LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

AGENCIA NACIONAL DE TIERRAS

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

CONTENIDO

INTRODUCCIÓN

Como parte de 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 implementar las mejores prácticas en materia de tecnologías de información y comunicaciones; En ese sentido, a continuación, se presentan los lineamientos, mediante los que 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 la Agencia 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 el Gobierno de la Seguridad el cual contempla la política de seguridad de información de la Agencia, la Norma Técnica Colombiana ISO/IEC 27001:2013, modelos de seguridad como ITGI, NIST, SoGP, ISMS entre otros.

DEFINICIONES (Términos y Siglas)

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[1].

COLCERT: El CSIRT-CCIT es un punto de contacto nacional, mediante el cual la comunidad nacional e internacional puede comunicarse con las más grandes empresas proveedoras de Internet en Colombia, con el objetivo de gestionar una pronta y eficiente atención a los incidentes de seguridad informática que involucren redes y/o servicios colombianos[2].

DGOSP: Dirección de Gestión del Ordenamiento Social de Propiedad de la Agencia Nacional de Tierras.

SSIT: Subdirección de Sistemas de Información de Tierras.

SGSI: Sistema de Gestión de Seguridad de la Información.

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 semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 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

[1] http://www.colcert.gov.co
[2] http://www.csirt-ccit.org.co/nosotros.html

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.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado6

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.

Base de datos:[3] Conjunto organizado de datos personales que sean objeto de tratamiento.

Comunicación del riesgo: Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas[4].

Dato personal:[5] Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.[6]

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo[7].

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo[8].

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados[9].

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén

[3] Definición del artículo 3 de la ley 1581 de 2012

[4] ISO/IEC Guía 73:2002
[5] Definición del artículo 3 de la ley 1581 de 2012
[6] ISO/IEC Guía 73:2002
[7] ISO/IEC Guía 73:2002
[8] ISO/IEC Guía73:2002
[9] NTC – ISO – IEC 27005 Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.

configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad10.

Principio de confidencialidad:[11] Todas las personas que intervienen en el tratamiento de datos personales que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación laboral o contractual con la entidad.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad de consecuencias negativas o su impacto o ambas12.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la entidad, se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias13.

Transferencia del riesgo: Compartir con otro actor responsable, la pérdida o la ganancia de un riesgo[14].

[10] Guía 2 Elaboración de la política general de seguridad y privacidad de la información. Seguridad y privacidad de la información. MINTIC.
[11] Ley 1581 de 2012
[12] ISO/IEC Guía 73:2002
[13] NTC – ISO – IEC 27005 Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Términos y definiciones
[14] ISO/IEC Guía 73:2002

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 los estándares de seguridad y de gobierno en línea.

ALCANCE

El presente documento tiene aplicabilidad para los elementos que hacen parte de la arquitectura tecnológica de la Agencia Nacional de Tierras, particularmente para los activos de información de todos los procesos (se incluyen todos los dominios de Arquitectura empresarial propuestos por MINTIC: Estrategia de TI, Gobierno de TI, Datos, 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 las partes interesadas.

1. DISPOSICIONES GENERALES

1.1 Frecuencia de actualización de los lineamientos de seguridad de la información

Los lineamientos tendrán una revisión de actualización semestral o anual (dependiendo de las decisiones tomadas en el comité de arquitectura, mesa técnica o quien haga sus veces), de igual forma, se revisarán cuando hayan surgido actualizaciones o cambios significantes a los procesos, procedimientos, servicios informáticos, leyes o normatividad aplicable.

2. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

LINEAMIENTO No. 1 SEGURIDAD FÍSICA Y DEL ENTORNO

Regla No.1 Acceso al edificio en el Nivel Central

En aras de preservar la integridad, confidencialidad y disponibilidad de los activos de información de la ANT, así como de sus bienes, se debe dar cumplimiento al siguiente protocolo de seguridad en el edificio del nivel central:

- El ingreso y salida de funcionarios, contratistas y terceros se realizará únicamente por la puerta principal, validando mediante la huella dactilar el ingreso y salida. (Salvo en los casos de emergencia institucional y en condiciones especiales)
- Durante su permanencia en las instalaciones de la Agencia los funcionarios y contratistas de la ANT deben portar en un lugar visible su carnet y los terceros o visitantes el sticker entregado en la recepción en el momento de su registro.
- Si el funcionario, contratista, colaborador o tercero no tiene su carnet y su huella dactilar no está activada deberá registrarse en la recepción, indicando la dependencia a la que se dirige y portar el sticker entregado en un lugar visible.
- El personal de vigilancia y seguridad está autorizado para revisar el contenido de los elementos que se ingresen; así mismo los elementos electrónicos como estaciones de trabajo, servidores, equipos portátiles, medios de almacenamiento extraíbles y demás recursos tecnológicos deberán contar con el debido registro en las bitácoras establecidas tanto al ingreso como a la salida de las instalaciones.
- Los visitantes que requieran acceso a la red de comunicaciones de la entidad, deberán solicitar el acceso directamente al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT una vez hayan realizado su ingreso efectivo a las instalaciones.
- No se autorizará el acceso a las instalaciones de la Agencia a los visitantes, a menos que un funcionario activo de la Entidad lo apruebe. Dicho funcionario será

responsable por el visitante durante su permanencia en las instalaciones de la Entidad.

- Si el visitante requiere una reunión o visita adicional en un piso o área diferente al inicialmente autorizado, deberá realizar nuevamente el proceso de registro y autorización en la recepción del edificio.
- En caso de desvinculación laboral del funcionario o terminación de labores por parte del contratista y/o tercero, éste debe hacer la correspondiente devolución del carnet asignado en desarrollo de sus actividades.
- Cuando exista una desvinculación contractual de funcionarios, contratistas o terceros con la ANT. El supervisor o jefe designado deberá reportar dicha desvinculación para efectos de bloqueo de cuenta, correo y huella de acceso a la Entidad

Regla No.2 Áreas seguras

Las áreas seguras son lugares donde se realiza el procesamiento de información como el centro de cómputo, centros de cableados y demás áreas en la cuales se encuentre información sensible y confidencial; en estas áreas se deberán aplicar las siguientes reglas:

- Estar protegidas de accesos no permitidos con mecanismos de seguridad.
- Contar con un control de entrada para garantizar solo acceso a personal autorizado.
- Contar con un registro de las personas que ingresan a estas áreas, para ser auditados e identificar acceso no autorizados.
- La información o mecanismos de acceso a estas áreas son responsabilidad de las personas autorizadas y no deben ser entregadas a otros funcionarios o terceros sin previa autorización.
- Los visitantes deberán estar siempre acompañados de un funcionario durante su visita a las áreas seguras de la Entidad.
- Deberán contar con un sistema de cámaras de vigilancia o de seguridad electrónica.
- Tener las condiciones físicas y ambientales necesarias para la protección y correcta operación de los recursos de la plataforma tecnológica; deben contar con sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, así como sistemas de descarga eléctrica.
- Asegurar que el centro de cómputo y los centros de cableado se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- Monitorear y adoptar los controles necesarios para el buen funcionamiento de los mecanismos de seguridad como también de los equipos de cómputo de estas áreas.
- Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y debidamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
- En caso de evidenciarse un riesgo de seguridad en estas áreas, debe ser reportado directamente a la mesa de servicios.

Regla No.3 Protección de equipos de cómputo

Los equipos de cómputo deberán asegurarse y cumplir con los siguientes parámetros:

- No serán movidos o reubicados por los usuarios, esta labor será exclusiva del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT.
- Estar protegidos y ubicados en áreas resguardadas de riesgos ambientales.
- Deben ser utilizados únicamente por las personas autorizadas por la Entidad.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT debe asegurar el monitoreo y el mantenimiento preventivo.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT debe generar estándares de configuración segura para los equipos de cómputo asignados a los funcionarios, contratistas o terceros y configurar dichos equipos acogiendo los estándares generados.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT debe mantener la infraestructura eléctrica conforme a la regulación y estándares vigentes (NEC, NEMA, ICONTEC, CEN).
- El usuario no deberá intentar acceder a las partes internas del equipo, solo está autorizado el personal especializado del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT.
- Cada usuario deberá garantizar la seguridad física y reportar algún daño, condición insegura o pérdida del mismo mediante la mesa de servicio.
- Es responsabilidad del jefe inmediato o supervisor del contrato solicitar a la mesa de servicios una copia de respaldo de la información generada por el usuario, en un medio de almacenamiento diferente al del equipo asignado.
- Antes de reutilizar o desechar los equipos de cómputo se deberá realizar el procedimiento definido por la Secretaría General y asegurar que la información del usuario anterior sea eliminada, garantizando que se haya suprimido de manera segura y completa.

- La ANT no se hará responsable de los equipos que estén en sus instalaciones y no sean de su propiedad.
- En caso de que funcionarios, contratistas, terceros u otros, necesiten utilizar equipos personales para el desarrollo de sus obligaciones, estos equipos deben ser llevados al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT para verificar el licenciamiento de software tanto del sistema operativo, como de ofimática, antivirus, entre otros.
- En cuanto al uso y manejo de los puertos de salida de información (USB, unidades de almacenamiento externos), éstos serán deshabilitados de los equipos propiedad de la agencia asignados a funcionarios, contratistas y/o terceros, y únicamente se habilitarán para aquellos funcionarios cuyo perfil de cargo y funciones lo requieran.
- Cuando el funcionario, contratista, colaborador o tercero termine su vinculación, labor u obra, está en la obligación de entregar su puesto de trabajo al funcionario designado por el jefe inmediato o supervisor, junto con la copia de la información crítica que maneja, de igual manera, debe hacer entrega de todos los recursos tecnológicos y otros activos que le fueron suministrados, así mismo debe diligenciar el formato definido dentro del sistema integrado de gestión donde se indica la formalización de dicha entrega, para proceder a la correspondiente remoción de derechos de acceso sobre los recursos tecnológicos, sistemas de información y acceso físico a las instalaciones de la ANT.

LINEAMIENTO No. 2 SEGURIDAD RELACIONADOS CON RECURSOS HUMANOS

Regla No.1 Responsabilidades del personal de la ANT

- La Subdirección de Talento Humano de la Entidad, realizará la revisión de los antecedentes fiscales, disciplinarios y judiciales antes de realizar la posesión del empleado, conforme a lo establecido por la Función Pública y los entes de control.

  Los contratos de los funcionarios, contratistas y terceros involucrados con la Agencia deben incluir como documento anexo la aprobación de los apartados relacionados con derechos de propiedad intelectual, 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. Se debe incluir cualquier insumo o componente original que desarrolle para la Agencia, en especial la cesión de los derechos de reproducción, distribución, trasformación, comunicación pública y/o cualquier otro derecho necesario para su comercialización y/o explotación total o parcial. En virtud del derecho de transformación cedido, el tercero deberá autorizar a que la Agencia

realice, directa o indirectamente, las modificaciones que considere convenientes, respecto de los resultados de su trabajo, cediendo también los derechos de explotación derivados de las modificaciones realizadas.

- Los funcionarios, contratistas y terceros de la ANT están en la obligación de conocer y cumplir cabalmente la política y lineamientos establecidos para la seguridad de la información de la Agencia.
- La Subdirección de Talento Humano y el Grupo Interno de Trabajo – Coordinación para la Gestión Contractual de la Entidad deben certificar, según corresponda, que los funcionarios, contratistas y/o terceros relacionados con la Agencia firmen un acuerdo y/o cláusula de confidencialidad y un documento de aceptación de las Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo o formalización del contrato y deberán ser diligenciados previo a la autorización de acceso a las instalaciones y/o a la plataforma tecnológica, para el caso de contratistas y/o terceros relacionados con la Agencia estos documentos deben ser solicitados y gestionados por el área objeto de la contratación.
- Es de obligatorio cumplimiento, asistir a las capacitaciones y charlas sobre seguridad de la información que organice la Agencia.
- Todos los funcionarios, contratistas, y/o terceros relacionados con la Agencia, tendrán acceso permanente a la política de seguridad, sus lineamientos y procedimientos, a través de la intranet, página web, campañas de divulgación, procesos de inducción y reinducción, entre otros.
- Será responsabilidad de la Subdirección de Talento Humano y de la Secretaria General enviar al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT la información del personal que tenga novedades relevantes a su contrato o situaciones administrativas como vacaciones, licencias o termine su vinculación con la Entidad, para realizar el respectivo bloqueo de los derechos de acceso. De presentarse un cambio en las funciones, cargo o responsabilidades de un funcionario o contratista, se debe seguir el mismo procedimiento, de manera que se asegure la entrega de los activos de información, la actualización de los accesos físicos y lógicos y la posterior entrega de los mismos de acuerdo con su nuevo rol.
- Todos los funcionarios, contratistas, y/o terceros relacionados con la Agencia, que finalicen su vínculo laboral o contractual deben mantener el cumplimiento de las políticas de seguridad de la Información y los compromisos adquiridos en torno a ella.

Regla No.2 Proceso disciplinario

- En caso de identificarse un incidente de seguridad, éste será registrado y auditado por la dependencia de la Agencia que tenga a cargo el control disciplinario para realizar la investigación respectiva y así determinar las causas y responsabilidades, la ANT tomará las acciones pertinentes para el funcionario, contratista, colaborador o tercero vinculado con el incidente, mediante un proceso disciplinario formal, de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la Entidad.

Regla No.3 Formación en seguridad informática

- La DGOSP o la SSIT, realizarán procesos de capacitación y socialización de la política y los lineamientos en seguridad de la información a todos los usuarios, a través de los mecanismos más adecuados, en coordinación con la Subdirección de Talento Humano de la Entidad.
- Al iniciar el contrato o la vinculación laboral se darán las pautas básicas de seguridad y se entregarán los datos de usuario, contraseña temporal y sus condiciones de utilización.
- Cada una de las dependencias de la ANT deberá convocar al nuevo personal a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información,
- La Subdirección de Talento Humano de la Entidad será la encargada de proveer los recursos para la ejecución de las capacitaciones, controlar la asistencia a dichas charlas y eventos, dejar el correspondiente registro de asistencia y reportar ante la autoridad competente los actos irregulares o de indisciplina de los funcionarios.

LINEAMIENTO No. 3 GESTIÓN DE ACTIVOS DE INFORMACIÓN

Regla No.1 Manejo de datos personales de los funcionarios, contratistas, colaboradores y terceros de la Agencia

- La Agencia mantendrá la confidencialidad, integridad y disponibilidad de las bases de datos que contengan información personal de los funcionarios, contratistas, colaboradores y/o terceros, tales como: sistemas administrativos y financieros, sistema de acceso biométrico y los demás que administren información sensible tanto de funcionarios, contratistas y terceros, así como también realizarán copias de seguridad de la información contenida en dichas bases de datos.
- La Agencia se compromete a tomar todas las precauciones y medidas necesarias para garantizar la reserva de la información confidencial, cumpliendo así el

principio de confidencialidad de la ley 1581 de 2012 y el artículo 15 de la Constitución Política Nacional.

- La Agencia se compromete a utilizar la información suministrada única y exclusivamente para el propósito para la que fue creada, entre otros: garantizar la seguridad de las personas que ingresen a las instalaciones de la Agencia, así como de sus activos de información.
- De llegarse a solicitar o exigir información mediante una orden judicial, requerimiento administrativo u otro mecanismo similar, la Agencia se reserva el derecho de divulgar esta información conforme a la regulación legal vigente.

Regla No.2 Inventario de activos de información

- La ANT debe contar con un inventario de sus activos de información que le permita identificar y clasificar la información sensible generada u obtenida en el ejercicio de sus funciones, así como la respectiva ubicación a nivel físico y digital, para tal fin, cada dependencia de la Agencia debe elaborar y mantener actualizado su inventario de activos de información dando cumplimiento a la Ley de Transparencia 1712 de 2014 y bajo las directrices definidas por la DGOSP y la SSIT con apoyo de la Secretaria general . Dicho inventario, debe incorporar la clasificación, valoración, ubicación y acceso a la información, de manera que permita identificar la información categorizada como pública susceptible de divulgación en los medios oficiales de la Agencia.
- La infraestructura de procesamiento de información (equipos de hardware, software, elementos de red y comunicaciones, instalaciones físicas) deberá estar protegida con base en los resultados del análisis de riesgos.

Regla No.3 Clasificación de activos de información

- La Agencia Nacional de Tierras definirá los niveles más adecuados para clasificar la información de acuerdo con su nivel de confidencialidad, y generará los lineamientos necesarios para la gestión y clasificación de los activos de Información para que sus propietarios la cataloguen y determinen los controles requeridos para su protección.
- Todos los activos de información de la Agencia deberán ser clasificados según su contenido y atributos de confidencialidad, disponibilidad y calidad; para lo cual, la entidad se encargará de proporcionar los recursos y controles necesarios, que además permitan preservar dichos atributos en los niveles y condiciones óptimas.
- Una vez clasificada la información, la ANT proporcionará los recursos necesarios para la aplicación de controles en busca de preservar su confidencialidad, integridad, disponibilidad y autenticidad, con el fin de promover un uso adecuado de la misma por parte de los funcionarios de la entidad y de los terceros que se encuentren autorizados y que requieran de la información para la ejecución de sus actividades.

Regla No.4 responsables y dueños de activos de información

La responsabilidad frente a la administración de la seguridad de la información se encuentra distribuida a lo largo del mapa de procesos y, por lo tanto, no es responsabilidad exclusiva de la SSIT o del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT; en ese sentido a continuación se delegan los roles y las responsabilidades que recaen en los propietarios de la información, sus custodios y usuarios, así como sobre la Oficina de Planeación y la Oficina de Control Interno.

- **Propietario de la información:**
  El propietario de la información puede ser un cargo, proceso, o grupo de trabajo al cual se le delega la responsabilidad de verificar la calidad de la información desde su origen y velar porque ésta se mantenga a lo largo del ciclo de vida de información en la Agencia. Debe garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, así como de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso15

  En la ANT los propietarios 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.

  Entre las responsabilidades de los propietarios de la información se tienen:

  - Asignar los niveles iniciales de clasificación de confidencialidad de la información de acuerdo a los lineamientos para la gestión y clasificación de activos de información creados para tal fin.
  - Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
  - Determinar los criterios y niveles de acceso a la información.
  - Revisar periódicamente los niveles de acceso a los sistemas a su cargo y realizar la reclasificación en caso de ser necesario.
  - Determinar los requerimientos de copias de respaldo para la información que les pertenece.
  - Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.

[15] Adaptado de ISO/IEC 27002:2013

- **Responsabilidades del Custodio 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 de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado[16].

  Los custodios de la información tienen la responsabilidad de garantizar la disponibilidad, la integridad y la confidencialidad de la información y sus responsabilidades son:

  - Administrar los accesos de red incluyendo sistema operativo y acceso al dominio de la Agencia.
  - Administrar los accesos a manejadores de bases de datos.
  - Administrar los accesos a archivos físicos e información almacenada en medios magnéticos
  - Implementar controles definidos para los sistemas de información incluyendo actualizaciones de seguridad en los sistemas (parches, service packs, fixes, etc.)
  - Desarrollar procedimientos de autorización y autenticación
  - Administrar los documentos de licenciamiento y medios magnéticos del software adquirido por la entidad.
  - Asistir y administrar los procesos de copia de seguridad, de recuperación y del plan de continuidad de negocio y sistemas de información.
  - Proveer los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin.
  - Efectuar la eliminación segura de la información física, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
  - Utilizar los medios adecuados para destruir o desechar correctamente la documentación física, con el fin de evitar su reconstrucción una vez cumplido su ciclo de almacenamiento.
  - Monitorear el cumplimiento de la política y lineamientos de seguridad en los activos de información que custodia.

- **Responsabilidades de Usuario:**
  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 para propósitos

[16] Adaptado de ISO/IEC 27002:2013

propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información[17]

Sus responsabilidades son:

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar amenazas y violaciones de la seguridad de la información mediante el mecanismo apropiado.
- Asegurarse de ingresar información adecuada y de calidad a los sistemas según el rol desempeñado.
- Utilizar la información de la Agencia únicamente para los propósitos institucionales autorizados.
- Conocer y aplicar los lineamientos de seguridad de la Agencia.
- Realizar la eliminación adecuada de la información una vez cumplido su periodo de almacenamiento definido.
- Los usuarios deben asegurar que cuando impriman, escaneen, saquen copias o envíen faxes, en los equipos utilizados no queden documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Los funcionarios, contratistas, colaboradores y terceros de la ANT deben asegurarse de que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, que puedan contener información confidencial de la ANT.
- Es responsabilidad de todos los funcionarios, contratistas y colaboradores de la Agencia borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deberán dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

LINEAMIENTO No. 4 CONTROL DE ACCESO A LA INFORMACIÓN

Regla No.1 Cuentas de usuario y contraseñas

Las siguientes consideraciones corresponden a la creación de usuarios con un nivel de acceso estándar, denominado también un usuario convencional, cuyos privilegios

[17] Tomado de la Guía para la gestión y clasificación de los activos de información: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

corresponden entre otros al acceso a la red, a la infraestructura tecnológica, así como también a los usuarios de los sistemas de información que maneja la Agencia:

- La solicitud de creación de usuarios deberá ser proyectada desde la Subdirección de Talento Humano, en el caso de los funcionarios y desde el área respectiva del supervisor, para los contratistas, mediante una solicitud vía mesa de servicios. El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General valida la información y realiza el respectivo procedimiento, esta solicitud deberá contener como mínimo los siguientes datos:
    - Nombre completo
    - Número de identificación
    - Área o dependencia
    - Cargo a desempeñar
    - Copia digitalizada del acta de posesión

  Adicional para los contratistas:

    - Número del contrato
    - Fecha de inicio de contrato
    - Fecha finalización del contrato
    - Nombre del supervisor del contrato
    - Copia digitalizada del contrato

- Los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y contraseña, el cual es único por cada funcionario, contratista, colaborador o tercero.
- El estándar para la creación de las cuentas de usuarios se define así: Se tomará el primer nombre seguido de un punto y el primer apellido, configurado en minúscula (1ernombre.1erapellido). Si la cuenta ya existe se debe configurar el primer nombre y el primer apellido seguido de la primera letra del segundo apellido más un punto y (1ernombre.1erapellido+1erletradel2doapellido), si la cuenta también ya existe se debe configurar el primer nombre, más un punto, el primer apellido, más la primera letra del segundo apellido, seguido de los últimos tres dígitos de la cédula (1ernombre.1erpapellido+1erletradel2doapellido+###), si el nombre del nuevo colaborador contiene eñe “ñ” en su nombre o apellido esta se deberá reemplazar con una ene “n”, si el nombre o apellido contienen caracteres especiales como “ ¨ ” ó “ ´ ” estos deberán omitirse y colocar la vocal o consonante correspondiente.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, así como la SSIT, mediante la mesa de servicios, deberán mantener registro en el cual, cada uno de los responsables de los procesos (propietarios de la

información) hayan autorizado a los funcionarios, colaboradores o terceros el acceso a los diferentes sistemas de información de la entidad, en el marco de sus competencias.

- Es responsabilidad de cada usuario realizar la actualización de sus credenciales de acceso en su primer ingreso a la red de la Agencia, esto, debido a que se asigna una contraseña provisional genérica por parte del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la ANT.
- Es responsabilidad de cada usuario realizar la actualización de sus credenciales de acceso en su primer ingreso a los sistemas de información, esto, debido a que se asigna una contraseña provisional genérica.
- Es responsabilidad del usuario realizar el cambio periódico de sus credenciales de acceso.
- Las contraseñas no deberán ser reveladas ni compartidas por vía telefónica, correo electrónico o por ningún otro medio.
- Las contraseñas tendrán una caducidad de 45 días y no se podrán utilizar las últimas tres contraseñas utilizadas.
- Las contraseñas deberán cumplir con los siguientes requisitos:
    - Tener una longitud mínima de 7 caracteres alfanuméricos
    - No contener nombres o números telefónicos, ni tampoco números o letras consecutivas repetidas
    - Contener al menos un número, una letra minúscula y una mayúscula
- Se debe reportar cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
- Se debe reportar cualquier sospecha en la cual una persona esté utilizando una contraseña o un usuario que no le pertenece.
- Después de tres (3) intentos fallidos de ingreso la cuenta quedará bloqueada por un tiempo de 15 minutos y como último recurso, deberá gestionarse mediante la mesa de servicios el correspondiente desbloqueo.
- Cada persona debe hacer buen uso de sus credenciales (nombre de usuario y contraseña) y será responsable por las operaciones que se realicen con ésta.
- El uso de las credenciales es personal e intransferible, por tal motivo está estrictamente prohibido el préstamo de usuarios y contraseñas a otras personas.
- Es responsabilidad de la Secretaria General en cabeza de la Subdirección de Talento Humano enviar al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General y a la SSIT, la información del personal que se retire de la Agencia termine contrato, tome licencias o vacaciones, sea trasladado o cambie de cargo para que, de esta forma, se realicen los pertinentes bloqueos en las cuentas de los diferentes sistemas que tenga el usuario.

- Las contraseñas no pueden ser almacenadas en repositorios y en caso de estar en medio impreso, no deben estar en lugares visibles, de libre acceso y sin la seguridad adecuada.
- Las cuentas de usuario y contraseñas de administración de sistemas de información deberán ser controladas, aseguradas y almacenadas de forma segura.

Regla No.2 Gestión de acceso de usuario

- Los usuarios siempre deben realizar la autenticación para utilizar los servicios informáticos e infraestructura tecnológica.
- De acuerdo con los roles y responsabilidades definidos en la Regla No.4 responsables y dueños de activos de información del Lineamiento No. 3 Gestión de activos de información, el acceso a los activos de información estará autorizado por el propietario de la información y éste deberá solicitar la activación, modificación o desactivación del usuario vía correo electrónico.
- Los administradores de los sistemas de información deben realizar revisiones periódicas, al menos una (1) vez cada tres (3) meses, a los permisos de acceso de los usuarios, para ser contrastada con los reportes de la Subdirección de Talento Humano con el fin de realizar el trámite de actualización de roles o su inactivación.
- La red Wi-Fi está destinada para el uso exclusivo de los funcionarios, colaboradores, contratistas y visitantes, y deberá ser utilizada únicamente para fines de apoyo institucional; contará con un identificador de Red y contraseña diferenciado entre funcionarios y visitantes.
- El acceso a los servidores web y de bases de datos deben estar tipificados de acuerdo con el rol de usuario que ejerce en la entidad y está definido por la SSIT y/o el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- Se debe mantener un inventario de los usuarios que acceden a los servidores organizacionales y los periodos en los cuales están las cuentas activas en el servidor.
- Se deben crear usuarios en los sistemas para la administración de servicios web y de bases de datos, los cuales deben ser diferentes a las cuentas de los administradores o usuarios convencionales.
- Se tiene que definir la jerarquización de los usuarios para poder hacer soporte, administración y uso convencional de la infraestructura, cada usuario debe tener privilegios y gestiones diferentes de acuerdo al ciclo de vida de la información.

Regla No.3 Responsabilidades de los usuarios

- Los usuarios son responsables del uso de sus credenciales.

- Es responsabilidad de los usuarios mantener secreta la información de sus credenciales de autenticación de los diferentes sistemas a los que tenga acceso.
- El usuario deberá tener total reserva de la información que se obtenga de cualquier activo de información y que sea de carácter privado o confidencial.
- Los activos de información en papel deberán estar organizados conforme a las condiciones establecidas en la Ley General de Archivos (Ley 594 de 2000) y al Programa de Gestión Documental de la ANT.

Regla No.4 Control de acceso a sistemas y aplicaciones

- El acceso a la información de la ANT debe realizarse exclusivamente por los aplicativos o sistemas de información autorizados, utilizando el rol que le haya sido asignado; únicamente los administradores de bases de datos del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General y de la SSIT pueden acceder directamente a la base de datos de los sistemas.
- Los sistemas de información deben tener habilitados módulos de auditoria y "logs"[18] transaccionales, los cuales deben ser administrados y respaldados adecuadamente.
- Esta estrictamente prohibida la instalación de herramientas que permitan realizar seguimiento interno a los sistemas tales como Sniffers[19], KeyLoggers[20], entre otros.
- La utilización de herramientas informáticas que tengan la capacidad de inhabilitar cualquier sistema de información, así como las herramientas para extracción de datos e información desde equipos, será limitada y controlada únicamente por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- El usuario deberá mantener total reserva de los mecanismos de control de acceso y no divulgarlos a personal ajeno a la Entidad.
- Los equipos de los funcionarios que manejan información sensible para la organización deben tener los discos cifrados para su protección ante alguna pérdida o robo.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General deberá contar con un registro de eventos, en el cual almacenará todas las operaciones realizadas por los usuarios frente a los accesos a los sistemas de información de soporte y su navegación por las redes internas de la Entidad. Las mismas consideraciones procederán para la SSIT frente a los sistemas de información misionales.

[18] Logs: Registros de actividades y eventos realizados en los sistemas
[19] Definición de Sniffer: http://culturacion.com/que-es-un-sniffer/
[20] Definición de KeyLogger: https://blog.kaspersky.com.mx/que-es-un-keylogger-2/453/

- Se debe realizar monitoreo y reporte de los accesos tanto físicos como lógicos en horarios no hábiles a las áreas y sistemas donde se procesa información.
- Se debe garantizar el control de la seguridad mínima requerida sobre la información que se entregué a actores externos, para tal efecto se deberán realizar acuerdos de confidencialidad y protección de la información, además, revisiones periódicas con el fin de estar al tanto de cómo se manipula y protege la información; estas revisiones deben ser supervisadas y monitoreadas por la DGOSP y la SSIT.
- Los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información se otorgarán únicamente a aquellos funcionarios designados para dichas funciones.
- La manipulación y acceso a los códigos fuente de los sistemas de información solo estará disponible para los administradores y desarrolladores de cada sistema de información, y esta manipulación deberá ser aprobada en el Comité de Cambios, adscrito al Comité de Arquitectura Empresarial de la Agencia o quien haga sus veces.
- Los recursos de la plataforma tecnológica y los servicios de red serán operados y administrados en condiciones controladas y de seguridad; y deben permitir un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre los mismos.
- Se debe verificar que los administradores de los recursos tecnológicos y servicios de red no poseen acceso a sistemas de información en producción.
- Se debe asegurar que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

Regla No.5 Escritorio y Pantalla Limpia

- Cada vez que el usuario deje su puesto de trabajo deberá dejar bloqueado el equipo de cómputo, para evitar accesos no permitidos (aplicando la combinación de teclas Win + L ó Ctrl + Alt + Supr y seleccionando la opción de bloqueo.)
- El equipo de cómputo tendrá configurado un fondo de pantalla y un protector de pantalla definido por el área de comunicaciones (prensa) o la Secretaría General de la Agencia.
- El usuario tiene la responsabilidad de apagar el equipo, una vez culmine sus labores diarias, para cumplir así mismo con las políticas ambientales amigables con el medio ambiente; salvo en los casos en que los equipos se encuentren en procesos de ejecución extensos.

- Los funcionarios, contratistas, colaboradores y terceros de la ANT deben asegurar que sus escritorios se encuentran libres de documentos utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General realizará apagado remoto de los equipos de cómputo de la entidad, permitiendo disminuir el riesgo de incidentes de fuga de información, de igual manera contribuyendo con nuestro compromiso medioambiental y de austeridad del gasto.
- De igual manera el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General realizará limpieza remota de escritorio a los equipos de cómputo de la entidad, evitando de esta manera la exposición de información y contribuyendo con la implementación de pantallas y escritorio limpios en la Entidad.

LINEAMIENTO No. 5 SEGURIDAD DE LAS OPERACIONES

Regla No.1 Uso de Internet

- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General deberá implementar reglas de navegación para internet, en función de los perfiles de usuario definidos.
- En caso de que se identifiquen riesgos graves que afecten la infraestructura tecnológica, el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General podrá reaccionar e incorporar inmediatamente, sin previa aprobación, reglas de seguridad e informar posteriormente las acciones tomadas.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General deberá diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El acceso a internet desde los equipos institucionales deberá realizarse a través de la red propia de la Agencia, en caso de necesitar la utilización de otros equipos para este objetivo, se requiere de los permisos especiales otorgados por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General y solicitados mediante la mesa de servicio de la Agencia.
- Debe entenderse que el uso del servicio de internet es con propósitos institucionales. Sin embargo, este recurso podrá ser utilizado para fines personales, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, la imagen o la protección de la información de la Entidad.
- Los usuarios no deben visitar páginas web, descargar y almacenar contenidos que incumplan con las leyes de derechos de autor y propiedad intelectual consignadas

en el Artículo 61 de la Constitución Política de Colombia, la ley 23 de 1982, la ley 44 de 1993 y la ley 599 del 2000.

- No se permite el acceso a páginas relacionadas con pornografía, drogas, alcohol, música, concursos en la web, juegos entre otras que puedan comprometer la seguridad y el buen uso del internet en la Entidad.
- No se permite la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, software malicioso, o que generen un riesgo para la Información de la Entidad.
- El monitoreo general de la navegación realizada por los usuarios se podrá realizar como parte de las funciones de administración de la plataforma tecnológica, sin necesidad de aprobación por parte la Dirección de Gestión del Ordenamiento Social de la Propiedad, siempre y cuando exista una causa debidamente justificada que genere e riesgo.
- Cada uno de los usuarios es el directo responsable de dar el uso adecuado a este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información de la Agencia, entre otros.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General o la SSIT podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación de cada usuario, desde cualquier puerto y/o protocolo utilizado, previa aprobación de la Dirección General y la Secretaría General de la Entidad.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General podrá mantener una base de datos de direcciones WEB que son bloqueadas y consideradas peligrosas y/o malintencionadas y es deber de esta área bloquear el acceso a las mismas.
- Los funcionarios, contratistas, colaboradores y terceros, al igual que los empleados o contratistas de estos, no podrán asumir en nombre Institucional, posiciones frente a encuestas de opinión, foros u otros medios similares.
- Los funcionarios, contratistas o colaboradores que hagan parte de redes sociales virtuales como Facebook, Twitter, LinkedIn, Instagram u otros que permitan cualquier tipo de opinión no deberán publicar datos Institucionales, que no sean avalados y publicados por la Oficina de Comunicaciones.
- La mensajería instantánea de uso interno o externo deberá ser usada exclusivamente para el desempeño de las funciones asignadas. La información y los mensajes contenidos en dichas herramientas son propiedad de la ANT, quien tendrá la potestad de inspeccionar, registrar y evaluar la información intercambiada por este medio, con previa aprobación de la DGOSP, la SSIT y la

Secretaría General, la cual estará debidamente justificada y contará con los soportes y registros probatorios necesarios para tal fin.

- Por ningún motivo se puede difundir información confidencial que infrinja la ley de transparencia y acceso a la información pública.

Regla No.2 Uso de medios de almacenamiento

- El uso del almacenamiento de información en los equipos de cómputo debe ser únicamente para información de tipo Institucional, por ende, el usuario es responsable de proteger su integridad, confidencialidad y disponibilidad.
- Se podrá realizar uso del almacenamiento de datos en la nube de forma institucional.
- La ANT debe garantizar que la información confidencial o reservada cuenta con medios de almacenamiento seguros, para lo cual debe encaminar iniciativas de diagnóstico, prevención y corrección de posibles anomalías presentadas en los activos de información institucionales.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe garantizar la correcta actualización del software antivirus y su base de definición de nuevos virus; de igual manera, debe monitorear el software antivirus, para que permanezca configurado y soporte el escaneo automático en las unidades de almacenamiento y también para impedir la reproducción automática de archivos ejecutables.
- Los servidores base que soporten los sistemas de información estratégicos, misionales, y de apoyo de la Agencia, así como las bases de datos del ambiente de producción, deben tener asignados procesos de copia de seguridad (backups) diario diferencial, semanal total y un full mensual en el cual se deberán llevar los logs correspondientes, esta acción deberá ser realizada por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- La ANT se compromete a mantener la información almacenada en sus bases de datos bajo los siguientes controles técnicos:
    - Mantener una VLAN[21] exclusiva para los sistemas de seguridad de la organización, es decir, que ésta no tendrá interacción con otros sistemas de información o con otros segmentos de red.
    - Las bases de datos y sus sistemas manejadores (DBMS) deben ser almacenadas en el Centro de Datos de la Agencia, el cual cuenta con acceso restringido y controlado; también pueden ser alojadas en servicios de plataforma como servicio o infraestructura como servicio en la nube
    - La infraestructura tecnológica de la ANT debe contar con firewall de alta tecnología para la protección de sus equipos, con dispositivos de seguridad

[21] Definición de VLAN: http://es.ccm.net/contents/286-vlan-redes-virtuales

de protección y control de bases de datos propios y otros controles que garanticen la seguridad de la información.

- La información sensible de las bases de datos será cifrada bajo un algoritmo AES de 128 bits[22], el cual ofrece seguridad y no limita el tamaño del archivo a cifrar, permitiendo que no sea legible para otros sistemas o personas.

Regla No.3 Copias de Respaldo

- La Subdirección de Sistemas de Información y el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, deberán contar con la clasificación de los activos de información, a los cuales, y de acuerdo con su clasificación, se les establecerá periodicidad, prioridad, medio de respaldo y método de generación de copia de seguridad.
- Los responsables de los activos de información, activos tecnológicos y recursos informáticos deben acatar las estrategias definidas por el gobierno del dato para la correcta y adecuada generación, retención y rotación de las copias de respaldo de la información definidas por la Entidad.
- Es responsabilidad del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General y la SSIT, llevar a cabo el desarrollo de las políticas y los procedimientos para realizar copias de respaldo, así como las pruebas de recuperación para comprobar su integridad y la posibilidad de uso ante la ocurrencia de desastres.
- Cada vez que se realice una reasignación de un equipo a un usuario diferente, la información contenida en el mismo debe ser resguardada en un medio de almacenamiento alterno e inmediatamente el equipo debe ser formateado.
- Los equipos cliente deben contar con una partición de disco duro adicional (D), la cuál será la unidad de trabajo del usuario, para así permitir que un agente de red se encargue de manera periódica e incremental de realizar copias de respaldo de dichas unidades, los anteriores procesos deben realizarse en jornadas nocturnas o en periodos de baja utilización.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General y la SSIT deberán definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información en caso de que éstas sean almacenadas externamente.

Regla No.4 Instalación de software

- Los usuarios no pueden realizar instalación de ningún tipo de software en los equipos de cómputo asignados para el desarrollo de las actividades institucionales de la ANT.

[22] https://www.adslzone.net/2016/04/19/las-cinco-mejores-aplicaciones-cifrar-archivos-windows/

- Las actividades correspondientes a actualizaciones de software requieren ser planificadas con anterioridad por parte del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, por tanto, deben ser informadas con anticipación a los usuarios utilizando los mecanismos adecuados (Intranet y/o correo institucional) y deben ser realizadas de forma centralizada y automatizada.
- Las solicitudes de instalación de software deben estar autorizadas por el jefe inmediato del usuario y aprobadas por la SSIT y el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe mantener actualizado el inventario de software e informar a la DGOSP y a la SSIT, para garantizar que el software utilizado por la Agencia se encuentra debidamente licenciado.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe realizar el monitoreo del software y las actualizaciones instaladas en las máquinas de los clientes y servidores de forma periódica.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General es el área encargada exclusivamente de la instalación del software requerido en las diferentes direcciones y oficinas de la ANT, incluyendo las Unidades de Gestión Territorial; y es a su vez, la encargada de la administración del licenciamiento del software adquirido por la Agencia.

Regla No.5 Protección contra códigos maliciosos

- La ANT a través del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria Generaly la Subdirección de Sistemas de Información, proveerán los recursos necesarios para garantizar la protección de la información y los recursos de procesamiento, adoptando los controles necesarios para evitar su divulgación, modificación o daño permanente ocasionados por la contaminación y/o el contagio de software malicioso.
- La ANT a través del Equipo de Soporte e Infraestructura tecnológica, debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos del proveedor del servicio.
- La ANT a través del Equipo de Soporte e Infraestructura tecnológica, debe garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- La ANT a través del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria Generaly, debe garantizar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- La ANT a través del Equipo de Soporte e Infraestructura tecnológica, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- El usuario no deberá hacer uso de software que no sea instalado por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, ya que esto puede llevar a infecciones por virus u otro tipo de código malicioso.
- Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso.
- Para evitar problemas de códigos maliciosos a través de medios extraíbles o correo electrónico, los usuarios, deben realizar la verificación respectiva de los archivos a través del software de antivirus instalado en sus equipos cada vez que instalen o conecten un dispositivo o se reciban archivos sospechosos por correo electrónico.
- Por ningún motivo se permite la descarga de software sin la debida autorización y/o revisión por parte del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar inmediatamente al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General con el fin de adoptar las medidas de control correspondientes.

Regla No.6 Separación de entornos de desarrollo, prueba y producción

- La ANT en cabeza de la SSIT y con apoyo del Equipo de Soporte e Infraestructura tecnológica, debe disponer de diferentes ambientes para el desarrollo, pruebas y puesta en producción de las aplicaciones para reducir los riesgos de acceso o cambios no autorizados en el entorno operacional, prevenir fallos e implementar controles. Dichas aplicaciones deben correr en ambientes física/lógicamente separados con accesos lógicos diferentes para cada uno de los ambientes y teniendo en cuenta los controles para el intercambio de información entre los ambientes de desarrollo y producción, en especial los datos sensibles no deben ser copiados hacia ambientes de desarrollo o pruebas. Los sistemas de pruebas deben emular lo más cercano posible a los ambientes de producción, entre otros, para prevenir situaciones en las cuales el software desarrollado presente comportamientos y/o errores diferentes en esos ambientes; para esto se debe utilizar la guía de desarrollo seguro del MINTIC.

- Se recomienda la utilización de componentes de cifrado de datos o anonimización para los ambientes de pruebas, de tal forma que los datos de producción no sean conocidos por los equipos de desarrollo y parametrización.

LINEAMIENTO No.6 SEGURIDAD DE LAS COMUNICACIONES E INTERCAMBIO DE INFORMACIÓN

Regla No.1 Acceso a la red institucional

- Se debe definir una segmentación de la red inalámbrica: (a) la red de funcionarios y (b) la red de visitantes en la cual se establezcan accesos limitados a la infraestructura local. Esta red no podrá alcanzar la VLAN de base de datos de la ANT.
- Solo tendrán acceso a la red de la Agencia, los equipos previamente autorizados por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General; el acceso a la red inalámbrica podrá autorizarse o limitarse por la dirección MAC[23] o por reserva de IP para usuarios fijos. del equipo.
- La red inalámbrica de la Entidad deberá heredar las políticas de filtrado y seguridad configuradas en el firewall de la Entidad.
- La contraseña de la red inalámbrica de visitantes de la ANT deberá ser cambiada con una periodicidad de 30 días por parte del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General de la Secretaria General.
- Los puertos físicos de los equipos activos que no estén en uso deben estar desactivados.
- Las conexiones que se requieran para intercambiar información con cualquier otra entidad deben estar cifradas y la comunicación debe ser monitoreada.
- Las especificaciones técnicas del intercambio de información entre entidades deben realizarse con la debida formalidad utilizando los acuerdos de intercambio establecidos y aprobados por la DGOSP, la SSIT y la Secretaría General.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe gestionar las claves de Administración para los equipos de impresión y las multifuncionales que cuenten con claves para que solo el personal autorizado haga uso de estos equipos y evitar que personal no autorizado acceda a la misma.
- Los funcionarios, contratistas, colaboradores y terceros de la ANT, antes de contar con acceso lógico por primera vez a la red de datos de la Entidad, deben contar con la solicitud de creación de usuarios debidamente diligenciada y autorizada, así como el Acuerdo de Confidencialidad firmado previamente.

[23] Dirección MAC: https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.es

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Entidad deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- El Acceso a la red Institucional desde las UGT ubicadas en diferentes puntos del país, se realizarán mediante canal MPLS.

Regla No.2. Uso de correo electrónico

- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General proveerá un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La Subdirección de Sistemas de Información y la Secretaria General, generarán campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.
- Todos los funcionarios y contratistas deben tener asignada una cuenta de correo institucional para el desarrollo de sus funciones u obligaciones.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, contratista, colaborador o tercero, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- La información enviada y recibida por correo electrónico institucional es de propiedad de la Agencia, por tal motivo este no debe ser usado para temas personales.
- Por ningún motivo el usuario debe utilizar cuentas de correo electrónico gratuitas o personales para el intercambio de información institucional, salvo para los casos autorizados por la SSIT y/o el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- Todos los correos enviados deben respetar el estándar de formato e imagen corporativa definidos por la Entidad y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Los usuarios deberán abstenerse de abrir correos electrónicos de origen desconocido. Estos deberán ser reportados al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General. De igual forma, es deber del usuario no abrir, ni renviar archivos adjuntos de correos electrónicos de los cuales no se tengan la certeza de su procedencia.

- Se acepta el uso eventual de cuentas de correo externas (Hotmail, Gmail, Yahoo, entre otras) para fines personales, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva, y que no interfiera con las actividades de la Entidad. Además de no violar ninguna de las políticas o lineamientos de seguridad de la información de la Agencia.
- No se podrán enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales. Únicamente, la Dirección General, Secretaria General, Subdirección de Talento Humano y el Área de Prensa son las áreas autorizadas para enviar correos electrónicos masivos.
- Todas las actividades que sean realizadas desde la cuenta de correo institucional serán responsabilidad del propietario de la misma.
- Por ningún motivo el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, solicitará las claves de los correos institucionales a los funcionarios, contratistas, colaboradores o terceros de la Entidad.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General puede solicitar autorización para el cambio de la contraseña en caso de ser requerido.
- La información confidencial debe tener los controles necesarios para ser enviada por correo electrónico, en el caso de no conocerse la confidencialidad de la información ésta puede ser consultada con el apoyo de la SSIT o del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.
- El administrador del correo electrónico revisará periódicamente las cuentas de correo electrónico activas, contrastando con los tiempos de caducidad de cada cuenta de correo, el listado de dichas cuentas se obtiene de las incidencias en la creación de cuentas de correo obtenidas en la plataforma de mesa de servicios.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, en el marco de sus funciones de administrador de la plataforma de correo electrónico, podrá hacer el seguimiento y monitoreo que considere necesario para el correcto funcionamiento del servicio. La Agencia podrá suspender el servicio de correo electrónico sin previo aviso, en caso de que se demuestre un mal uso del servicio por parte del usuario.
- El uso del correo electrónico institucional debe hacerse de manera adecuada y en ningún caso deberá ser usado como un chat para intercambio de información inmediata.

Regla No.3 Dispositivos móviles

- Los usuarios no deben utilizar equipos de comunicación diferentes a los autorizados por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General para acceder a redes internas o externas de la Entidad.
- Las estaciones de trabajo ya sean equipos portátiles o equipos de escritorio asignados por la Entidad, no deberán ser prestados a personas externas.
- Los equipos portátiles de la Agencia y los que sean llevados por contratistas y/o terceros, deben contar con software antivirus, cifrado de datos, restricción en la ejecución de aplicaciones y protección física mediante la guaya de seguridad. Para el cifrado de datos se recomienda que se encuentre cifrada bajo un algoritmo AES de 128 bits[24]
- Los funcionarios, contratistas, colaboradores y terceros 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 por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General. Dejando registro documentado de la autorización.
- Preferiblemente, se debe contar con certificados seguros SSL y/o firma digital para la página web para las personas que posean firmas digitales para comunicados externos e internos a través de Orfeo, así mismo, para las firmas digitales de los servicios web que la Entidad exponga a entes externos y otros canales cifrados para cualquier tipo de comunicación con otros actores.
- 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.
- El personal autorizado únicamente deberá establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.
- Los equipos portátiles propiedad de la Agencia son de responsabilidad del usuario a quien se autoriza su transporte, por tal razón, no debe dejarse a la vista en el interior de los vehículos y en casos de viaje siempre se deberán llevar como equipaje de mano.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos.
- En caso de pérdida o robo de un equipo portátil o disco duro externo propiedad de la Agencia el usuario deberá se debe informar inmediatamente al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General para que este proceda con los bloqueos respectivos, así como a la DGOSP, la SSIT y la

[24] https://www.adslzone.net/2016/04/19/las-cinco-mejores-aplicaciones-cifrar-archivos-windows/

Secretaría General e instaurar inmediatamente la denuncia ante la autoridad competente.

Regla No.4 Transferencia de Información

- El intercambio y transferencia de información institucional solo se realizará por los canales de comunicación autorizados por la DGOSP, la SSIT y la Secretaria General; entre estos canales se encuentran los convenios interadministrativos en los que se establecen cláusulas de responsabilidad, deberes y derechos. En cualquier caso, esta podrá ser acordada entre las partes involucradas en cabeza de la Dirección de Gestión del Ordenamiento Social de la Propiedad, Subdirección de Sistemas de Información y/o la Secretaría General.
- La información intercambiada debe cumplir con los estándares para los datos, mensajes y documentos; esta información de dominio público debe contar con la seguridad necesaria que avale su legitimidad, integridad y confiablidad.
- El contenido de los archivos enviados por los canales institucionales es responsabilidad de cada propietario de la información.
- Los funcionarios, contratistas, colaboradores y terceros involucrados en el proceso de intercambio de información deben cumplir con los lineamientos legales para evitar trasferir o revelar información confidencial.
- Las herramientas de comunicación institucional de la ANT son propias y de uso exclusivo para las labores de la Entidad; la ANT es propietaria de la información que se encuentre en estos medios, y el usuario es responsable del manejo que les da a estas herramientas.
- Los propietarios de los activos de información deben velar porque la información sea protegida de divulgación no autorizada por parte de los terceros a quienes se le entrega, verificando el cumplimiento de las cláusulas relacionadas en los contratos, acuerdos de confidencialidad o acuerdos de intercambio establecidos.
- Los propietarios de los activos de información deben asegurar que los datos de información personal sólo puedan ser entregados a terceros, previo consentimiento de sus titulares, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- 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 la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información deben autorizar los requerimientos de información a la Entidad por terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- Los propietarios de los activos de información deben asegurarse de que el Intercambio de información (digital) solamente se realice si se encuentra autorizado y dando cumplimiento a las políticas de administración de redes, de acceso lógico y de protección de datos personales, así como el tramite de intercambio de información.
- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.
- Los terceros con quienes se intercambia información deben darle manejo adecuado a la información recibida, en cumplimiento de las políticas de seguridad, de las condiciones contractuales establecidas y el trámite de intercambio de información.
- Los terceros con quienes se intercambia información deben destruir de manera segura la información suministrada, una vez ésta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.
- Los funcionarios, contratistas, colaboradores y terceros de la ANT no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Entidad.
- No está permitido el intercambio de información sensible por vía telefónica.

Regla No.5 Compromiso de usuario

- La Subdirección de Talento Humano y el Grupo Interno de Trabajo – Coordinación para la Gestión Contractual de la Entidad deben certificar, según corresponda, que los funcionarios, contratistas, colaboradores y/o terceros relacionados tengan firmado el documento “Compromiso de usuario en aplicativos, herramientas informáticas o información institucional”.
- Todos los usuarios de sistemas de información y de la red de datos de la ANT, deberán firmar un acuerdo de Confidencialidad el cual será entregado y socializado por la Subdirección de Talento Humano y la SSIT.

Regla No.6 Gestión de seguridad de las redes

- Las redes junto a los servicios de red deben estar asegurados y controlados con mecanismos de seguridad y acuerdos de servicio (ANS), garantizando la protección de los sistemas de información y aplicativos.
- La información que es transportada por la red de datos es monitoreada para garantizar así la seguridad de la misma.
- Las redes de la ANT deben estar segmentadas de manera lógica teniendo en cuenta los usuarios, sistemas de información (aplicaciones, bases de datos, etc.), accesos externos autorizados y el intercambio de datos con otras entidades, estos

segmentos se deben asegurar con los sistemas de seguridad perimetral gestionados por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General.

- Los equipos tecnológicos que almacenen y procesen información confidencial, deberán mantenerse en una red lógica aislada y segura.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General será el administrador u operador de los equipos activos y del firewall; y debe respaldar periódicamente la configuración de éstos, asegurando su disponibilidad, confidencialidad e integridad.
- Los equipos activos y firewall deben ubicarse en áreas seguras, con restricciones de acceso físicas e ingreso autorizado solo para los administradores.
- Los cambios en las configuraciones de los equipos activos y firewall deben llevar un registro, así mismo se debe realizar una copia de la configuración anterior y una posterior al cambio, en mínimo dos lugares físicos distintos con acceso restringido.
- Por ningún motivo los usuarios pueden usar herramientas de software o hardware para saltar o vulnerar los controles de seguridad aplicados en la Agencia sin la autorización del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General. Esto podrá ser catalogado como un incidente de seguridad y podrá acarrear los procesos a que haya lugar.
- La red inalámbrica debe contar con autenticación y cifrado en la trasmisión de información, para este último se recomienda que se encuentre cifrada bajo un algoritmo AES de 128 bits[25].
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

LINEAMIENTO No. 7 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Regla No.1 Adquisición de sistemas de información

- 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 DGOSP y la SSIT

[25] https://www.adslzone.net/2016/04/19/las-cinco-mejores-aplicaciones-cifrar-archivos-windows/

- Se deben contemplar las características de seguridad que requiere la Agencia y realizar un proceso formal de pruebas, que haga parte del proceso de evaluación de las ofertas.
- Se debe adquirir productos de software únicamente con proveedores acreditados o productos ya evaluados en materia de seguridad de la información.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General 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.

Regla No.2 Desarrollo de sistemas de información

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la Entidad formalmente asignada.
- Los desarrollos realizados por personal interno o externo contratado y administrados por la Agencia deben considerar las políticas de derechos de autor que rigen la Republica de Colombia y/o las cláusulas contractuales estipuladas en los contratos de desarrollo.
- Todo desarrollo de Sistemas de Información deberá ser avalado y aprobado en su pertinencia desde la SSIT
- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que en los sistemas de información construidos no se permitan conexiones simultáneas con el mismo usuario.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.
- Los cambios solicitados a los sistemas de información deben pasar por un proceso de pruebas antes de ser aplicados en producción y se debe cumplir con el ciclo establecido en las políticas de desarrollo desarrolladas por la DGOSP.
- Antes del paso a producción de los sistemas de información, los propietarios son responsables 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.

- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe certificar que la información a ser entregada a los desarrolladores para sus pruebas sea enmascarada y no revele información confidencial de los ambientes de producción.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.
- 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.
- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Previo a la puesta en producción de los sistemas e información, los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- La gestión de los repositorios de las plataformas misionales es realizada por la SSIT y la gestión de las plataformas de apoyo es realizada por el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, así mismo, le corresponde a cada una asegurar que los sistemas de información desarrollados cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- 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; este debe contar con estándares mínimos de seguridad (aplicando los lineamientos de desarrollo seguro propuestos por MINTIC).
- Con el fin de proporcionar una visión clara desde el comienzo del ciclo de desarrollo de software, los responsables de la construcción de soluciones de software deben crear y mantener una metodología que controle el ciclo completo, que incluya la definición de requerimientos de seguridad y la aplicación de buenas prácticas de desarrollo seguro de software.
- Se debe nombrar un custodio de los códigos fuente de los sistemas de información que maneja la ANT.
- Se debe mantener una biblioteca que conserve las versiones del código fuente y de los sistemas de información de la Agencia, la cual estará alineada con el Repositorio de Arquitectura Empresarial definido por la Dirección de Gestión de Ordenamiento Social de Propiedad.

Regla No.3 Mantenimiento de sistemas de información

- La Secretaría General 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.
- La información que se encuentra en los sistemas de información en ambiente de producción no puede ser disminuida en los niveles de protección, ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como para el desarrollo de soluciones.

- 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 software a que haya lugar; para lo cual se debe presentar el procedimiento en el Comité de Cambios de la ANT, la mesa técnica o quien haga sus veces.
- Cuando se realicen cambios que modifiquen los sistemas de información, se debe informar al usuario del activo de información que procese dicho activo.
- Los cambios a los sistemas de información se deben implementar en ventanas de mantenimiento para no afectar la disponibilidad del servicio.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software desarrollado; dicho soporte debe contemplar tiempos de respuesta aceptables.

LINEAMIENTO No. 8 INCIDENTES SEGURIDAD DE LA INFORMACIÓN

Regla No.1 Reporte y manejo de incidentes de seguridad de la información

- El usuario que tenga conocimiento o sospecha de alguna ocurrencia de filtración o vulnerabilidad en los activos de información deberá reportarlo inmediatamente al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, mediante la mesa de servicio, quienes elevaran el caso a la Dirección de Gestión del Ordenamiento Social de la Propiedad y/o a la Subdirección de Sistemas de Información.
- Cualquier incidente generado durante la utilización u operación de los activos de información de la ANT que afecte su integridad, confidencialidad o disponibilidad, deberá ser reportado al Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, quienes se encargaran de investigar el posible incidente de seguridad y remitirán un informe a la Dirección de Gestión del Ordenamiento Social de la Propiedad, a la SSIT y a la secretaría General de la Entidad.
- La Dirección de Ordenamiento Social, la SSIT y la Secretaría General, definirán las responsabilidades y los procedimientos a seguir para la gestión de incidentes de seguridad de la información, así mismo organizarán el equipo de respuesta a incidentes, de manera que se asegure una respuesta rápida, ordenada y efectiva frente a los incidentes que se puedan llegar a presentar.
- El equipo conformado para la respuesta a incidentes deberá, con el apoyo del Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo.

- 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 del incidente que amerite ser tratado; los tipos de incidentes que pueden considerase graves se presentan en la tabla a continuación[26]:

Categoría	Criterios de clasificación Se asigna la categoría si:
Fuga de información	-Se evidencia divulgación no autorizada de información de la Agencia -Prácticas de Ingeniería social
Acceso no autorizado	- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso - Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario - Ingreso de personal no autorizado a las instalaciones de la Agencia
Ataque	- Se evidencia intención de afectar un recurso específico - Se modifica la imagen institucional en aplicaciones de la Agencia - No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio (Clasificación asociada al ítem 3 Denegación de servicio) - Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web - Se evidencia borrado alteración de la información de terceros.
Código dañino	- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información - El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso
Denegación de servicio	- El sistema de información no responde por alta cantidad de peticiones - El sistema de información se encuentra lento
Robo o pérdida	- Se presenta robo o pérdida de información confidencial. - Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida

[26] https://www.cert.uy/inicio/incidentes/que_es-un-incidente/

	- Se presenta robo o pérdida de elementos personales en las instalaciones de la Agencia
Alarmas de sistemas de monitoreo	- Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas
Usos inadecuados	- Se ingresa texto copiado de internet en documentación oficial de la Agencia, sin registrar la fuente - Se publican comunicados en nombre de la Entidad sin revisión y aprobación de la Oficina Asesora de Comunicaciones

Tabla 1- Categorías de Incidentes de Información

LINEAMIENTO No. 9 SEGURIDAD DE LA INFORMACIÓN, EN RELACIÓN CON LOS PROVEEDORES

Regla No.1 Relaciones con los proveedores

- Se debe incluir un acuerdo formal de niveles de servicio en seguridad de la información, en el que se detallen los compromisos frente al cuidado de los recursos de Información de la Agencia, los requisitos de seguridad de la información con los que deben cumplir los proveedores de servicios y las sanciones en caso de incumplimiento. Dicho acuerdo debe ser divulgado a todas las áreas que adquieran o supervisen los recursos y/o servicios tecnológicos.
- El cumplimiento de los niveles de servicio de seguridad de la información de terceros debe ser verificado y controlado permanentemente por quienes ejerzan las funciones de supervisión de los contratos suscritos por la ANT; cuando la supervisión sea contratada, se debe incluir esta obligación dentro de los contratos. En el caso en que la supervisión sea realizada por funcionarios de la Agencia, se entiende que el cumplimiento de la política está incorporado dentro de sus obligaciones como funcionario y como supervisor.
- Todos los requisitos de seguridad de la información pertinentes deben estar establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de la ANT.

LINEAMIENTO No. 10 SEGURIDAD INFORMÁTICA EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Regla No.1 Continuidad de la seguridad información

- La ANT deberá realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente, proponer estrategias de recuperación en caso de activarse el plan de contingencia o continuidad.
- La ANT deberá 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.
- La estrategia de recuperación 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.
- 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.
- La ANT debe validar que los planes de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- La ANT analizará y establecerá los requerimientos de redundancia para los sistemas de información críticos y la plataforma tecnológica que los apoya.
- La ANT debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumpla los requerimientos de la Agencia.
- La ANT, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad.

LINEAMIENTO No. 10 TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales” y del artículo 13 Decreto 1377 de 2013, la Agencia Nacional de Tierras – ANT, desarrolla la política y lineamientos generales para el tratamiento de datos personales.

Los datos del responsable del tratamiento y protección de los datos personales:

Entidad: Agencia Nacional de Tierras
Dirección: Calle 43 No.57-41, Bogotá, Colombia
Teléfono: (57 - 1) 5185858, opción 0, y a nivel nacional en 01-8000-933-881.

Página Web: www.agenciadetierras.gov.co
Correo electrónico: info@agenciadetierras.gov.co
atencionalciudadano@agenciadetierras.gov.co

Regla No.1 Finalidad de los Datos

La Agencia Nacional de Tierras – ANT, es la Entidad responsable del tratamiento y protección de los datos personales que registre y almacene, y hará uso de los mismos únicamente para las finalidades para las que se encuentra facultado, especialmente las señaladas a continuación, contando previamente con la autorización del titular de los datos personales:

1. Para los fines administrativos y misionales de la Entidad.
2. Caracterizar ciudadanos y grupos de interés, para adelantar estrategias de mejoramiento en los trámites y en la prestación del servicio.
3. Gestionar y dar respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la ANT.
4. Conocer y consultar la información del titular del dato que repose en las bases de datos de entidades públicas o privadas.
5. Adelantar encuestas de satisfacción de usuarios.
6. Enviar información de interés general.
7. Enviar mensajes con contenidos institucionales, notificaciones, información relevante para el titular y demás información relativa al portafolio de servicios de la Agencia, a través de correo electrónico y/o mensajes de texto al teléfono móvil.

NOTA. Cualquier otro tipo de finalidad que se pretenda dar a los datos personales registrados por la ANT, deberá ser informado previamente en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato, según sea el caso, teniendo en cuenta los principios legales para el tratamiento de los datos personales.

Regla No. 2 Derechos de los Titulares de los Datos Personales.

La Agencia Nacional de Tierras – ANT, garantiza al titular de datos personales, el goce de los derechos que se enlistan a continuación:

1. Conocer, actualizar, rectificar, suprimir el dato y revocar la autorización. Este derecho se podrá ejercer también, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
2. Solicitar prueba de la autorización otorgada al responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, como lo es el caso de: Información requerida por una entidad pública o administrativa en

ejercicio de sus funciones legales o por orden judicial; Datos de naturaleza pública; Casos de urgencia médica o sanitaria; Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; Datos relacionados con el Registro Civil de las Personas.

3. Ser informado del uso y tratamiento dado a sus datos personales, previa solicitud realizada a la ANT a través de los canales de servicio.
4. Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento de los datos se ha incurrido en conductas contrarias a la ley y a la Constitución.
5. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.
6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Regla No. 3 Responsables de Gestionar las Peticiones, Quejas y Reclamos sobre el Tratamiento de Datos Personales.

El Equipo de Servicio al Ciudadano de la Secretaría General de la ANT, es el responsable de atender y gestionar las peticiones, quejas y reclamos sobre tratamiento de datos, los cuales pueden ser recibidos mediante los canales dispuestos por la Entidad, así:

Escrito: Comunicación enviada a la Calle 43 No.57-41, Bogotá, Colombia.

Presencial: En las instalaciones de la Agencia Nacional de Tierras, ubicadas en la Calle 43 No.57-41, Bogotá, Colombia.
Adicionalmente, lo ciudadanos pueden dirigirse al Centro Integrado de Servicios de Chaparral Tolima, a las Unidades de Gestión Territorial de la Entidad, en las ciudades de: Pasto, Villavicencio, Medellín, Cúcuta y Montería; y en los Puntos de Atención de Tierras en: Sincelejo, Mocoa, Arauca, Florencia y Tumaco.

Telefónico: En la línea (+57 1) 5185858, opción 0, en la ciudad de Bogotá y a nivel nacional en el número 018000-933881.

Virtual: Portal web www.agenciadetierras.gov.co, correo electrónico info@agenciadetierras.gov.co y atencionalciudadano@agenciadetierras.gov.co

Regla No. 4 Gestión de la Política de Tratamiento y Protección de Datos.

La Agencia Nacional de Tierras – ANT, garantiza a los ciudadanos, el derecho de acceso a sus datos personales registrados en la Entidad, previa verificación de la identidad del titular, su causahabiente y/o representante. Este derecho se hace efectivo mediante petición del ciudadano, haciendo uso de los canales dispuestos por la Entidad para este fin, registrados en la Regla 3 (Responsables de Gestionar las Peticiones, Quejas y Reclamos sobre el Tratamiento de Datos Personales) del presente documento, la consulta debe ser realizada a través de comunicación dirigida a la Agencia Nacional de Tierras con el nombre completo del titular, la descripción de la consulta, dirección de residencia y teléfono de contacto

Independientemente del mecanismo utilizado para la radicación de solicitudes de consulta, la Entidad dará respuesta a la petición del ciudadano en un periodo máximo de diez (10) días hábiles contados a partir del día siguiente a la fecha de radicación de la solicitud. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Regla No. 5 Recopilación, Actualización y Rectificación de Datos.

La Agencia Nacional de Tierras – ANT, podrá hacer recopilar información de ciudadanos asistentes a las ventanillas de Servicio al Ciudadano de la ANT y de los que se comunican a través del call center de la Entidad.

A su vez se solicita a los Titulares de los datos, de manera expresa, libre y voluntaria autorice el tratamiento de datos personales sensibles como los descritos en el artículo 5 de la ley 1561 de 2012, al tenor de acuerdo con lo dispuesto en el artículo 6 de la misma ley.

La Agencia Nacional de Tierras – ANT, como responsable del tratamiento de los datos personales, deberá rectificar y actualizar a solicitud del titular la información que reporte como incompleta o inexacta. Para estos efectos, el titular o su causahabiente y/o representante, señalará las actualizaciones y rectificaciones a que dieran lugar, haciendo uso de los canales dispuestos por la Entidad y presentados en la Regla 3 (Responsables de Gestionar las Peticiones, Quejas y Reclamos sobre el Tratamiento de Datos Personales) del presente documento, la solicitud debe ser realizada a través de comunicación dirigida a la Agencia Nacional de Tierras con el nombre completo del titular, la descripción de la solicitud, dirección de residencia y teléfono de contacto.

Si la solicitud o reclamo resulta incompleto, se le requerirá dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

Las solicitudes de actualización, corrección, rectificación o supresión de los datos serán contestadas dentro de los diez (10) días hábiles siguientes, contados a partir del día siguiente a la fecha de su recibo del reclamo completo. Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Regla No. 6 Datos Personales de Niños, Niñas y Adolescentes

Es posible que la Agencia Nacional de Tierras – ANT, reciba o haya recibido datos de niños, niñas y adolescentes que acceden a sus productos y servicios. El suministro de datos personales de niños, niñas y adolescentes es de carácter facultativo, tanto para ellos como para quienes actúen a su nombre.

La Agencia Nacional de Tierras- ANT, velará por el uso adecuado de los datos personales de los niños, niñas y adolescentes y respetará en su tratamiento el interés superior de aquellos, asegurando la protección de sus derechos fundamentales y, en lo posible, teniendo en cuenta su opinión como titulares de sus datos personales.

Regla No. 7 Datos Personales Sensibles

Dada la naturaleza de algunos de los procesos de la Agencia, es posible que reciba datos personales sensibles frente a los cuales se advierte que su suministro es de carácter facultativo y, en caso de suministrarlos, su tratamiento se efectuará con las finalidades antes mencionadas.

Para controlar y registrar el ingreso, permanencia y salida de las instalaciones de la Agencia en desarrollo de nuestro sistema de seguridad, se hace necesario el registro de datos personales, lo que puede incluir el suministro verbal de datos básicos de identificación, la toma de una fotografía, huella, y la utilización de medios de videovigilancia, según el caso. En estos eventos, mediante carteleras o avisos o verbalmente, según el caso, se informará la finalidad y el tratamiento de los datos así recaudados.

Regla No. 8 Supresión de Datos.

Los Titulares de la información podrán solicitar a la Agencia Nacional de Tierras – ANT, en cualquier momento y cuando consideren que los datos no están recibiendo un tratamiento adecuado, o los mismos no son pertinentes o necesarios para la finalidad para la cual fueron recolectados, la supresión de sus datos personales mediante la presentación de una petición o un reclamo a través de los canales presencial, escrito, virtual y telefónico.

No obstante, la solicitud de supresión de datos no procederá cuando el titular tenga un deber legal o contractual de permanecer en la(s) base(s) de datos de la Entidad por un impedimento en actuaciones administrativas o judiciales relacionadas a obligaciones fiscales, investigación de delitos o actualización de sanciones administrativas. Si vencido el término legal respectivo, no se han eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la supresión de los datos personales.

Regla No. 9 Almacenamiento de Datos Personales.

La ANT solicita los datos necesarios para el ejercicio de sus funciones, en algunos casos, puede solicitar información adicional y sensible, la cual es de libre y voluntaria entrega por parte del titular del dato. Una vez suministrados sus datos personales, los mismos son almacenados en la base de datos pertinente. Las bases de datos se encuentran debidamente protegidas mediante equipos de infraestructura y de acuerdo con los lineamientos de seguridad definidos por la entidad velando por su confidencialidad, seguridad, acceso y circulación restringida.

Regla No. 10 Modificaciones a las Políticas de Tratamiento de Datos Personales.

La Agencia Nacional de Tierras – ANT, se reserva el derecho de modificar, en cualquier momento, de manera unilateral, sus políticas y procedimientos de tratamiento de datos personales. Sin embargo, cualquier cambio será publicado y anunciado. Además, se conservarán las versiones anteriores de la presente políticas de tratamiento de datos personales. El uso continuo de los servicios o la no desvinculación de los mismos por parte del titular del dato una vez notificados los nuevos lineamientos de la entidad, constituyen la aceptación de la misma.

Regla No. 11 Revelación de la Información.

El titular del dato, con la aceptación de esta política de tratamiento de datos personales, declara conocer que la ANT, puede suministrar esta información a las entidades

vinculadas y aliadas y a las entidades judiciales o administrativas y demás entes del Estado que, en ejercicio de sus funciones, soliciten esta información. Igualmente, acepta que pueden ser objeto de procesos de auditoría interna o de auditoría externa por parte de empresas encargadas de este tipo de control. Lo anterior, sujeto a la confidencialidad de la información.

3. CUMPLIMIENTO

3.1 Cumplimiento de requisitos legales

- Los funcionarios, contratistas, colaboradores y terceros 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 terceros.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General debe realizar el control del licenciamiento del software instalado en todos los equipos de cómputo la agencia.
- Se debe mantener alineación del conjunto de las licencias de los productos instalados en la agencia entre los sistemas de Gestión de Servicios (Aranda) y el repositorio de Arquitectura Empresarial de la Agencia.
- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General realizará revisiones periódicas del software instalado en los equipos de cómputo la agencia.

3.2 Revisión de cumplimiento de la seguridad de la información

- El Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, 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 o correctivas necesarias.
- La SSIT y el Equipo de Infraestructura y Soporte Tecnológico de la Secretaria General, 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 Secretaría General de la Entidad.

HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
19-09-2017	01	Primera versión del documento.

Elaboró: Hilda Ramirez Villegas	**Revisó:** William Sandoval Sandoval	**Aprobó:** Juliana Cortés Guerra
Cargo: Contratista Secretaria General	**Cargo:** Subdirector de Sistemas de Información de Tierras	**Cargo**: Directora de Gestión del Ordenamiento Social de la Propiedad
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**
Elaboró: Francisco Rodriguez Eraso		
Cargo: Contratista Subdirección de Sistemas de Información de Tierras		
Firma: **ORIGINAL FIRMADO**		
Elaboró: Erika Ladino Garzón		
Cargo: Contratista Subdirección de Sistemas de Información de Tierras		
Firma: **ORIGINAL FIRMADO**		
Elaboró: Victor Valencia Gutierrez		
Cargo: Contratista Subdirección de Sistemas de Información de Tierras		
Firma: **ORIGINAL FIRMADO**		