cláusulas que especifiquen las sanciones si los colaboradores o terceros intentan un acceso no autorizado.

4.9.4. Suspensión o Terminación de Acceso

El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador de RMS SAS que se encuentre en licencia, permisos, vacaciones, entre otras novedades; si por necesidad del negocio se requiere mantener habilitado, únicamente para cargos a nivel de Jefatura y Gerencia, para los demás cargos si existen funciones que se deban reasignar para dar continuidad durante dichas novedades, los jefes o delegados deben realizar las solicitudes de acceso necesarias a los colaboradores que ejecutaran las actividades, una vez cumplido el plazo se debe solicitar retiro de los permisos, además:

- a. La OTI debe mantener actualizado el Directorio Activo con la información de los usuarios de funcionarios y colaboradores, de acuerdo con el último formato IMAC solicitado para la gestión de los usuarios de RMS SAS; en la cual debe registrarse las novedades de estos para que se realice la suspensión o eliminación según corresponda.
- b. Se debe definir y aplicar reglas para deshabilitar las cuentas de usuarios de red que no han cambiado la contraseña durante 60 días, igualmente se debe definir qué cuentas deben quedar bloqueadas porque no fueron reactivadas y eliminar aquellas cuentas que no presentan ninguna actividad desde su creación.
- c. Los usuarios creados con acceso a las bases de datos que no hayan sido utilizados en un período mayor o igual a 3 meses debe ser inhabilitados por los administradores de Base de Datos, así mismo, si éstas no han sido utilizadas en un periodo igual o mayor a 6 meses debe ser eliminadas.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 30 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

d. La OTI debe disponer de mecanismos documentados para desactivar el acceso a los usuarios, en las siguientes, situaciones:

- Desvinculación por parte de los funcionarios a RMS SAS.
- Ausencias temporales de los colaboradores por motivo de vacaciones, viajes o licencias.
- Los funcionarios de la Entidad que no han accedido a los recursos tecnológicos por un período de tiempo determinado.
- Número de intentos fallidos durante el ingreso de la contraseña a un recurso tecnológico o aplicativo o cuando se presente algún tipo de incidente de seguridad de la información sobre el código de usuario.
- Cuando el responsable de la información lo solicite.

4.9.5. Revisión o Validación de Accesos

Las autorizaciones de acceso a sistemas y/o aplicaciones deben ser revisadas periódicamente por los coordinadores de grupo y/o propietarios de la información.

El Oficial de Seguridad de la Información debe revisar o monitorear en intervalos de tiempo regulares los privilegios asignados a los usuarios, para asegurar que no tengan accesos no autorizados; teniendo en cuenta los siguientes aspectos:

- a. Validar solicitudes de accesos especiales como USB y VPN, administrador de máquina y acceso remoto.
- e. Los derechos de acceso de un usuario se deben revisar y reasignar, ya sea por cambio de cargo o traslado de área, dentro de la misma Entidad. Teniendo en cuenta:
 - El nuevo jefe debe realizar los requerimientos de acceso a los sistemas de información que el colaborador requiera según las funciones que le sean asignadas en el área.
 - Se asignan los permisos autorizados por el nuevo jefe y se eliminan los demás permisos y privilegios del cargo anterior.

4.9.6. Identificación de los Usuarios

Todos los usuarios deben tener un identificador único (ID de usuario) para uso personal y se debe seleccionar una técnica de autenticación adecuada para garantizar la identidad del usuario. Este control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, proveedores, programadores de sistemas y administradores de bases de datos etc.).

4.9.7. Normas para la Creación de Contraseñas

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del colaborador. Como medida de seguridad los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

- a. Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 31 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- b. La contraseña debe tener al menos ocho (8) caracteres, donde se tengan letras en mayúscula, minúscula y números o caracteres especiales.
- c. Las contraseñas deben cambiarse mínimo cada 60 días y no se pueden repetir las últimas 10 contraseñas.
- d. Si se digita más de 3 veces la contraseña de forma inválida, la cuenta del usuario debe ser bloqueada. Solicitar el desbloqueo a través de un requerimiento desde Mesa de Ayuda. Para el desbloqueo de la cuenta a través de unas validaciones el usuario puede rescatar su contraseña de manera autónoma en una interfaz web de RMS SAS.
- e. La contraseña no debe incluir un nombre o palabra en algún lenguaje común (español, inglés, etc. evitando que éstas sean vulnerables a los ataques de diccionarios.) u otra información pública como números de tarjeta de crédito, nombres de calles y números telefónicos. Una contraseña debe incluir información que solo sea conocida por el usuario.
- f. No utilizar contraseñas por defecto, éstas se deben cambiar una vez se adquieran componentes tecnológicos nuevos o sistemas de información que perfectamente las puedan incluir.
- g. No es permitido compartir usuarios, contraseñas y cualquier mecanismo de autenticación asignado (ej. Tokens).
- h. Dispositivos como los Tokens que permitan el acceso a un sistema de información en la Entidad o Entidades externas deben ser almacenados y salvaguardados en lugares seguros, donde solamente el dueño del Token tenga acceso.
- i. En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad, ésta debe ser cambiada inmediatamente por el administrador de la aplicación y debe reportarse al Oficial de Seguridad de la Información.
- j. Los usuarios deben tener presente no incluir las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en una macro o sistema de información.

4.9.8. Segregación de Funciones

La segregación de funciones en RMS SAS representa una actividad de control clave para separar las responsabilidades de las diversas actividades que intervienen en la ejecución de los procesos, una adecuada segregación de funciones permite mantener la confidencialidad, integridad y disponibilidad de la información.

- a. La segregación de funciones permite reducir el riesgo de un mal uso accidental o deliberado del sistema, razón por la cual se debe definir lineamientos para evitar accesos no autorizados que permitan, modificar o utilizar los activos sin autorización o detección.
- b. La segregación de funciones en cada uno de los procesos de la Entidad, debe garantizar como mínimo la independencia de las siguientes actividades:
 - Operación de equipos de cómputo
 - Administración de red
 - Administración de sistemas Operativos
 - Administración de Bases de datos

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 32 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- Administración de aplicaciones (Administradores Funcionales)
- Desarrollo de software
- Gestor de cambios
- Administración de seguridad informática

Teniendo en cuenta lo anterior los líderes de cada proceso, tienen la responsabilidad de generar las respectivas matrices de Segregación de Funciones las cuales deben ser validadas periódicamente.

4.9.9. Requerimientos de negocio para el acceso lógico

Las Jefaturas, Vicepresidencias, Presidencia o líderes de proceso deben definir los privilegios de los colaboradores a su cargo siempre, bajo los conceptos de menor privilegio y necesidad de saber, igualmente es responsabilidad de la Jefatura de la OTI establecer procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por los responsables del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación.

4.9.9.1. Control de Acceso a las Aplicaciones y Recursos Tecnológicos

- Los accesos a las aplicaciones y recursos tecnológicos deben ser restringidos y monitoreados de acuerdo con las necesidades del negocio.
- El Oficial de Seguridad de la Información debe definir y mantener los lineamientos para controlar el acceso de los colaboradores a las aplicaciones o recursos tecnológicos.
- El Oficial de Seguridad de la Información debe implementar mecanismos de monitoreo de accesos, control de privilegios con el fin de identificar posibles incumplimientos a las políticas de Seguridad de la Información.
- La selección de los mecanismos de control de acceso a las aplicaciones se define de acuerdo con la criticidad y/o sensibilidad de la información (procesada, almacenada, usada) utilizada por el proceso.
- Se debe utilizar medidas de seguridad para restringir el acceso a los aplicativos, bases de datos y en general a los recursos tecnológicos.
- Las aplicaciones de la Entidad deben contar con mecanismo para el manejo de contraseñas, los cuales sean interactivos y cumplan con los parámetros de seguridad definidos, para ello debe tener en cuenta:
 - Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación.
 - En los aplicativos y/o sistemas de información, tener en cuenta los lineamientos de contraseñas robustas.
 - Los aplicativos deben obligar a los usuarios a cambiar las contraseñas temporales en su primer ingreso o registro.
 - Mantener un registro de claves de usuario previas y evitar el re-uso.
 - No mostrar las contraseñas en la pantalla en el momento de ingresarlas.
 - Almacenar las contraseñas cifradas con algoritmos fuertes, mediante uso de funciones hash.
 - Validar el nivel de seguridad de las contraseñas de acceso creadas por los colaboradores, permitiendo

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 33 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

solamente el uso de contraseñas fuertes.

- Solicitar la modificación en un periodo definido de las contraseñas de ingreso a los aplicativos de RMS SAS.
- Implementar políticas de bloqueo automático del usuario cuando la contraseña se haya ingresado de manera errónea por tres veces, igualmente definir e implementar mecanismos que permitan su desbloqueo incluyendo: un tiempo de desbloqueo automático de 15 minutos, asignación de nueva contraseña haciendo uso del sistema de control de acceso, entre otras alternativas.

4.9.9.2. Restricción del Acceso a la Información

- a. El acceso de los usuarios a la información y las funciones del sistema de la aplicación debe limitarse de acuerdo con la política de control de acceso definida.
- b. Las restricciones para el acceso a las aplicaciones se deben basar en el rol que el usuario desempeñara, para ello se debe cumplir con los siguientes aspectos:
 - Generar menús para controlar el acceso a las funciones del sistema de aplicación.
 - Controlar los permisos de acceso de los usuarios: lectura, escritura, modificación y eliminación.
 - Controlar y definir la interacción e intercambio de datos entre sistemas (internos y externos).
 - Hay que asegurar que las salidas de información de los sistemas, aplicaciones o plataformas que manejan información confidencial sólo contengan la información requerida para el cumplimiento de las labores y solamente el personal autorizado tenga acceso a esta.
- c. Restricciones de uso sobre los sistemas operativos.
- d. Dentro de los aspectos para tener en cuenta por parte de los usuarios, para un buen uso de los sistemas operativos están:
 - El administrador de la plataforma es el responsable de otorgar los accesos a los recursos del sistema operativo.
 - Las autorizaciones a las rutinas del sistema operativo no deben permitir modificaciones, en caso de requerirse, éstas deben ser autorizadas y documentadas.
 - El uso de herramientas o utilitarios propios de los sistemas operativos deben ser limitado a personal autorizado y su uso está restringido a casos específicos, debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados.
 - Los administradores y operadores de plataformas no deben tener acceso a aplicaciones en producción, archivos y transacciones en línea.
 - Está prohibido el uso de herramientas intrusivas con fines de vulnerar la seguridad del sistema operativo, bases de datos, redes etc.; solamente el Oficial de Seguridad de la Información podrá utilizarlas en la realización de pruebas de hacking ético o quien este delegue.
 - Las sesiones que no han presentado ningún tipo de actividad por un período de tiempo determinado

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 34 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

deben finalizar automáticamente de acuerdo con la configuración definida; esto mismo aplica para los accesos remotos.

- Todos los colaboradores de RMS SAS deben cumplir con las normas de contraseñas.
- Todas las estaciones de trabajo deben estar plenamente identificadas para garantizar la conexión de equipos confiables, esto debe venir acompañado de correctas configuraciones de red que restrinjan la conexión a los equipos de la granja de servidores permitiendo solamente las conexiones necesarias.
- Se deben registrar los intentos exitosos y fallidos de autenticación del sistema.

4.9.9.3. Uso de las Utilidades del Sistema

El jefe de la Oficina de Tecnología e Información debe implementar procedimientos para restringir y controlar el uso de los programas de utilidad que podrían ser capaces de vulnerar los controles del sistema y/o aplicación y mantener un inventario de éstos. Se debe tener en cuenta entre otros aspectos:

- Limitar el uso de los programas utilitarios a un número práctico mínimo de usuarios autorizados y confiables.
- Registro de todo uso de los programas de utilitarios.
- Definir y documentar los niveles de autorización de los programas de utilitarios.
- Grabar las sesiones sobre servidores críticos de las cuentas privilegiadas.

4.9.9.4. Control de Acceso a la Red

El jefe de la Oficina de Tecnología e Información debe implementar procedimientos para controlar el acceso a la red de RMS SAS proporcionando a los funcionarios o colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se debe considerar entre otros los siguientes lineamientos:

- a. La utilización de recursos de red debe ser limitada a usuarios autorizados.
- b. Para acceder a las redes de datos de RMS SAS, se requiere autenticación individual.
- c. Las contraseñas de red de usuario y las contraseñas de usuarios privilegiados deben ser cambiadas periódicamente (mínimo una vez por mes).
- d. Cuando se requiera realizar transferencia de información del negocio, en especial la clasificada como publica confidencial o publica reservada, se debe utilizar mecanismos de cifrado o canales seguros.
- e. RMS SAS permite a usuarios externos (proveedores o terceros) acceder a las redes institucionales desde redes externas, bajo ciertas condiciones de seguridad. Dicha autorización debe ser tramitada por el líder del proceso ante la OTI, en caso de ser aprobada, no se deben utilizar identificadores genéricos.
- f. Los líderes de proceso que tienen acuerdos contractuales con proveedores o terceros y, si éstos requieren acceso a los recursos tecnológicos de la Entidad, se debe contar con autorización previa de parte de la Jefatura de la OTI. De igual manera se debe asegurar que los proveedores o terceros conozcan y acepten las políticas de Seguridad de la Información y que las normas o acuerdos específicos de seguridad que apliquen para la actividad contractual queden registrados en el documento de acuerdo contractual.
- g. Los administradores de sistemas deben identificar y documentar los niveles máximos de servicio. Así

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 35 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

mismo, hay que asegurar que el acceso y utilización de los recursos informáticos cumplen con los requerimientos de seguridad.

- h. Se deben definir validaciones o revisiones teniendo en cuenta la criticidad de los proveedores o terceros ante el cumplimiento de la política de Seguridad de la Información, como los acuerdos específicos de seguridad para el desarrollo de las labores con los terceros. Este cumplimiento podrá ser validado por entes de control.
- i. Cuando los usuarios acceden a datos en redes locales y remotas vía VPN, debe utilizar mecanismos de seguridad para autenticarse ante las redes. Las solicitudes deben ser realizadas ante la OTI quienes deben realizar el trámite respectivo y para lo cual es requisito contar con usuario de red asignado, posteriormente se remite al jefe de la OTI para asignar el acceso.
- j. El jefe de la OTI debe mantener las redes de datos internas segmentadas por VLANS, grupos de servicios, usuarios y sistemas de información.
- k. Todas las estaciones de trabajo conectadas a la red de RMS SAS deben contar con herramientas de seguridad, como firewalls, HIDS, Filtros de Contenido, Antivirus, Endpoint, entre otros.
- l. El servicio de correo externo no debe ser habilitado para proveedores o terceros y temporales, salvo casos excepcionales por funcionalidad de un servicio.

4.9.9.5. Acceso a datos de producción

El jefe de la OTI debe tener en cuenta las siguientes consideraciones respecto al acceso a datos de producción:

- a. Se deben definir un procedimiento para el control de acceso el cual incluya la aprobación, supervisión etc. a los datos de producción.
- b. Para todo usuario autorizado, la disponibilidad de la información debe ser limitada.
- c. Los procedimientos deben ser definidos para conceder el acceso de emergencia de usuarios a datos de producción.
- d. El acceso a datos de producción debe ser auditable. El acceso a los datos de producción debe generar archivos de trazabilidad (logs) que pueden ser auditados, por entes de control.
- e. Para acceder a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación) se debe contar con autorización de la Oficina de Tecnología e Información, lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.

4.9.9.6. Conexiones remotas

Se define como acceso remoto cualquier conexión establecida desde fuera de la Entidad que requiere acceso a la red o aplicaciones internas de RMS SAS por parte de funcionarios, proveedores entre otros.

Para dichos accesos se debe tener en cuenta las siguientes consideraciones:

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 36 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- a. Iniciar la conexión remota de red desde computadores y sitios seguros, evitar conexiones remotas desde computadores públicos o desconocidos como, cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.
- b. Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- c. La autenticación para los accesos remotos debe complementarse con doble factor de autenticación y/o a través de la plataforma de seguridad CyberArk.
- d. Si es el caso se debe aprobar o aceptar del lado de la Entidad para que el proveedor tome el control remoto. No debe permitirse el acceso y control total de manera automática, sino cuando RMS SAS lo autorice y monitorear las actividades realizadas por estos proveedores.
- e. El trabajo remoto por VPN lo debe solicitar el jefe directo, conforme al procedimiento definido de solicitud de requerimientos (IMAC). la OTI valida la pertinencia de dicha solicitud y otorga el privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.
- f. El acceso remoto a los servidores debe estar controlado por las políticas del Directorio Activo para el ingreso por este servicio, es decir quién puede o no ingresar por este servicio, teniendo presente que este servicio debe ser autorizado únicamente para los administradores de los servidores, los usuarios o proveedores fuera de la oficina no deben tener estos accesos o llamado a este servicio.
- g. Las aplicaciones críticas de RMS SAS deben forzar la autenticación mediante el protocolo HTTPS.

4.10. CONTROLES CRIPTOGRÁFICOS

4.10.1. La Oficina de Tecnología e Información debe:

- a. Determinar los algoritmos criptográficos y protocolos autorizados para su uso en RMS SAS y configurar los sistemas para permitir únicamente aquellos permitidos, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrado débil.
- b. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.
- c. La administración de llaves criptográficas y certificados digitales están a cargo de La Oficina de Tecnología e Información. Sin embargo, la administración de tokens bancarios, tokens para acceso a SIIF (Sistema Integrado de Información Financiera) y firmas digitales están a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus labores.
- d. Los administradores de bases de datos de la OTI deben establecer una estrategia para cifrar las bases de datos críticas de RMS SAS, velando por no afectar el desempeño del sistema de información.
- e. La OTI debe dar a conocer y capacitar a los funcionarios, contratistas, proveedores o terceros en el uso de las herramientas de uso criptográfico, cuando así se requiera su uso.
- f. Realizar revisiones periódicas a las herramientas de uso criptográfico (Tokens, Firma Digital, etc.), con el fin

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 37 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

de detectar fallas o vulnerabilidades.

- g. Notificar con anterioridad a los dueños de la información, aplicaciones, software que requieran de certificados digitales, la fecha de caducidad de éstos para su renovación.
- h. Realizar la entrega de los certificados digitales generados con el debido procedimiento para su aplicación y uso.
- i. Realizar las configuraciones requeridas para el uso y administración de los certificados de firma digital.
- j. Prestar soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.
- k. Velar porque la información clasificada y reservada (en reposo y transmisión), viaje siempre cifrada, por los métodos que RMS SAS haya adoptado.
- l. Comunicar al Comité Institucional de Gestión y Desempeño, los eventos o incidentes que conlleven al no cumplimiento de los objetivos institucionales por el no uso de controles criptográficos para la información clasificada y reservada.
- m. Proporcionar los recursos necesarios para la administración y monitoreo en el uso de controles criptográficos a través de herramientas o software de seguridad.
- n. Identificar los puertos USB para quienes estén autorizados para la firma digital y contar con este inventario con el fin de dar seguimiento al buen uso de la información.

4.10.2. Los funcionarios y Colaboradores de RMS SAS deben:

- a. Conocer y cumplir la política de uso de controles criptográficos.
- b. Los funcionarios o contratistas a quienes les fueron asignados tokens bancarios y tokens de acceso a SIIF, deben almacenarlos bajo llave cuando no hagan uso de éstos, o cuando se van a retirar de sus puestos de trabajo.
- c. Informar a los líderes del proceso, las desviaciones que se presenten por el no uso de los controles criptográficos para la información clasificada y reservada.
- d. Administrar los riesgos que se presenten por el no uso de controles criptográficos para la protección de la información clasificada y reservada.
- e. Mantener bajo custodia la clave, llave o token, que le ha sido suministrada desde la Oficina de Tecnología e Información.
- f. Ser responsable del manejo de la información clasificada y reservada, para que ésta esté protegida con las medidas de seguridad necesarias.
- g. En caso de pérdida o daño de un token, comunicar este incidente a la Oficina de Tecnología e Información a través de la Mesa de Ayuda, para su respectiva reposición, al igual, si la clave secreta o llave de cifrado ha sido vulnerada.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 38 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- h. Devolver a la Oficina de Tecnología e Información, el token y las llaves de cifrado en caso de situaciones administrativas que lo desvinculen laboral o temporalmente como (vacaciones, licencias, permisos, etc.). Esta verificación se debe dar a través del Paz y Salvo de entrega del cargo y que sea aceptado por la OTI.

4.10.3. Firma Digital

El uso de firma digital es seguro por el hecho de usar mecanismos y algoritmos de cifrado bastantes robustos. Sin embargo, la seguridad puede ser comprometida si el funcionario que hace uso de la firma digital no toma las medidas necesarias para proteger la clave, llave o token que le ha sido asignado para su uso.

- a. Los funcionarios autorizados para hacer uso de la Firma Digital son: Jefes de Oficina y Gerente.
- b. La firma digital se utilizará para cumplir con las normativas legales, para identificar al firmante de manera inequívoca, para certificar la integridad del documento o cuando se requiera proteger un documento o la información (autenticidad e integridad) con un riesgo asociado resultado de una evaluación de riesgos.
- c. Para el uso de firma digital dentro de RMS SAS, se ha establecido que éstas deben ser individuales, es decir cada funcionario que esté autorizado para el uso de la firma digital, es responsable único de la firma del documento.
- d. La firma digital individual, se da mediante un token personalizado, con estampado cronológico e incorporando la identificación de las características del creador del documento.
- e. Por ser una firma individual, RMS SAS debe adquirir los tokens, que se requieran para el uso de la firma digital y su asignación a cada funcionario que adopte esta responsabilidad.
- f. La firma digital, debe ser verificada a través de una llave pública incluida en un certificado válido emitido por una Entidad certificadora, a la cual, se le debe exigir acuerdos de niveles de servicio para el servicio de certificación o verificación.
- g. Se debe realizar mantenimiento anual a todas las firmas digitales, así como las API correspondientes.
- h. Una vez firmados los documentos con la firma digital, debe conservarse en su estado electrónico para garantizar su validez.
- i. Una vez firmados digitalmente los documentos, se deben convertir en formato PDF y debe visualizarse a través del sistema de Gestión Documental.
- j. Los artículos 20 y 21 de la Ley 527 de 1999 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.
- k. Los certificados digitales, firmas digitales, llaves de cifrado de la información, token criptográfico (físico o lógico), son de uso personal e intransferible.
- l. Si el documento que se firma es confidencial, sensible o reservado, es importante conocer que la firma digital no da privacidad a la información, por lo que su tratamiento requiere de otro control criptográfico. (Ej. Una herramienta de cifrado de información para su transporte o almacenamiento).

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 39 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- m. Los funcionarios autorizados para el uso de firma digital en RMS SAS, antes de firmar un documento que tiene otras firmas digitales, debe asegurarse de que estas firmas previas no han sido alteradas.
- n. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:
 - Es única a la persona que la usa.
 - Es susceptible de ser verificada.
 - Está bajo el control exclusivo de la persona que la usa.
 - Está ligada a la información o mensaje de datos, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
 - Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

El uso de firma digital y según la Ley 527 de 1999 establece a su favor tres atributos fundamentales en el aseguramiento jurídico, por lo que es necesario que los funcionarios autorizados para el uso de la firma digital velen por que estos tres atributos se cumplan en su implementación y uso.

- a. **La autenticidad:** En la medida que se puede verificar en un mensaje de datos firmado digitalmente quién es su autor, es quién se compromete jurídicamente.
- b. **La integridad:** El destinatario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica, lo que es muy útil para determinar la originalidad electrónica del mensaje de datos, especialmente a la luz de los artículos 8 y 9 de la Ley 527 de 1999.
- c. **El no repudio:** Quien firma digitalmente se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto.

4.10.4. Firma Electrónica

Todos los funcionarios y contratistas que desde el directorio activo se autenticuen a un sistema de información de RMS SAS, pueden hacer uso de la firma electrónica, enviando el contenido del mensaje a través de un medio electrónico válido, ejemplo., una solicitud a través del formato IMAC. Para el envío de información externa, será con base en su clasificación y será autorizada por el dueño del proceso.

En RMS SAS se contempla la firma electrónica bajo las siguientes circunstancias:

- Permitir la identificación de quien firma con el fin de determinar que la persona es quién dice ser.
- La firma electrónica solo puede ser generada por el emisor del documento.
- La firma electrónica podrá ser validada pero no falsificada.
- La firma electrónica está creada de un modo que solo está bajo el control de quien firma.
- La firma electrónica está vinculada a los datos de tal forma que si los datos son alterados la firma dejará de ser válida.
- La firma electrónica debe servir para indicar que el contenido cuenta con su aprobación.
- Debe ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.

4.10.5. Cifrado de la Información

RMS SAS debe contar con controles que permitan definir y administrar los mecanismos de cifrado de información,

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 40 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

para este propósito, se ha definido un Instructivo Seguridad Cifrado, que permita el intercambio de información cifrada, para minimizar los riesgos en este proceso de intercambio o transporte de la información, que puedan brindar seguridad y confianza, además:

- Se debe hacer uso de cifrado para la protección de claves de acceso, llaves criptográficas a datos, información clasificada y reservada, y todos aquellos servicios que estén expuestos a internet.
- Cifrado en la transmisión de información clasificada y reservada por los diferentes canales de comunicación que utilice en el Entidad.
- Cifrado en el resguardo de información clasificada y reservada en cualquier medio físico o componente tecnológico, o cuando así surja de la evaluación de riesgos realizada por el Dueño de la información y el Oficial de Seguridad de la Información.

4.10.6. Llaves Criptográficas

Con el fin de garantizar la confidencialidad e integridad de los datos o la información de un documento, RMS SAS debe garantizar la protección de la información en reposo como en tránsito, para lo cual ha adoptado hacer uso de algoritmos de seguridad que cumplan con la reglamentación legal y la protección y privacidad de la información.

Por lo que es importante además de la información, proteger las claves secretas o llaves criptográficas para que no sean vulneradas ni modificadas sin autorización. Por consiguiente, la Oficina de Tecnología e Información debe velar por la custodia de estas y todo su ciclo de vida que se relaciona a continuación.

- Generación:** Es la selección del valor que se va a utilizar para ser usado por un algoritmo criptográfico específico o aleatorio, La llave debe ser elegida de tal manera que no sea previsible y que en el proceso no se presente un acceso no autorizado.
- Distribución:** Es el proceso de traslado de una llave desde el punto de su generación hasta el punto donde va a ser usada, siendo la mayor exigencia en los algoritmos simétricos. En RMS SAS, se exige el uso de cifrado para las llaves.
- Instalación:** Es el proceso de almacenamiento de la llave en el dispositivo o proceso que se va a usar y debe mantener en todo momento la protección para evitar el acceso no autorizado. En RMS SAS se exige el uso de cifrado para las llaves.
- Almacenamiento:** Las llaves solo pueden ser almacenadas en forma cifrada, con el fin de evitar su manipulación o intento de acceso no autorizado.
- Cambio:** Establece la vigencia de una llave, a mayor tiempo de vigencia de una llave, mayor será la probabilidad de acceso no autorizado. El periodo se define en cada caso particular dependiendo del nivel de riesgo identificado en el activo de información.
- Eliminación:** Las llaves debe ser eliminadas para evitar su divulgación, esto aplica para los valores de las llaves que por algún momento puedan encontrarse en forma clara o sin cifrado en algún medio de almacenamiento.
- Protección:** Se debe usar mecanismos que protejan las llaves de accesos y modificaciones no

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 41 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

autorizadas.

- h. **Revocación:** hace relación a la invalidez de una llave antes de cumplir el periodo de vigencia establecido y el responsable de esta acción es el funcionario al que le fue asignada la llave correspondiente.

Las razones por las cuales un funcionario debe solicitar a la Oficina de Tecnología e Información la revocación de una llave, clave secreta o token bajo su responsabilidad son las siguientes:

- Pérdida del dispositivo en el cual se encuentra almacenada la llave.
- Se evidencia alguna circunstancia en la cual se ha dado acceso no autorizado a la llave, clave secreta o token.
- Reporte de ataques informáticos o acción de algún tipo de programa maligno.
- Cuando el funcionario responsable de la gestión de la llave termina su relación laboral o contractual con la Entidad.

4.10.7. Certificados Digitales

Los responsables de los sistemas de información deben ser conscientes en el uso y caducidad que pueda tener un certificado digital, esto con el fin de comunicar a la Oficina de Tecnología e Información para su emisión e implementación.

El responsable de la solicitud ante la entidad certificadora para la emisión de los certificados también debe velar por la caducidad de éstos, teniendo como control un listado de todos los certificados emitidos con la fecha de caducidad y la asignación de éstos en los sistemas de información. En RMS SAS, se establece el uso de certificados digitales para:

- Garantizar la autenticidad del sitio, servicio o aplicativo Web.
- Evitar el riesgo de ataques de suplantación de identidad o phishing de los sitios Web.
- Proteger la confidencialidad de la información intercambiada entre la Entidad y sus ciudadanos o titulares mineros a través del sitio Web.
- Establecer conexiones seguras cifrando la información intercambiada entre los aplicativos y los ciudadanos o titulares mineros.
- Salvaguardar la integridad de la información intercambiada, porque el certificado presenta las características de la Entidad, algoritmo de cifrado, fecha de emisión del certificado, etc.

4.11. SEGURIDAD FÍSICA Y DEL ENTORNO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, debe contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. Toda área donde se solicite o capture datos personales debe contar con anuncio al público de dicha

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 42 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

actividad, a su vez esta información debe ser conservada de acuerdo con la Ley 1581 de 2012 de Protección de Datos Personales.

4.11.1. Áreas Seguras

RMS SAS en sus instalaciones tiene implementado un sistema de control de acceso físico mediante huella biométrica por cada piso, sin embargo (por pandemia se requiere retomar el control de tarjeta de proximidad). Adicionalmente, cada piso cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros. A sí mismo RMS SAS debe exigir a los proveedores que gestionen o procesen información por fuera de las instalaciones de RMS SAS, cumplir con las políticas de seguridad de ANM y las que disponga el proveedor en sus instalaciones.

El Datacenter o centros de cableado debe contar con mecanismos que cumplan los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga, igualmente debe contar con sistemas mecánicos para control de incendios, impedir el acceso a personal no autorizado, consumo de alimentos, bebidas o cigarrillo.

RMS SAS cuenta con un Sistema de Seguridad CCTV, para otorgar la mayor seguridad posible tanto a los ciudadanos como a los funcionarios que ingresan a sus instalaciones. El Sistema de Seguridad CCTV opera bajo las siguientes directrices:

- a. La Oficina de Tecnologías e Información es la responsable del mantenimiento y soporte de la plataforma tecnológica que soporta el sistema CCTV.
- b. La Oficina de Tecnologías de Información debe garantizar el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año. La oficina de Servicios Administrativos garantizará la operación y monitoreo.
- c. El acceso al centro de monitoreo es de carácter restringido. Las únicas personas que tienen permiso de acceder son los operadores, o aquellos funcionarios que autorice la Oficina de Servicios Administrativos.
- d. Cuando el operador de medios tecnológicos del CCTV deba ausentarse de su puesto de trabajo, éste procederá a notificar o registrar en la bitácora diaria.
- e. El operador de medios tecnológicos del CCTV debe registrar en la bitácora diaria cualquier evento ocurrido durante su turno.
- f. El operador de medios tecnológicos del CCTV debe notificar vía telefónica o electrónica a la Oficina de Tecnología e Información acerca de las fallas o ausencias de video que se presenten en las cámaras del sistema CCTV (Circuito Cerrado de Televisión) de la Agencia. Lo anterior con el fin de restablecer dicho servicio y mantener su correcto funcionamiento.
- g. Cuando el operador detecte que alguna cámara ha sido girada sin autorización, debe informar a la Oficina de Servicios Administrativos, para que se genere la evidencia y se autorice devolverla a su posición original.
- h. Cuando el operador de medios tecnológicos del CCTV detecte anomalías o incidentes en las zonas de monitoreo, éstas deben ser reportadas inmediatamente al Supervisor de contrato de Vigilancia y Seguridad Privada.
- i. Toda solicitud de copias de video debe hacerse por escrito a la Oficina de Servicios Administrativos.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 43 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- j. La descarga de videos es posible realizarla únicamente en el centro de monitoreo de la sede principal de RMS SAS. En las diferentes sedes de la entidad no existe la posibilidad de descarga de videos, solo se permite la visualización.
- k. Todas las grabaciones tienen una duración mínima de 30 días y después se reescribe.
- l. Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.
- m. Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.
- n. La oficina de Tecnologías e información debe brindar un repositorio para almacenamiento de videos históricos garantizado la confidencialidad y disponibilidad de esta información.
- o. RMS SAS debe contar con un plan de emergencias definido por el Grupo de Servicios Administrativos, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.
- p. La carga se recibe y despacha por el parqueadero del edificio. La recepción y despacho de carga es controlada por la administración del edificio y se tienen horarios específicos para la realización de estas actividades.

4.11.2. Ubicación y Protección de los Equipos

El Datacenter está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por la Oficina de Tecnología e Información.

Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar adversamente el Datacenter.

4.11.3. Servicios de Suministro

RMS SAS cuenta con aire acondicionado de contingencia, UPS (sistema de alimentación ininterrumpida, en inglés (Uninterruptible Power Supply). que asegura el tiempo necesario de 12 minutos de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica. ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del Datacenter.

4.11.4. Seguridad del Cableado

El Datacenter de RMS SAS cumple con la normatividad de cableado estructurado y está debidamente certificado. A sí mismo RMS SAS debe exigir a los proveedores de servicios informáticos, cumplir con las políticas de seguridad de ANM.

4.11.5. Mantenimiento de Equipos

La Oficina de Tecnología e Información debe establecer y ejecutar planes anuales de mantenimiento de la infraestructura tecnológica de RMS SAS.

4.11.6. Seguridad de Equipos y Activos Fuera de las Instalaciones

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 44 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

La salida de elementos de RMS SAS es controlada mediante el formato APO2-P-001-F-006 Formato Único de Retiro de Elementos ANM.

- a. Los equipos y medios removibles que son retirados de las instalaciones de RMS SAS deben estar debidamente cifrados.
- b. Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones de RMS SAS deben seguir las siguientes directrices:
 - En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
 - Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
 - En caso de pérdida o robo de un equipo de RMS SAS, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al Jefe de Grupo y al Grupo de Servicios Administrativos para que se inicie el trámite interno correspondiente.

4.11.7. Disposición Segura o Reutilización de Equipos

Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información de RMS SAS que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. Ver indicaciones adicionales en el procedimiento de borrado seguro.

4.11.8. Política de Equipo Desatendido, Escritorio Limpio y Pantalla Limpia

Todos los colaboradores de RMS SAS deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

- a. Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser enviados con pin de seguridad y retirados de la impresora inmediatamente.
- b. Los computadores deben cargar por defecto el fondo de pantalla de RMS SAS, éste no debe ser modificado y debe permanecer activo.
- c. Los funcionarios y contratistas de RMS SAS deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo simultáneamente las teclas Windows + L), a su vez, la Oficina de Tecnología e Información debe implementar mecanismos para cierres de sesión automáticos no superior a cinco minutos.
- d. Los usuarios son responsables y asumen las consecuencias por la pérdida de información que este bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores de RMS SAS.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 45 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

El escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

- e. La información de gestión del área deber ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de One Drive corporativo de Office 365.

4.12. SEGURIDAD DE LAS OPERACIONES

4.12.1. Documentación de Procedimientos Operativos

Se debe contar con procedimientos documentados de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

4.12.2. Control de Cambios

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se deben realizar de acuerdo con los lineamientos del Procedimiento de Gestión de Cambios Tecnológicos.

4.12.3. Gestión de Capacidad

RMS SAS debe gestionar la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del Procedimiento de Gestión de Capacidad.

4.12.4. Separación de los Ambientes

RMS SAS debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y máquinas virtuales.

RMS SAS debe controlar el acceso al ambiente de pruebas de la misma forma que controla el acceso al ambiente de producción.

4.13. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- a. Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de RMS SAS contra códigos maliciosos.
- b. Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.
- c. El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.
- d. El único servicio de antivirus autorizado en RMS SAS es el asignado directamente por la Oficina de Tecnología e Información (OTI), el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.
- e. El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 46 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

o códigos maliciosos o sean sospechosos de estar infectados.

- f. El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.
- g. Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la Oficina de Tecnología e Información.
- h. El programa de antivirus debe ser instalado única y exclusivamente por la Oficina de Tecnología e Información en los servidores y estaciones de trabajo.

4.14. COPIAS DE RESPALDO

RMS SAS debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la Oficina de Tecnología e Información define el Procedimiento de Copias de Respaldo e Instructivo, que definen las actividades para la estrategia de backup requeridas; además:

- a. La Oficina de Tecnología e Información debe establecer las políticas de copias de seguridad desde la herramienta de backups, para los sistemas de información y bases de datos.
- b. Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la Oficina de Tecnología e Información.
- c. La Oficina de Tecnología e información debe realizar copias de respaldo a las carpetas compartidas definidas en el servidor de archivos de RMS SAS.
- d. La Oficina de Tecnología e Información debe realizar copias de respaldo a las carpetas con información de RMS SAS de los equipos portátiles y/o computadores de escritorio críticos de cada uno de los grupos de las Vicepresidencias (funcionarios VIP).
- e. Todas las copias de respaldo deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.
- f. Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.
- g. Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.
- h. Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de RMS SAS.

4.15. REGISTRO Y SUPERVISIÓN DE EVENTOS

4.15.1. Registro de Eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de RMS SAS, deben generar archivos de registro de eventos

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 47 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

(logs) definidos en conjunto por los responsables de su administración.

4.15.2. Protección de la Información de Registro

La Oficina de Tecnología e Información con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información debe implementar mecanismos de copiado de logs en “tiempo real” a un sistema por fuera del control de administradores y operadores de los sistemas.

4.15.3. Sincronización de Relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por RMS SAS debe estar sincronizados utilizando como referencia la hora oficial de Colombia de INM (Instituto Nacional de Metrología) <https://horalegal.inm.gov.co/>

4.16. CONTROL DE SOFTWARE OPERACIONAL

4.16.1. Instalación de Software en Sistemas Operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la Oficina de Tecnologías e Información. Por lo tanto, a los funcionarios o contratistas no les es permitido realizar esta labor.

Para la instalación de software se debe seguir las siguientes directrices:

- El software licenciado debe contar con su respectiva documentación (Licencia) y en el caso del software libre debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.
- Debe dejarse evidencia documentada de que las directrices anteriores fueron seguidas a cabalidad.

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de las nuevas adquisiciones de software o mejoras al software existente, antes de su puesta en producción.

Todo el software nuevo y mejorado debe estar completamente soportados por una documentación suficientemente amplia y actualizada, y no debe ser puesto en el ambiente de producción sin contar con la debida documentación.

- **Documento de Licencia del Software** (representa el permiso que le da el fabricante para la instalación y uso de su producto)
- **Manual de Instalación del Software** (Para determinar que el software ha sido instalado apropiadamente)
- **Manual del Usuario para uso del Software** (Para guiar al usuario en su uso y apropiación)

La OTI debe realizar revisiones periódicas del uso del software instalado en las estaciones de trabajo y

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 48 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 de Derechos de Autor, conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual.

Todo software que viole los acuerdos de licenciamiento debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política y de los términos y condiciones de uso, poniendo en riesgo la seguridad de la información y quizás sanciones económicas por incumplimiento a la Ley 603 de 2000 de derechos de autor.

Para contar con una trazabilidad del software instalado en los componentes tecnológicos de RMS SAS, (sistemas operativos, programas ofimáticos, sistemas de información), entre otros, se debe contar con un sistema de control de la configuración, en donde se observen los cambios ejecutados en dicho software, como (instalación de parches, cambios de versionamiento, actualizaciones, etc., con el fin de mantener el historial y el control del software operacional en RMS SAS.

Toda reproducción del software, transporte, almacenamiento, adquisición para la venta o distribución sin la debida autorización del titular, se constituye como un delito a los Derechos Patrimoniales del Autor.

Todo software que RMS SAS adquiera debe ser del conocimiento de Arquitectura Empresarial quien a su vez debe emitir criterios adicionales con el fin de que el software a adquirir cuente con la interoperabilidad en su instalación y uso con los demás sistemas de información de la Entidad.

La OTI debe comunicar a los funcionarios y contratistas sobre las consecuencias por utilizar software ilegal; conjuntamente con la Oficina Asesora Jurídica debe definir y establecer las cláusulas de los contratos para cumplir con la legislación vigente relacionada con los derechos de autor y datos personales.

El software que desde Fábrica de Software se contemple y, los desarrollos Inhouse debe anexar un certificado de uso y cesión de derechos según sea el caso, cuando de adquisición se trate.

Es importante que la Oficina Asesora Jurídica haga parte de esta adquisición en cuanto a la lectura que se haga a la licencia, derechos de autor y propiedad intelectual del software adquirido y que será propiedad de RMS SAS., cuando de desarrollos de Fábrica de Software y Desarrollos Inhouse se trate.

Para llevar el Control del Software Operacional instalado en RMS SAS, se han establecido los siguientes procedimientos:

- Procedimiento de Derechos de Propiedad Intelectual
- Formato Dar de Baja un Software

4.17. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

La Oficina de Tecnología e Información, es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la Entidad, Adicionalmente, debe contar con un procedimiento y análisis de vulnerabilidades que permitan la identificación y mitigación de las vulnerabilidades identificadas en toda la plataforma tecnológica de RMS SAS.

4.17.1. Gestión de las Vulnerabilidades Técnicas

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 49 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- a. Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o Hacking Ético para las plataformas críticas de la Entidad, cuya viabilidad técnica y de administración lo permita. Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la Entidad, la identificación de estas vulnerabilidades o hallazgos se deben remediar de acuerdo con los lineamientos establecidos desde el Procedimientos de Gestión de Vulnerabilidades.
- b. Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de La Oficina de Tecnología e Información, para estas remediaciones se debe tener en cuenta las directrices establecidas en el Procedimiento de Gestión de Cambios cuando su aplicación se lleve al ambiente de producción.

4.18. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

4.18.1. Controles sobre auditorías de sistemas de información

Para la ejecución de auditorías a los sistemas de información se debe tener en cuenta las siguientes consideraciones:

- a. Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con los jefes de la(s) Dependencia(s) involucradas.
- b. El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.
- c. Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se debe realizar en horario laboral en un ambiente controlado.
- d. Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.
- e. Las pruebas de auditoría se deben limitar a acceso a software y datos únicamente para lectura.

4.19. SEGURIDAD EN LAS COMUNICACIONES

La Oficina de Tecnología e Información debe definir e implementar los mecanismos de control que considere apropiados para proteger la Confidencialidad, Integridad y Disponibilidad de la información en las redes definidas en la Entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información que viajan a través de estos canales de redes de comunicaciones.

4.19.1. Gestión de la Seguridad en las Redes

La Oficina de Tecnología e Información debe definir e implementar mecanismos de separación de las redes de RMS SAS con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), por dependencias (por ejemplo, oficina de talento humano, oficina de servicios administrativos, oficina de gestión financiera, oficina de tecnología e información) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias), además:

- a. La Oficina de Tecnología e Información debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.
- b. El acceso remoto a las redes de RMS SAS se controla mediante conexiones VPN, las cuales deben

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 50 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

estar monitoreadas para que se evidencie la desactivación de ésta en el tiempo que se ha definido.

4.19.2. Transferencia de Información

RMS SAS debe firmar acuerdos o compromisos de confidencialidad con los servidores públicos y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo deben quedar especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se debe firmar antes de permitir el acceso o uso de dicha información.

Todos los lineamientos para la transferencia de información deben aplicarse en toda la Entidad, proveedores y terceros que dentro de sus funciones se establezca la necesidad de intercambio de información física como digital.

Actualmente se cuenta con el formato de intercambio de información entre Entidades, el cual deber ser firmado por los representantes de las partes cuando se lleve a cabo esta transferencia de información, además tener en cuenta:

- a. Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad sobre la misma, así como, los lineamientos que se establecen en el Procedimiento de Intercambio Seguro de Información.
- b. Todos los responsables de la información deben asegurar que el intercambio de información con el tercero (Contratos, convenios, pólizas, etc.), esté debidamente autorizada y protegida conforme a los lineamientos del procedimiento Intercambio Seguro de Información.
- c. Todos los responsables de la información son quienes autoricen la transferencia de la información que esté bajo su responsabilidad, teniendo en cuenta la legislación (Ley 1581 de 2014 y Ley de Habeas Data de 2008).
- d. Todos los responsables de la información deben seguir las indicaciones del Procedimiento de Gestión de Activos de Información, para la transferencia y transporte de la información, teniendo presente que esté totalmente etiquetada como se indica en este procedimiento.
- e. La transferencia de información digital debe contemplar una trazabilidad de toda la actividad de envío de los datos, a través de logs, en donde se registre la siguiente información:
 - Fecha y hora de envío
 - Dirección IP de origen y destino
 - Usuario que envía la información
 - Algoritmo de cifrado o firma digital usada
- f. El proveedor de servicios en la Nube para los servicios con los que cuenta RMS SAS, debe certificar que se dispone de una transferencia de información segura hacia la Nube.
- g. Independientemente del modo en el que se produzca el intercambio de información es necesario contar con los controles de seguridad, que mediante éstos se genere confianza y protección de la información

4.20. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 51 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

La Oficina de Tecnología e Información debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en RMS SAS. Las dependencias que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la Oficina de Tecnología e Información para definir los requisitos de seguridad de la información. Para ello, debe tener en cuenta los lineamientos establecidos en el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de información, además los siguientes:

4.20.1. Requisitos de Seguridad de los Sistemas de Información.

- a. El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reutilización.
- b. Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.
- c. Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.
- d. Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas, uso de firmas digitales.
- e. Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
- f. La necesidad de exigir la implementación de metodologías de desarrollo seguro.
- g. Los desarrolladores propios de RMS SAS liberan de derechos de autor cualquier desarrollo hecho para el cumplimiento de sus funciones u obligaciones contractuales, siendo estos derechos de autor únicamente de la Agencia.

4.20.2. Seguridad en los Procesos de Desarrollo y Soporte

La Oficina de Tecnología e Información debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de construcción. También se debe revisar regularmente para que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los lineamientos para el desarrollo seguro deben aplicarse también para los sistemas de información existentes en RMS SAS y, a los de uso externo con los proveedores (Fábrica de desarrollo), teniendo en cuenta el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, además:

- a. RMS SAS (OTI y supervisor del contrato); deben velar por el desarrollo tanto interno como externo de los sistemas de información, cumplan con los requisitos de seguridad esperados, así como con pruebas

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 52 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

de aceptación y seguridad al software desarrollado. Además, RMS SAS debe asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Entidad.

- b. Los cambios en sistemas deben realizarse de acuerdo con el Procedimiento de Gestión de Cambios.
- c. En todo desarrollo interno, externo y/o a través de la Fábrica de Desarrollo, se debe hacer uso de metodologías de desarrollo seguro, que contemplen lineamientos de seguridad en todas las etapas del desarrollo.

4.20.3. Ambiente de Desarrollo Seguro

- a. La Oficina de tecnología e Información debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).
- b. La Oficina de Tecnología e Información debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el Procedimiento de Cambios Tecnológicos.
- c. La Oficina de Tecnología e Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de RMS SAS.

4.20.4. Desarrollo Contratado Externamente

Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por RMS SAS. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación, además:

- a. Las dependencias deben asegurarse que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.
- b. Las dependencias deben exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.
- c. Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.
- d. Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.
- e. Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.
- f. Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de RMS SAS a realizar auditorías durante el desarrollo del contrato.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 53 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

4.20.5. Pruebas de Seguridad de Sistemas

Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

4.20.6. Pruebas de Aceptación de Sistemas

Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad, además:

- Se debe realizar pruebas de aceptación del software que sea una persona diferente de quien han desarrollado el software, además estas pruebas evidenciadas a través de un documento deben estar firmadas por quienes realizaron las pruebas, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso. Para mayor detalle se debe dirigir al “Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de RMS SAS, y que las pruebas son confiables.
- En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados.

4.20.7. Datos de Prueba

La Oficina de Tecnología e Información debe certificar que la información entregada a los desarrolladores (tanto internos como externos) para sus pruebas debe ser enmascarada y los datos sensibles deben ser eliminados con el fin de no revelar información confidencial de los ambientes de producción, dando cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

4.21. RELACIÓN CON LOS PROVEEDORES

4.21.1. Seguridad de la Información en las Relaciones con los Proveedores.

RMS SAS debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente aquellos proveedores críticos para RMS SAS por el manejo de información crítica o confidencial, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que cumplan con las políticas de seguridad de la información, es fundamental que se lleven a cabo visitas a los proveedores con el fin de identificar situaciones que puedan comprometer la información de RMS SAS en el no cumplimiento de los lineamientos establecidos en este manual. Para estas visitas se ha establecido el Procedimiento Gestión de Proveedores.

4.21.2. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores.

- Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 54 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- b. El Grupo de contratación debe incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:
- Cláusula de confidencialidad.
 - Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
 - Cumplimiento de las políticas de seguridad de la información de RMS SAS.
 - Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento de gestión de incidentes de seguridad de la información.
 - Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento de gestión de activos.
 - Cláusula de seguimiento y revisión de los servicios de los proveedores o terceros para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, en los acuerdos contractuales correspondientes.
- c. Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.
- d. Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Administración de Tecnología e Información utilizando el formato IMAC.

4.22. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad debe estar basados de acuerdo con los lineamientos del Procedimiento de Gestión de Incidentes, donde se debe establecer como mínimo: quiénes deben reportar, los canales de comunicación, tipo de situaciones que se deben reportar, decisiones sobre las situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales.

Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en este manual.

Cualquier incumplimiento identificado debe remitirse al Oficial de Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación.

Categorías de incidentes de seguridad de la información: Si el incumplimiento es sujeto de clasificación teniendo en cuenta las siguientes categorías, se debe considerar como incidente de seguridad de la información:

- a. **Fuga de información:** Se evidencia divulgación no autorizada de información de RMS SAS.
- b. **Acceso no autorizado:**

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 55 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso.
- Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario.
- Personal no autorizado ingresa a las instalaciones de RMS SAS.

c. **Ataque:**

- Se evidencia intención de afectar un recurso específico.
- Se modifica la imagen institucional en aplicaciones de RMS SAS.
- No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio.
- Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web.

d. **Código dañino:**

- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información.
- El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.

e. **Denegación de servicio:**

- El sistema de información no responde por alta cantidad de peticiones.
- El sistema de información se encuentra con latencia o degradación del servicio.

f. **Robo o pérdida:**

- Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida.
- Se presenta robo o pérdida de elementos personales en las instalaciones de RMS SAS.

g. **Alarmas de sistemas de monitoreo:**

Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas.

h. **Usos inadecuados:**

- Si se ingresa texto copiado de internet en documentación oficial de RMS SAS, sin registrar la fuente.
- Si se publica comunicados en nombre de la Entidad sin revisión y aprobación del proceso de comunicación estratégica.

4.23. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Al incurrir en el incumplimiento de estas políticas se debe notificar inmediatamente a la Oficina de Tecnología e Información a través de los siguientes canales.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 56 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- E-mail: servicios.tecnologia@rmsltda.com

Así mismo, se debe notificar situaciones tales como: personas ajenas a RMS SAS en oficinas y centros de cómputo, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso de software ilegal, divulgación, alteración y robo de información.

4.24. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL RIESGO

La gestión del riesgo de Seguridad de la información y Ciberseguridad se encuentra alineada a la Metodología del Sistema Integral para la Administración y Gestión de Riesgos de RMS SAS y, a los lineamientos que desde la Norma ISO 31000:2018 - Sistema de Gestión de Riesgos se describen.

La matriz de riesgos definida en la metodología de riesgos de seguridad incluye el análisis de los atributos generales de Seguridad de la Información y Ciberseguridad; (Confidencialidad, Integridad y Disponibilidad), es decir, se identifican y analizan para cada uno de los riesgos, estos pilares.

4.24.1. La Gestión del Riesgos para la Confidencialidad

Se define como riesgos que afectan este pilar, aquellos que describen que la Información puede ser conocida o utilizada sin autorización por cualquier colaborador, persona o ente dentro o fuera de RMS SAS. Así mismo, la información que pueda estar expuesta para ser utilizada por personas no autorizadas.

4.24.2. La Gestión del Riesgos para la Integridad

Se define como riesgos que afectan este pilar, los que hagan referencia a aquella información que puede ser manipulada o alterada, es decir se tendrán en cuenta aquellas situaciones o escenarios en que la información no pueda mantener la exactitud, modificaciones indebidas que afecten el orden lógico de los datos cambiando su estructura o significado.

4.24.3. La Gestión del Riesgos para la Disponibilidad

Se define como riesgos que afectan este pilar, los que describan aquella información que no pueda ser accesible y utilizable en el momento que sea necesario o se requiera por las personas, sistemas o procesos operacionales.

4.25. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

4.25.1. Continuidad de la Seguridad de la Información

RMS SAS, debe contemplar una estrategia de Continuidad de Negocio basada en los resultados del BIA (Business Impact Analysis por sus siglas en inglés) y demás documentación que se ha desarrollado que permiten contar con lineamientos para la continuidad de las operaciones de negocio entre ésta se encuentra; (Política de Continuidad de Negocio, Manual Continuidad de Negocio, Análisis GAP y Plan de Gestión de Crisis).

Planificar e implementar la Continuidad de Negocio en RMS SAS, debe ser un aspecto fundamental teniendo en cuenta no sólo los recursos tecnológicos, sino también activos de información crítica de los procesos, los cuales han sido definidos y estructurados en el BIA, además:

- Se deben realizar pruebas periódicas a los controles de Continuidad de Negocio y de continuidad de la Seguridad de la Información implementados, con el fin de asegurar que son válidos y eficaces durante

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 57 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

situaciones adversas.

- b. Los responsables de los procesos e información deben asegurar que se actualicen los Planes de Continuidad de Negocio posterior a los cambios en la infraestructura tecnológica con respaldo de la Oficina de Tecnología e Información.
- c. Contemplar un sitio alternativo, donde los controles implementados en el ambiente de producción deben ser consistentes con el sitio alternativo.
- d. Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de contingencia.
- e. El Plan de Continuidad de Negocio debe ser protegido contra accesos no autorizados, contemplando a su vez copias de respaldo y que éstas sean resguardadas en un sitio externo con la protección adecuada tanto física como medioambiental.

4.25.2. Redundancias

- a. RMS SAS debe establecer e implementar un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.
- b. RMS SAS debe realizar pruebas periódicas al DRP, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

4.26. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

4.26.1. Identificación Legislación Aplicable y Requisitos Contractuales

La Oficina Asesora Jurídica y el Oficial de Seguridad de la Información deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a RMS SAS y relacionados con seguridad de la información. Para ello, se pueden apoyar en los Jefes de Oficina, tales como el Grupo de Gestión de Talento Humano, Gestión Documental.

4.26.2. Derechos de Propiedad Intelectual

- a. La Oficina de Tecnología e Información debe asegurarse de que todo el software que se ejecute en RMS SAS esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- b. Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus actividades.
- c. Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, basado en el Procedimiento Derechos de Propiedad Intelectual.
- d. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de Ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 58 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

- e. El Grupo de Contratación debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

4.26.3. Protección de Registros

RMS SAS se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo las directrices del Procedimiento de Gestión de Activos.

4.26.4. Privacidad y Protección de Información de Datos Personales

RMS SAS, quien será responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, RMS SAS debe implementar los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la Ley lo permita.

4.26.5. Reglamentación de Controles Criptográficos

RMS SAS, se regirá por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según aplique.

4.27. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

4.27.1. Revisión de la Seguridad de la Información

El proceso de Evaluación, Control y Mejora debe realizar auditorías internas de revisión independiente al menos anualmente. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la Entidad para gestionar la seguridad de la información. Esta revisión que es responsabilidad de Control Interno de RMS SAS debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

4.27.2. Revisión Cumplimiento Técnico

El jefe de la Oficina de Tecnología e Información debe coordinar la revisión periódica (al menos anualmente) de los sistemas de información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se le hará revisión.

4.28. CUMPLIMIENTO

El incumplimiento de esta política está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión.

4.29. BIBLIOGRAFÍA

La debida documentación de las Políticas de Seguridad de la Información establecidas en este manual, han

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Código SG-SI-12
		Página 59 de 59
		Ver. 1.2
		Vigente a partir de: 2025/02/11

sido estructuradas teniendo en cuenta las buenas prácticas de los marcos de referencia que se citan a continuación.

- a. NTC ISO/IEC 27001:2013 - Norma Técnica Colombiana Sistemas de Gestión de Seguridad de la Información.
- b. NTC ISO/IEC 27002:2013 - Norma Técnica Colombiana Sistemas de Gestión de Controles de Seguridad de la Información.
- c. Norma ISO 22301:2019 - Sistema de Gestión de Continuidad de Negocio.
- d. Norma ISO 31000:2018 - Sistema de Gestión de Riesgos

ELABORÓ:	REVISÓ	APROBÓ:
Nombre: Ing. Enith Enilse Gustin Cargo: Asesor Externo Fecha: 10/02/2025	Nombre: Diego Córdoba Cargo: Gerente Fecha: 11/02/2025	Nombre: Diego Córdoba Z Cargo: Gerente Fecha: 11/02/2025

CONTROL DE CAMBIOS		
Versión No.1.0	2024/02/01	Creación del Documento
Versión No.1.2	2025/02/11	Actualización del Documento