MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

AGENCIA DE RENOVACIÓN DEL TERRITORIO

Bogotá D.C, diciembre de 2020

Documento aprobado el 17 de diciembre de 2020, mediante Acta N°. 5 del Comité Institucional de Gestión y Desempeño.

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

La Agencia de Renovación del Territorio – ART (en delante la Agencia), para el cumplimiento de la misión y el cumplimiento del objetivo, requiere la implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El presente manual establece las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la ART, estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de Seguridad de la Información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. OBJETIVO

Establecer las políticas que regulan la seguridad de la información en la Agencia de Renovación del Territorio - ART y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Agencia de Renovación del Territorio, ART- bajo el liderazgo de la Oficina de Tecnologías de la Información.

3. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los procesos, procedimientos y activos de información de la Agencia, las cuales deben ser cumplidas por los directivos, funcionarios, contratistas y/o terceros cuando sea el caso o de ser necesario, que presten sus servicios o tengan algún tipo de relación con la Agencia de Renovación del Territorio - ART para el adecuado cumplimiento de sus funciones y para fortalecer los niveles de seguridad como lo son la confidencialidad, la integridad y la disponibilidad.

Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité Institucional de Gestión y Desempeño.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas del Sistema de Seguridad de la Información - SGSI aplican y son de obligatorio

cumplimiento para la Alta Dirección, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios que permitan el cumplimiento de los propósitos generales de la Agencia.

5. TÉRMINOS Y DEFINICIONES

- **Acción correctiva:** Acción tomada para eliminar las causas de una no conformidad detectada u otra situación indeseable.

- **Acción preventiva:** Acciones que buscan mitigar los riesgos, que conlleven a la implementación de una no conformidad.

- **Aceptación del Riesgo:** Decisión de que puede tolerarse el riesgo asociado a cualquier situación bajo el supuesto de que se cuenta con un plan de acción para afrontarlo.

- **Activo:** Según la norma ISO/lEC 13335-12004 Cualquier cosa que tiene valor para la organización o activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Agencia. Se pueden clasificar de la siguiente manera:

    - Datos / Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
    - Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
    - Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
    - Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
    - Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
    - Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

- **Administración de riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, acciones de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las acciones incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

  Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la Agencia, de manera rápida y eficaz, no se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

  - Detectar cualquier alteración en los servicios TI.
  - Registrar y clasificar estas alteraciones.
  - Asignar el personal encargado de restaurar el servicio.

- **Alcance:** Ámbito de la Agencia sujeto al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Almacenamiento en la Nube**: Es un modelo de almacenamiento de datos basado en redes de computadoras, que consiste en guardar archivos en un centro de datos y la conexión se realiza a través de Internet.

- **Amenaza:** Según [ISO/IEC 13335-1:2004): Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgos:** Proceso de identificar y analizar situaciones potenciales dentro del contexto TI que puedan tener impacto negativo en las iniciativas misionales u operativas de la Agencia, con el objetivo de contribuir a la eliminación o mitigación de esos riesgos.

- **Auditoria**: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Autenticidad:** Nivel de certeza de que un mensaje, transacción u otro intercambio de información proviene de la fuente que declara. La autenticidad implica prueba de identidad y aplica para entidades como usuarios, procesos y sistemas de información.

- **Características de la Información:** En el contexto de seguridad de información hace referencia a la confidencialidad, disponibilidad e integridad de la misma.

- **Checklist (lista de chequeo):** Lista de apoyo con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la Agencia con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - **Sistema de Gestión de la Seguridad de la Información**.

- **Cómputo forense:** El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- **Confiabilidad:** Capacidad o probabilidad de que un producto o proceso realizará su función prevista o se ejecutará sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- **Confidencialidad:** “Acceso a la información por parte únicamente de quienes estén autorizados, según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no

autorizados.

- **Control:** Todas las políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (nota: Control es también utilizado como sinónimo de salvaguarda).

- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la Agencia, -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección, como de la exclusión de controles incluidos en el anexo A de la norma ISO 27001.

- **Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de las ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

- **Directiva:** Según [ISO/IEC 13335-1: 2004): Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** Según [ISO/IEC 13335-1: 2004): Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso de comparar el riesgo

estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

- **Evento:** Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- **FTP**: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

- **Impacto:** Resultado de un incidente de seguridad de la información.

- **Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

- **Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **IPS:** Sistema de prevención de intrusos, es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **ISO:** Organización Internacional de Normalización, es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799, primera publicación en 2005, segunda publicación en 2013.

- **ISO 27002:** Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799), cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

- **ISO 9000:** Normas de gestión y garantía de calidad definidas por la ISO.

- **ITIL IT Infrastructure Library:** Un marco de gestión de los servicios de tecnologías de la información.

- **Keyloggers:** Son software o aplicaciones que almacenan información digitada

mediante el teclado de un computador por un usuario; es común relacionar este término con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

- **Legalidad:** El principio de legalidad o primacía de la ley es un principio fundamental del derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, seguridad de Información, seguridad informática y garantía de la información.

- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **No repudio:** Garantía de que alguien no puede negar algo. Normalmente, el no rechazo se refiere a la capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje que se originó.

- **PHVA Planear-Hacer-Verificar-Actuar:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

- **Phishing:** Tipo de delito enmarcado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Agencia en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la Agencia en la gestión de la seguridad de la información.

- **Política de escritorio despejado:** Documento que obliga a los funcionarios, contratistas y demás colaboradores de la Agencia a asegurar la información pública reservada o información pública clasificada (privada o semiprivada) en lugares que ofrezcan la protección necesaria, así mismo establece la necesidad de los escritorios (tanto físicos como lógicos) de permanecer libres de documentos o informaciones susceptibles de ser afectados en su integridad, confidencialidad y/o disponibilidad.

- **Punto Único de Contacto (PUC):** Entiéndase como mesa de ayuda de acuerdo con las mejores prácticas basadas en ITIL.

- **Protección a la duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

- **Ransomware**: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- **Salvaguarda:** Véase: Control.

- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e información deliberado o por negligencia.

- **Seguridad de la información:** Según la norma ISO/IEC 27002:20005 hace referencia a la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **SGSI Sistema de Gestión de la Seguridad de la Información:** Según la norma ISO/IEC 27001: 2013 hace referencia a un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

- **Servicios de tratamiento de información:** Según la norma ISO/IEC 27002:2013 hace referencia a cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

- **Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

- **Sniffers:** Programa de captura de las tramas de red, generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

- **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

- **Tratamiento de riesgos:** Medidas que pueden incluir evitar, optimizar, transferir o aceptar un riesgo. Estas medidas (normalmente medidas de seguridad) pueden ser seleccionadas del set de medidas definidas en el Sistema de Administración y Seguridad de la Información de una organización.

- **Trazabilidad:** Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

- **Usuario:** Todos los directivos, funcionarios, contratistas, terceros y otros colaboradores de la Agencia, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Agencia y a quienes se les otorga un nombre de usuario y una clave de acceso.

- **Valoración de riesgos:** Según la norma ISO/IEC Guía 73:2002 hace referencia a un proceso completo de análisis y evaluación de riesgos.

- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario, el cual buscan dañar, modificar, destruir o robar archivos o datos almacenados.

- **VPN** (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según la norma ISOIlEC 13335-1:2004 hace referencia a la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. ROLES Y RESPONSABILIDADES

- **Líder o responsable de protección de datos personales:** Establecer lineamientos para la protección de los datos personales tratados en la Agencia.

- **Comité Institucional de Gestión y Desempeño:** Aprobar los lineamientos en materia de seguridad de la información, asegurar el cumplimiento de las políticas en toda la Agencia y Tomar decisiones frente a la seguridad de la información.

- **Líderes de proceso:** Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados.

- **Responsable de TI:** Participar en la elaboración del cronograma de capacitación de seguridad digital en la entidad. Implementar las mejorar identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI. Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la Agencia, la importancia de satisfacer los requisitos de seguridad digital.

- **Partes interesadas (Funcionarios, Contratistas y Proveedores):** cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el MSPI

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la declaración general de la Política de Seguridad de la Información de la

Agencia de Renovación del Territorio -ART se establecen las siguientes políticas específicas.

7.1 Políticas de Gestión de Activos

La Agencia establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información de la Agencia debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder de proceso, coordinador, jefe de área o Director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Los funcionarios y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Agencia.

Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

7.1.1 Política de uso de equipos de computo

La Agencia de Renovación del Territorio – ART, debe establecer reglas que permitan comunicar a todos sus colaboradores que la seguridad es parte integral de los activos de información, mediante la correcta utilización de equipos de cómputo por parte de los usuarios finales. Los funcionarios deben solicitar el equipo tecnológico al Grupo Interno de Trabajo de Servicios Administrativos quien brindará la orientación sobre el uso adecuado del bien. Al recibir el equipo, el funcionario deberá garantizar que el equipo nunca será abierto ni modificado su hardware o su sistema operativo, como tampoco realizará copias directas al disco duro del equipo. Solo el personal definido dentro de la Oficina de Tecnologías de la información podrá realizar dichos cambios bajo el visto bueno del jefe de la oficina.

Es responsabilidad Jefe de la Oficina de Tecnologías de la Información crear, normatizar, implementar y optimizar herramientas, procesos y procedimientos que garanticen un uso adecuado de equipos de cómputo por parte de los funcionarios de la Agencia, además de velar por el buen uso de los equipos de la Agencia utilizados por los contratistas en calidad de préstamo, esto debido a que los contratistas solo podrán utilizar equipos prestados por

la agencia en tiempos estipulados entre el contratista y la Oficina de Tecnologías de la información.

Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a. Al momento de retirar un equipo de la organización y pase a almacén, el proceso de TI realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.

Todo aplicativo informático o software dentro del equipo de cómputo debe ser licenciado o aprobado por la Oficina de Tecnologías de la Información, en concordancia con los lineamientos en materia de adquisición de Bienes de la Agencia.

7.1.2 Política de uso de impresoras y del servicio de Impresión

No se permite el uso de los servicios de impresión para fines ajenos a lo estrictamente relacionado con las funciones u obligaciones contractuales de los usuarios de la Agencia, incluyendo información personal sensible.

El Jefe de la Oficina de Tecnologías de la Información debe implementar controles de seguimiento de los niveles de impresión para los usuarios de la Agencia que incluyan como mínimo el nombre del usuario, la dirección IP y el nombre del archivo y la fecha y hora de impresión. Estas mediciones estarán sujetas a controles periódicos con el objetivo de identificar patrones atípicos en el uso de este servicio y reportar posibles incidentes de seguridad de la información.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora por parte del usuario de forma inmediata y no se deben dejar en el escritorio sin custodia.

7.2 Políticas de seguridad del recurso humano

El Grupo Interno de Trabajo del Talento Humano y los Grupos Internos de Trabajo de Contratación Misional y Contratación de Funcionamiento al realizar el proceso de vinculación o contratación de personal con la Agencia debe realizar las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de La Agencia y con la ética pertinente.

Todo funcionario y/o contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.

La Oficina de Tecnologías de la información establece directrices para asegurar que los funcionarios y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación con la seguridad de la información.

Los acuerdos contractuales entre la Agencia y los funcionarios y/o contratistas especifican el cumplimiento a los lineamientos de seguridad de la información establecidos en la Agencia.

El Grupo Interno de Trabajo del Talento Humano y los Grupos Internos de Trabajo de Contratación Misional y Contratación de Funcionamiento realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, Así mismo, los directores, jefes, supervisores de contrato, coordinadores o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente a la Oficina de Tecnologías de la Información.

La Agencia debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

7.2.1 Proceso Disciplinario y Responsabilidad Jurídica Disciplinaria

Dentro de la estrategia de la Seguridad de la Información de la Agencia, es responsabilidad de la Secretaría General de la Agencia; crear, normatizar, implementar y optimizar un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. Para el caso de contratistas será responsabilidad del supervisor, informar al organismo competente en caso de configurarse un incumplimiento a las políticas de seguridad de la información adoptadas por la agencia según su responsabilidad jurídica disciplinaria.

Las investigaciones disciplinarias y las acciones de los supervisores corresponden a actividades pertenecientes a actuaciones que conllevan a la violación de la seguridad de la información establecidas:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información sin autorización.
- Ingresar a carpetas compartidas de otros procesos, unidades, grupos o áreas, sin autorización.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los

estándares establecidos para este fin.

- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, *"documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)*".
- No guardar la información digital, producto del procesamiento de la información perteneciente a la entidad.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Agencia, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Agencia.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular, su jefe inmediato o supervisor.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilizar software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Oficina de Tecnologías de la Información de la Agencia.
- Permitir el acceso de funcionarios o contratistas a la red corporativa, sin la autorización de la Oficina de Tecnologías de la Información.
- Utilizar servicios disponibles a través de internet, como FTP, Telnet y almacenamiento en la nube, no permitidos por la Agencia o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Hacer mal uso de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Agencia.
- No cumplir con las actividades designadas para la protección de los activos de información de la ART.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la Agencia, sin las medidas apropiadas de seguridad que garanticen su protección.

- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a la Agencia o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la ART, sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promocionar o negocios personales, o utilizar los recursos tecnológicos de la ART para beneficio personal.
- Destruir, dañar o borrar datos informáticos o un sistema de información de la ART.
- Distribuir, enviar o instalar software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la ART.
- Violar datos personales de las bases de datos de la ART.
- Vulnerar las medidas de seguridad informática o suplantar a un usuario ante los sistemas de autenticación y autorización establecidos por la entidad.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la ART o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la ART a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de la ART o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la ART.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones de la ART, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la ART, para traslado, reasignación o para disposición final.
- Ejecutar cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la ART o de alguno de sus colaboradores.
- Realizar cambios no autorizados en la plataforma tecnológica de la ART.
- Acceder, almacenar o distribuir pornografía.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Oficina de Tecnologias de la Información.
- Copiar sin autorización los programas de la ART, o violar los derechos de autor o acuerdos de licenciamiento.

7.3 Política de seguridad física y entorno

El Grupo Interno de Trabajo de Servicios Administrativos debe implementar un Sistema de Seguridad Física para las instalaciones de la Agencia, que permita crear las reglas y pautas para el acceso controlado y documentado al personal autorizado.

El acceso a los sitios de trabajo, donde se encuentran los equipos de cómputo de la Agencia debe contar con acceso a las instalaciones físicas con lector de huellas o tarjetas de proximidad, para todos los funcionarios contratistas o terceros, así como de manejar una minuta física o digital para el registro de personal visitante o invitado, también se debe poseer el uso de cámaras de video vigilancia para verificar cualquier novedad, evento o incidente de seguridad de la información.

Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de la Agencia.

Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

El Grupo Interno de Trabajo de Servicios Administrativos de la Agencia debe realizar y mantener actualizado un programa de seguridad física de las instalaciones, así como verificar el uso, apropiación y administración de las barreras de seguridad (perimetrales e internas) en las que se destacan, personal de vigilancia, minutas de acceso de personal, sistemas de videovigilancia y controles de acceso en todas las oficinas y sedes pertenecientes a la Agencia.

7.3.1 Políticas de seguridad del centro de datos y centros de cableado

La Oficina de Tecnologías de la Información debe asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del Centro de Datos o de los Centros de Cableado de la Agencia, **NO** estará permitido

- Fumar dentro del centro de datos.
- Introducir alimentos o bebidas al centro de datos.
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.

- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Cada gabinete o armario debe contener llave de ingreso, así como cada Centro de Cableado, las cuales deben permanecer almacenadas en la debida caja de seguridad dispuesta para ello dentro del Centro de Cómputo.

El centro de datos debe tener control de acceso a través de sistema de huellas y tener sistema de videovigilancia en caso de incidentes de seguridad.

7.4 Política de control de acceso

La Agencia define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.

Es así como la Oficina de Tecnologías de la Información debe definir, publicar y socializar un reglamento para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de la Agencia.

Para el control de acceso a los recursos tecnológicos a través de usuario y contraseña en la Agencia se definen cinco (5) recursos: sistemas operativos, bases de datos, aplicaciones, correo electrónico e internet.

- El manejo para el acceso a los sistemas operativos de los equipos con los que cuenta la Agencia está administrado por el Directorio Activo, este provee el usuario y la contraseña de acceso al dominio, tanto para los funcionarios y colaboradores (contratistas).

- Ningún usuario debe tener acceso a las bases de datos sin previa autorización de los responsables. El Jefe de la Oficina de Tecnologías de la Información es el responsable de establecer mecanismos formales de autorización de acceso a las bases de datos en caso de requerirse.

- Las aplicaciones deben manejar un usuario y una contraseña propia de la aplicación, las cuales podrían ser independientes o estar sujetas al Directorio Activo. Existen otros recursos como acceso a servidores de impresión y servidores de archivos compartidos, a estos recursos se accede estableciendo el usuario y la contraseña a

partir del Directorio Activo.

- El correo electrónico de la Agencia también debe tener acceso controlado por usuario y contraseña que es creado por el usuario y contraseña de Directorio Activo.

- El acceso a Internet a través de la Red LAN y red WIFI estará sujeta al acceso permitido por el directorio Activo. Adicionalmente para el acceso a la red WIFI la Oficina de Tecnologías de la Información proporcionara las credenciales que serán de tipo confidencial e intransferible por parte de los usuarios.

- La Oficina de Tecnologías de la Información debe brindar las herramientas de auditoria que permitan identificar los accesos a los activos de información de tipo software en cualquier momento y en correspondencia a las acciones que se deban verificar.

- Todas las contraseñas otorgadas deberán cumplir con la política de establecimiento, uso y protección de claves de acceso del presente manual.

La conexión remota a la red de área local de la ART debe realizarse a través de una conexión VPN segura suministrada por la Agencia, la cual debe ser aprobada, registrada y auditada, por la Oficina de Tecnologías de la Información.

El responsable de la administración del control de acceso debe definir el procedimiento de asignación, modificación, revisión periódica o revocación de accesos y privilegios, de los usuarios, teniendo en cuenta los derechos de usuario, los derechos de usuarios avanzados y los derechos de administradores, así como de desactivar o eliminar las cuentas de usuario una vez finalizada la relación contractual. Lo anterior es aplicable para los sistemas de información misionales y de apoyo, servidores de archivo, directorio activo y sistemas de gestión de usuarios, a través de sus respectivos administradores técnicos y funcionales.

Si una entidad pública, entidad privada, o personal externo requiere acceso a información sensible o crítica, se deben suscribir acuerdos de confidencialidad o de no divulgación para la salvaguarda de la información, y acogerse a los protocolos de intercambio de información establecidos por la Oficina de Tecnologías de la Información, mediante la aplicación de un anexo técnico que se deberá coordinar con las áreas institucionales con competencia en la materia; así como realizar el cumplimiento de la normatividad vigente para la Agencia.

Es responsabilidad de la Oficina de Tecnologías de la Información, crear, normatizar, implementar y optimizar herramientas, procesos y procedimientos que garanticen un adecuado control de acceso a la información y a la plataforma tecnológica de la Agencia por parte de los usuarios, a través de sus respectivos administradores técnicos y funcionales.

7.4.1 Política de establecimiento, uso y protección de claves de acceso

Ningún usuario debe acceder a la red o a los servicios Tecnológicos de la Agencia, utilizando una cuenta de usuario o clave de otro usuario. La Oficina de Tecnologías de la Información es responsable de suministrar a los usuarios las claves respectivas para el acceso a los servicios de red, para los sistemas de información esta labor deberá ser coordinada con los respectivos administradores técnicos y funcionales, para lo cual las claves de acceso son de uso personal e intransferible y no se deben dejar por ningún motivo en lugares a la vista de terceros.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red y correo electrónico.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al correo soporte_TI@renovacionterritorio.gov.co dispuesto por la Agencia, en donde se llevará a cabo la validación de los datos personales; en caso de solicitarse el cambio de contraseña para otro usuario, esta debe ser realizada por el jefe inmediato del usuario, previa autorización por parte de la Oficina de Tecnologías de la Información. Para el caso de las aplicaciones misionales, los administradores técnicos y funcionales deberán definir los procedimientos adecuados para garantizar la protección de la clave de acceso al momento de asignación o cambio.

Las claves o contraseñas deben:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Ser distintas por lo menos de las últimas doce contraseñas anteriores.
- Cumplir con los siguientes requisitos:
  - Caracteres en mayúsculas
  - Caracteres en minúsculas
  - Base de 10 dígitos (0 a 9)
  - Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)
  - No colocar nombres ni apellidos de los usuarios dentro la contraseña.

7.4.2 Manejo de contraseñas para administradores de tecnología

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directa de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas de accesos a las consolas administrables se deben dejar en custodia en sobre sellado en el área segura

designada por el responsable de la Oficina de Tecnologías de la Información, las credenciales allí contenidas deben ser modificadas periódicamente o de forma excepcional cuando así lo amerite.

Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal de la Oficina de Tecnologías de la Información y la subdirección de gestión de la información que administre sistemas de información no debe dar a conocer su clave de usuario a terceros.

Los usuarios y claves de los administradores de la plataforma tecnológica y del personal de la Oficina de Tecnologías de la Información son de uso personal e intransferible.

El personal de la Oficina de Tecnologías de la Información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Agencia de acuerdo con el rol asignado y acorde a la política de establecimiento, uso y protección de claves de acceso.

Los administradores técnicos y funcionales de los sistemas de información deben seguir las políticas de cambio de clave e implementar un procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el jefe de la Oficina de Tecnologías de la Información y el Subdirector de Gestión de la Información.

7.5 Política de escritorio y pantalla limpia

La Oficina de Tecnologías de la Información debe definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios, mediante el resguardo de información en un lugar diferente al escritorio del equipo y mediante resguardo de documentos que se dejan sobre los diferentes puestos de trabajo de los colaboradores de la Agencia.

- Los funcionarios, deben conservar escritorio libre de información propia de la Agencia, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- Los contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la Agencia con los equipos en préstamo deberán conservar escritorios limpios evitando que la información pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento

- Los funcionarios y/o contratistas usuarios de los Sistemas de Información y Comunicaciones de la Agencia deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba ausentarse de su puesto de trabajo.

- Los funcionarios y/o contratistas, usuarios de los sistemas de información y comunicaciones de la Agencia deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

7.6 Política para realización de copias de información

La información generada por los usuarios y relacionada con actividades propias de la Agencia debe ser almacenada en los repositorios definidos por la Oficina de Tecnologías de la Información con el fin de garantizar el resguardo y custodia de esta.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la solicitud de soporte establecida por la Oficina de Tecnologías de la Información.

Diariamente los administradores de plataforma de copias de seguridad de la Oficina de Tecnologías de la información verificarán la correcta ejecución de los procesos de copias de seguridad sobre los repositorios definidos, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

Para la información almacenada en esquemas de nube publica o privada se deberán de garantizar los procedimientos de copia de seguridad y de respaldo realizados por los proveedores de servicio.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El administrador de la plataforma de copias de seguridad de la Agencia debe generar tareas periódicas de restauración aleatorias de la información las cuales deben ser documentadas.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Oficina de Tecnologías de la Información.

La Oficina de Tecnologías de la Información brindara las herramientas para la custodia y protección de la información de los usuarios, cuando se realice copias de seguridad a los equipos de cómputo, repositorios en nube y correo electrónico.

La seguridad de la información es parte integral de toda la Agencia y es responsabilidad de todos los funcionarios y contratistas salvaguardar la información, es por esto que la Oficina de Tecnologías de la Información debe hacer las campañas de comunicación necesarias, para la divulgación de los procedimientos que permitan generar copias de seguridad de información generada por parte de los usuarios de la Agencia.

El Grupo Interno de Trabajo de servicios administrativos, definirá la política de gestión documental y establecerá los procedimientos para la clasificación de la información y la retención documental.

La Oficina de Tecnologías de la Información debe definir un lugar para el almacenamiento y custodia de las copias de seguridad que garanticen su correcta conservación, previendo las distintas situaciones que puedan afectar estos elementos como perdidas, ciberataques, robos, inundaciones, terremotos, catástrofes naturales, incendios, asonadas etc.

7.7 Políticas de controles criptográficos

La Agencia asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocoló HTTPS con un nivel de cifrado actualizado.

El acceso remoto a la red LAN y los almacenamientos de información de la Entidad desde una red externa será a través de conexiones seguras VPN, que serán configuradas por solicitud a la Oficina de Tecnologías de la Información.

Se debe contar con buenas prácticas para la gestión de llaves criptográficas.

7.8 Políticas Seguridad en las Operaciones

Es necesario realizar la documentación de los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.

La Oficina de Tecnologías de la información garantizará que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.

Los cambios en la Agencia deben ser tratados a través de un proceso establecido con el fin de minimizar los riesgos de alteración de los sistemas de información.

Según la clasificación de la información establecida por la Agencia, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube.

Los responsables de la Oficina de Tecnologías de la Información definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para la política de copias de respaldo de la información.

La Oficina de Tecnologías de la información es la encargada de aplicar los parches, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades.

7.9 Políticas Adquisición, Desarrollo y Mantenimiento de Sistemas

La Oficina de Tecnologías de la Información garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo identifica y gestiona los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

La Oficina de Tecnologías de la información busca que la Seguridad de la Información sea parte integral dentro ciclo de vida de desarrollo de los sistemas de información, para ello establece un procedimiento para el desarrollo seguro de software, así como un procedimiento para la revisión técnica y la detección de vulnerabilidades y el procedimiento de cumplimiento de la política.

La Oficina de Tecnologías de la Información asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro

La Agencia a través de la Oficina de Tecnologías de la Información establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de todos los sistemas

de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

Además, la subdirección de gestión de la información cuenta con un ambiente de desarrollo y de pruebas seguro. Para el caso de desarrollo de software tercerizado la Oficina de Tecnologías de la Información, exigirá a los proveedores acuerdos de confidencialidad, con el fin de establecer controles de seguridad de la información sobre los ambientes de desarrollo y pruebas.

Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y custodiados de forma segura para evitar fugas de información.

La Agencia a través de la Oficina de Tecnologías de la Información definirá y elaborará los lineamientos de desarrollo de software y velará por su respectivo cumplimiento.

7.10 Política de relaciones con los proveedores

Para proveedores críticos de tecnología que ameriten continuidad y disponibilidad de los servicios, así como de procesos misionales, la Agencia exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que el proveedor contratado pueda responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Agencia.

La Agencia controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.

Cualquier cambio que se realice con algún proveedor de tecnología sobre la infraestructura tecnológica, debe aplicarse mediante el procedimiento de gestión de cambios establecido por la Oficina de Tecnologías de la Información.

La Agencia realiza revisiones periódicas al cumplimiento de las Políticas de Seguridad y Privacidad de la Información a los Proveedores.

7.11 Políticas de dispositivos móviles.

La Agencia establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

Los funcionarios con equipos asignados a su inventario y contratistas con equipos en calidad

de préstamo, no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos institucionales que se les entregue como recurso para la ejecución de sus obligaciones contractuales o funciones.

Es responsabilidad del funcionario y/o contratista al que se le asignó o en su defecto, se le realizo el préstamo del dispositivo móvil, evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Los colaboradores de la Agencia deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.

Los funcionarios y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Oficina de Tecnologías de la Información para el proceso de análisis, evaluación y tratamiento del incidente.

Los dispositivos móviles que son autorizados para salir de las instalaciones por la Agencia deben ser protegidos mediante el uso e implementación de los controles apropiados como: cifrado de información, políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

Todos los dispositivos móviles propiedad de la Agencia pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

Es responsabilidad de los contratistas, adecuar sus equipos móviles personales con niveles de seguridad aceptables para el ingreso a los servicios de red LAN y almacenamiento de datos de la Agencia donde se deberá como mínimo tener actualizaciones del sistema operativo y antivirus actualizado. Para verificar estos niveles de seguridad aceptables el contratista deberá tener el visto bueno de revisión de la Oficina de Tecnologías de la Información para su verificación.

7.12 Política de seguridad en el trabajo remoto

Toda información gestionada por la Agencia, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones

contractuales con esta.

La Agencia a través de la Oficina de Tecnologías de la Información brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza trabajo remoto y se hace uso de los recursos tecnológicos autorizados por la Entidad para el desarrollo de las actividades de Trabajo remoto.

La Oficina de Tecnologías de la Información establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

La Oficina de Tecnologías de la Información, elaborará un lineamiento con recomendaciones sobre el entorno del sitio donde se va a realizar el trabajo remoto, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

Es importante establecer la responsabilidad frente a la seguridad de la información que tienen los funcionarios y contratistas cuando realicen trabajo remoto, para no acceder a paginas peligrosas, o insertar dispositivos de almacenamiento USB que puedan infectar los equipos de la Agencia o equipos personales debido a que cuando se conecten de nuevo a la red de la misma Agencia o a través de la VPN que se le brinda a funcionarios y contratistas para el acceso a repositorios de información, puedan propagar software malicioso y generar una violación a la seguridad de la información.

7.13 Política de seguridad de las comunicaciones

La Oficina de Tecnologías de la Información realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso del filtrado web del firewall (*ver política de uso de internet*).

La Oficina de Tecnologías de la Información asegura la protección de las redes y la trasferencia de información. Según corresponda, para los intercambios de información se deberán considerar los documentos correspondientes de formalización del intercambio de información y los acuerdos de confidencialidad.

La Oficina de Tecnologías de la información implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Agencia.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada y alineado al protocoló de intercambio de información.

7.13.1 Política de uso de Internet

La Agencia permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

La Oficina de Tecnologías de la Información tiene la responsabilidad de administrar las autorizaciones y los cambios de permisos solicitados por los usuarios de la Agencia, previa solicitud del jefe o coordinador de cada una de las dependencias u Oficinas de la Agencia. Así mismo, debe implementar herramientas que impidan la descarga de software no autorizado y/o código malicioso en los equipos institucionales, y controlar el acceso a la información contenida en los portales de almacenamiento en la nube para prevenir la fuga de información.

Los usuarios de los activos de información de la Agencia deben tener acceso restringido a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucionales. En caso de ser requerido por las funciones del cargo o las obligaciones contractuales, el jefe inmediato debe remitir una solicitud al Jefe de la Oficina de Tecnologías de la Información, para que sea puesta a su consideración. Toda autorización será objeto de auditorías y logs de seguridad para revisión del Administrador de la infraestructura tecnológica.

Es responsabilidad de la Oficina de Tecnologías de la información, crear, normatizar, implementar y optimizar herramientas, procesos y procedimientos que garanticen un uso adecuado de internet por parte de los usuarios de la Agencia.

7.13.2 Política de uso de mensajería instantánea y redes sociales

La Oficina de Tecnologías de la Información en conjunto con la Oficina de Comunicaciones deben definir las pautas generales para asegurar una adecuada protección de la información de la Agencia, en el marco del uso del servicio de mensajería instantánea y redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Agencia, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se

considera fuera del alcance de la política General de la Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Agencia debe ser autorizada por la Oficina de Comunicaciones para ser socializadas y con un vocabulario institucional.

La información misional o de uso interno de la Agencia trasmitida por la Oficina de Comunicaciones a través de mensajes o redes sociales debe ser recibida, utilizada y entregada o transmitida de manera confiable, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

Es prohibido utilizar el nombre de la Agencia en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

7.14 Política de Gestión de los Incidentes de la Seguridad de la Información

Todos los funcionarios y/o contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información que se realiza a través del correo soporte_TI@renovacionterritorio.gov.co.

La Oficina de Tecnologías de la Información tiene la responsabilidad de crear, normatizar, implementar y optimizar herramientas, procesos y procedimientos orientados al tratamiento efectivo de los incidentes de seguridad de la información.

Los procedimientos asociados al tratamiento de incidentes de seguridad de la información deben incluir como mínimo:

- Una clara identificación y clasificación del incidente, análisis de causa raíz y análisis de vulnerabilidad.
- Acciones orientadas a mitigar el impacto del incidente.
- Acciones orientadas a la contención del incidente.
- Acciones correctivas para reparar y prevenir reincidencia.
- Acciones que garanticen la comunicación oportuna y efectiva a aquellos colaboradores afectados de forma directa e indirecta por la ocurrencia del incidente.

Los procedimientos implementados también deben incluir una sección que se refiera a la recopilación de cualquier evidencia que pueda ser necesaria para el análisis como evidencia

forense. Un conjunto de acciones específicas para preservar toda evidencia que debe ser seguida cuidadosamente.

Las acciones requeridas para recuperarse del incidente de seguridad deben estar bajo control formal. Solo personal identificado y autorizado debe tener acceso a los sistemas afectados durante el incidente y todas las acciones correctivas deben documentarse con el mayor detalle posible.

La información debe ser recopilada y revisada regularmente por la Oficina de Tecnologías de la Información, así como los patrones o tendencias identificadas. Cualquier cambio en el proceso realizado como resultado de la revisión posterior al incidente debe procesarse formalmente y generar mejoras o nuevas versiones del procedimiento de ser necesario.

Los colaboradores de la Agencia se obligan a informar a la Oficina de Tecnologías de la Información cualquier incidente de seguridad que se presente de forma inmediata utilizando los canales definidos en los procedimientos.

Es obligación de los responsables del tratamiento de los incidentes de seguridad de la información mantener en reserva la identidad del colaborador que reporta el incidente de seguridad de la información, en tanto se soluciona de forma definitiva el tratamiento al mismo, si quien reporta el incidente de seguridad solicita de forma explícita e inequívoca la reserva de su identidad.

Es responsabilidad de todos los colaboradores de la Agencia, reportar posibles debilidades de seguridad de la información a la Oficina de Tecnologías de la Información. Todo reporte debe generar un plan de acción que derive en un flujo de tratamiento de la debilidad reportada de forma suficiente y exhaustiva hasta su total resolución.

Los resultados del tratamiento de los incidentes de seguridad de la información deben ser reportados a la instancia correspondiente definida en los procedimientos dispuestos. Los incidentes de alto impacto deben ser comunicados al jefe de la Oficina de Tecnologías de la Información quien reportara si es necesario a la alta dirección.

La Oficina de Tecnologías de la Información debe contar con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Si se descubre que algún usuario ha incumplido esta política, puede estar sujeto a procedimientos de tipo disciplinario. Si se considera que un delito ha sido cometido, se tomarán las medidas correspondientes con las autoridades competentes.

7.15 Política de revisiones de seguridad de la información

Es responsabilidad de la Oficina de Tecnologías de la Información, garantizar la implementación y funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados, con el fin de realizar mejora continua al sistema mismo.

Los directores, secretarios, jefes de oficina, jefes de área y coordinadores, deben verificar y supervisar el cumplimiento de las Políticas de Seguridad de la Información en su área de responsabilidad.

La Oficina de Control Interno en conjunto con la Oficina de Tecnologías de la Información deben asignar a un colaborador para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las Políticas de Seguridad de la Información en las instalaciones de la Agencia.

La Oficina de Tecnologías de la Información debe establecer mecanismos o procedimientos para revisar periódicamente los Sistemas de Información con herramientas automáticas y especialistas técnicos.

7.16 Políticas de cumplimiento

La Agencia gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.

La Agencia asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

8. APOYO O SOPORTE

8.1. Toma de Conciencia

La Oficina de Tecnologías de la Información brindará campañas de sensibilización para los funcionarios, contratistas de la Agencia para que tomen conciencia adecuada de políticas y procedimientos sobre la seguridad de la información.

El Grupo Interno de trabajo de Talento Humano apoyará a la sensibilización e los funcionarios mediante sus capacitaciones de inducción y reinducción.

Los grupos internos de trabajo de contratación de funcionamiento y misional apoyarán la seguridad de la información, incluyendo dentro de las obligaciones generales de los contratos de prestación de servicios, la reserva y la confidencialidad de toda la información que los contratistas manejen en el cumplimiento de sus actividades.

8.2. Comunicación

El presente manual de políticas de Seguridad y Privacidad de la Información será comunicado a todas las partes interesadas de la Agencia, a través de la Oficina de Tecnologías de la Información y medios físicos de ser necesario.

La AGENCIA DE RENOVACION DEL TERRITORIO - ART deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son: Correo Electrónico, sitios web, comunicación impresa, charlas y capacitaciones.

8.3. Acuerdos de Confidencialidad

Que propendan por la privacidad y confidencialidad de la información, que se aplican a los usuarios cuando se realiza el proceso de vinculación o contratación de funcionarios y contratistas que laboren para la Agencia.

9. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
- Código Penal Colombiano - Decreto 599 de 2000.
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia,

Gobierno en línea.

- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

10. REVISIONES DEL COMITE INSTITUCIONAL DE GESTIÓN Y DESEMPÉÑO

El Comité Institucional de Gestión y Desempeño, realizará revisiones periódicas al Modelo de Seguridad y Privacidad de la Información teniendo en cuenta las siguientes condiciones (entradas para la revisión por la Alta Dirección):

a. Seguimiento a las tareas, actividades o acciones asignadas.

b. Informe de resultados de las revisiones del Modelo de Seguridad de la Información al interior de los procesos.

c. Resultados del último ciclo de auditoría interna al MSPI (informe de Auditoría Interna).

d. Cambios en el contexto interno y externo que sean pertinentes al MSPI.

e. Propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas.

f. Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad de la Información sólo aplica las acciones correctivas y de mejora.

g. Retroalimentación de las partes interesadas.

h. Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.

i. Vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.

j. Revisión anual de la política, objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.