MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

AGENCIA DE RENOVACIÓN DEL TERRITORIO

Diciembre de 2023

Documento aprobado por el Comité Institucional de Gestión y Desempeño en sesión del 28 de febrero de 2024, mediante acta N°.02 de 2024.

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 de los objetivos institucionales, requiere definir e implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vidade 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 políticas 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 27001:2022 y al Modelo de Seguridad y Privacidad de la Información – MSPI, de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MinTIC.

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.

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, que presten sus servicios o tengan algún tipo de relación con la Agencia de Renovación del Territorio – ART, con el fin de dar cumplimiento de sus funciones y fortalecer la confidencialidad, integridad y disponibilidad de los activos dela información de la ART.

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

Cualquier evento o acción que no se encuentre en las políticas de seguridad de la información y que afecte la confidencialidad, integridad y disponibilidad de la misma se cataloga como incumplimiento.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas del Sistema de Gestión de Seguridad de la Información - SGSI aplican y son de obligatorio cumplimiento para la Alta Dirección, secretarios, jefes de Oficina, jefes de Área, Líderes de Proceso, funcionarios, contratistas, y en general todos los usuarios que permitan el cumplimiento de los niveles de seguridad de la Agencia.

5. TÉRMINOS Y DEFINICIONES

Consultar el glosario general de seguridad de la información.

6. POLÍTICAS ORGANIZACIONALES

6.1. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Alta Dirección	Autorizar la disponibilidad de personal competente para liderar y controlar el desarrollo del Sistema de Gestión de la Información.
	Gestionar dentro de las posibilidades presupuestales los recursos necesarios para el óptimo desarrollo de las actividades del SGSI.
Comité Institucional de Gestión y Desempeño	Evaluar, revisar y aprobar por lo menos una vez al año la operación del Sistema a través del informe del Sistema de Gestión de Seguridad de la Información.
	Realizar seguimiento al Sistema de Gestión de Seguridad de la Información.
	Asegurar la implementación y desarrollo de las políticas de seguridad de la información.
	Aprobar y realizar seguimiento a los planes, programas, proyectos y estrategias necesarias para la implementación del Sistema de Gestión de Seguridad de la Información.
	Contribuir al mejoramiento continuo del SGSI.

Rol	Responsabilidad
Responsable de Seguridad de la Información	Definir y liderar la implementación y gestión de la Política General de Seguridad y Privacidad de la Información y el Manual de Políticas de Seguridad Digital y de la Información.
	Definir y actualizar el Plan de acción del Sistema de Gestión de Seguridad de la Información de la ART, alineado con los objetivos y el plan institucional.
	Gestionar la elaboración o actualización de las políticas, procedimientos y documentación del SGSI.
	Realizar las actividades de estructuración e implementación del Sistema de Gestión de Seguridad de la Información.
	Planificar, elaborar, controlar y gestionar las políticas, procedimientos y acciones de mejora del Sistema de Gestión de Seguridad de la Información dando cumplimiento a los lineamientos y estándares emitidos en la estrategia de seguridad digital de MINTIC.
	Preparar a la Entidad en el cumplimiento de las buenas prácticas de seguridad de la información, la norma ISO 27001, con el fin de dar respuesta a auditorías internas o externas presentadas en el marco del Sistema de Gestión de Seguridad de la Información.
	Definir y gestionar las especificaciones técnicas de los proyectos de seguridad, así mismo el modo de contratación, ejecución y actividades a desarrollar en cumplimiento al Sistema de Gestión de Seguridad de la Información y la normativa vigente.
	Realizar la definición y medición de indicadores del Sistema de Gestión de Seguridad de la Información.
	Atender las auditorias tanto internas como externas respecto al Sistema de Gestión de Seguridad de la Información, definir el plan de mejoramiento, , y gestionar el seguimiento a la implementación de las acciones propuestas.
	Gestionar e implementar los controles de seguridad que se definan en el marco de la implementación del SGSI y que son definidos en la declaración de aplicabilidad.
	Gestionar y liderar la actualización anual o cuando hayan cambios significativos en los activos de información en coordinación con los Delegados de Seguridad de cada una de las áreas y procesos de la Entidad.

Rol	Responsabilidad
	Liderar la gestión de activos, riesgos de seguridad digital y de la información, teniendo en cuenta las metodologías establecidas por la Entidad y a nivel normativo, desde la identificación, análisis, valoración y definición de los planes de tratamiento en la Entidad.
	Gestionar los eventos, incidentes, riesgos y vulnerabilidades de seguridad de la información de acuerdo con las políticas, procedimientos, metodologías y formatos de seguridad establecidos por la Entidad.
	Definir, liderar y gestionar el plan de capacitación y propender por generar la cultura organizacional en seguridad de la información.
	Apoyar las revisiones técnicas a la infraestructura tecnológica frente a posibles vulnerabilidades, riesgos y amenazas, con el fin de mitigar la materialización de estos y así prevenir incidentes de seguridad de la información.
	Elaborar estrategias para el mantenimiento y mejora del sistema de gestión de seguridad de la información.
	Gestionar el envío de comunicados de sensibilización y apropiación, así como dar capacitaciones sobre la seguridad de la información al interior de la ART a las partes interesadas.
	Elaborar, mantener actualizado, gestionar y apoyar la implementación del plan de continuidad de las operaciones con las partes interesadas.
	Realizar acompañamiento técnico a los entes de control y entidades externas a la ART en las auditorías asociadas al Sistema de Gestión de la Seguridad de la Información.
	Realizar gestión de vulnerabilidades de seguridad, con el fin de validar su mitigación con los responsables.
	Actualizar la declaración de aplicabilidad de acuerdo con los lineamientos descritos en la norma ISO 27001 de Sistemas de Gestión de Seguridad de la Información.
	Realizar seguimiento a los procesos de la Entidad, para mejorar o implementar controles de seguridad que sean necesarios para la mitigación de riesgos, dando cumplimiento a las políticas de seguridad establecidas en la entidad.
	Poner en conocimiento de Control Interno Disciplinario de la ART cuando se advierta alguna posible violación de la seguridad de la información.

Rol	Responsabilidad
Oficial de protección de datos personales	Establecer lineamientos para la protección de los datos personales tratados en la Agencia. Gestionar la documentación relacionada en la materia. Realizar levantamiento de bases de datos y clasificarla. Gestionar la implementación de los lineamientos basados en la Ley en toda la ART.
Jefe de Oficina de Tecnologías de la Información	Asegurar canales de comunicación que permitan recolectar información manifestada por los servidores públicos, terceros y grupos de interés frente a incidentes de seguridad de la Información.
	Gestionar la implementación de controles seguridad informática sobre la plataforma tecnológica.
	Apoyar la atención de incidentes de seguridad que requiera participación por parte del proceso de TI.
	Liderar e implementar el plan de continuidad de la operaciones de la ART, con el apoyo de las partes interesadas.
	Reportar información clara, completa y veraz sobre la materialización de riesgos de seguridad digital y de la Información.
Líderes de proceso	Identificar e inventariar los nuevos activos digitales de información y los riesgos en seguridad de la información asociados.
	Apropiar y apoyar la sensibilización en Seguridad y privacidad de la Información.
	Implementar y mantener los controles de seguridad que correspondan al proceso.
Control Interno	Realizar seguimiento al cumplimiento de las políticas y al Sistema de Gestión de Seguridad de la Información conforme con los requisitos legales, normativos y técnicos establecidos por la Agencia.
	Notificar los hallazgos y acciones de mejora a las partes interesadas.
	Realizar acompañamiento en la definición de los planes de mejoramiento y hacer seguimiento.
Servidores públicos (funcionarios y	Conocer y cumplir con la política general, políticas específicas, procedimientos, y demás lineamientos emitidos desde el Sistema de Gestión de Seguridad de la Información.

Rol	Responsabilidad
contratistas) terceros y grupos de interés	Apropiar y aplicar las políticas y lineamientos de seguridad de la información.
	Aplicar los controles de seguridad de la información que correspondan al rol que desempeña en el SGSI.
	Reportar los incidentes y riesgos de seguridad de la información que identifique en cumplimiento de sus funciones y obligaciones contractuales.
	Participar de las sesiones de capacitación y sensibilización en seguridad de la información y ciberseguridad.
	Participar en el levantamiento del inventario de activos de información bajo su responsabilidad o custodia.
	Cumplir y firmar los acuerdos de privacidad y manejo de la información, cuando por funciones u obligaciones contractuales frente a responsabilidad o custodia de activos de información se requiera.
	Apoyar la gestión de riesgos para prevenir la materialización de amenazas de los activos de información bajo su responsabilidad y custodia.
Directores, subdirectores, jefes de Oficina, coordinadores y asesores de la Dirección General	Propender por el cumplimiento de las políticas de seguridad de la Información por parte de los servidores públicos o terceros a su cargo.
	Designar un servidor público de su área como delegado de seguridad de la información.
Supervisores de contratos	Propender por el cumplimiento de las políticas de seguridad de la Información por parte de los contratistas a su cargo.
	Hacer firmar los acuerdos de privacidad y manejo de la información de los contratistas a su cargo.
	Reportar el incumplimiento o violación de las políticas de seguridad de la información al responsable de seguridad de la información de la Agencia.
	Asegurar la entrega de información al finalizar la vinculación contractual.
Delegados de seguridad de la información	Apoyar la actualización de los inventarios de activos de información, gestión de riesgos e incidentes de seguridad de la información que hagan parte de su proceso.
	Apoyar las actualizaciones y mejora continua del SGSI.

Rol	Responsabilidad
	Atender las solicitudes de apoyo que en temas de seguridad de la información realice el responsable de seguridad de la información.

6.2. INTELIGENCIA DE AMENZAS

Definir un plan de implementación de inteligencia de amenazas, con el fin de proteger la seguridad de la información y los datos.

La Entidad debe realizar correlación de fuentes de datos que permitan la detección de ciberamenazas potenciales, con el fin de establecer los planes de mitigación para los activos de información de la Entidad.

Definir los controles, lineamiento y documentación necesaria para realizar una adecuada identificación de amenazas que permitan recopilar procesar, identificación y analizar ciberamenazas que puedan poner en riesgo la seguridad de la información de la Entidad.

Articular el proceso de gestión de incidente y riesgos de ciberseguridad con la inteligencia de amenazas, con el fin de prevenir incidentes de alto impacto para la Entidad.

6.3. SEGURIDAD EN LA GESTIÓN DE PROYECTOS

La ART debe desarrollar las siguientes acciones para garantizar la seguridad en la gestión de proyectos:

Definir los lineamientos y controles de seguridad que se deben tener en cuenta durante el ciclo de vida de los proyectos.

Todos los proyectos que se lleven a cabo en la Agencia, deben involucrar los controles de seguridad de la información que se dispongan para tal fin.

Incluir en cada uno de los proyectos las cláusulas de confidencialidad y protección de datos personales.

Todos los proyectos deben contar con identificación y análisis de riesgos de seguridad.

Se debe incluir los controles de cumplimiento de seguridad para los proveedores y terceros.

Realizar seguimiento de la gestión de proyectos en la cadena de suministro

con el fin de mitigar posibles riesgos de seguridad.

6.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Para garantizar la gestión de activos de información, se deben tener en cuenta los siguientes aspectos:

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 asegurar 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 supervisor, líder de proceso, coordinador, jefe de oficina 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.

Los activos de información son de propiedad de la Entidad y el uso de éstos debe ser exclusivamente con propósitos laborales.

Los activos de información serán tratados de acuerdo con su nivel de clasificación indicado por los propietarios de los activos de información.

Los funcionarios y/o aliados no almacenarán información de uso personal en los equipos de cómputo o portátiles asignados para el desarrollo de sus funciones.

Todos los requerimientos relacionados con los activos de información serán solicitados por supervisor, líder de proceso, coordinador, jefe de oficina o director a través de la Mesa de Servicio de la Oficina de Tecnologías de la Información.

Se encontrarán bajo la custodia de la Oficina de Sistemas todos los medios magnéticos y/o electrónicos (disquetes, CDs u otros) que vengan originalmente con el software adquirido, sus respectivos manuales y licencias de uso; por lo cual se debe dar el adecuado tratamiento de acuerdo con su nivel de clasificación.

Todos los activos de información se deben etiquetar con base en los lineamientos establecidos por el GIT de Servicios Administrativos y de acuerdo con su clasificación.

7. CLASIFICACIÓN DE INFORMACIÓN

La entidad debe establecer los lineamientos para realizar la clasificación de la información, de acuerdo con la normativa legal y reglamentaria que aplica, es así como se definen los siguientes criterios para clasificar la información:

Clasificación	Definición
Información Pública	Es toda información que un sujeto obligado genere obtenga, adquiera, o controle en su calidad de tal. Documentos generados en el ejercicio de sus funciones que pueden ser consultados por cualquier ciudadano sin excepción de ley.
Información Pública Clasificada	Es toda aquella información pública, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos: • El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011; • El derecho de toda persona a la vida, la salud o la seguridad; • Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011. Ejemplo: Derechos privacidad y a la intimidad que esté incluida en hojas de vida, historia laboral y expedientes pensionales, estudio técnico de riesgo que se haga a personas que requieran protección; los cuadros de frecuencia del proveedor de redes que no pueden ser examinados por terceros.
Información Pública Reservada	Es toda aquella información pública cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: • La defensa y seguridad nacional; • La seguridad pública; • Las relaciones internacionales; • La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; • El debido proceso y la igualdad de las partes en los procesos judiciales; • La administración efectiva de la justicia; • Los derechos de la infancia y la adolescencia; • La estabilidad macroeconómica y financiera del país; • La salud pública. Ejemplo: Documentos, información y elementos técnicos de las

	entidades que realizan actividades de inteligencia y contrainteligencia; las actuaciones disciplinarias son reservadas hasta que se formule el pliego de cargos o la providencia que ordene el archivo definitivo; datos personales de niños, niñas y adolescentes; la información que al divulgarse cause un daño a un bien público que afecte la diversidad e integridad del ambiente (vulneración de derechos fundamentales), entre otros.
No Clasificada	Toda información que no se encuentra clasificada se considerará y tratará como Información Publica Reservada.

8. TRANSFERENCIA Y/O INTERCAMBIO DE INFORMACIÓN

Para la transferencia y/o intercambio de información, es necesario tener en cuenta:

La Agencia de disponer de mecanismos necesarios que sean seguros para realizar la transferencia o intercambio de información.

Se debe contar con herramientas o servicios cifrados para realizar transferencia o intercambio de información de manera segura, en los casos que se requiera por la clasificación de la información pública clasificada o pública reservada.

Definir controles de seguridad para la protección de la información en tránsito y en reposo.

Para la transferencia o intercambio de información, se debe firmar un acuerdo de confidencialidad, no divulgación o transferencia, con el fin de describir los controles que debe ser de cumplimiento por las partes interesadas.

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

9. SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

La ART debe garantizar la seguridad de información en el momento que mantenga relacionamiento o vínculos con los proveedores, es por ello que se debe tener en cuenta las siguientes actividades:

Se debe llevar el control con la clasificación de los proveedores, con el fin de identificar cuáles son críticos.

Realizar auditorías y revisiones de cumplimiento de requisitos y políticas de seguridad a los proveedores críticos de la Entidad.

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, implementados y probados, 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.

Todos los proveedores deben firmar acuerdos de confidencialidad y no divulgación, y en los contratos contar con las cláusulas de confidencialidad, donde se debe contemplar el 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.

10. SEGURIDAD CLOUD

La Entidad debe proteger la información en tránsito y en reposo de la infraestructura tecnológica que se encuentra en la Nube, para ello, se debe tener presente:

Se debe hacer uso de servicios y herramientas de cifrado para la protección de la información.

Se debe hacer uso de los servicios que proveen las nubes, con el fin de contar con una gestión adecuada de llaves y claves criptográficas.

Hacer uso de los servicios de conexión segura como Virtual Protocol Network (VPN).

En los casos que se considere necesario, realiza comprensión cifrada de información.

Para la protección de la infraestructura tecnológica, se debe contar con controles de seguridad como Firewall, Web Application Firewall (WAF), certificados digitales seguros y modelos de tráfico.

Se debe realizar la encriptación de información a nivel de block storage, a nivel de base de datos con TDE y encriptación de datos sensibles a nivel de aplicación.

11. GESTIÓN DE INCIDENTES DE 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 de la Mesa de Servicios y el correo seguridaddigital@renovacionterritorio.gov.co como medidas adicionales se debe tener en presente.

Es responsabilidad de todos los colaboradores de la Agencia, reportar posibles incidentes y debilidades de seguridad de la información.

Se deben definir procedimientos asociados a la respuesta y tratamiento de incidentes de seguridad de la información.

Los procedimientos implementados 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.

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.

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.

Se 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.

Se deben dejar documentadas las lecciones aprendidas y realizar sensibilización en la gestión de incidentes de seguridad.

12. SEGURIDAD DE LA CONTINUIDAD DE NEGOCIO

La Entidad debe establecer el análisis de impacto al negocio (BIA por sus siglas en ingles), por medio del cual se identifiquen los servicios críticos de compañía.

Identificar y evaluar los riesgos asociados a la continuidad del negocio y las operaciones de la Compañía.

Diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos de la compañía.

El área de tecnología debe disponer de planes de contingencia de los servicios Tecnológicos de Información y un plan de recuperación ante desastres, enfocados a lograr el retorno normal de la operación.

Definir los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) para los servicios ofrecidos.

Se deben realizan pruebas a los planes de continuidad y recuperación de manera periódica y documentarlas.

Se debe realizar revisiones a los planes y medir la eficacia de cada uno.

Se deben planificar, implementar, evaluar y mantener los mínimos controles de seguridad ante una eventual activación del plan de continuidad de negocio, donde se asegure la confidencialidad, integridad y disponibilidad de los activos de información involucrados en dicha continuidad.

13. 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.

14. SEGURIDAD PARA LOS RECURSOS HUMANOS

El Grupo Interno de Trabajo del Talento Humano y los Grupos Internos de Trabajo de Contratación Misional 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 o rol, la formación académica, experiencia y demás información que se requiera, de acuerdo con 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.

El Grupo Interno de Trabajo de Talento Humano notifica al equipo de Seguridad de la Información de los cambios administrativos que surgen, con el fin de realizar la inactivación, bloqueo o eliminación de ser necesario de los usuarios.

15. SEGURIDAD FÍSICA Y DEL 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 hacer 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 a las oficinas.

16. SEGURIDAD DE CENTRO DE DATOS

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, centro de cableado, entre otros, deben contar con control de acceso, ya sea través de llave de ingreso, acceso biométrico, etc, y las llaves o tarjetas de acceso deben almacenarse de manera segura.

El centro de datos debe tener control de acceso biométrico a través de sistema de huellas, tarjeta de proximidad o cerradura; y tener sistema de videovigilancia en caso de incidentes de seguridad.

17. USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

a. Uso aceptable:
   - El correo electrónico institucional debe utilizarse principalmente para fines relacionados con la entidad. El uso personal está permitido dentro de unos límites razonables, siempre que no interfiera con las responsabilidades laborales ni infrinja ninguna otra política.
   - Los colaboradores deben evitar enviar correos electrónicos innecesarios y ser conscientes del tiempo y los recursos que implica la

comunicación por correo electrónico.

b. Conducta profesional:
   - Todos los correos electrónicos deben atenerse a normas profesionales y mantener un tono respetuoso. Están estrictamente prohibidos el lenguaje y los contenidos ofensivos, despectivos o inapropiados.
   - Los colaboradores deben abstenerse de enviar o reenviar cualquier contenido discriminatorio, acosador, difamatorio o que infrinja cualquier ley o normativa.

c. Confidencialidad y privacidad:
   - Los colaboradores deben tener cuidado al enviar información sensible o confidencial por correo electrónico. Deberán utilizarse métodos de cifrado cuando sea necesario.
   - El acceso o uso no autorizado del correo electrónico institucional de otra persona cuenta está estrictamente prohibido.
   - Los colaboradores no deben revelar sus credenciales de correo electrónico institucional a nadie ni compartir sus datos de acceso con personas no autorizadas.

d. Seguridad:
   - Los colaboradore deben estar alerta ante intentos de phishing, archivos adjuntos sospechosos y enlaces en los correos electrónicos. Si se recibe algún correo electrónico sospechoso, debe comunicarse inmediatamente al departamento de OTI.
   - Los colaboradores no deben abrir ni descargar archivos adjuntos ni hacer clic en enlaces de fuentes desconocidas o no fiables.
   - El software antivirus y de seguridad aprobado por la entidad debe actualizarse periódicamente en todos los dispositivos que accedan al sistema de correo electrónico.

e. Eliminación de correo electrónico:
   - Los correos electrónicos relacionados con transacciones comerciales, contratos, asuntos legales o cualquier otra correspondencia importante deben conservarse.

18. MEDIOS DE ALMACENAMIENTO

Los medios o dispositivos de almacenamiento propios de la Entidad deben estar identificados, etiquetados, valorados y clasificados en la matriz de activos de información.

Revisar los casos que se considere necesario, proveer a los usuarios de la compañía los mecanismos y herramientas para el cifrado de información para los medios de almacenamiento.

Todo dispositivo extraíble debe ser analizado mediante las herramientas de exploración de virus o código malicioso actualizada.

Establecer controles de borrado seguro de información en dispositivos autorizados que almacenen información de la compañía, con el fin de controlarel acceso y recuperación de dicha información.

Asegurar las condiciones apropiadas para salvaguardar los principios de seguridad de la información en el transporte de medios de almacenamiento.

Los dispositivos personales que sean autorizados deben contar con una revisión y controles mínimos de seguridad para la protección de la información.

19. MANTENIMIENTO DE EQUIPOS

La Agencia debe establecer un programa o plan de mantenimiento para los equipos, servidores y dispositivos que hacen parte de sus operaciones, conforme a las especificaciones de los fabricantes y buenas prácticas establecidas.

La Oficina de TI es la responsable de gestionar el soporte y mantenimiento del hardware y software de dispositivos institucionales para el correcto funcionamiento de los equipos, así mismo para el desarrollo de trabajo remoto.

Los dispositivos personales utilizados por los colaboradores (empleados de planta, contratistas o terceros) para el desarrollo de las actividades laborales o contractuales, no son sujetos de soporte y mantenimiento por parte de la Entidad. Esta responsabilidad recae en cada colaborador, por lo tanto debe velar por el cumplimiento de la presente política en realizar el mantenimiento de sus dispositivos, con el fin de tener un buen funcionamiento de su equipo o dispositivo personal.

20. SEGURIDAD EN LOS EQUIPOS

La Agencia de Renovación del Territorio – ART, establece los lineamientos para comunicar a todos sus colaboradores que la seguridad es parte integral de los activos de información, mediante el uso adecuado de los 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 asegurar 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 del Jefe de la Oficina de Tecnologías de la Información crear, normatizar, implementar y optimizar herramientas, procesos y lineamentos que aseguren 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 Entidad y pasen almacén, la Oficina de Tecnologías de la Información realizará una copia de respaldo de la información almacenada en este activo.
b. La OTI realizará el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la Entidad con la herramienta adquirida para tal fin.
c. 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, con forme a la normativa y leyes vigentes.

Todo aplicativo informático / tecnológico o software dentro del equipo de cómputo de funcionarios, 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.

Los colaboradores y terceros cuando sea el aso deberán velar por la seguridad física de los equipos portátiles cuando se encuentre fuera de las instalaciones.

En viajes terrestres o aéreos, siempre debe mantener el equipo como equipaje de mano.

No se permite el préstamo del equipo a terceros no autorizados.

Los equipos de cómputo y medios extraíbles deben tener controles de cifrado y copias de seguridad.

Los equipos deben permanecer actualizados, con el fin de prevenir incidentes de seguridad de la información.

Está prohibido instalar o desinstalar software de los equipos sin autorización de la

Oficina de Tecnologías de la Información.

No consumir bebidas ni alimentos en los puestos de trabajo cerca de los equipos de cómputo, instalaciones eléctricas, entre otros.

21. POLÍTICA PARA USO DE DISPOSITIVOS FINALES

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 sistema antimalware 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, cuando no se requiera su uso.

Los funcionarios y/o contratistas 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.

22. GESTIÓN DE CAPACIDAD

La Oficina de Tecnologías de la Información de la ART vela por la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la Entidad, realizando las proyecciones de crecimiento y provisiones en la infraestructura tecnológica con una periodicidad definida.

La Oficina de Tecnologías de la Información realiza las actividades necesarias para la optimización de los servicios tecnológicos, sistemas de información y aplicaciones.

La Oficina de Tecnologías de la Información debe realizar la proyección de capacidades futuras, con el fin de dar continuidad a la operación.

23. 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, contratistas, personal en comisión, pasantes y terceros que tienen algún vínculo con la Agencia, deben conservar el escritorio virtual de su equipo de cómputo 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 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.

24. POLÍTICA CONTRA SOFTWARE MALICIOSO

La Entidad establece los controles de detección y prevención para la protección contra software malicioso; así como la implementación de controles y lineamientos como:

- Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida de precaución rutinaria.
- Prohibir el uso de software no autorizado en la Entidad.
- Realizar sensibilización, con el fin de generar conciencia respecto a los riesgos relacionados con la descarga de información y software desde redes externas u otro medio.
- Revisar periódicamente el estado de la infraestructura tecnológica de la

compañía que soporta los procesos misionales de la compañía.
- Verificar antes de su uso, la presencia de malware en archivos de medios electrónicos de origen incierto, dispositivos de almacenamiento USB o en archivos recibidos a través de redes no confiables.

25. GESTIÓN DE VULNERABILIDADES TÉCNICAS

La Oficina de Tecnologías de la Información de la ART es la encargada de aplicar o gestionar la instalación de los parches, controles o remediaciones derivadas de la ejecución de pruebas de seguridad periódicas como análisis de vulnerabilidades ingeniería social, ethical hacking, etc. sobre la infraestructura tecnológica.

La Entidad define procedimientos que permiten la gestión adecuada de las vulnerabilidades técnicas en la infraestructura tecnológica.

La Entidad establece controles para la gestión eficaz de las vulnerabilidades técnicas que se identifiquen o se notifiquen por los diferentes canales.

La Entidad debe realizar pruebas de seguridad que permitan identificar las vulnerabilidades y así realizar una gestión adecuada de las mismas, con el fin de mitigar la materialización de los riesgos que estás pueden ocasionar.

Se debe llevar el control de las vulnerabilidades detectadas, con el fin de realizar seguimiento de su mitigación.

26. GESTIÓN DE LA CONFIGURACIÓN

La configuración de la infraestructura tecnológica en la nube, equipos de cómputo de la Entidad y sistemas de información, se realiza bajo las buenas prácticas, cumpliendo con los estándares y políticas de seguridad de la Agencia.

Se debe documentar las configuraciones de seguridad o lineamientos de aseguramiento de la infraestructura tecnológica, incluido los sistemas y dispositivos.

Se debe aplicar por parte de los responsables de la infraestructura tecnológica, una política de "mínimo privilegio" en la configuración de los sistemas de información y dispositivos.

La Entidad debe realizar pruebas de seguridad periódicas para verificar la configuración de la infraestructura tecnológica.

27. PREVENCIÓN DE FUGA Y ELIMINACIÓN DE LA INFORMACIÓN

La Entidad debe realizar sensibilización a las partes interesadas para reducir la pérdida o fuga de información y los datos de la ART.

Aplicar controles de seguridad a la infraestructura tecnológica.

Cualquier sistema de información o equipo de cómputo que sea dado de baja o reutilizado, deberá contar con un proceso de borrado seguro.

El proceso de borrado seguro debe asegurar la destrucción de la información que está almacenada en el dispositivo.

La Entidad debe definir los lineamientos técnicos para la prevención de fuga o eliminación de la información.

28. ENMASCARAMIENTO DE DATOS

La Entidad debe establecer, mediante los acuerdos contractuales de transferencia o transmisión de información la existencia de cláusulas que especifican los requisitos de anonimización o seudonimización con el objetivo de asegurar que los datos no puedan técnicamente ser asociados con los titulares de la información.

La Entidad debe asegurar la trazabilidad de los datos personales, así mismo que se encuentren anonimizados, seudoanimizados o en claro, para identificar inequívocamente los usuarios y las acciones realizadas sobre ellos.

Se debe verificar que las técnicas de enmascaramiento de datos, seudonimización o anonimización utilizadas por la Entidad cumplan con los criterios más seguros definidos por la industria, con el fin de reducir el riesgo de reasociación de los datos con sus titulares.

29. COPIAS DE SEGURIDAD DE LA 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 asegurar 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 a la Mesa de Servicios establecida por la Oficina de Tecnologías de la Información.

Para la información almacenada en esquemas de nube pública o privada se deben establecer los procedimientos de copia de respaldo.

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 brinda las herramientas para la custodia y protección de la información de los usuarios, cuando se realice copias de respaldo a los equipos de cómputo, repositorios en nube y correo electrónico.

Es responsabilidad de todos los funcionarios y contratistas salvaguardar la información y almacenarla en los repositorios designados para tal fin.

Es responsabilidad del equipo de seguridad de la información realizar campañas de sensibilización para la divulgación de los procedimientos que permitan a los usuarios de la Agencia realizar una adecuada gestión.

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

La Oficina de Tecnologías de la Información debe definir un espacio 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.

30. REDUNDANCIA TECNOLÓGICA

La Entidad debe disponer de infraestructura tecnológica redundante para los servicios considerados como críticos, a través de la disposición de canales alternos de comunicación, copias de seguridad actualizadas y probadas, e instalaciones físicas alternas siempre y cuando así lo amerite, con el fin de asegurar la operatividad.

31. GESTIÓN DE RESGISTROS (LOGS)

Los sistemas de información que se encuentran en la Nube o en Onpremise, deben registrar los eventos de procesamiento de la información.

Se deben definir, conservar y revisar o monitorear los eventos necesarios para llevar un control de la trazabilidad de los usuarios, fallas de seguridad en los sistemas y transacciones realizadas en las mismas.

Se debe realizar copia de respaldo para los Logs de los activos de información críticos de la Entidad.

Se debe realizar revisiones cada seis (6) meses del cumplimiento del monitoreo de logs.

La Entidad debe centralizar a través de herramientas de correlacionador de eventos los logs de los activos de información críticos de la Entidad.

32. GESTIÓN DE MONITOREO

Desde la ART se llevan a cabo las siguientes acciones de gestión de monitoreo:

Configurar las opciones de supervisar de forma activa y pasiva los recursos de Nube mediante métricas, informes y alarmas, sobre el estado, la capacidad y el rendimiento de recursos de la infraestructura tecnológica.

Generar alertas en los activos de información de on-premise o nube en caso de que las métricas definidas alcancen parámetros establecidos.

El acceso a los datos obtenidos de las métricas establecidas debe ser sólo por parte de usuarios con privilegios de consulta y gestión de estos.

Asegurar los acuerdos de niveles de servicio acordados con los Clientes, conforme con los indicadores de operación de la infraestructura tecnológica establecidos.

Realizar correlación de registro y eventos para mitigar posibles riesgos e incidentes de seguridad de la información.

Realizar monitoreo del cumplimiento de las políticas de seguridad cada seis (6) meses.

33. SINCRONIZACIÓN DE RELOJES

Todos los sistemas de información de la Entidad deben estar sincronizados con la hora legal colombiana, asegurando el control adecuado del procesamiento de la información en las operaciones.

Realizar revisión del cumplimiento cada seis (6) meses, con el fin de prevenir riesgos en la sincronización de los relojes de los activos de información de la Entidad.

Realizar sensibilización a las partes interesadas sobre la importancia de mantener los activos de información con la hora local establecida.

34. USO DE PROGRAMAS PRIVILEGIADOS

Solo el personal autorizado de la Oficina de Tecnologías de la Información tendrá acceso a los programas con privilegios elevados.

Todos los usuarios finales deben realizar el proceso de solicitud formal para ser revisado, aprobado y/o denegado por el proceso o rol responsable, para acceder a los programas con privilegios elevados a través del procedimiento de control de accesos lógicos establecido por la Entidad.

Los usuarios deben informar cualquier riesgo o incidente relacionado con el uso de los programas con privilegios elevados de manera inmediata a través de la Mesa de

Servicios o el correo seguridaddigital@renovacionterritorio.gov.co.

Para solicitar acceso a programas privilegiados, se debe contar con autorización del responsable y ejecutar el proceso establecido.

35. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

La Entidad define e implementa controles para la instalación de software en sistemas operativos por parte de los colaboradores.

Los equipos se deben entregar con privilegios estándar y no de administración o que permitan la instalación de programas sin autorización.

Si se requiere permisos de administrador o instalación de algún software específico en los equipos de la compañía, por el desempeño de sus actividades laborales o contractuales, se debe realizar la solicitud al jefe inmediato para que sea revisado, gestionado y aprobado en conjunto con el líder de seguridad.

Se deben realizar revisiones periódicas mínimo 1 vez al año de la instalación de software en los equipos de la compañía, por parte del área de TI y con apoyo del líder de seguridad de la información.

36. 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.

La Oficina de Tecnologías 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 asegurar 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 involucrado y alineado al protocoló de intercambio de información.

37. CRIPTOGRAFIA

La ART establece el uso de controles criptográficos para la transferencia de la información Pública Reservada, Pública Clasificada, Pública / Pública, enlaces de comunicaciones, protección de medios fijos y/o removibles, acceso remoto, firmas electrónicas y digitales con entidades externas, datos y servicios, cuando sea necesario, para el resguardo de información basado en la evaluación de riesgos.

Para todo software desarrollado por la Entidad y/o por un tercero se debe hacer uso de certificados digitales firmados por una entidad de certificación (CA) confiable.

La Entidad gestiona los controles criptográficos para protección de claves de acceso a sistemas, datos y servicios.

Verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.

En cabeza de los proveedores de software asegurar que los controles criptográficos de los sistemas construidos por estos cumplen con los estándares establecidos por la compañía.

Se debe contar con un archivo protegido donde se encuentren todas las llaves criptográficas.

La información clasificada como información pública reservada y pública clasificada debe almacenarse en repositorios cifrados, asegurando su confidencialidad, integridad y disponibilidad.

Los medios removibles que contenga información catalogada como reservada o clasificada, y que deban salir de las instalaciones de Entidad, deberán hacer uso de esquemas de cifrado autorizados por la Oficina de Tecnologías de la Información.

Se debe disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red de la Entidad.
Todas las llaves criptográficas de la Entidad deben estar resguardadas en sistemas de cifrado que aseguren su confidencialidad, integridad y disponibilidad, en caso de desastres o incidentes de alto impacto

Establecer un mecanismo de gestión de claves donde se asegure:
.
Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.

Almacenar claves, incluyendo la forma de obtención de acceso a las claves por los usuarios.

Cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse.

Tratar las claves comprometidas (afectadas).

Revocar claves, incluyendo la forma de desactivarla o retirarlas.

Recuperar claves que se han perdido o corrompido, por ejemplo, para recuperar la información cifrada.

La administración de llaves criptográficas y certificados digitales estará a cargo de la Oficina OTI.

La solicitud de acceso o actualización al sistema y/o llaves de cifrado, se efectuará de manera formal en la mesa de servicios, en la medida en que las actividades laborales asignadas así lo determinen.

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 certificados digitales.

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, adicionalmente, el acceso MFA o 2FA.

38. DESARROLLO SEGURO

Asegurar 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.

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

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 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.

La Agencia define y elabora los lineamientos de desarrollo de software seguro y vela por su respectivo cumplimiento.

La Agencia define la necesidad de ejecución de pruebas de seguridad y de aceptación en los desarrollos que se realicen para la Entidad.

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 Entidad debe contar con una metodología y lineamientos de desarrollo seguro de software.

La Oficina de Tecnologías de la Información provee los recursos necesarios para la implementación de controles que permitan la separación de ambientes de desarrollo/pruebas, calidad y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

Se deben realizar pruebas de seguridad antes del paso a producción, después de mejoras del sistema o creación de nuevas funcionalidades.

Asegurar que las herramientas de desarrollo, utilizadas por el equipo de profesionales estén actualizadas con las últimas versiones conocidas.

Implementar controles de desconexión o cierre de sesión de los sistemas de información desarrollados, que permiten terminar completamente la sesión abierta previamente.

Protección de código fuente de los desarrollos realizados al interior de la Entidad de tal forma que no pueda ser obtenidos ni alterados por usuarios no autorizados.

Cualquier aplicación o sistema de información debe tener en cuenta los aspectos de seguridad de la información relacionados con los perfiles de usuario, así como el acceso a procesos y datos a nivel transaccional y más allá.

39. POLÍTICA PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La ART realiza el análisis e implementación de los requerimientos de seguridad en los sistemas de información desarrollados internamente o adquiridos, que incluyen la validación de usuarios, datos de entrada, salida y procesamiento de los mismos.

Los responsables de los sistemas de información deben considerar los requerimientos de seguridad necesarios para mantener la integridad y confidencialidad, en la etapa temprana del desarrollo y la incorporación de controles relevantes.

Para esto es necesario, junto con la "GUÍA PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO SISTEMAS DE INFORMACIÓN", tener en cuenta los siguientes aspectos:

La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o transversales, desarrollados al interior de la entidad o contratados con terceras partes, deben contemplar un completo análisis de requerimientos en cuanto a seguridad de la información, análisis de riesgos y posibles escenarios de riesgos asociando los controles respectivos para la mitigación de estos.

Todas las solicitudes para compra, actualización y/o desarrollo de software deben ser direccionadas y orientadas, con el acompañamiento y bajo los estándares definidos por la Oficina de Tecnologías de Información.

Los procesos de adquisición de aplicaciones y paquetes de software cumplen con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor y deben ser autorizados y bajo los estándares definidos por la Oficina de Tecnologías de Información

Únicamente está permitido el uso de software autorizado por la Oficina de Tecnologías de la Información. Para ambientes de Desarrollo se debe utilizar el estándar adoptado por la Entidad que es .NET y DevOps, así como la plataforma para Bases de Datos es SQL server.

El acceso de los usuarios a los sistemas de información misionales y transversales se restringe mediante autenticación por usuario y clave de acceso, para cada usuario se delimitarán los perfiles de acceso y procesamiento de información según las necesidades. La definición de los tipos de perfiles será determinada por los administradores de los sistemas de información de cada uno de los procesos.

40. 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.

Los funcionarios autorizados para realizar trabajo remote deben asegurar el uso de las conexiones VPN “Client to Site”; y canales seguros suministrados por la Entidad para el acceso, procesamiento, almacenamiento y transporte de los datos.

Los funcionarios autorizados para teletrabajar no realizarán conexiones remotas desde sitios como cafés internet o similares consideradas redes públicas y/o no seguras.

Los funcionarios y contratistas son responsables de la seguridad de la información cuando realicen trabajo remoto, por lo tanto, no deben ingresar a paginas peligrosas, conectar dispositivos de almacenamiento USB de dudosa procedencia que puedan infectar a los equipos de la Agencia o a equipos personales que acceden de manera remota a la infraestructura tecnológica e información de la Entidad.

41. 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 – Proceso de Jurídica; crear, estandarizar, implementar y optimizar un proceso disciplinario formal para los funcionarios que hayan incumplido 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.

El reporte se debe realizar teniendo en cuenta el impacto ocasionado por el incumplimiento a las políticas de seguridad de la información, ya que esto se cataloga como un incidente de seguridad de la información, que pude ser Alto, Medio o Bajo donde en cada uno de ellos se realizara de la siguiente manera:

- Alto y medio: Documentar e iniciar el proceso disciplinario
- Bajo: Reforzar la sensibilización en seguridad de la información.

Las investigaciones disciplinarias y las acciones de los supervisores corresponden a actuaciones pertenecientes a actuaciones que conllevan al incumplimiento y por tanto a vulnerar de la seguridad de la información, entre ellas se describen las relacionadas a continuación, sin limitarse sólo a ellas:

- No firmar o cumplir con los acuerdos de confidencialidad y privacidad de la información.
- Realizar entrega de información o activos de información sin autorización a personal no autorizado.
- Ingresar a carpetas compartidas de otros procesos, unidades, grupos o áreas, sin autorización.
- No reportar los incidentes, riesgos o vulnerabilidades de Seguridad de la Información.
- 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.
- Compartir las claves de accesos.
- Actuar como juez y parte en los procesos y ciclos que desarrollan en el desempeño de las funciones o actividades laborales o contractuales.
- No almacenar 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)*".
- 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 o no bloquear la sesión.
- 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.
- 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, información pública clasificada o de datos personales 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 pública clasificada de la Agencia, sin las medidas apropiadas de seguridad que aseguren su protección.
- Registrar información pública reservada o pública clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Almacenar información pública reservada o pública 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 pública clasificada, sin los controles definidos y aprobados por la Entidad (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.
- Vulnerar 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 pública 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 tecnológicade 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 Tecnologías de la Información.
- Copiar sin autorización los programas de la ART, o vulnerar los derechos de autor o acuerdos de licenciamiento.

42. POLÍTICA DE USO Y SERVICIOS 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.

El Jefe de la Oficina de Tecnologías de la Información implementa 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 o que contenga datos personales, deben ser retirados de la impresora por parte del usuario de forma inmediata y no se deben dejar en el escritorio sin custodia.

43. POLÍTICA DE CONTROL DE ACCESOS

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 auditoría 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.
- Se debe contar con doble factor de autenticación MFA o 2FA para los usuarios administradores y finales cuando sea requerido.

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, 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.

44. POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESOS

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, sistemas de información y demás activos.

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 o compartirlas.

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 nueve (9) 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.
  - Realizar cambio de claves de acceso a los activos de

información cada 45 días.

45. USO Y ADMINISTRACIÓN DE CONTRASEÑAS DE ADMINISTRADORES TECNOLÓGICOS

Se debe asegurar 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 superadministradores 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.

46. POLÍTICAS DE 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.

De acuerdo con la clasificación de la información establecida por la Agencia, se definen 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.

47. POLÍTICA DE USO DE INTERNET

La Agencia permite el acceso al servicio de internet, estableciendo lineamientos que aseguren 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 aseguren el uso adecuado de internet por parte de los usuarios de la Agencia.

48. POLÍTICA DE USO DE MENSAJERÍA INSTANTANEA 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, entre otras, se considera fuera del alcance de la política General de la Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad, así como 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.

49. POLÍTICA DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Es responsabilidad de la Oficina de Tecnologías de la Información, asegurar 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.

50. APOYO O SOPORTE

50.1. 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 de 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.

50.2. 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.

50.3. 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.

51. MARCO LEGAL

Consultar el normograma de la Agencia de Renovación del Territorio.

52. 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 y Privacidad de la Información al interior de los procesos.

c. Resultados del último ciclo de auditoría interna al Modelo de Seguridad y Privacidad de la Información (informe de Auditoría Interna).

d. Cambios en el contexto interno y externo que sean pertinentes al Modelo de Seguridad y Privacidad de la Información.

e. Propuestas o mejoras al Modelo de Seguridad y Privacidad de la Información 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.