LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN DE GESTIÓN DE ORDENAMIENTO SOCIAL DE LA PROPIEDADSUBDIRECCIÓN

DE SISTEMAS DE INFORMACIÓN DE TIERRAS

TABLA DE CONTENIDO

1 INTRODUCCIÓN

Como complemento a la Política General de Seguridad de la Información, la Agencia Nacional de Tierras – ANT ha identificado la necesidad de crear lineamientos de seguridad de la información que permitan asegurar la confidencialidad, integridad y disponibilidad de los activos de información. En ese sentido, a continuación, se presentan los lineamientos, mediante los cuales se gestionará la Seguridad de la Información como un proceso sistemático, documentado y conocido por toda la Entidad.

Entendiendo que la información es parte fundamental de los servicios que presta laAgencia Nacional de Tierras, y que, para garantizar su confidencialidad, integridad y disponibilidad, es necesario adoptar estrategias que permitan establecer niveles adecuados de protección que aseguren la continuidad en la prestación de los servicios a sus diferentes usuarios, la Dirección de Gestión de Ordenamiento Social de la Propiedad ha establecido el presente documento de Lineamientos de Seguridad de la Información, como una herramienta para el logro de los objetivos estratégicos planteados para la Agencia por la Alta Dirección y por la Presidencia de la Republica. En este contexto, los lineamientos son aplicables de manera institucional y se encuentran alineados con la estrategia de Gobierno Digital.

2 OBJETIVO

Establecer los lineamientos, reglas e instrucciones detalladas que permitan implementar un gobierno de Seguridad de la información de la ANT, con el fin de proteger los activos de información y dar cumplimiento a los requisitos legales y losestándares de seguridad de la política de Gobierno Digital.

3 ALCANCE

El presente documento tiene aplicabilidad para los elementos que hacen parte de la arquitectura tecnológica de la ANT, particularmente para los activos de información de todos los procesos (se incluyen todos los dominios de Arquitectura empresarial propuestos por MINTIC: Misional o de Estrategia de TI, Gobierno de TI, Gestión de información, Sistemas de Información, Servicios Tecnológicos, Uso y Apropiación); de igual manera aplica a todos los funcionarios, contratistas, terceros y entidades externas que tengan acceso a la información institucional, sistemas de información, servicios de red y de intercambio de información, deberán cumplir estrictamente con la política y los lineamientos de la seguridad de la información definidos por la ANT. Los cuales deberán ser publicados y socializados a todas laspartes interesadas.

4 DISPOSICIONES GENERALES

4.1 Frecuencia de actualización de los lineamientos de seguridad de lainformación

Los lineamientos tendrán una revisión de actualización semestral o anual (dependiendo de las decisiones tomadas en la Mesa Técnica de TI o quien haga sus veces), de igual forma, se revisarán cuando hayan surgido actualizaciones o cambios significativos a los procesos, procedimientos, servicios informáticos, leyes o normatividad aplicable.

5 LINEAMIENTO ORGANIZACIÓN, ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN,

Objetivo: Definir y asignar las responsabilidades para una adecuada gestión de la seguridad de la información.

5.1 Asignación de responsabilidades

a) La asignación de responsabilidades sobre la gestión de la seguridad de la información se realiza para cada funcionario, contratista y parte interesada de laAgencia, con base en la política general de seguridad de la información.

b) Las diferentes responsabilidades asignadas se documentan formalmente a través de instrumentos que son comunicados y formalmente aceptados por el responsable de la actividad o control de seguridad de la información.

c) La asignación de responsabilidades para la seguridad de la información tiene enconsideración la identificación y análisis de los factores internos y externos (obligaciones legales, contractuales o regulatorias) y tendencias institucionales que puedan influir en el diseño del modelo de gobernabilidad de la tecnología dela ANT.

d) La determinación de las responsabilidades que se asignan en materia de seguridad de la información considera la competencia necesaria para cumplir dichas responsabilidades.

e) La verificación del cumplimiento de las responsabilidades asignadas en materiade seguridad de la información a cada funcionario, contratista y parte interesadade la Agencia es realizada por un superior, supervisor u otro rol pertinente, formalmente nombrado por la Entidad.

f) El incumplimiento de las responsabilidades asignadas sobre la seguridad de la información se trata mediante procedimientos administrativos y en los casos en los que normativamente se evidencien incumplimientos con afectación legal se evalúa la aplicación de los procedimientos de control disciplinario o legal según aplique de acuerdo con la evaluación e investigación que realicen las instanciaspertinentes dentro de la ANT.

g) Funcionarios, contratistas y partes interesadas a los que se les han asignado responsabilidades de seguridad de la información pueden delegar a otros las tareas de seguridad de la información. No obstante, siguen siendo responsabley deben determinar la ejecución correcta de cualquier tarea delegada.

5.2 Responsabilidades generales aplicables a todos los funcionarios,contratistas y partes interesadas

a) Cumplir con diligencia, eficiencia e imparcialidad del servicio que le sea encomendado y abstenerse de cualquier acto u omisión que cause la suspensióno perturbación injustificada de un servicio esencial, o que implique abusoindebido del cargo o función.

b) Conocer y cumplir con las políticas de seguridad de la información, procesos, procedimientos y controles del sistema de gestión de la seguridad de la información y no impedir el correcto y permanente funcionamiento de estos.

c) Utilizar los activos de información asignados para el desempeño de su empleo,cargo o función, las facultades que le sean atribuidas, o la información reservadaa que tenga acceso por razón de su función, en forma exclusiva para los fines aque están afectos.

d) Custodiar y cuidar la documentación e información que por razón de su empleo,cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

e) Ejercer sus funciones consultando permanentemente los intereses del bien común, y teniendo siempre presente que los servicios que presta constituyen elreconocimiento y efectividad de un derecho y buscan la satisfacción de las necesidades generales de todos los ciudadanos.

f) Vigilar y salvaguardar los activos de información que le han sido encomendadosy cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.

g) Informar sobre las debilidades, eventos/incidentes de seguridad de la información, potenciales delitos informáticos, contravenciones o incumplimientos de las políticas de seguridad de la información de los cuales tuviere conocimiento, salvo las excepciones de ley a la Subdirección

de Sistemas de Información de Tierras - SSIT.

h) Participar en las actividades de formación, capacitación o sensibilización en seguridad de la información, divulgación de componentes del Sistema de Gestión de Seguridad de la Información y demás actividades diseñadas por la Entidad, para mejorar las habilidades y competencias del personal en materia de seguridad de la información.

i) Participar en las actividades de evaluación, medición y análisis del desempeño de la seguridad de la información.

j) Colaborar en la correcta ejecución de las actividades de auditoría al sistema de gestión de seguridad de la información.

k) Participar dentro del ámbito de su competencia en las actividades de identificación, valoración, evaluación y tratamiento de riesgos de seguridad de lainformación.

l) Nunca ocasionar daño o dar lugar a la pérdida de activos de información que hayan llegado a su poder por razón de sus funciones.

m) Nunca dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas.

n) Suscribir con la ANT los acuerdos sobre cesión de derechos de autor, explotación, comercialización y protección de la información,compromiso de confidencialidad, compromiso de usuario en aplicativos, herramientas informáticas o información institucional y los demás aplicables para el uso adecuado de los recursos de información tecnológicos.

5.3 Responsabilidades de los niveles directivos

a) Participar activamente de las actividades de planificación y revisión del sistema de gestión de seguridad de la información.

b) Establecer la política general de la seguridad de la información de la Entidad.

c) Asegurar, que los requisitos de la gestión de la seguridad de la información estén incorporados al Sistema Integrado de Gestión Institucional.

d) Asegurar la existencia de los recursos humanos, económicos y técnicos necesarios para la gestión adecuada de la seguridad de la información en la Entidad.

e) Garantizar que se incluyen en los planes de comunicaciones institucionales la importancia de la gestión de la seguridad de la información y la necesidad de mantener la conformidad con los requisitos de seguridad institucionales.

f) Evaluar los resultados de la gestión de la seguridad mediante la revisión periódica del sistema integrado de gestión.

g) Dirigir y orientar a los funcionarios, contratistas y terceras partes interesadas en la gestión de la seguridad para lograr la eficacia del sistema.

h) Fomentar y promover la adopción de oportunidades de mejora en la gestión de la seguridad.

i) Designar y apoyar los roles necesarios para una adecuada gestión de la seguridad de la información.

j) Participar en la revisión anual del sistema de gestión de seguridad de la información para asegurarse de que permanece conveniente, adecuado y eficaz frente a las necesidades de la Entidad.

k) Evaluar la necesidad de realizar la separación de deberes y áreas de responsabilidad en materia de seguridad de la información con potenciales conflictos.

l) Verificar que en los contratos de sus subordinados estén contempladas las responsabilidades en materia de seguridad de la información aplicables a la función o empleo asignado.

m) Dentro del ámbito de su competencia aprobar los planes de tratamiento de los riesgos de seguridad de la información bajo su responsabilidad.

n) Dentro del ámbito de su competencia evaluar y cuando sea pertinente aprobar el nivel de riesgo residual de seguridad de la información identificado.

5.4 Responsabilidades del oficial de seguridad de la información

a) Asesorar a la Mesa Técnica de TI en la planificación, diseño, implementación, operación, revisión y mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI en la Entidad, sus políticas, lineamientos y controles, conforme a los requerimientos legales y buenas prácticas de normas técnicas.

b) Apoyar a la Mesa Técnica de TI en las actividades de implementación del Modelo de Seguridad

y Privacidad de la información – MSPI de la estrategia de Gobierno Digital.

c) Apoyar a la Mesa Técnica de TI en las actividades de implementación de la estrategia de ciberseguridad definida por el Ministerio de Defensa Nacional.

d) Apoyar a la Mesa Técnica de TI en las actividades de divulgación y promoción de la importancia del Sistema de Gestión de Seguridad de la Información, los beneficios de la seguridad de la información para la Entidad, y las implicaciones de la no conformidad con los requisitos de seguridad de la información de la Agencia, mediante la elaboración de propuestas de programas de toma de conciencia y formación en seguridad de la información.

e) Velar por el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información a nivel de su operación, desarrollo e implementación de sistemas de información, bases de datos y sistemas de comunicaciones informáticos.

f) Proponer y coordinar las acciones necesarias para identificar, controlar, reducir y evaluar incidentes de seguridad de la información.

g) Preparar los informes del estado de la seguridad de la información y la efectividad de los controles de la seguridad, para realizar la revisión periódica del estado del sistema y acompañar a la Entidad en la evaluación de este, paraasegurar que el Sistema de Gestión de Seguridad de la Información permanece conforme a las necesidades de la Entidad, y se identifiquen mejoras sobre el mismo.

h) Proponer, diseñar y fomentar la implementación de mejoras a los controles y herramientas de seguridad de la información necesarias para el fortalecimiento de la seguridad de la información en la Entidad, y el adecuado tratamiento de los incidentes de seguridad de la información detectados.

i) Ser punto de enlace con los grupos de interés que determine el gobierno nacional en materia de ciberseguridad como ColCERT, CSIRT Policía Nacional, CSIRT Gobierno, grupos de trabajo sectorial en materia de seguridad de la información.

j) Participar como punto de contacto con las autoridades y entes de control en los aspectos referentes a la gestión de la seguridad de la información, respuesta a eventos y atención de incidentes de seguridad de la información.

5.5 Separación de deberes

a) Se considera un conflicto de interés como aquella situación en la que el juicio del individuo -

concerniente a su interés primario- y la integridad de una acción tienden a estar indebidamente influidos por un interés secundario, estas situaciones pueden provenir de condiciones de tipo económico, personal o técnico, entre otras. A fin de evitar estas situaciones los deberes y áreas de responsabilidad en conflicto se separan para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Entidad. En las actividades en donde la seguridad de la información es un factor esencial se designa un responsable de autorización y un responsable de ejecución.

b) Las labores de control y seguimiento al cumplimiento de la debida separación de deberes son ejecutadas mediante el proceso de SEGUIMIENTO, EVALUCIÓN Y MEJORA del sistema integrado de gestión institucional.

c) Cuando el funcionario, contratista o parte interesada evidencien imposibilidad de separar debidamente actividades que entran en conflicto, se debe notificar al superior responsable a fin de establecer el mecanismo de comunicación de la toma de decisiones por parte del responsable de la tarea en conflicto.

5.6 Seguridad en la gestión de proyectos

a) Los roles responsables de la dirección o ejecución de proyectos de tecnología de información y comunicaciones deben incluir en los procesos de planificación,ejecución, control y seguimientos las actividades necesarias para identificar, valorar, evaluar y tratar los riesgos de seguridad de la información de los proyectos.

b) La gestión de riesgos de seguridad de la información en proyectos se realiza deacuerdo con la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el diseño de controles en Entidades públicas.

c) Los aspectos específicos del tratamiento y gestión de riesgos de proyectos relacionados con el desarrollo de software se administran de acuerdo con el lineamiento Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

6 LINEAMIENTO USO DE DISPOSITIVOS MÓVILES

a) Los usuarios no deben utilizar equipos de comunicación diferentes a los autorizados por el Equipo de Infraestructura y Soporte Tecnológico – EIST de la SG para acceder a redes internas o externas de la Entidad.

b) Las estaciones de trabajo ya sean equipos portátiles o equipos de escritorio asignados por la

Entidad, no deberán ser prestados a personas externas.

c) Los equipos portátiles de la Agencia y los que sean llevados por contratistas y/oterceros, deben contar con software antivirus, cifrado de datos, restricción en la ejecución de aplicaciones y protección física mediante la guaya de seguridad.

d) Los colaboradores y partes interesadas de la ANT, que requieran tener acceso a la información de la Agencia desde redes externas, se conectarán mediante un proceso de autenticación con uso de conexiones seguras cifradas (VPN) provistas y autorizadas por el EIST.

e) Las conexiones remotas a los recursos de la plataforma tecnológica serán restringidas y únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

f) El personal autorizado únicamente deberá establecer conexiones remotas en computadores previamente identificados y bajo ninguna circunstancia, en computadores públicos que no cumpla los controles de seguridad definidos porel EIST.

7 LINEAMIENTO SEGURIDAD DEL TALENTO HUMANO

Objetivo: Asegurar que funcionarios, contratistas y terceras partes a las que se les asignen responsabilidades contractuales comprendan sus responsabilidades y se pueda asegurar su idoneidad para la ejecución de las labores asignadas.

7.1 Seguridad en el ingreso del talento humano

El talento humano es el activo más importante con el que cuentan las Entidades y, por lo tanto, como el factor crítico de éxito que les facilita la gestión y el logro de susobjetivos y resultados. El talento humano, es decir, todas las personas que laboran en la administración pública, en el marco de los valores del servicio público, contribuyen con su trabajo, dedicación y esfuerzo al cumplimiento de la misión estatal, a garantizar los derechos a responder las demandas de los ciudadanos.

7.1.1 Selección

a) La Subdirección de Talento Humano de acuerdo con la política de gestión estratégica del talento humano del Modelo Integrado de Planeación y Gestión - MIPG desarrolla las actividades para la gestión del ciclo de vida del servidor público, en específico la identificación de los mecanismos para evaluar las competencias para los candidatos, cubrir vacantes temporales o de libre nombramiento y remoción.

b) La Subdirección de Talento Humano a través del procedimiento Selección de Talento Humano GTU-P-06, realiza las actividades de selección del personal que reúna los requisitos mínimos establecidos en el manual de funciones, con las competencias comportamentales y experiencia laboral acorde con las necesidades de la Entidad.

c) La Subdirección de Talento Humano verifica los soportes de los candidatos aplicando la guía para el nombramiento y toma de posesión, verificando información sobre: antecedentes judiciales, fiscales, disciplinarios y del ejercicio de la profesión, revisión de soportes de formación académica, experiencia laboral, habilidades y aptitudes para el desempeño de las funciones de acuerdo con los requisitos mínimos exigidos por el manual de funciones y competenciaslaborales de la Entidad.

7.1.2 Términos y condiciones del empleo

a) Los términos y condiciones de los empleos de los funcionarios de la ANT se describen en el manual de funciones y competencias laborales de la Entidad.

b) Los términos y condiciones de los contratos de los contratistas de la ANT, se gestionan a través del procedimiento CONTRATACIÓN DIRECTA, ADQBS-P- 006 y el procedimiento GESTIÓN CONTRACTUAL ADQBS-P-004, el cual contempla la verificación de los requisitos del formulario Hoja de vida del Sistemade Información y Gestión del Empleo Público – SIGEP , la Certificación sobre idoneidad y experiencia del contratista según sea el caso y la lista de verificación de requisitos para contratación diseñada por el proceso de ADQUISICIÓN DE BIENES Y SERVICIOS, ADQBS- Caracterización.

7.1.3 Sobre los derechos de autor de trabajos de funcionarios de la ANT

De conformidad con el artículo 91 de la ley 23 de 1982, sobre derechos de autor, "los derechos de autor sobre las obras creadas por empleados o funcionarios públicos, en cumplimiento de las obligaciones constitucionales y legales de su cargo, serán de propiedad de la Entidad pública correspondiente". Como lo establece el mismo artículo de la citada ley, "Se exceptúan de esta disposición las lecciones o conferencias de los profesores. Los derechos morales serán ejercidos por los autores, en cuanto su ejercicio no sea incompatible con los derechos y obligaciones de las Entidades públicas afectadas.

7.1.4 Sobre los derechos de autor de los trabajos de contratitas de la ANT

a) Los derechos patrimoniales de autor sobre las obras, informes, artículos, guiones o documentos que han sido creados o que creen los contratistas de la ANT en ejercicio de sus funciones o con

ocasión a ellas pertenecen a la ANT. Todo lo anterior sin perjuicio de los derechos morales de autor que permanecerán en cabeza del creador de la obra, de acuerdo con la ley 23 de 1982 y demás normas reglamentarias y complementarias con la materia.

b) Si con ocasión al cumplimiento de las funciones propias del contrato de trabajo se generó o se genera la creación de elementos susceptibles de ser objeto de propiedad intelectual y/o industrial, los resultados del trabajo de este forman parte de una obra colectiva cuya titularidad pertenece única y exclusivamente a la ANT. Por ello los contratistas deben ceder a la ANT expresamente en exclusiva y con facultad de cesión a terceros, los derechos de explotación en cualquier forma y en toda su extensión de los resultados de su trabajo, ya sean derechos de propiedad intelectual o industrial, incluyendo cualquier componente original del mismo, que desarrolle para la ANT y, en especial, cede los derechos de reproducción, distribución, trasformación, comunicación pública y cualesquiera otros derechos necesarios para el cumplimiento de las funciones misionales de la Entidad, incluido comercialización de todas sus labores.

7.1.5 Sobre la protección de la confidencialidad de la información

a) De conformidad con el Artículo 34, deberes, numeral 4, de la ley 734 de 2002, código único disciplinario, los funcionarios de la ANT deben “utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, la facultad que le sean atribuidas, o la información reservada a que tengan acceso por razón de su función, en forma exclusiva para los fines a que están afectos”,Subrayado fuera de texto.

b) De conformidad con el artículo 35, prohibiciones, numeral 21 de la ley 734 de 2002 código único disciplinario, los funcionarios de la ANT no deben “dar lugar al acceso o exhibir expedientes o archivos a personas no autorizadas”.

c) De conformidad con el numeral 6, del artículo 62 TERMINACIÓN SIN PREVIO AVISO, del código sustantivo del trabajo. Son justas causas para dar por terminado unilateralmente, el contrato de trabajo sin previo aviso: “6. El que el trabajador revele los secretos técnicos o comerciales o dé a conocer asuntos de carácter reservado, con perjuicio de la empresa;”.

7.1.6 Obligaciones sobre el uso de la información, servicios y plataformas informáticos

a) Como parte de sus obligaciones, los funcionarios, contratistas y terceras partes cuando aplique, suscriben un compromiso de cumplimiento de las políticas y lineamientos de seguridad de la información institucionales, confidencialidad y no divulgación de la información.

b) Dentro del alcance de sus competencias, la Subdirección de Talento Humano o el grupo interno

de trabajo coordinación para gestión contractual preservan la documentación de los soportes de los compromisos suscritos sobre cumplimiento de las políticas de seguridad, acuerdos de confidencialidad y no divulgación, cesión de derechos patrimoniales y demás documentación relacionada con los compromisos de funcionarios, contratistas o partes interesadas en materia de seguridad de la información y derechos de autor.

7.2 Seguridad durante el desarrollo del talento humano

7.2.1 Compromiso de la alta dirección

a) Como parte de su compromiso con la seguridad de la información, la alta dirección de la ANT exige a todos los funcionarios, contratistas y partes interesadas el cumplimiento de las políticas, lineamientos, procesos, procedimientos y controles de seguridad de la información institucionales. Este compromiso se evidencia a través de las actividades de inducción, reinducción, entrenamiento para funcionarios y el establecimiento de acuerdos de confidencialidad y compromiso de cumplimiento de las políticas y lineamientos de seguridad de la información para contratistas y demás partes interesadas dela ANT.

b) La alta dirección de la ANT coordina las actividades necesarias para garantizarlas actividades de capacitación, toma de conciencia y competencia del talento humano, los funcionarios y contratistas de la ANT:
   1. Conozcan la política de seguridad de la información y el sistema de gestión de seguridad de la información institucional.

   2. Identifiquen su contribución al logro de la eficacia del sistema de gestión de la seguridad de la información.

   3. Conozcan las implicaciones del incumplimiento de los requisitos del sistema de gestión de seguridad de la información institucional.

c) Todos los funcionarios contratistas y partes interesadas tienen acceso a la política de seguridad de la información, sus lineamientos y procedimientos a través de recursos como la Intranet, sitio web institucional, campañas de divulgación, procedimientos de inducción, reinducción y entrenamiento.

7.2.2 Toma de conciencia, educación y formación en seguridad de lainformación.

a) Como parte de la política de gestión estratégica del talento humano del MIPG, la ANT realiza

actividades de inducción, reinducción y entrenamiento específico para sus funcionarios. El proceso INDUCCIÓN, REINDUCCIÓN Y ENTRENAMIENTO ESPECÍFICO EN EL PUESTO DE TRABAJO, GTHU-P-017 permite el cumplimiento. Los funcionarios de la ANT deben participar en las actividades de inducción dentro de los cuatro (4) meses siguientes al ingreso del trabajador. La reinducción debe impartirse a todos los trabajadores de la Entidad por cambios estructurales en elquehacer de la Entidad o cada dos años en cumplimiento de las normas que regulan la materia.

b) Todos los funcionarios, contratistas y cuando sea pertinente las partes interesadas a la ANT deben participar en las actividades de toma de conciencia, educación y formación en materia de seguridad de la información que ejecuta la Subdirección de Sistemas de Información de Tierras, en coordinación con la Subdirección de Talento Humano.

c) Las actividades de toma de conciencia, educación, formación, diseñadas por la SSIT deben estar orientadas a que los funcionarios, contratistas, y en donde sea pertinente, las partes interesadas de a ANT, tomen conciencia de sus responsabilidades de seguridadde la información, y de los medios por los cuales se cumplen estas responsabilidades.

d) La SSIT diseña un programa anual de toma de conciencia en seguridad de la información, en línea Plan Institucional de Capacitación, desarrollado mediante el procedimiento FORMACIÓN Y CAPACITACIÓN, GTHU-P-001, del proceso de gestión de Talento Humano. El programa de capacitación tiene en cuenta las necesidades en materia de capacitación de los funcionarios, contratistas y partes interesadas.

7.2.3 Procesos disciplinarios por incumplimiento de las obligaciones enmateria de seguridad de la información

a) El incumplimiento de los requisitos del sistema de gestión de seguridad de la información de la ANT se gestiona a través del procedimiento de gestión de incidentes de seguridad de la información, cual es administrado por la SSIT. El proceso disciplinario sobre incumplimiento de obligaciones de seguridad de la información, no se debe iniciar sin antes verificar que ha ocurrido una violación a la seguridad de la información.

b) El incumplimiento de las obligaciones en materia de seguridad de la información por parte de funcionarios de la ANT se gestiona a través de los procedimientos: CONTROL INTERNO DISCIPLINARIO-PROCESO ORDINARIO, GTHU-P-016 y CONTROL INTERNO DISCIPLINARIO-PROCESO VERBAL, GTHU-P-018, que cumplen con lo definido en la Ley 734 de 2002 y la Ley 1474 de 2011.

c) El incumplimiento de las obligaciones en materia de seguridad de la información por parte de

contratistas se gestiona a través de acción contractual que de acuerdo con sus resultados puede conducir a procesos disciplinarios o penalesde acuerdo con la gravedad del incumplimiento.

7.3 Seguridad al terminar o cambiar funciones o empleo

a) La desvinculación de funcionarios de la ANT se realiza a través del procedimiento de desvinculación de personal, GTHU-P-009, que gestiona lo pertinente para formalizar el retiro de los servidores públicos de la Agencia Nacional de Tierras, según la situación o causal presentada y de acuerdo con lanormatividad vigente.

b) La desvinculación de contratistas de la ANT se realiza de acuerdo con los términos del contrato suscrito con el colaborador.

c) La SSIT debe notificar a los contratistas que terminen sus vínculos con la ANT, sobre la obligatoriedad de mantener los acuerdos de confidencialidad, cesión de derechos de autor y demás obligaciones en materia de seguridad de la información aplicables tras la finalización de sus contratos.

d) La Subdirección de Talento Humano o el Grupo Interno de Trabajo Coordinación para la Contratación, deben notificar en el ámbito de su competencia al EIST cuando se produzcan cambios de funciones, novedades como vacaciones, licencias, permisos o terminación de labores para realizar los ajustes pertinentes sobre el acceso a los activos de información, instalaciones de procesamiento de información o equipos informáticos sobre los cuales tuviera acceso el colaborador.

e) La Subdirección de Talento Humano o el Grupo Interno de Trabajo en coordinación para la contratación, deben notificar periódicamente el ámbito de su competencia a los demás procesos institucionales y cuando sea pertinente a las partes interesadas la finalización de los vínculos contractuales o laborales del personal de la ANT.

8 LINEAMIENTO SEGURIDAD DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Objetivo: Identificar los diferentes activos de información institucionales y establecer pautas para su apropiada protección. Asegurar que la información recibe un nivel apropiado de calificación y protección de acuerdo con los requisitos legales y contractuales. Establecer pautas para el uso seguro de medios de almacenamiento extraíbles.

8.1 Responsabilidad de los activos de información

8.1.1 Inventario de activos de información

a) En cumplimiento de los requisitos de la Ley 1712 de 2014, por medio de la cualse crea la Ley de transparencia y acceso la información pública y del derecho a la información pública, la ANT debe mantener los siguientes instrumentos de gestión de información pública de acuerdo con lo definido por el artículo 4 del decreto 103 de 2015: Registro de Activos de Información, el índice de Información Clasificada y Reservada y el Esquema Publicación de Información.

b) La SSIT es la responsable de liderar el levantamiento del inventario de activos de información de los diferentesprocesos institucionales.

c) Los responsables de procesos institucionales deben participar en el levantamiento, registro, clasificación y actualización de los activos deinformación institucionales.

d) El levantamiento de los activos de información institucionales se debe realizar de acuerdo con el instructivo de inventario de activos de información, del procesode Gestión de Información.

e) El inventario de activos de información de la ANT debe ser exacto, actualizado, consistente y alineado con otros inventarios institucionales como: tablas de retención documental, instrumentos de gestión pública de información, inventarios de infraestructura tecnológica e inventarios de activos fijos institucionales que sean formalizados mediante el comité institucional.

f) Dentro del inventario de activos de información institucionales se debe incluir lossiguientes tipos de activos:

1. Activos primarios: son activos de información indispensables para el cumplimiento de las funciones institucionales y que están directamenteasociados a la generación de información. Los activos de información primarios de la ANT incluyen: Los procesos de negocio y la información sin importar en que medio este contenida

2. Activos de soporte de los cuales dependen los elementos primarios, incluyen activos como: hardware, software, redes, personal, instalaciones físicas y estructura organizacional.

g) Para el caso de los sistemas de información institucionales, se considera como servicio el conjunto de activos de información que permite a los usuarios utilizar las funciones del sistema de información, en este caso, el responsable del servicio rinde cuentas por la prestación del servicio y debe gestionar el correctofuncionamiento de los activos de información que suportan el servicio con sus respectivos responsables.

8.1.2 Responsables de los activos de información

a) Todos los activos institucionales deben tener un responsable definido.

b) El responsable del activo puede ser un individuo o una Entidad que tenga la responsabilidad de gestión aprobada para controlar el ciclo de vida entero del activo de información. En la ANT los responsables de la información son los directores, subdirectores y jefes de dependencia; ellos son los responsables de la información que se genera, se gestiona y se utiliza en los diferentes procesos a su cargo y deben ser conscientes de los riesgos asociados de tal forma que sea posible tomar acciones para mitigarlos.

c) El responsable del activo debe ser responsable de su gestión apropiada durante todo su ciclo de vida, es decir, desde su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

d) El responsable debe verificar periódicamente la confidencialidad, integridad, disponibilidad y coherencia de la información producto de los procesos de su área.

e) El responsable del activo debe:

1. Asegurarse de que los activos están inventariados.

2. Asegurarse de que los activos están clasificados de acuerdo con los procedimientos institucionales y protegidos apropiadamente de acuerdo con los lineamientos, políticas, procedimientos y controles de seguridad establecidos por la ANT.

3. Definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.

4. Determinar los criterios y niveles de acceso a la información de acuerdo con las tablas de control de acceso adoptadas por la Entidad.

5. Determinar los requerimientos de copias de respaldo para la información bajo su responsabilidad.

6. Asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

f) El responsable del activo de información es único, sin embargo, puede delegar a otras personas como custodios del activo de información. Los custodios de los activos de información son responsables de velar por que los controles de seguridad de la información definidos sobre el

activo se cumplan de acuerdo conlo establecido por el responsable del activo.

g) Los activos de información son responsabilidad de los líderes de los procesos institucionales.
Los activos de información tipo hardware, software y redes, son definidos por la Mesa Técnica de TI y el EIST.
Los activos de información tipo personas son responsabilidad de Subdirección de Talento Humano, los activos de información tipo procesos y estructura organizacional son responsabilidad de la Oficina de Planeación.

8.1.3 Custodios de la información

El custodio de la información puede ser un cargo, proceso, o grupo de trabajo encargado de administrar y de hacer efectivos los controles técnicos de seguridad de la información que el responsable de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Los custodios de la información tienen la responsabilidad de garantizar la disponibilidad, la integridad y la confidencialidad de la información.

Los custodios de los activos de información son responsables de:

a) Administrar los accesos de red incluyendo sistema operativo y acceso al dominiode la Agencia.

b) Administrar los accesos a manejadores de bases de datos.

c) Administrar los accesos a archivos físicos e información almacenada en mediosmagnéticos.

d) Implementar controles definidos para los sistemas de información incluyendo actualizaciones de seguridad en los sistemas (parches, service packs, fixes, etc.).

e) Desarrollar procedimientos de autorización y autenticación.

f) Administrar los documentos de licenciamiento y medios magnéticos del softwareadquirido por la Entidad.

g) Asistir y administrar los procesos de copia de seguridad, de recuperación y del plan de continuidad de negocio y sistemas de información.

h) Proveer los métodos de cifrado de la información, así como administrar el software o

herramienta utilizado para tal fin.

i) Efectuar la eliminación segura de la información física, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dadosde baja o cambian de usuario.

j) Utilizar los medios adecuados para destruir o desechar correctamente la documentación física, con el fin de evitar su reconstrucción una vez cumplido suciclo de almacenamiento.

k) Monitorear el cumplimiento de la política y lineamientos de seguridad en los activos de información que custodia.

8.2 Uso aceptable de los activos de información

a) Los diferentes activos de información institucionales solo deben ser utilizados para las tareas afectas a los servicios que presta la Entidad.

b) Las tareas de rutina sobre el uso de los activos de información pueden ser delegadas a un custodio o un usuario del activo de información, pero la rendiciónde cuentas sobre la seguridad de la información del activo sigue siendo del responsable del activo de información.

c) Los usos autorizados para los activos de información institucionales deben cumplir con las políticas técnicas de seguridad de la información aprobadas porla ANT.

8.3 Usuarios de los activos de información

El usuario de la información es cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Entidad.

Los usuarios de los activos de información son responsables de:

a) Conocer y aplicar los lineamientos y políticas de seguridad de la información dela Agencia.

b) Mantener la confidencialidad, integridad y disponibilidad de los activos de información a los cuales se les ha otorgado acceso.

c) Reportar amenazas y violaciones de la seguridad de la información mediante losmecanismos que defina la Mesa Técnica de TI de la ANT.

d) Asegurarse de ingresar información adecuada y de calidad a los sistemas de información según el rol desempeñado.

e) Utilizar la información de la Agencia únicamente para los propósitosinstitucionales autorizados.

f) Apoyar el proceso de eliminación adecuada de la información una vez cumplidosu periodo de almacenamiento definido, aplicando los procedimientos definidospor la Entidad.

8.4 Devolución de activos de información al finalizar la relación contractual

a) Al finalizar la relación contractual, de prestación de servicios o cambios de funciones definitivos, el responsable del activo debe coordinar las actividades dedevolución de todos los activos físicos, electrónicos y de información entregados previamente al custodio, y que sean propiedad de la Entidad o que se le han confiado a ella, incluida propiedad de clientes externos.

b) En los casos en que el colaborador o parte externa haga uso de sus propios equipos para el tratamiento de información institucional, se debería evaluar la conveniencia de seguir procedimientos para asegurar que toda la información institucional transferida a esos equipos sea borrada del equipo en forma segura.

c) En casos en que un colaborador posea conocimientos que son vitales y esenciales para el cumplimiento de las funciones misionales, esa información sedebería documentar y transferir a la Entidad mediante informes o reportes de actividades.

d) Los responsables de activos de información tipo información deben verificar periódicamente la calidad de la información desde su origen y velar porque éstase mantenga a lo largo del ciclo de vida de información en la Agencia.

e) Debe garantizar que la información y los activos asociados con los servicios deprocesamiento de información se clasifican adecuadamente.

8.5 Clasificación de la información

a) Los responsables de los diferentes activos de información son responsables de la adecuada clasificación de la información de los activos a su cargo.

b) Los activos de información institucionales se deben calificar de acuerdo con lo definido en el instructivo de calificación y etiquetado de información del procesode gestión de información y los

lineamientos para la gestión y calificación de activos de información del mismo proceso.

c) De acuerdo con el nivel de clasificación de la información contenida en el activo de información (Información pública reservada, Información pública clasificada, Información privada o Información de datos abiertos) y los resultados de la gestión de riesgos de seguridad de la información, el responsable del activo de información en coordinación con la Mesa Técnica de TI, establecerán los controles de seguridad que se deben aplicar al activo para preservar su confidencialidad, integridad y disponibilidad.

9 LINEAMIENTO DE CONTROL DE ACCESO A LA INFORMACIÓN

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información solamente los debidamente autorizados y bajo condiciones controladas que garanticen la confidencialidad, integridad y disponibilidad de la información.

9.1 Acceso a los activos de información

a) Las decisiones sobre el control de acceso a la información gestionada por los procesos de la ANT deben ser documentadas en la Tabla de Control de Acceso, según lo establecido por el Decreto 2609 de 2017, Art. 8 compilado en el actual Decreto 1080 de 2015, Artículo 2.8.2.5.8. Instrumentos archivísticos para la gestión documental. i) Tablas de Control de Acceso para el establecimiento categorías adecuadas de derechos y restricciones de acceso y seguridad aplicables a los documentos.

b) El control de acceso a la información debe cumplir con los requisitos de la ley 1712 de 2014, por la cual se crea la ley de transparencia y acceso a la información pública.

c) El acceso a los activos de información e instalaciones de procesamiento de información de la ANT debe cumplir con la política de control de acceso a la información definida por la Entidad.

d) Los responsables de los activos de información deben determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a sus activos, con la cantidad de detalle y severidad de los controles, que reflejen los riesgos de seguridad de la información asociados.

e) La asignación de roles o permisos de acceso privilegiado o administrador de activo de información se debe realizar únicamente si las labores designadas asílo requieren.

f) Al establecer reglas para control de acceso, el responsable del activo debe verificar la posibilidad

de aplicar los siguientes lineamientos:

1. Solamente se concede acceso a la información que la persona necesita parala realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).

2. Solamente se les concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

g) El Grupo Interno de Trabajo Gestión Documental es el responsable de administrar las Tablas de Control de Acceso a la información institucional.

h) La SSIT y la SG son las áreas responsables de implementar los controles tecnológicos necesarios para dar cumplimiento a los requisitos de control de acceso definidos por los responsables de la información institucional.

i) Los controles de acceso físico a los activos de información deben ser gestionados por el responsable del activo de información ante el responsable delproceso al que pertenece el activo.

9.2 Acceso a las redes de datos y servicios de redes de datos

a) Solo se permite el acceso de los usuarios a las redes y los servicios de red de laEntidad cuando han sido formalmente autorizados.

b) El acceso a redes públicas abiertas de la Entidad para acceso al ciudadano se debe gestionar con controles de seguridad que prevengan incidentes de seguridad de la información sobre la infraestructura de servicios institucionales. La SSIT es la responsable de definir los controles y condiciones para el uso de dichas redes públicas.

c) El acceso a las redes y servicios de red institucionales se debe realizar cumpliendo las políticas técnicas de seguridad de la información institucionales.

d) Todos los funcionarios, contratistas y partes interesadas deben seguir el procedimiento de administración y gestión de cuentas de usuario para solicitar acceso a las redes y servicios de red, lo anterior definido por el área de soportetecnológico.

e) La navegación por Internet y sus niveles (Deepweb o DarkNet) se autoriza a los usuarios únicamente si es indispensable para el cumplimiento de las funciones que se les asigna. Las

redes y servicios de red a los que un funcionario, contratista o parte interesada, puede tener acceso dependen de las funciones que se le asignen y de las autorizaciones otorgadas por el responsable del proceso para el cual desempeñe las funciones el colaborador.

f) La SSIT es la responsable de determinar e implementar los controles de acceso a las redes, servicios de red y servicios de navegación en la Internet para la ANT.

9.3 Acceso de los usuarios a los activos de información

9.3.1 Identificadores de cuenta de usuario

a) El acceso a los activos de información institucionales debe contemplar laasignación de cuenta de usuario con roles y privilegios conformes con las labores asignadas al funcionario, contratista o parte interesada.

b) La asignación de la cuenta de usuario para acceso a los servicios, sistemas de información y activos de información de la ANT se debe realizar mediante el procedimiento de administración y gestión de cuentas de usuario que es administrado por el EIST de la SG.

c) Las cuentas de usuario deben cumplir con requisitos mínimos de seguridad incluyendo:

1. Ser únicas, personales e intransferibles.
2. El uso de cuentas compartidas debe ser autorizado y documentado formalmente por la Mesa Técnica de TI y el EIST.
3. Las cuentas de usuario deben ser deshabilitadas al finalizar el vínculo laboralo contractual del colaborador con la Entidad.
4. No se deben reasignar cuentas que hayan sido deshabilitadas.
5. Semestralmente se debe ordenar el retiro o suspensión de cuentas de usuario redundantes o innecesarias de acuerdo con los requisitos de los líderes funcionales.

9.3.2 La asignación de privilegios de acceso sobre servicios, sistemas deinformación

Cuando se requiera asignar o recovar permisos a los usuarios se deben contemplarlos siguientes lineamientos:

a) El usuario o parte interesada debe obtener la autorización de uso o acceso por parte del responsable del sistema de información, aplicación o activo de información en el que está

interesado.

b) El responsable del activo de información o sistema de información debe verificar que la autorización de acceso o privilegios que se desean otorgar sea la mínima necesaria para el cumplimiento de las labores asignadas, no se deben asignar más privilegios de los necesarios sobre un sistema o activo de información.

c) No se deben activar derechos de acceso sobre el activo o sistema de información hasta que no se hayan completado todas las actividades del procedimiento de administración y gestión de cuentas de usuario definidos por el área de soporte tecnológico de la SG.

d) La Mesa Técnica de TI debe mantener el registro de las autorizaciones de acceso y privilegios otorgados a los diferentes usuarios de activos o sistemas de información.

e) Semestralmente la Mesa Técnica de TI debe gestionar la revisión de privilegios de acceso otorgados sobre los diferentes activos o sistemas de información.

9.3.3 Asignación de privilegios de administrador

a) El acceso a privilegios de nivel administrador sobre las aplicaciones debe ser autorizado formalmente por la Mesa Técnica de TI y el de infraestructura por el EIST.

b) La asignación de privilegios de nivel administrador debe obedecer a una necesidad real y demostrada sobre la base de funciones misionales o de apoyo.

c) Se debe considerar la posibilidad de que los privilegios de acceso a nivel de administrador tengan una fecha de expiración después de la cual sea necesario reactivarlos mediante el procedimiento de administración y gestión de cuentas de usuario.

d) Los usuarios con nivel de autorización de administración deben tener cuentas diferentes para sus labores rutinarias, no se debe usar cuentas de nivel “administrador” para labores regulares que no requieren privilegio de administrador.

e) Los sistemas de información deben establecer y mantener procedimientos genéricos preconfigurados y controlados que reduzcan la necesidad de otorgardiversas cuentas de usuario con privilegio de administrador.

f) Cuando se autorice el uso de credenciales compartidas para labores de administración se debe mantener estricta confidencialidad de las claves de acceso, rotación frecuente de contraseña y notificación inmediata a todo el grupode usuarios administradores cuando un miembro de grupo

cesa sus funciones, se retira de la Entidad o se le revoca el privilegio de administración.

9.3.4 Administración de claves y mecanismos de autenticación

a) Las contraseñas son mecanismos de seguridad que permiten autenticar a los usuarios de las diferentes cuentas de acceso a sistemas de información y aplicaciones.

b) Las contraseñas deben cumplir con políticas de seguridad que obliguen al uso de un número de caracteres que impidan que sean adivinadas fácilmente por software o técnicas de ingeniería social. Las contraseñas deben incluir el uso de caracteres alfabéticos, numéricos, símbolos especiales o signos de puntación de acuerdo con las directrices que imparta la Mesa Técnica de TI y el ESIT de la ANT.

c) Los usuarios deben cambiar periódicamente sus contraseñas de acuerdo con las directrices que imparta el EIST de la SG.

d) Las contraseñas son información calificada como clasificada de acuerdo con la Ley 1712 de 2014, por lo que:

1. Las contraseñas no deben ser divulgadas a personal no autorizado.

2. Si existe sospecha de que la contraseña ha sido comprometida se deben cambiar sin demoras injustificadas.

3. Para equipos con la posibilidad de asignación de contraseñas, el EIST debe gestionar las claves de Administración de equipos y dispositivos de uso compartido como equipos de impresión, máquinas de copiado, y demás.

4. Las contraseñas no deben ser enviadas por sistemas inseguros como correos sin cifrar o medios impresos.

5. Las contraseñas no deben ser almacenadas en repositorios inseguros o no cifrados.

e) La asignación de las contraseñas o mecanismos de autenticación para las cuentas de usuario se debe realizar siguiendo el procedimiento de administración y gestión de cuentas de usuario.

f) Los usuarios deben firmar en su acuerdo de confidencialidad donde se comprometan de no divulgar las contraseñas o mecanismos de autenticación que se les asignen.

g) Antes de proporcionar las contraseñas o mecanismos de autenticación a un usuario se debe

verificar su identidad mediante comprobación con el responsable del activo, mediante comunicación formal o mediante documento de identidad.

h) Cuando sea posible, los usuarios deben recibir una claveo mecanismo de autenticación inicial que deben cambiar en su primer acceso alactivo o sistema de información.

i) La entrega de clave o mecanismo de autenticación inicial se debe suministrar de manera segura al usuario, se debe evitar el envió de los mismos con terceras partes, correos o mensajes no seguros (no cifrados).

j) La clave o mecanismo de autenticación inicial debe ser única para cada individuo y no deben ser fácil de adivinar.

k) Los usuarios deben realizar el acuso de recibo clave, contraseña o mecanismo de autenticación inicial.

l) Cualquier contraseña o mecanismo de autenticación inicial configurado por el proveedor de un equipo, activo o sistema de información deben ser cambiado al momento de instalar el equipo.

9.3.5 Retiro de derechos de acceso

a) Los derechos de acceso se deben suspender o revocar cuando cesan las funciones o finaliza el vínculo del colaborador o parte interesada con la ANT.

b) Los cambios de labores deben reflejarse en la asignación de privilegios de acceso.

c) Los derechos de acceso físico y lógico se deben revocar o suspender al finalizar la relación o vínculo con la Entidad.

d) Los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información se deberían reducir o retirar antes de que el vínculo o relación con la Entidad termine o cambie, dependiendode la evaluación de factores de riesgo tales como:

1. Si la terminación o cambio lo inicia el colaborador, el usuario de la parte externa o la Entidad, y la razón de la terminación.

2. Las responsabilidades actuales del colaborador, el usuario de la parte externa o cualquier otro usuario.

3. El valor o criticidad de los activos a los que tiene acceso el colaborador ousuario de parte externa.

e) La revocación o suspensión de acceso a usuarios se debe comunicar al grupo de trabajo del colaborador cuando finaliza su vínculo con la Entidad o cambian sus funciones.

9.3.6 Responsabilidades de los usuarios

a) Todos los usuarios son responsables de mantener en estricta confidencialidad la información de autenticación que se les asigna.

b) Los usuarios deben aplicar todas las medidas de seguridad a su alcance para proteger la información de autenticación secreta que les ha asignado, incluyendo, pero sin limitarse a:

1. Memorizar y no escribir las contraseñas que les han asigando.
2. Cambiar las contraseñas de acuerdo con la política definida por la ANT.
3. Usar claves fáciles de recordar, pero difíciles de adivinar.
4. Evitar el uso de información personal para crear claves o contraseñas.
5. No usar palabras de diccionarios de ningún idioma para crear claves ocontraseñas.
6. Combinar números, letras y caracteres especiales en cantidad suficiente para evitar ataques de software de adivinación de contraseñas.
7. No compartir las claves o contraseñas.

9.3.7 Control de acceso a sistemas de información

a) Los sistemas de información y aplicaciones deben implementar mecanismos decontrol de acceso que limiten el acceso a sus funciones de acuerdo con los rolesy responsabilidades asignados a los usuarios de estos.

b) El acceso a las funciones de los sistemas de información y aplicaciones debe ser implementado a través de menús que restrinjan las funciones a las que puede tener un determinado usuario.

c) Los mensajes de salida de los sistemas de información deben desplegar únicamente la información necesaria y relevante para el cumplimiento de las labores de los usuarios, se debe

evitar el despliegue de información que pueda representar riesgos para confidencialidad, integridad o disponibilidad delsistema.

d) Se deben implementar tanto controles de acceso lógico como físico a las aplicaciones y equipos terminales desde los que se accede a sus funciones.

e) Los sistemas de información y aplicaciones deben tener implementados mecanismos de autenticación o verificación de la identidad de los usuarios que acceden a sus funciones: Autenticación, Autorización, Rendición de cuentas.

f) Para los sistemas de información críticos o altamente sensibles se debe considerar la posibilidad de adoptar esquemas de verificación de identidad y autorización fuertes como uso de biometría, firma electrónica o tokens de seguridad.

g) Todos los sistemas de información deben desplegar la advertencia a los usuariosacerca de que el uso del sistema se debe realizar solo para el cumplimiento de las funciones asignadas, que las acciones ejecutadas pueden ser registradas para procesos de seguimiento y control y que el usuario acepta las políticas de seguridad digital de la ANT cuando ingresa al sistema o aplicación.

h) Se debe validar la información de ingreso del usuario solamente al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta.

i) Todos los sistemas deben implementar restricción de acceso o bloqueo de cuenta de usuario cuando el número de intentos fallidos de autenticación sea superior a tres (3).

j) Los sistemas de información o aplicaciones deben mantener un registro (bitácora) de los intentos de ingreso tanto exitosos como fallidos.

k) Los sistemas de información deberían cerrar las sesiones que presentan inactividad del usuario después de 30 minutos.

l) Se debe preferir el esquema de autenticación de usuarios centralizado en lugarde autenticación gestionada por la misma aplicación o sistema de información.

m) Para los sistemas de conexión que gestionen información sensible o reservada, se debe considerar la posibilidad de que los sistemas de información o aplicaciones limiten el tiempo máximo de conexión de un usuario para impedir sesiones de tiempo ilimitado.

n) Los sistemas de información o aplicaciones no deben transmitir claves en texto claro por las redes de comunicaciones.

9.3.8 Uso de programas utilitarios privilegiados

a) Los programas utilitarios privilegiados con software que puede tener la capacidad de evadir los controles de seguridad de los sistemas operativos, aplicaciones, sistemas de información o activos de información institucionales. El uso de programas utilitarios privilegiados debe estar restringido al personal que autorice la Mesa Técnica de TI y el EIST de la ANT.

b) La instalación y habilitación de los programas utilitarios privilegiados está a cargodel EIST.

c) Para el adecuado control de uso de los programas utilitarios privilegiados el EIST debe:

1. Mantener un registro de los usuarios a los que se les autoriza el uso de dichosprogramas, así como las tareas para las cuales se les autorizó su uso.

2. Deshabilitar de las estaciones de trabajo de usuario final cualquier programautilitario que no haya sido autorizado por la Mesa Técnica de TI o el EIST de la ANT.

3. Controlar y limitar el uso de los programas utilitarios privilegiados solamente a las tareas indispensables, únicamente durante el tiempo necesario para la ejecución de la tarea delegada y solo al personal al cual se le autoriza expresamente el uso de dichos programas.

9.3.9 Control de acceso al código de fuente

a) El acceso a los códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de pruebas), debe estar restringido únicamente al personal autorizado por Mesa Técnica de TI o EIST de la ANT con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios no intencionales y mantener la confidencialidad de propiedad intelectual de la ANT.

b) El control de las versiones de código fuente de las aplicaciones y sistemas de información se debe realizar cumpliendo la política general de sistemas de información y los documentos asociados a esta.

c) Los cambios sobre el código fuente de aplicaciones y sistemas de información se deben gestionar a través de los procedimientos definidos para la gestión de cambios y de acuerdo con las directrices de la Mesa Técnica de TI.

d) La gestión y acceso a los códigos fuente de los sistemas de información solo debe estar disponible a los administradores y desarrolladores de cada sistema de información.

10 LINEAMIENTOS SOBRE USO DE CONTROLES DE CRIPTOGRAFÍA

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger laconfidencialidad, la autenticidad y/o la integridad de la información.

10.1 Política de uso de controles criptográficos

a) La implementación de controles criptográficos en los sistemas de información y repositorios de almacenamiento de información debe cumplir la política institucional de controles criptográficos.

b) El uso de controles criptográficos debe estar orientado primordialmente a la preservación de la confidencialidad de la información pública clasificada y pública reservada.

c) La selección de los tipos de algoritmos y soluciones de controles criptográficos debe considerar los resultados del análisis de riesgos de seguridad asociados ala pérdida de confidencialidad, las capacidades tecnológicas de la plataforma sobre la que se implementará el control y el nivel de calificación de la informacióna ser protegida (pública clasificada y pública reservada).

d) El uso de criptografía en medios de almacenamiento extraíble y/o dispositivos móviles debe ser aprobado por la Mesa Técnica de TI y/o el EIST respectivamente.

e) Los procedimientos de control de las llaves criptográficas aplican desde la generación, almacenamiento, inclusión en archivos permanentes, recuperación, distribución, retiro y destrucción de las llaves son responsabilidad de EIST.

f) El uso de sistemas de llaves criptográficas debe cumplir con las normas que rigen el uso de mensajes de datos y su validez legal en el territorio colombiano.

g) Como mecanismo de seguridad sobre la vida útil de las llaves criptográficas, el EIST, definelas fechas de activación y desactivación de las llaves, de manera que solo puedan usarse durante un periodo de tiempo definido.

11 LINEAMIENTOS SOBRE SEGURIDAD FÍSICA Y AMBIENTAL

11.1 Gestión de áreas seguras

a) Las áreas de procesamiento y almacenamiento de información se consideran áreas seguras y deben tener definido un perímetro de control de acceso que impida su acceso a personal no autorizado.

b) Las áreas que contengan activos de soporte de servicios esenciales: agua, energía, telecomunicaciones, se consideran áreas seguras y deben tener definido un perímetro de control de ingreso que impida su acceso a personal no autorizado.

c) Las áreas de procesamiento, almacenamiento de información o soporte de servicios esenciales, deben tener protecciones físicas solidas en techos, pisos y paredes que protejan adecuadamente contra acceso no autorizado.

d) Los centros de procesamiento de información deben contar con controles de acceso físico como puertas, sistemas de alarma, video vigilancia, control de variables ambientales que permitan monitorizar permanentemente las condiciones de seguridad del área.

e) Las áreas seguras deben permanecer cerradas tanto en puertas o ventanas cuando no estén supervisadas.

f) Las áreas de procesamiento y almacenamiento de información (electrónica o física) deben contemplar el uso de sistemas de detección y control de incendios(autónomos o manuales).

g) Anualmente se debe verificar el correcto funcionamiento de los controles de video vigilancia, detección y control de incendios, acceso físico, identificación de visitantes y colaboradores (sistemas biométricos, tarjetas de proximidad, sistemas de registro de visitantes).

11.2 Gestión de ingreso a las instalaciones de la ANT

a) El ingreso a las instalaciones de la Entidad debe ser gestionado a través de su área de recepción de las sedes de la ANT, considerando:

1. Los visitantes deben ser identificados, anunciados y autorizados por un colaborador de la ANT antes de permitir su ingreso a las instalaciones de la Entidad.

2. Los colaboradores de la Entidad deben identificarse en la recepción de las instalaciones de la ANT con los mecanismos de control adoptados por la Entidad: sistemas biométricos, carné digital, tarjetas de proximidad o identificación presencial ante el personal de vigilancia de las instalaciones.

3. La salida de las instalaciones de la Entidad se debe realizar por las áreas derecepción de las diferentes sedes, salvo situaciones de emergencia, fuerza mayor o caso fortuito que son gestionadas por el plan de gestión de emergencias institucional.

4. Se deben mantener un registro de fecha y hora de ingreso a las instalacionesde visitantes.

5. Durante su permanencia en las instalaciones de la ANT, los visitantes debenportar en lugar visible el distintivo de identificación suministrado por el personal de recepción de las diferentes sedes de la Entidad.

6. El acceso a las áreas de procesamiento y/o almacenamiento de información por parte de visitantes, debe ser autorizado por el responsable del área o delproceso.

7. Los visitantes autorizados para ingresar a las áreas de procesamiento y/o almacenamiento de información, deben permanecer acompañados de un colaborador de la ANT durante su visita.

8. Se debe mantener un registro de ingreso a las áreas de procesamiento y/o almacenamiento de información por parte de visitantes, incluyendo fecha, hora, propósito de la visita, persona que autorizó el ingreso, colaborador queacompañó la visita, así como fecha y hora de salida del área segura.

9. Los colaboradores de la ANT deben reportar sin demoras injustificadas la presencia de personal sospechoso en las instalaciones de la ANT, ante la compañía de vigilancia.

10. El personal con autorización de ingreso permanente a las áreas seguras debe estar plenamente identificado y se deben verificar los permisos de ingreso a las áreas seguras trimestralmente.

11.3 Seguridad en oficinas y recintos

a) Las áreas seguras deben estar ubicadas de forma que se impida su fácil accesoa personal no autorizado.

b) En la medida de lo posible no se deben identificar con marcas evidentes las áreas clave de procesamiento o almacenamiento de información.

c) No se deben modificar los controles se seguridad de oficinas, recintos y centros de procesamiento o almacenamiento de información: sistemas de detección y control de incendios, sistemas de control de ingreso, sistemas de video vigilancia, barreas físicas de control de

acceso.

d) Solo el personal debidamente autorizado debería conocer la ubicación y controles de seguridad de las áreas seguras y las áreas clave de procesamientoo almacenamiento de información.

e) El uso de equipo de filmación o fotográfico en áreas seguras debe ser autorizado por el EIST de SG y el autorizado debe suscribir acuerdo de confidencialidad cuando así lo determine el EIST de la ANT. Informar y solicitar autorización al titular sobre el tratamiento de datos personales.

f) Los puntos de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, deben permanecer vigilados. En los casos en que sea viable, se deben aislar las áreas de despacho y carga de las instalaciones de procesamiento de información.

g) Todo material que ingrese a las instalaciones de la ANT se debe inspeccionar y examinar para determinar la presencia de explosivos, químicos u otros materiales peligrosos.

h) Todo material que ingrese por las áreas de despacho y carga se debe registrar de acuerdo con los procedimientos de gestión de activos de la ANT.

i) Todo material entrante se debe inspeccionar para determinar evidencia de manipulación durante el transporte. Si se descubre esta manipulación, se debe reportar de inmediato al personal de seguridad de la sede de la ANT.

11.4 Seguridad de los equipos

a) Los equipos de cómputo y equipos de soporte de servicios esenciales (energía, aire acondicionado, video vigilancia, control ambiental, etc.,) deben estar ubicados de forma segura para evitar accesos no autorizados o innecesarios, caídas, impactos, daños por agentes ambientales (agua, polvo, humedad, otros).

b) Solo se debe permitir el acceso a los equipos de procesamiento y/o almacenamiento de información a personal autorizado.

c) Los equipos y activos de información deben ser ubicados y de ser necesario asegurados físicamente para impedir substracción o daño.

d) No se debe permitir el consumo de alimentos, bebidas y bajo ningún caso fumar dentro de las instalaciones de procesamiento de información durante la jornada laboral y en horarios extra.

e) Todos los equipos de procesamiento y/o almacenamiento de información deben contar y

mantener activas la protección eléctrica regulada y polo a tierra para prevenir descarga eléctrica atmosférica o corto circuito.

f) Los servicios de suministro (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) debe cumplir con los requisitos normativos o las recomendaciones de los proveedoreso fabricantes.

g) Anualmente se debe verificar si la capacidad de los servicios de suministro (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) es la adecuada de acuerdo con el consumo, ampliaciones de capacidad o crecimiento en el número de equiposde procesamiento y/o almacenamiento de información.

h) Los cables de potencia y telecomunicaciones deben ser instalados de forma que se impida interferencia, interceptación o daños a los mismos.

i) Los cables de potencia y los cables de telecomunicaciones deben estar separados por barreras que prevengan la interferencia de señales.

11.5 Mantenimiento de equipos

a) Se debe realizar el mantenimiento de los equipos de procesamiento y/o almacenamiento y servicios de soporte y suministro de acuerdo con los intervalos y esquemas recomendados por el proveedor o fabricante.

b) El mantenimiento y/o reparación de los equipos debe ser realizado únicamente por personal autorizado.

c) Se debe llevar un registro de los mantenimientos y/o reparaciones realizadas alos equipos.

d) Se debe llevar un registro de todas las fallas reales o potenciales de los diferentes equipos.

e) Se deben aplicar controles que prevengan la divulgación de información cuando se realice mantenimiento de equipos con información pública clasificada o pública reservada por parte de personal externo o cuando el mantenimiento/reparación se realice fuera de las instalaciones de la ANT.

f) Después de completar un mantenimiento o reparación de un equipo de procesamiento y/o almacenamiento de información se deben realizar pruebas para certificar su correcto

funcionamiento antes de ponerlo en producción.

11.6 Retiro de equipos de las instalaciones de la ANT

a) El retiro de equipos de cómputo y elementos se debe realizar de acuerdo con los protocolos y procedimientos definidos por la SG, registrando los datos del retiro en el formato ADMBS-F-032 FORMA SALIDA INDIVIDUAL DE ELEMENTOS V4.

1. En el caso de equipos de cómputo la autorización de salida debe ser suscrita por el líder del EIST.
2. Para el retiro de las instalaciones de la ANT de elementos diferentes a equipos de cómputo o tecnológicos, la salida debe ser suscrita por la Subdirección Administrativa y Financiera.
3. En el caso de expedientes, documentos o archivo físico, la autorización de salida debe ser suscrita por el líder de Gestión Documental.

b) El ingreso y salida de equipos de propiedad personal debe ser registrado en la bitácora de la recepción de la sede de la ANT que se visita.

c) Las bitácoras de registro de equipos se deben inspeccionar periódicamente por parte de la empresa de vigilancia, para verificar su correcto diligenciamiento.

d) Al retirar equipos de propiedad de la ANT el colaborador autorizado debe aplicarlos protocolos de seguridad que establezca la SG, incluyendo:

1. Cuando se autorice el retiro de equipos de propiedad de la Entidad se debería registrar el tiempo que se autoriza la salida del equipo. La fecha de salida y la fecha en que el equipo volvió a las instalaciones de la Entidad.

2. Al retornar el equipo a las instalaciones se debería registrar las actividades que se ejecutaron con el equipo, y las personas que realizaron trabajos o manejaron el equipo.

3. Los equipos propiedad de la ANT no deberían ser retirados sin seguros que cubran hurto o daño parcial o total.

4. Nunca se deben dejar desatendidos los equipos de la ANT cuando están fuera de las instalaciones de la Entidad.

5. Al salir de las instalaciones de la Entidad, los equipos deben ser transportados en condiciones que eviten impactos que los puedan dañar, igualmente se debe prevenir que queden expuestos a agentes ambientales extremos como: sol directo, extremo calor, agua,

tierra, agentes químicos, exposición a campos magnéticos fuertes o radiación que pueda alterar sus componentes de almacenamiento.

6. En los casos en los que el equipo contenga información pública clasificada o pública reservada y deba ser manipulado por múltiples personas se debería llevar un registro de quién, cuándo y con qué fin tuvo acceso al equipo.

7. En lugares de trabajo externos a las instalaciones de la ANT, los computadores portátiles deben permanecer asegurados con guayas de seguridad a anclajes fijos.

8. No se deben colocar el portátil o dispositivo móvil sobre el piso o en lugares no visibles. Siempre se debe mantener a la vista.

11.7 Disposición segura o reutilización de equipos

Antes dar de baja o realizar la disposición final de equipos o medios de almacenamiento se debe verificar que no contengan información institucional o licencias de software. En caso de que el equipo o el medio de almacenamiento contenga información pública reservada, pública clasificada o licencias de softwarepropiedad de la ANT, se debe realizar un proceso de borrado seguro de dichos datos.

Los medios de almacenamiento que contengan información pública clasificada o pública reservada que se deban dar de baja deben ser destruidos o inutilizados cumpliendo los procedimientos de disposición de residuos electrónicos para evitar daños al medio ambiente.

Cuando se decida transferir o reasignar medios de almacenamiento como discos duros a terceras partes, se debe realizar borrado seguro de la información institucional contenida en el medio.

11.8 Equipos de usuario desatendido.

Una vez finalizan sus labores, todos los colaboradores de la ANT deben cerrar su sesión de trabajo y apagar sus computadores. En caso de ausencia temporal del puesto de trabajo, todos los colaboradores deben bloquear su sesión o apagar su equipo si la ausencia es prolongada.

La ANT debe implementar los mecanismos o política de cierre de sesión, cuando el equipo se encuentra inactivo por un lapso de tiempo de más de 5 minutos.

No se deben dejar medios de almacenamiento extraíbles desatendidos en las estaciones de trabajo.

La información impresa pública clasificada o pública reservada, debe almacenarse en lugar seguro cuando no se encuentre en uso, de igual manera los medios de almacenamiento externos y dispositivos electrónicos de autenticación como tokens, deben almacenarse en lugar seguro cuando no estén en uso y al finalizar la jornada laboral.

Al terminar la jornada laboral los puestos de trabajo y escritorios deben quedar libres de cualquier tipo de información pública clasificada o pública reservada y la misma se debe almacenar en lugar seguro.

Los equipos que no se encuentren en uso deben permanecer bloqueados para evitar accesos no autorizados: los computadores con bloqueo de sesión, los equipos de copiado con bloqueo de menú, las impresoras con bloqueo de la sesión deadministrador.

Los documentos impresos con información pública clasificada o pública reservada deben ser retirados una vez impresos.

12 LINEAMIENTO DE SEGURIDAD EN LAS OPERACIONES TECNOLÓGICAS

12.1 Procedimientos de operación tecnológica

a) El Equipo de Infraestructura y Soporte Tecnológico de la SG de la ANT es el responsable de diseñar, implementar, mantener y mejorar los procedimientos operacionales necesarios para la gestión de los diferentescomponentes y servicios de soporte tecnológico incluyendo:

1. Encendido y apagado de equipos de procesamiento y/o almacenamiento deinformación.
2. Ejecución de copias de respaldo y restauración de información.
3. Mantenimiento de equipos tecnológicos.
4. Instalación y configuración de sistemas operacionales.
5. Instalación y configuración de soluciones de ofimática (procesador de texto, hoja electrónica, software de diseño y software de usuario final).
6. Restricciones sobre uso e instalación de software y programas utilitarios.
7. Gestión de licenciamiento de software.

8. Gestión de proveedores de soporte tecnológico.

9. Gestión de canales de comunicación.

10. Gestión de infraestructura de soporte de centro de datos (Datacenter): aire acondicionado, sistema de control de acceso, sistema de detección y control de incendios, sistemas de monitoreo de condiciones ambientales (humedad, temperatura, etc.).

11. Restauración de sistemas de información a partir de copias de respaldo.

12. Gestión de eventos, incidencias y problemas de infraestructura tecnológica.

13. Procedimientos de recuperación ante desastres tecnológicos.

12.2 Gestión de cambios sobre infraestructura tecnológica

a) Todos los cambios sobre la infraestructura tecnológica deben ser controlados mediante los procedimientos definidos por el EIST de la ANT. Los procedimientos para la gestión de cambios deben incluir actividades para:

1. Identificación única y registro de los cambios.

2. Planificación de las actividades del cambio.

3. Prueba de las modificaciones de los cambios.

4. Valoración del impacto potencial del cambio, incluida la afectación a nivel deseguridad de la información.

5. Aprobación formal de los cambios.

6. Verificación de cumplimiento de los requisitos de seguridad de la informaciónde los cambios.

7. Comunicación oportuna de las actividades del cambio a todas las partesinteresadas.

8. Procedimientos para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos.

9. Procedimientos para aprobación y ejecución de cambios de emergencia.

12.3 Gestión de capacidad de la infraestructura tecnológica

a) El Equipo de Infraestructura y Soporte Tecnológico de la SG de la ANT debe realizar un seguimiento al uso de los recursos tecnológicos: accesoa redes, almacenamiento, capacidad de procesamiento, disponibilidad de equipos, energía eléctrica, servicios de soporte de centro de datos, suministrospara copias de respaldo, licenciamiento de software, y demás componentes de infraestructura de TIC necesarios para la normal prestación de servicios tecnológicos de la Entidad.

b) Los responsables de área de los diferentes procesos institucionales deben hacerseguimiento de la utilización de los recursos bajo su responsabilidad: equipos de cómputo, servicios de acceso a Internet, correo electrónico, equipos de impresión, equipos de digitalización o copiado, suministros tecnológicos.

c) La Mesa Técnica de TI de la ANT es la responsable de evaluar las necesidades de crecimiento de capacidad en los recursos el control de la demanda de recursos de TIC, las acciones mínimas a considerar deberían incluir:

1. Eliminación de la redundancia de datos.
2. Optimización de operaciones de procesamiento de información.
3. Racionalización en el uso de canales de comunicación.
4. Restricción en el uso de aplicaciones o servicios no esenciales para laprestación de servicios institucionales.
5. Racionalización en la asignación de licencias de uso de software y programasutilitarios.

d) Las decisiones sobre evaluación, control, optimización y mejoramiento de la capacidad deben ser documentadas por la Mesa Técnica de TI de la ANT o a quien ésta designe.

12.4 Separación de ambientes de desarrollo, pruebas y producción

a) Para reducir las posibilidades de cambios no autorizados sobre los sistemas de información y aplicaciones y mantener control de los cambios introducidos sobrelos mismos los ambientes de desarrollo, prueba y operación deberían separarsecon medidas físicas o lógicas de acuerdo con la disponibilidad de recursos.

b) A través de la metodología de desarrollo de software de la ANT, se deben documentar reglas

para:

1. Transferir código fuente y/o ejecutable entre el ambiente de desarrollo y el ambiente de pruebas, y del ambiente de pruebas al ambiente de producción.

2. Separar lógicamente los ambientes de desarrollo y producción de forma quese evite que los ambientes compartan las mismas posiciones de memoria o espacios de almacenamiento.

c) Antes de realizar cambios a nivel de sistema operacional en las plataformas de producción, se debe verificar el correcto funcionamiento de las plataformas en ambientes de prueba.

d) En los ambientes de producción no se deben mantener copias de herramientas de desarrollo o utilitarios que faciliten la modificación del software de producción.

e) Para la ejecución de pruebas no se deberían utilizar datos sensibles, informaciónpública reservada o información pública clasificada, en su lugar se deberían preparar conjuntos de datos que permitan verificar las funcionalidades sin comprometer la confidencialidad de la información institucional.

f) En los casos en los que se requiera uso de información de carácter personal para procesos de pruebas se deben adoptar medidas para anonimizar los conjuntos de datos de pruebas.

12.5 Protección contra códigos maliciosos

a) El Equipo de Infraestructura y Soporte Tecnológico de la SG dela ANT es el área responsable de:

1. La definición de procedimientos relacionados con la protección contra el software malicioso en los sistemas de información y equipos de infraestructura tecnológica de la ANT.

2. La preparación de planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación.

3. La implementación de procedimientos para recolectar información en forma regular como, por ejemplo, la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso.

4. La implementación de procedimientos para verificar información relacionadacon el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos.

b) Las estaciones de trabajo de los colaboradores de la ANT, los servidores y en general los equipos de procesamiento y almacenamiento de información deben contar con protecciones para detectar, prevenir y recuperarse de software de código malicioso.

c) Semestralmente todos los colaboradores de la ANT deben recibir capacitación y/o sensibilización en materia de seguridad de la información que incluya aspectos relativos a la prevención, detección y reporte de códigos maliciosos.

d) Todos los colaboradores de la ANT deben aplicar la política de seguridad de la información y los controles de seguridad para prevenir eventos asociados a códigos maliciosos.

e) Los servicios de navegación por Internet de la ANT deben contar con filtros de contenido que permitan la identificación de sitios web potencialmente peligrososo que se sospeche que lo son.

f) Semestralmente se deben ejecutar análisis de vulnerabilidades sobre los servidores de la ANT para identificar fallas potenciales o reales que puedan afectar a los equipos.

g) Todos los equipos de la infraestructura tecnológica de la ANT deben aplicar los parches de seguridad y de resolución de vulnerabilidades técnicas recomendadas por el fabricante para resolver brechas de seguridad.

h) Anualmente se deben realizar revisiones del software y del contenido de datos de los sistemas que apoyan los procesos críticos misionales para identificar la presencia de archivos no aprobados o de cambios no autorizados.

i) El software de prevención de código malicioso de las estaciones de trabajo debe ser actualizado periódicamente.

j) Cualquier medio de almacenamiento que deba ser utilizado en las estaciones de trabajo o servidores de la ANT debe ser inspeccionado con software de prevención de código malicioso para identificar la presencia de amenazas.

k) Cualquier archivo adjunto o descarga de archivos de las redes de la ANT o redesexternas debe ser analizado para identificar y prevenir la presencia de códigos maliciosos.

12.6 Copias de respaldo

a) Se deben hacer copias de respaldo de la información institucional, imágenes del software de sistemas operacional activo en los servidores, copia de seguridad de los sistemas de

información y aplicaciones a intervalos regulares y verificar su correcto funcionamiento.

b) La periodicidad de las copias de respaldo, su retención y mecanismos de protección se debe realizar de acuerdo con la política de copia de respaldo adoptada por la ANT.

c) Las copias de respaldo se deben almacenar en lugar seguro y en las condiciones recomendadas por el fabricante de los medios empleados para las copias de respaldo.

d) Los medios de respaldo se deben poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.

e) Al almacenar información pública reservada o pública clasificada en medios de respaldo se debe evaluar la necesidad de utilizar controles de criptografía para preservar su confidencialidad.

f) El almacenamiento de información en servidores y repositorios compartidos debe seguir las directrices definidas en los lineamientos de file server, FTP y bases de datos.

g) La SSIT y SG son los responsables de definir lineamientos técnicos para la realización de copias de respaldo, custodia y recuperación de la información.

12.7 Registro y seguimiento de eventos

a) Se deben conservar y revisar regularmente los registros acerca de actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información que afecten a los sistemas de información institucionales.

b) Los registros de eventos de los componentes de infraestructura tecnológica deberían considerar el almacenamiento de la siguiente información en la medida de sea factible su generación y almacenamiento:

1. Identificación de usuarios.
2. Actividades ejecutadas.
3. Fechas y horas del evento clave.
4. Identificación de dispositivos.
5. Cambios en configuración de los dispositivos.
6. Alarmas.
7. Transacciones realizadas por el usuario.

c) En cumplimiento de los requisitos legales los relojes de los diferentes sistemas y dispositivos deben estar sincronizados con la hora legal colombiana.

d) Se deben adoptar controles para proteger de cambios no autorizados de la información del registro de eventos de los dispositivos, sistemas de información y componentes de infraestructura.

e) Se deben definir los periodos de retención de los registros de auditoria de sistemas de información, así como su periodicidad de copia de respaldo.

f) Las actividades de los administradores y operadores de los sistemas de información y compontes de infraestructura crítica se deben registrar, y los registros se deber proteger y revisar con regularidad.

12.8 Control de software de sistema operacional

a) El Equipo de Infraestructura y Soporte Tecnológico de la SG dela ANT es el área responsable de definir procedimientos para controlar la instalación de software de sistema operacional en servidores.

b) Solamente el personal autorizado por la Mesa Técnica de TI y el EIST de la ANT deben realizar actividades de actualización de software de sistema operacional, aplicaciones o bibliotecas de programas o sistemas de información.

c) Los sistemas operacionales solo deben ser actualizados con software autorizado por el fabricante de este.

d) Los cambios y actualizaciones en sistemas operacionales se deben verificar antes de aplicarlos a los sistemas en producción para prevenir malfuncionamiento de los sistemas de información institucionales.

e) Se debe mantener un registro de configuración de los diferentes dispositivos para llevar control de las versiones del sistema operacional instalado en los mismos.

f) Se debe mantener copia de las versiones anteriores del sistema operacional como medida de contingencia en caso de necesidad de devolver los cambios aplicados.

g) Sólo se debería conceder acceso lógico y físico a los proveedores para propósitos de apoyo cuando es necesario, y con aprobación de la Mesa Técnica de TIde la ANT y el EIST. Se deber hacer seguimiento a las actividades de los proveedores.

12.9 Gestión de vulnerabilidades técnicas

a) El equipo de Infraestructura y Soporte Tecnológico de la SG de la ANT debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información, mediante el monitoreo de listas de interés, información de proveedores, pruebas de técnicas u otras fuentes apropiadas.

b) El equipo de Infraestructura y Soporte Tecnológico de la SG de la ANT es el responsable de realizar el seguimiento de las vulnerabilidades, la valoración de riesgos de estas y recomendación sobre la aplicación de parchespara tratar las vulnerabilidades.

c) El equipo de Infraestructura y Soporte Tecnológico de la SG de la ANT debe adoptar un procedimiento para realizar el tratamiento de vulnerabilidades técnicas.

d) Los parches se deberían probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar.

e) Los procedimientos de gestión de vulnerabilidades técnicas deben estar alineados con las actividades de gestión de incidentes para dar respuesta a losmismos en caso de ocurrencia de incidentes de seguridad.

13 LINEAMIENTO SOBRE SEGURIDAD EN LAS COMUNICACIONES

13.1 Seguridad en redes

a) El EIST de la SG de la ANT es el responsable de implementar controles para asegurar la seguridad de la información en las redes y la protección de servicios relacionados contra acceso no autorizado.

b) Se deben establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes institucionales, por ejemplo, segmentación.

c) El EIST es el responsable de configurar el acceso de los equipos previamente autorizados.

d) El acceso de equipos a las redes institucionales debe requerir autenticación, lasclaves de acceso a redes deben seguir las políticas y lineamientos de uso de información de autenticación secreta institucionales.

e) Las redes de acceso a Internet de la ANT deben tener políticas de filtrado de contenido y restricción de acceso solo a los sitios web asociados a la prestaciónde servicios institucionales.

f) Sobre los diferentes equipos de redes y telecomunicaciones, solo deben estar habilitados los servicios necesarios para la prestación de servicios institucionales.

g) La calidad y capacidad de los servicios de acceso a Internet se deben supervisar permanentemente para garantizar continuidad del servicio.

h) En contratación de servicios de acceso a redes se deben contemplar las características de seguridad, los niveles de servicio y los requisitos de gestión.

13.2 Seguridad en la transferencia de información

a) La Mesa Técnica de TI de la ANT es la responsable de definir los procedimientos y controles que se deben adoptar para proteger la información transferida contra interceptación, copiado, modificación, cambio de enrutamiento y destrucción.

b) Los responsables de los procesos institucionales en coordinación con los responsables de gestión documental deben definir y documentar las directrices sobre retención y disposición para toda la información en formato digital, incluidos mensajes de correo electrónico, de acuerdo con el programa de gestióndocumental institucional.

c) Todas las transferencias de información deben ser verificadas para comprobar que están libres de códigos maliciosos.

d) Al transferir información calificada como pública clasificada o pública reservada, se deben

adoptar controles criptográficos para prevenir la pérdida de confidencialidad.

e) El contenido de cualquier comunicación o transferencia de información realizada a través de los canales institucionales es responsabilidad del custodio de la información.

f) Las transferencias de información de carácter personal se deben realizar cuandose cumplan todos los requisitos definidos en la Ley de protección de datos personales, ley 1581 de 2012, se cuente con la autorización del titular de los datos en los casos que la ley determine.

g) La Mesa Técnica de TI de la ANT es la responsable de definir los procedimientos, responsabilidades y controles de la transferencia segura de información institucional entre dependencias y las partes externas.

h) Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro de la información intercambiada, el emisor y el receptor de estas y la fecha de entrega/recepción.

i) Los propietarios de los activos de información deben autorizar los requerimientosde información a la Entidad por terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

j) Los propietarios de los activos de información deben verificar que los terceros realicen el borrado seguro de la información suministrada una vez se han cumplido los propósitos para los cuales fue intercambiada y esta no sea requerida para otros propósitos de prestación de servicio al ciudadano o no searequerida su conservación por mandato legal.

k) Los propietarios de los activos de información deben requerir a las partes interesadas con la que intercambian información, que se adopten todas las medidasadministrativas y técnicas necesarias para la protección de la confidencialidad, integridad y disponibilidad de la información intercambiada con la ANT.

l) Los procedimientos para la transferencia segura de la información deben considerar aspectos como:

1. Uso de mecanismos para mantener la trazabilidad y el no repudio de las comunicaciones.

2. Estándares técnicos para transmisión.

3. Cifrado de los datos cuando aplique.

4. Responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos o divulgación no autorizada.

5. Calificación de la información de acuerdo con los requisitos legales (pública clasificada, pública reservada, datos abiertos, información privada).

6. Cadena de custodia para la información mientras está en tránsito, cuando sea requerida, ejemplo en transferencias mediante medios físicos.

13.3 Uso de servicios de mensajería electrónica

a) El EIST es el responsable de suministrar, mantener y mejorar un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico institucional.

b) El EIST debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido o recibido a través de los mensajes.

c) El uso del correo electrónico institucional se debe realizar de acuerdo con la política institucional de correo electrónico.

d) La información enviada y recibida por correo electrónico institucional es de propiedad de la Agencia Nacional de Tierras, los usuarios del servicio de correo electrónico no deben usar los servicios institucionales de mensajería para comunicaciones de carácter personal.

e) La plataforma de correo electrónico oficial de la Entidad es la aprobada por el EIST de la ANT, el uso de otras plataformas no está autorizado para comunicaciones oficiales salvo autorización expresa de la Entidad.

f) Todas las actividades que sean realizadas desde la cuenta de correo institucional serán responsabilidad del usuario al que se le asigne la cuenta de acceso.

g) El uso del servicio de correo institucional se debe realizar de acuerdo con las normas que determine La Mesa Técnica de TI de la ANT, incluyendo:

1. Uso de firma institucional.

2. Uso de nota de confidencialidad.

3. Formato de imagen institucional.

13.4 Acuerdos de confidencialidad

a) Los acuerdos de confidencialidad o de no divulgación son aplicables tanto a las partes interesadas como a todos los colaboradores de la ANT.

b) Los acuerdos de confidencialidad o de no divulgación deben cumplir con los requisitos legales necesarios para proteger la información pública reservada o pública clasificada usando términos ejecutables legalmente en el ordenamientojurídico colombiano.

c) La Mesa Técnica de TI de la ANT es la responsable de identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades institucionales para la protección de la información.

d) La Mesa Técnica de TI de la ANT puede definir diferentes formas de acuerdos de confidencialidad o de no divulgación, en diferentes circunstancias.

e) La Mesa Técnica de TI de la ANT debe considerar los siguientes aspectos al momentode definir las condiciones de los acuerdos de confidencialidad o no divulgación:

1. Definiciones que establezcan la categoría de la información a proteger: clasificada, reservada, privada.

2. La duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente.

3. Las acciones requeridas cuando termina el acuerdo.

4. Las responsabilidades y acciones de los firmantes para evitar la divulgaciónno autorizada de información.

5. La propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información.

6. El uso permitido de información clasificada, reservada o privada y losderechos del firmante para usar la información.

7. El derecho a actividades de auditoría y de seguimiento que involucran información a proteger.

8. El proceso de notificación y reporte de divulgación no autorizada o fuga deinformación.

9. Los plazos para que la información sea devuelta o destruida al finalizar elacuerdo.

10. Las acciones que se espera tomar en caso de violación del acuerdo.

14 LINEAMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 Requisitos de seguridad de la información en el desarrollo de software

a) La seguridad de la información debe ser una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos parasistemas de información que prestan servicios en redes públicas.

b) Los requisitos relacionados con seguridad de la información se deben incluir enlos requisitos para nuevos sistemas de información o para mejoras a lossistemas de información existentes.

c) Los requisitos de seguridad de la información se deben identificar usando variosmétodos, tales como la obtención de requisitos de cumplimiento a partir de políticas y reglamentación, modelado de amenazas, revisiones de incidentes, ouso de umbrales de vulnerabilidad.

d) La identificación y gestión de los requisitos de seguridad de la información y los procesos asociados se debe integrar en las primeras etapas de los proyectos desistemas de información.

e) Los contratos con los proveedores deben tener en cuenta los requisitos de seguridad de la información.

f) La información involucrada en los sistemas de información que usan las redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

g) La información involucrada en las transacciones de los sistemas de informaciónse debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

h) Las consideraciones de seguridad de la información para las transacciones de los sistemas de información deberán incluir:

1. El uso de firmas electrónicas por cada una de las partes involucradas en latransacción.

2. La información de autenticación secreta de usuario, de todas las partes, se debe validar y verificar.

3. La transacción permanezca confidencial.

4. Se mantenga la privacidad asociada con todas las partes involucradas.

5. Los casos en que se use una autoridad confiable (por ejemplo, para los propósitos de emitir y mantener firmas o certificados digitales), la seguridad esté integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

14.2 Seguridad en los procesos de desarrollo de software

a) La Mesa Técnica de TI o el equipo de Arquitectura Empresarial de la ANT son los responsables de aprobar los lineamientos para el desarrollo del software de la ANT.

b) Los lineamientos para el desarrollo de software de la ANT deben incluir controlespara garantizar la seguridad de la información durante los procesos de desarrollode software.

c) Los lineamientos técnicos específicos para los procesos de desarrollo de software deben seguir las directrices definidas en el lineamiento de construcciónde software definido por la Entidad.

d) Las áreas misionales deberán proporcionar un líder funcional que acompañe el proceso de análisis de requerimientos, pruebas y validación de las funcionalidadesprovistas por los sistemas de información que conforman el ecosistema tecnológico de la ANT.

e) La Agencia Nacional de Tierras contempla la normatividad requerida para el control de los derechos de autor de los componentes tecnológicos construidos por parte de los contratistas o proveedores, los cuales se especifican en las cláusulas de contratos.

f) Todo desarrollo de Sistemas de Información misional deberá ser avalado y aprobado en su pertinencia desde la SSIT.

g) La SSIT debe certificar que todo sistema de información misional adquirido o desarrollado, utilice

herramientas licenciadas por la organización y hagan parte del ciclo de vida de construcción de software, de igual manera y con soporte técnico.

h) La ANT debe contar con un sistema para el manejo de versiones del código fuente, tanto para los ambientes de producción, como para los que se encuentran en ambiente de desarrollo.

i) Se debe mantener una biblioteca que conserve las versiones del código fuente y de los sistemas de información de la Agencia, además de los artefactos técnicos generados por el área técnica, los cuales deberán estar respaldados y alineados en el Repositorio de Arquitectura Empresarial definido por la SSIT.

14.3 Datos de prueba

a) Se deberá evitar el uso de datos de producción reales que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba.

b) La SSIT deberá certificar que la información entregada a los desarrolladores para sus pruebas tenga implementados mecanismos de seguridad para conservar la confidencialidad de la información, por ejemplo, enmascarar los datos evitando revelar la información confidencial de los ambientes de producción.

c) Si es estrictamente necesario el uso de datos personales u otra información confidencial para propósitos de las pruebas, todos los detalles y contenido reservados o clasificados se deben proteger eliminándolos o modificándolos mediante la técnica de anonimización. La SSIT debe certificar el borrado seguro de los datos usados en los ambientes de pruebas.

d) Los procedimientos de control de acceso, que se aplican a los sistemas de información, se deberían aplicar también a los sistemas de información en fasede pruebas.

e) Se debe hacer una autorización separada cada vez que se copia información deproducción a un ambiente de pruebas.

f) Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

g) Si se autoriza el uso de información real de producción en ambientes de pruebasse debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.

h) Antes del paso a producción de los sistemas de información, los propietarios sonresponsables de

realizar las pruebas para asegurar que se cumplen con requerimientos de seguridad establecidos, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

14.4 Adquisición de software, servicios y sistemas de información.

a) La adquisición de sistemas de información para la Agencia se debe realizar conforme a la política y lineamientos de Desarrollo de Software formulados por la SSIT.

b) Se deben contemplar las características de seguridad que requiere la Agencia y realizar un proceso formal de pruebas, que haga parte del proceso de evaluaciónde las ofertas.

c) Se debe adquirir productos de software únicamente con proveedores acreditados o productos ya evaluados en materia de seguridad de la información.

d) La SSIT debe asegurar que los sistemas de información adquiridos cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

14.5 Mantenimiento del software, servicios y sistemas de información.

a) La SG a través del Equipo de Infraestructura y Soporte Tecnológico, debe asegurar la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información, para que permanezcan constantemente actualizados, con todos los parches generados para las versiones en uso y que además ejecuten la última versión aprobada del sistema.

b) La información que se encuentra en los sistemas de información en ambiente deproducción debe mantener el máximo nivel de protección, no debe ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como para el desarrollo de soluciones.

c) Cuando se realicen cambios en los sistemas de información, se debe verificar que éstos estén autorizados, que sean realizados por personal competente y que se respeten los términos y condiciones de uso de las licencias del softwarea que haya lugar; para lo cual se debe presentar el procedimiento en la Mesa Técnica de TI de la ANT, el comité de cambios o quien haga sus veces.

d) Cuando se realicen cambios que modifiquen los sistemas de información, se debe informar al usuario del activo de información que procese dicho activo.

e) Los cambios a los sistemas de información se deben implementar en ventanas de mantenimiento para no afectar la disponibilidad del servicio.

15 LINEAMIENTO DE SEGURIDAD CON PROVEEDORES

a) La Mesa Técnica de TI de la ANT es la responsable de definir los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.

b) Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor para que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la Agencia Nacional de Tierras.

c) Los supervisores de los contratos con proveedores deben realizar el seguimiento y la revisión para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionen apropiadamente.

d) Las consideraciones de seguridad que se deben acordar con los diferentes proveedores de la ANT, que incluye:

1. La definición de los tipos de acceso a la información que se permitirá a diferentes proveedores, y el seguimiento y el control del acceso.

2. Los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso, que sirvan como base para los acuerdos con proveedores individuales, con base en las necesidades y requisitos del negocio de la organización y su perfil de riesgo.

3. Los procesos y procedimientos para hacer seguimiento del cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por una tercera parte cuando sea aprobada entre las partes.

4. Los tipos de obligaciones aplicables a los proveedores para proteger la información de la ANT.

5. La estrategia y procedimientos para el manejo de incidentes y contingencias asociadas con el

acceso de proveedores.

e) Verificar las obligaciones sobre la formación y toma de conciencia en seguridad de la información, para el personal del proveedor.

f) Al autorizar el acceso a los sistemas de información o activos de información institucionales a un proveedor, se deben contemplar los siguientes controles de seguridad:

1. Una descripción de la información que se va a suministrar o a la que se va atener acceso, y los métodos para suministrar la información o para acceder a ella.

2. La descripción de los niveles de la calificación de la información institucional.

3. Establecer los requisitos legales y contractuales, sobre la protección de datos personales, institucionales y de partes interesadas, así como los derechos de propiedad intelectual y derechos de autor de la información a la que se otorgará acceso.

4. Las reglas de uso aceptable de la información, incluido el uso no permitido, si es necesario.

5. Una lista explícita de personal del proveedor autorizado para tener acceso a la información de la Agencia y los procedimientos o condiciones para la autorización, y el retiro del acceso o recibo de información institucional por parte del personal del proveedor.

6. Las políticas de seguridad de la información pertinentes al contratoespecífico.

7. Los requisitos y procedimientos de gestión de incidentes de seguridad de lainformación y las responsabilidades de las partes.

8. Las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.

16 LINEAMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LAINFORMACIÓN

a) La SSIT es responsable de aprobar los procedimientos para la gestión de incidentes de seguridad de la información.

b) Todos los colaboradores de la ANT y cuando sea pertinente, las partes interesadas, deben informar los eventos de incidentes de seguridad de la información.

c) Todos los colaboradores de la ANT deben recibir capacitación y toma de conciencia de su responsabilidad de reportar eventos de seguridad de la información tan pronto como sea posible a la SSIT.

d) Todos los colaboradores y cuando aplique, las partes interesadas deben informar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios a la SSIT.

e) Todos los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

f) Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados definidos por la Mesa Técnica de TI de la ANT.

g) Se debe recolectar y analizar la información asociada a los eventos e incidentesde seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros.

h) La ocurrencia de incidentes de seguridad informática que se consideren graves o de difícil control relacionados con cualquier ataque cibernético, serán reportados al COLCERT y/o CSIRT-CCIT para pedir el apoyo necesario delincidente que amerite ser tratado.

17 LINEAMIENTO SEGURIDAD INFORMÁTICA EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

a) La ANT debe realizar los análisis de impacto al negocio y los análisis de riesgosde continuidad para, posteriormente, proponer estrategias de recuperación en caso de activarse el plan de contingencia o continuidad.

b) La ANT debe gestionar la planeación e implementación de las estrategias de recuperación para los sistemas de información que apoyan los procesos misionales de la Agencia, a través de un plan de gestión de recuperación de desastres y de incidentes de seguridad.

c) La estrategia de recuperación ante desastres de la ANT estará alineada con los objetivos de negocio, formalmente documentada y con los procedimientos para asegurar la restauración de los procesos críticos del negocio comprobados.

d) La ANT debe asegurar la realización de pruebas periódicas de la estrategia de continuidad de negocio, con el fin de verificar que cumple con la seguridad de la información durante su realización, estas pruebas deben quedar documentadas.

e) La ANT debe validar que los planes de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

f) La ANT analizará y establecerá los requerimientos de redundancia para los sistemas de información críticos y la plataforma tecnológica que los apoya.

18 LINEAMIENTO CUMPLIMIENTO DE LEGISLACIÓN EN MATERIA DE SEGURIDAD

18.1 Derechos de Autor

a) Mediante su sistema integrado de gestión, la ANT debe identificar y documentar todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y elenfoque institucional para cumplirlos.

b) Los responsables de los procesos institucionales deben identificar toda lalegislación aplicable a sus funciones y las de su proceso para cumplir los requisitos exigidos.

c) Todos los funcionarios, contratistas, colaboradores y partes interesadas de la ANT deben cumplir con la legislación aplicable a la seguridad de la información, de acuerdo con sus funciones, con las obligaciones contractuales contraídas y las previsiones establecidas con partes interesadas.

d) El EIST y la SSIT son responsables de implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

e) La adquisición de software deberá ser solo a través de fuentes conocidas y confiables, para asegurar que no se violan los derechos de autor.

f) El Equipo de Infraestructura y Soporte Tecnológico es el responsable de mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales y demás elementos que demuestren la legalidad del software institucional.

g) El EIST es el responsable de implementar controles para asegurar que no se exceda ningún número máximode usuarios permitido dentro de la licencia de cada software.

h) La ANT puede llevar a cabo revisiones del software autorizado y/o productos con licencia en las estaciones de trabajo.

18.2 Revisión de cumplimiento de la seguridad de la información

a) A través de los procedimientos de Seguimiento Evaluación y Mejora la ANT realiza la revisión independiente del estado de la gestión de la seguridad de la información.

b) El EIST de la SG, realizará monitoreo permanente para comprobar el estado de los controles, verificar los informes de los sistemas de información, software de antivirus y firewall, con el fin de evitar o detectar algún mal uso de los equipos de cómputo o la red de datos. De encontrarse algún tipo de violación de la política o sus lineamientos de seguridad, se deberá realizar su correspondiente registro,análisis y toma de las acciones preventivas y/o correctivas necesarias.

c) La SSIT y el EIST, realizarán revisiones periódicas y aleatorias para verificar la implementación y aplicación de las políticas y lineamientos de seguridad de la información y darán informe a la Oficina de Control Interno de la Entidad sobre las anomalías, incidentes y problemas relacionados con la seguridad de información y todos los aspectos encontrados en las revisiones. Para esto se generará, un cronograma de trabajo conjunto, el cual será aprobado por la DGOSP y la SG de la Entidad.

GLOSARIO

ANT: Agencia Nacional de Tierras.

CSIRT-CCIT: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional.

COLCERT: El CSIRT-CCIT es un punto de contacto nacional, mediante el cual la comunidad nacional e internacional puede comunicarse con las grandes empresas proveedoras de Internet en Colombia, con el objetivo de gestionar una pronta y eficiente atención a los incidentes de seguridad informática que involucrenredes y/o servicios colombianos.

Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos; Ley 1712 de 2014, Transparencia y Derecho de acceso a la información pública.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada. Norma ISO/IEC 27000.

EIST: Equipo de Infraestructura y Soporte Tecnológico.

DGOSP: Dirección de Gestión del Ordenamiento Social de Propiedad.

Información: Datos relacionados que tienen significado para la Entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstanciaslegítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 del 2014.

Integridad: Propiedad de precisión y completitud de la información. Norma ISO/IEC27000.

SSIT: Subdirección de Sistemas de Información de Tierras.

SGSI: Sistema de Gestión de Seguridad de la Información.

Agencia Nacional de Tierras	**POLÍTICA**	**LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	**CÓDIGO**	INTI-Política-008
	ACTIVIDAD	GOBIERNO DE TIC	**VERSIÓN**	3
	PROCESO	INTELIGENCIA DE LA INFORMACIÓN	**FECHA**	19/09/2022

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
19/09/2017	1	Primera versión del documento.
25/02/2020	2	Actualización de los lineamientos conforme a actualización depolíticas de seguridad de la información
19/09/2022	3	Documento actualizado por cambios organizacionales, culturales, del entorno, operativos o normativos que afectan la ANT, creación mesa técnica de TI, equipo de trabajo de infraestructura, ajuste de responsabilidades. Ajustes del documento con el formato estándar de la ANT.

Elaboró: Carlos Eduardo Alfonso Pinilla	**Revisó: Duberly Eduardo Murillo Barona**	**Aprobó**: **José Carlos Orozco Zequeda**
Cargo: Contratista, Subdirección de Sistemas de Información de Tierras	**Cargo:** Subdirector de Sistemas de Información de Tierras.	**Cargo**: Director de Gestión de Ordenamiento Social de la Propiedad (E).
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO
Elaboró: Humberto Antonio Rosa Sarmiento		
Cargo: Contratista, Dirección de Gestión de Ordenamiento Social de la Propiedad		
Firma: ORIGINAL FIRMADO		
Elaboró: Rudyard Guillermo Guzmán Echavez		
Cargo: Contratista, Dirección de Gestión de Ordenamiento Social de la Propiedad		
Firma: ORIGINAL FIRMADO		