POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

TABLA DE CONTENIDO

INTRODUCCIÓN 4
1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 5
2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN. 5
3 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
4 SEGURIDAD DIGITAL DE LA AGENCIA NACIONAL DE TIERRAS 6
4.1 Ámbito de las políticas de la seguridad de la información 6
4.2 Revisión, actualización y vigencia 6
5 MEDIDAS A ADOPTAR EN CASO DE INCUMPLIMIENTO 6
6 ORGANIZACIÓN INTERNA DE LA SEGURIDAD 7
6.1 Roles y responsabilidades de Seguridad de la Información 8
6.2 Dirección General 8
6.3 Oficina de planeación 8
6.4 Comité Institucional de Gestión y Desempeño 8
6.5 Responsable de procesos 9
6.6 Subdirección de Sistemas de Información de Tierras. 9
6.7 Subdirección de Planeación Operativa (SPO) 10
6.8 Oficina de Control Interno 11
6.9 Subdirección de Talento Humano 11
6.10 Secretaría General 11
6.11 Oficina Jurídica 11
6.12 Funcionarios, contratistas y demás personas de la Entidad 11
7 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 12
7.1 Control de acceso a la información 12
7.2 Uso aceptable de activos de información 13
7.2.1 Uso de servicios de correo electrónico 15
7.2.2 Uso de servicio de acceso a internet 17
7.2.3 Servicios de computación en la nube 19
7.3 Uso de controles criptográficos 20
7.4 Transferencia o intercambio de información 21
7.5 Uso de dispositivos móviles 22

7.6 Relaciones con proveedores 23
7.7 Teletrabajo 24
7.8 Escritorio limpio, pantalla limpia 25
7.9 Respaldo de información 26
7.10 Ciberseguridad 28
7.11 Desarrollo Seguro 30
8 SENSIBILIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 31
9 NORMATIVIDAD APLICABLE A SEGURIDAD DE LA INFORMACIÓN 31
10 GLOSARIO 32

INTRODUCCIÓN

La Agencia Nacional de Tierras - ANT adopta un enfoque estructurado para la gestión de la seguridad de la información que le permite "promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".[1]

Entendiendo la importancia de la gestión de la información para el logro de los objetivos institucionales y estratégicos de la ANT, la Dirección de Gestión de Ordenamiento Social de la Propiedad – DGOSP está comprometida con la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI que proporcione un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, con estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Agencia.

Para el establecimiento, implementación, mantenimiento y proceso de mejora continua de su SGSI, la Agencia cumple las obligaciones del gobierno colombiano en materia de Seguridad Digital y aplica el Modelo de Seguridad y Privacidad de la información – MSPI de la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión -MIPG[2] del Departamento Administrativo de la Función Pública y las directrices de la Norma Técnica Colombiana NTC ISO/IEC 27001.

Este documento, constituye el marco general para el desarrollo de controles, procedimientos y estándares de seguridad de la información; estos son de obligatorio cumplimiento para funcionarios, contratistas y partes interesadas que presten sus servicios o tengan alguna relación con la Agencia.

[1] Implementación de la Política de Gobierno Digital, Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1
[2] http://www.funcionpublica.gov.co/web/mipg

1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Agencia Nacional de Tierras como máxima autoridad de tierras para consolidar y mantener el ordenamiento social de la propiedad rural y mejorar las condiciones de vida de la población, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información que genera, almacena, procesa, custodia y comparte, mediante la implementación del SGSI, su seguimiento y mejora continua, le permite a la Agencia ejercer una adecuada gestión de riesgos y cumplir los objetivos de seguridad de la información, las obligaciones legales y contractuales aplicables, además de, satisfacer las necesidades y expectativas de las partes interesadas en materia de seguridad de la información.

2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

- Realizar una adecuada gestión a los riesgos de seguridad de la información, para asegurar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la implementación de los lineamientos establecidos.

- Dar cumplimiento a los requisitos legales sobre seguridad de la información, regulatorios, contractuales y otros suscritos, vigentes y aplicables a las operaciones de la Agencia Nacional de Tierras.

- Capacitar y sensibilizar al personal de la ANT en temas relacionados con seguridad de la información, buscando fortalecer los conocimientos, concientizar sobre la responsabilidad de las acciones y aumentar progresivamente la cultura de la seguridad de la información al interior de la Entidad.

- Mejorar continuamente el desempeño del SGSI, mediante la implementación de acciones correctivas y de mejoras eficaces que se generen como resultado de las auditorías internas y externas.

- Gestionar de manera adecuada los incidentes de seguridad de la información, generando, documentando y aplicando las lecciones aprendidas, con el fin de mitigar el impacto de futuros incidentes.

3 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Agencia Nacional de Tierras mediante el SGSI, asegura la confidencialidad, integridad y disponibilidad sobre de los activos de información requeridos para el adecuado funcionamiento de los siguientes procesos:

- Misionales:
  - ✓ Planificación del Ordenamiento Social de la Propiedad Rural.
  - ✓ Seguridad Jurídica sobre la Titularidad de la Tierra y los Territorios.
  - ✓ Acceso a la Propiedad de la Tierra y los Territorios.
  - ✓ Administración de Tierras.
  - ✓ Gestión de la Información.
- Apoyo:
  - ✓ Administración de Bienes y Servicios.

Estos procesos se encuentran ubicados en la actual sede de la ANT: Calle 43 No. 57 - 41 Bogotá, D.C. – Colombia.

4 SEGURIDAD DIGITAL DE LA AGENCIA NACIONAL DE TIERRAS

4.1 Ámbito de las políticas de la seguridad de la información

Las políticas de Seguridad de la Información, aplica a todas las dependencias de la ANT, a todos los colaboradores y partes interesadas que presten sus servicios o tengan alguna relación con la Agencia, en particular para quienes:

- Accedan a la información análoga y/o digital de la ANT en cualquier formato.
- Operen equipos informáticos y/o de comunicaciones dentro de la red de la ANT.
- Diseñen, construyan, prueben y/o utilicen sistemas de información, bases de datos o servicios colaborativos de la ANT.
- Provean servicios de gestión de información y de tecnología.
- Accedan de manera virtual o presencial a las instalaciones de la ANT.

4.2 Revisión, actualización y vigencia

Cualquier excepción a lo establecido en las políticas de Seguridad de la Información, debe contar con la aprobación formal del Comité de Arquitectura Empresarial TIC de la Agencia Nacional de Tierras, la Mesa Técnica de TI o de quien haga sus veces.

Las políticas se revisan y actualizan, como mínimo una vez al año, cuando se presenten cambios organizacionales, culturales, del entorno, operativos o normativos que afecten a la Entidad. Así mismo, las políticas se revisan cuando ocurren incidentes de seguridad de la información que obliguen a su fortalecimiento, o de acuerdo con los resultados de las actividades de gestión de riesgos institucionales. Las políticas de seguridad se implementan mediante lineamientos, procedimientos y controles que especifican los detalles técnicos de su operación.

5 MEDIDAS A ADOPTAR EN CASO DE INCUMPLIMIENTO

El incumplimiento de las políticas de seguridad de la información se trata con un evento de seguridad de la información. Los incidentes de seguridad de la información se tratan mediante el procedimiento de incidentes de seguridad de la información. De acuerdo con la naturaleza de los incidentes de seguridad de la información, los responsables de los activos de información de la ANT evalúan la necesidad de adelantar procesos disciplinarios o legales por incumplimiento de las políticas de seguridad de la información o actividades calificadas como delitos en la normatividad vigente.

En caso de que se identifique el incumplimiento de las políticas descritas en el presente documento, se deberá emitir el reporte correspondiente al Grupo de Control Interno Disciplinario para que se ejecuten las medidas correspondientes.

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

Todas las acciones en las que se comprometa la seguridad de la información de la Agencia Nacional de Tierras y que no estén previstas en este documento, deberán ser revisadas por la Mesa Técnica de TI y la Oficina Apoyo Jurídico con el fin de establecer nuevos lineamientos en la Entidad.

Para los Contratistas de la ANT las medidas a adoptar en caso de incumplimiento de este documento se realizarán por medio de una denuncia penal interpuesta por el servidor público que evidenció la posible falta.

6 ORGANIZACIÓN INTERNA DE LA SEGURIDAD

La coordinación de las actividades referidas a la gestión de la seguridad de la información, son lideradas por la Mesa Técnica de TI; la Subdirección de Sistemas de Información de Tierras, es quien convoca al Comité de Arquitectura Empresarial TIC de la ANT y a la Mesa Técnica de TI o quien haga sus veces para el caso de ocurrencia de incidentes de seguridad y/o asuntos relacionados de seguridad informática que lo ameriten.

Todos los funcionarios, contratistas y partes interesadas dentro del ámbito de sus tareas asignadas son responsables del cumplimiento de las políticas de seguridad de la información, reportar debilidades, eventos o incidentes de seguridad de la información que puedan afectar a la entidad a través de los canales institucionales que defina el Comité de Arquitectura Empresarial TIC de la ANT.

Asimismo, se contempla el contacto con fuentes de conocimiento experimentadas en materia de seguridad de la información para el asesoramiento, cooperación y colaboración para el mejoramiento del Sistema de Gestión de Seguridad de la Información.

6.1 Roles y responsabilidades de Seguridad de la Información

Las siguientes responsabilidades de seguridad de la información serán inherentes al cargo desempeñado por los funcionarios y se relacionarán con las funciones esenciales descritas en el Manual de Funciones y de Competencias Laborales.

6.2 Dirección General

Para el Sistema de Gestión de Seguridad de la Información - SGSI, es el encargado de la aprobación de la Política general, objetivos y alcance del Sistema de Gestión de Seguridad de la Información.

6.3 Oficina de planeación

Es el responsable por el direccionamiento estratégico e impulso del SGSI. Establece su compromiso, mediante la asignación de recursos, responsabilidades y revisiones al Sistema de Gestión de Seguridad de la Información – SGSI:

Como parte de la gestión de la Oficina de Planeación para la Seguridad de la Información, se encuentran las siguientes responsabilidades:

a) Proponer el alcance, la política general y los objetivos de Seguridad de la Información.
b) Asegurar la definición y asignación de las responsabilidades de Seguridad de la Información.
c) Asegurar la integración y adopción de los requisitos del SGSI en los procesos de la Entidad.
d) Brindar apoyo en la asignación de los recursos necesarios para el SGSI.
e) Revisar el SGSI de la Entidad, para asegurarse de su conveniencia, adecuación y eficacia continúa.
f) Dirigir y apoyar a los funcionarios y contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del SGSI.
g) Apoyar los roles directivos de todas las áreas de la Entidad, para facilitar la consolidación del SGSI en sus respectivas áreas.

6.4 Comité Institucional de Gestión y Desempeño

La conformación de este comité se encuentra establecido en la Resolución N° 183 de 2018, quienes, para el SGSI deberán cumplir con las siguientes responsabilidades:

a) Apoyar la definición de las políticas de Seguridad de la Información.
b) Aprobar las técnicas específicas de Seguridad de la Información.
c) Asegurar la implementación de las políticas de Seguridad de la Información.
d) Revisar a intervalos planificados el estado del SGSI.

6.5 Responsable de procesos

Los jefes encargados de cada proceso deberán asumir y ejecutar las siguientes responsabilidades:

a) Difundir las políticas, procesos, procedimientos y documentos relacionados con el SGSI en su respectivo proceso.
b) Promover la vinculación y compromiso de los funcionarios y contratistas de su proceso, mediante el cumplimiento de las responsabilidades asignadas en el SGSI.
c) Liderar y apoyar continuamente la implementación y mantenimiento del SGSI al interior de su proceso.
d) Gestionar los recursos necesarios para la implementación de controles y mantenimiento del al interior de su proceso.
e) Asegurar la disponibilidad de los funcionarios y contratistas de su proceso para la asistencia a actividades de formación y sensibilización para el fortalecimiento de la cultura en Seguridad de la Información.
f) Asegurar la gestión de activos de información para su proceso de acuerdo al procedimiento establecido por la Entidad.
g) Asegurar la gestión de los riesgos de Seguridad de la Información para su proceso de acuerdo con la metodología establecida por la Entidad.
h) Definir en conjunto con el responsable de Seguridad, el plan de tratamiento de riesgos de Seguridad de la Información y aprobarlo.
i) Asegurar el cumplimiento del plan de tratamiento de riesgos y aceptar los riesgos residuales de Seguridad de la Información.
j) Revisar a intervalos planificados el cumplimiento de las políticas específicas y procedimientos de Seguridad de la Información dentro de su proceso a cargo.
k) Aprobar, a quien corresponda, los planes, procesos, procedimientos y demás documentación necesaria para el mantenimiento del SGSI relacionado con su proceso.

6.6 Subdirección de Sistemas de Información de Tierras.

Realiza la planeación, coordinación y administración del SGSI en la Entidad:

a) Asegurar que el SGSI opere de conformidad con los requisitos de la norma ISO-IEC 27001.
b) Identificar la brecha entre el SGSI y la situación de la Entidad a través de la herramienta (Arquitectura de Seguridad de la Información) establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.
c) Liderar la implementación y mantenimiento del SGSI, asegurando el cumplimiento de las políticas generales y específicas de Seguridad de la Información aprobadas por la Entidad.
d) Asegurar la ejecución de los planes del Sistema de Gestión de Seguridad de la Información - SGSI y el logro de los objetivos de Seguridad de la Información.
e) Realizar actualizaciones metodológicas y de lineamientos del Sistema de Gestión de Seguridad de la Información - SGSI de acuerdo con la normatividad vigente y aplicable.

f) Administrar, monitorear y coordinar permanentemente la Seguridad de la Información en la Entidad.
g) Apoyar la definición e implementación de controles para el tratamiento de riesgos de Seguridad de la Información para cada proceso.
h) Apoyar la definición de acciones que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
i) Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad de la Información.
j) Asegurar la adecuada gestión de los incidentes de Seguridad de la Información en la Entidad.
k) Promover la divulgación de las responsabilidades de Seguridad de la Información de los funcionarios, contratistas y demás personas vinculadas a la ANT.
l) Promover programas, campañas y actividades de sensibilización del Sistema de Gestión de Seguridad de la Información - SGSI al interior de la Entidad.
m) Gestionar la actualización del Sistema de Gestión de Seguridad de la Información - SGSI
n) Documentar el seguimiento, medición, análisis y evaluación del desempeño de la Seguridad de la Información y la eficacia del Sistema de Gestión de Seguridad de la Información - SGSI.
o) Actuar como enlace con las autoridades y grupos de interés relacionados con la Seguridad de la Información.
p) Gestionar la inclusión en el proceso de inducción y reinducción del personal, en aspectos de Seguridad de la Información.
q) Informar a intervalos planificados al Comité Institucional de Gestión y Desempeño sobre el funcionamiento del SGSI en la Entidad.

6.7 Subdirección de Planeación Operativa (SPO)

En coordinación con la SSIT, estará encargada de la gestión documental del Sistema de Gestión de Seguridad de la Información – SGSI:

a) Gestionar la documentación del Sistema de Gestión de Seguridad de la Información SGSI, de tal manera que esté alineada con los demás Sistemas de Gestión existentes en la Entidad. Esto incluye entre otras las siguientes actividades:
    - Mantener actualizada y publicada toda la documentación relacionada con el SGS.
    - Revisar continuamente la documentación del Sistema de Gestión de Seguridad de la Información - SGSI, para mantenerlos alineados a las normas y reglamentaciones vigentes respecto a la gestión documental.
    - Asegurar, desde el punto de vista documental, la integración del Sistema de Gestión de Seguridad de la Información - SGSI con otros sistemas de gestión cuando aplique.

b) Promover la formación, capacitación y sensibilización en Seguridad de la Información.
c) Asesorar metodológicamente a las áreas en la identificación y gestión de riesgos de Seguridad de la Información.

6.8 Oficina de Control Interno

Realiza revisiones regulares y planificadas de la eficacia del SGSI:

a) Realizar las auditorías internas, evaluaciones o seguimientos al Sistema de Gestión de Seguridad de la Información - SGSI y presentar los informes respectivos.

b) Evaluar la efectividad de las acciones correctivas o de mejora presentadas.

6.9 Subdirección de Talento Humano

Realiza la gestión de los aspectos asociados al talento humano, guiados por el Sistema de Gestión de Seguridad de la Información – SGSI:

Implementar los controles de Seguridad de la Información asociados a la administración del talento humano, de acuerdo con el SGSI:

- Antes de asumir el empleo.
- Durante la ejecución del empleo.
- Terminación y cambio del empleo.

6.10 Secretaría General

Realiza la gestión de los aspectos asociados a la seguridad física y del entorno, guiados por el Sistema de Gestión de Seguridad de la Información – SGSI:

a) Gestionar los recursos requeridos para la implementación de controles para la seguridad física de instalaciones, bienes y personas de la Entidad.
b) Asegurar el cumplimiento de las políticas de Seguridad de la Información en las áreas denominadas como seguras o restringidas.

6.11 Oficina Jurídica

Realiza la gestión de los temas pertinentes al cumplimiento de:

a) Evitar el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con la Seguridad de la Información y de cualquier requisito de seguridad.

6.12 Funcionarios, contratistas y demás personas de la Entidad

a) Aceptar y dar cumplimiento a las políticas generales y técnicas de Seguridad de la Información.
b) Gestionar la información y los activos a su cargo de acuerdo con las definiciones del Sistema de Gestión de Seguridad de la Información - SGSI.
c) Apoyar la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, de acuerdo con las metodologías, procesos, procedimientos y los demás lineamientos establecidos para tal fin.
d) Reportar eventos y/o incidentes de Seguridad de la Información de acuerdo con el procedimiento establecido por la Entidad.
e) Participar activamente en las actividades de sensibilización, formación y toma de conciencia en Seguridad de la Información desarrolladas por la Entidad.

7 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1 Control de acceso a la información

Objetivo: Limitar el acceso a la información y a instalaciones de procesamiento de la información, solamente a los debidamente autorizados.

Obligaciones:

1. Todos los activos de información o sistemas de información de la ANT deben tener asignado un responsable funcional que autoriza el acceso a la información contenida en el mismo.
2. La autorización de acceso a los activos de información solo puede ser otorgada por los responsables de los activos de información. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación de eventos o incidentes de seguridad de la información.
3. El acceso a la información y los activos de información que la soportan, es controlado conforme a los roles y responsabilidades de los funcionarios, contratistas o partes interesadas de la ANT.
4. Solo se otorga acceso a la información y activos de información bajo el principio de necesidad de conocer para poder ejecutar la función designada.
5. Todos los accesos a los activos de información institucionales deben cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido el ordenamiento legal o los determinados por el responsable del activo de información para un uso seguro del mismo.
6. Todo acceso a los activos de información debe considerar el nivel de clasificación legal asignado al activo de información según el instructivo de calificación y etiquetado de la información de la ANT.
7. Todo acceso a los activos de información debe ser autorizado formalmente por el responsable del activo o de la dependencia responsable del activo de información. Para la autorización de acceso se debe contemplar un análisis previo de la justificación de la necesidad de uso del activo y las actividades a realizar sobre el mismo. La trazabilidad de las acciones para

autorizar el acceso a los activos de información debe ser documentada en las herramientas dispuestas por la ANT para este fin.

8. La información de naturaleza pública debe de estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.
9. Los funcionarios, contratistas y partes interesadas de la ANT, tienen como responsabilidad mantener la integridad, confidencialidad y disponibilidad de la información, los activos y los sistemas informáticos para los cuales han sido designados y autorizados, asegurándose que estos solo sean utilizados para el desarrollo de las labores afectas al servicio que presta la Agencia.
10. Todo acceso físico o lógico, asignado a los funcionarios, contratistas o partes interesadas debe ser desactivado o modificado una vez se termina la autorización de uso sobre los mismos.
11. Todos los funcionarios, contratistas o partes interesadas de la ANT autorizadas para utilizar activos de información o instalaciones de la ANT deben contar con un identificador único (ID del usuario, Cuenta de usuario) para su uso personal e intransferible que le permite validar los accesos a los activos de información autorizados por la ANT.
12. El responsable funcional o encargado del activo de información es el responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios a la información, sistemas de información, activos de información o áreas de procesamiento de información.
13. Los accesos y utilización de los activos de información de la ANT se deben registrar para garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso y accesos denegados.
14. Los funcionarios, contratistas o partes interesadas no deben realizar modificaciones sobre la información o los activos de información sin la debida autorización.
15. De conformidad con el artículo 34 de la ley 734 de 2002 son deberes de todo servidor público: "… *Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida …*".
16. De conformidad con el artículo 35 de la ley 734 de 2002 a todo servidor público le está prohibido: "… *Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas …*".
17. En cumplimiento del Artículo 4°. Principios para el Tratamiento de datos personales de la ley 1581 de 2012 y en lo especifico al Principio de confidencialidad: Todas las personas que intervengan 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 con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

7.2 Uso aceptable de activos de información

Objetivo: Definir las pautas para realizar un uso seguro y aceptable de los activos de información, los sistemas de información, la infraestructura tecnológica y las instalaciones de procesamiento de información de la ANT.

Obligaciones:

1. Todas las actividades de administración, operación y uso de los activos de información, sistemas de información, la infraestructura tecnológica y las instalaciones de procesamiento de información de la ANT deben estar destinadas a garantizar la prestación de los servicios necesarios para el cumplimiento de la misión de la Agencia, los usos diferentes deben ser formalmente autorizados por el responsable del activo, de forma que se dé cumplimiento a lo definido en la ley 734 de 2002, por la cual se expide el Código Disciplinario Único. Artículo 34, Deberes. Numeral 4: "… *Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos*. …"
2. Todos los funcionarios, contratistas, partes interesadas o procesos que realicen actividades para la Agencia, solo deben tener acceso a la información necesaria para el desempeño de las actividades que les han sido autorizadas, de conformidad con el principio de "necesidad de conocer para realizar la actividad".
3. Todos los funcionarios, contratistas o partes interesadas que prestan sus servicios a la ANT se deben comprometer a realizar sus mejores esfuerzos para aplicar todos los controles pertinentes de seguridad de la información definidos por el Sistema de Gestión de Seguridad de la Información de la Entidad, para garantizar la preservación de la Confidencialidad, Integridad y Disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades.
4. Todos los funcionarios, contratistas o partes interesadas de la ANT deben reportar sin demoras injustificadas a los responsables de sus dependencias, o a los responsables de los procesos o la Subdirección de Sistemas de Información de Tierras cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información.
5. Todos los funcionarios, contratistas o partes interesadas deben aplicar el modelo institucional de gestión de riesgos para identificar y tratar los riesgos de seguridad de la información que puedan afectar a los activos de información a su cargo. Cada responsable de proceso o activo de información debe coordinar la aplicación del modelo institucional de gestión de riesgos sobre los activos a su cargo con la Mesa Técnica de TI.
6. Las modificaciones a los activos de información tecnológicos deben cumplir con los procedimientos para la gestión del cambio definidos por la Mesa Técnica de TI.
7. Todos los funcionarios, contratistas o partes interesadas de la ANT deben aplicar los controles de seguridad de la Información definidos por la Entidad para tratar los riesgos que afectan a la seguridad de la información y los activos de información institucionales.
8. Todos los funcionarios, contratistas o partes interesadas de la ANT están obligados a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está sometida la Entidad para la protección de la información a su cargo.

9. La Mesa Técnica de TI, en coordinación con el proceso de Gestión de Talento Humano realizará las campañas de sensibilización periódicas a los funcionarios, contratistas o partes interesadas, encaminadas al explicar el uso responsable de los activos de información.
10. Las siguientes actividades sobre los activos de información se consideran usos no autorizados y son calificadas como incidentes de seguridad de la información que se gestionan de acuerdo con los procedimientos adoptados por la Entidad:
    a. Modificación de la información sin contar con la autorización formal para dichas modificaciones.
    b. Divulgación no autorizada de información.
    c. Impedir el acceso a la información sin justificación real.
    d. Modificación o eliminación de los controles de seguridad que protejan la información.
    e. Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o procedimientos a los que está sometida la Entidad.
    f. Utilizar los activos de información de la Entidad para fines personales o diferentes a los requeridos para el cumplimiento de las actividades asignadas o el cumplimiento de las funciones institucionales.

7.2.1 Uso de servicios de correo electrónico

Objetivo: Establecer las reglas generales para asegurar una adecuada protección de la información cuando se usa el servicio de correo electrónico institucional por parte de los usuarios autorizados.

Obligaciones:

1. El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las actividades designadas al funcionario, contratista o parte interesada. El uso del servicio de correo electrónico para actividades diferentes a las necesarias para el cumplimiento de las actividades encargadas al funcionario, contratista o parte interesada requiere autorización del responsable del proceso en el que trabaja la persona. El uso del servicio de correo electrónico de la Entidad para fines personales no está autorizado.
2. El acceso al servicio de correo electrónico debe ser autorizado por el responsable del proceso o dependencia al que pertenece el funcionario, contratista o parte interesada que presta sus servicios para la Agencia.
3. La Secretaría General es la dependencia encargada de coordinar y ejecutar las actividades de copia de respaldo del servicio de correo electrónico. Al finalizar su relación con la ANT el funcionario, contratista o parte interesada, se debe deshabilitar su acceso al servicio de correo electrónico y realizar respaldo de la información almacenada en el buzón de correo electrónico.

4. Al finalizar su relación con la ANT todo funcionario, contratista o parte interesada que haya prestado sus servicios a la ANT, debe realizar la devolución de la cuenta de usuario de correo electrónico de acuerdo con los procedimientos definidos por la Entidad.
5. El servicio de correo electrónico oficial de la Agencia Nacional de Tierras es el aprobado por la Secretaría General. Los funcionarios, contratistas o partes interesadas reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad y los mismos serán gestionados acorde con la gestión de incidentes de seguridad.
6. La clave o contraseña de acceso al servicio de correo electrónico es personal e intransferible no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión, se debe seguir los controles de protección de contraseñas definidos por la Entidad.
7. La Entidad puede supervisar el uso del servicio de correo electrónico para verificar que se está usando para el cumplimiento de las funciones misionales; en los procesos de verificación de uso apropiado del servicio de correo electrónico se respetan los derechos a la privacidad e intimidad del titular de la cuenta de correo electrónico.
8. La Agencia puede supervisar el contenido de correos electrónicos con herramientas tecnológicas, evaluando los riesgosos o correos con elementos adjuntos identificados como software malicioso o ataques informáticos. En los procesos de verificación de los contenidos del servicio de correo electrónico se respetan, los derechos a la privacidad e intimidad del titular de la cuenta de correo electrónico.
9. Los correos electrónicos deben contener la nota de confidencialidad definida por la Entidad al final del cuerpo del texto, después de la firma institucional, este mecanismo es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico. La nota oficial de confidencialidad es establecida por la Subdirección de Sistemas de Información de Tierras.
10. Los usuarios del servicio de correo electrónico son completamente responsables de todas las actividades realizadas con sus cuentas de acceso al buzón de correo.
11. Si por cualquier motivo el usuario sospecha que la seguridad de su cuenta se ve comprometida de cualquier forma, debe reiniciar su contraseña y notificar a Secretaría General.
12. Los usuarios deben cambiar sus contraseñas o claves de acceso al servicio de correo electrónico, cada 45 días conforme lo establece la política de Directorio activo de la ANT.
13. De conformidad con los deberes de los servidores públicos descritos en el Artículo 34 del capítulo 2 del Código único Disciplinario, ley 734 de 2002, todo servidor público debe:
    "… *Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos. Realizar personalmente las tareas que le sean confiadas, responder por el ejercicio de la autoridad que se le delegue, así como por la ejecución de las órdenes que imparta, sin que en las situaciones anteriores quede exento de la responsabilidad que le incumbe por la correspondiente a sus subordinados. …*".
    Estas consideraciones aplican al uso del servicio de correo electrónico institucional o cuentas de acceso a sistemas de información.
14. Constituye un riesgo de seguridad de la información facilitar y ofrecer su cuenta de correo electrónico (e-mail) o cuenta de acceso a sistemas de información a personas no autorizadas,

la cuenta de usuario es exclusiva del cargo o dependencia y no es transferible. La delegación de las actividades para la gestión y uso de una cuenta de correo electrónico o de acceso a sistemas de información se deben realizar de manera formal en los casos en que un superior deba designar a un funcionario para la administración de su cuenta de usuario.

15. Los siguientes usos del servicio de correo electrónico se consideran usos no autorizados y pueden constituir un incidente de seguridad de la información que se gestionan de acuerdo con los procedimientos adoptados por la Entidad:
    a. Envío de correos masivos sin autorización oficial.
    b. Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM.
    c. Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Agencia o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la Entidad.
    d. Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
    e. Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
    f. Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.

7.2.2 Uso de servicio de acceso a internet

Objetivo: Definir las pautas y reglas generales para asegurar una adecuada protección de la información cuando se hace uso del servicio de Internet por parte de los usuarios autorizados de la Agencia Nacional de Tierras.

Obligaciones:

1. El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas asignadas al funcionario, contratista o partes interesadas.
2. El acceso al servicio de Internet podrá ser asignado a las personas que tengan algún tipo de relación con la ANT, ya sea como funcionario, contratista o parte interesada. La autorización de uso del servicio de acceso a internet para los visitantes de las instalaciones de la Entidad debe ser solicitada por los responsables de procesos o dependencias que visita la persona a la Secretaría General.
3. Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña para la Agencia y para los cuales este formal y expresamente autorizado.
4. El acceso a servicios de redes sociales, video en línea, audio o servicios no directamente afectos a la función misional solo están autorizados a las dependencias cuya función misional requiere del servicio. La Entidad define horarios específicos para permitir el acceso de todos sus funcionarios, contratistas o partes interesadas a estos servicios y se reserva el derecho

de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la Secretaría General.

5. Todo usuario del servicio de Internet es responsable de informar a su superior o la SSIT los contenidos o acceso a servicios que no le estén autorizados o no le correspondan para la ejecución de las funciones asignadas. La SSIT articulará lo correspondiente con la Secretaría General.
6. Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde las redes de la ANT o se descargue desde Internet usando su cuenta de acceso.
7. La Entidad puede supervisar el uso y acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales. En los procesos de verificación del uso apropiado del servicio de acceso a Internet, se respetan los derechos a la intimidad y privacidad del titular de la cuenta de acceso a Internet.
8. Cuando un funcionario, contratista o parte interesada al que le haya sido autorizado el uso de una cuenta de servicio de Internet o de acceso a la red local finalice su relación con la Entidad, debe seguir los procedimientos definidos por la Agencia para entregar su cuenta de usuario y accesos a servicios informáticos provistos.
9. Los siguientes usos del servicio de acceso a Internet se consideran usos no autorizados y pueden constituir un incidente de seguridad de la información que se gestiona de acuerdo con los procedimientos adoptados por la Entidad:
    a. No está autorizado el envío o descarga de información de sometida a derechos de autor cuando no se tienen esos derechos (música, videos, obras literarias, pictóricas e imágenes).
    b. No está autorizado el envío, descarga o visualización de información con contenidos que no forman parte de las actividades propias asignadas al usuario.
    c. No está autorizado el uso del servicio de acceso a Internet para actividades comerciales personales.
    d. No está autorizado el acceso a sitios de música, juegos, vídeos, u otros sitios de entretenimientos on-line.
    e. No está autorizado el acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos aquellos incluidos en la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
    f. Todas las conductas definidas como delito informático en la ley 1273 de 2009 están prohibidas y no se debe hacer uso del servicio de acceso a Internet para fines ilícitos.
    g. Está prohibido el uso del servicio de acceso a Internet para realizar o propiciar la propaganda de productos comerciales o propaganda política.
    h. No está autorizado el acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía.
    i. No está autorizado el acceso a sitios web que fomenten la discriminación por razones raciales, políticas, ideológicas, de género o de cualquier otra índole que vayan en contravía de la constitución política de Colombia o los derechos humanos.

j. Salvo autorización formal de la Mesa Técnica de TI, no está autorizado el acceso a sitios de "hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información.

7.2.3 Servicios de computación en la nube

Objetivo: Mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la Agencia Nacional de Tierra reduciendo los riesgos legales y técnicos a niveles aceptables.

Obligaciones:

1. Cuando se utilicen servicios de computación en la nube como: correo electrónico, almacenamiento, aplicaciones on-line, u otros provistos por operadores de servicios en Internet, se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información institucional, acceso a información personal, protección de secretos comerciales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal. El análisis y gestión de los riesgos se debe realizar de acuerdo con los procedimientos de gestión de riesgos institucionales. Los resultados del análisis y gestión de riesgos se deben documentar y considerar para autorizar el uso de dichos servicios de computación en la nube.
2. No se deben utilizar servicios de computación en la nube cuyo análisis de riesgos indique niveles no tolerables para la protección de información institucional o personal. Los resultados del análisis y gestión riesgos deben ser determinantes para aceptar o rechazar la utilización de servicios de computación en la nube, de pago o gratuitos.
3. En los contratos celebrados con proveedores de servicios de computación en nube, proveedores de servicios en línea en Internet o intermediarios de servicios, se debe cumplir la política de seguridad de la información de la ANT, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.
4. En los casos en que se requiera el almacenamiento de información en la nube clasificada como reservada, pública clasificada o información de carácter personal se deben aplicar controles de seguridad de la información que impidan su acceso no autorizado.
5. En los casos que se requiera el uso de plataformas gratuitas de almacenamiento o procesamiento de información en la nube, el jefe de la dependencia responsable debe tramitar la autorización de uso ante la SSIT.
6. El uso de plataformas internacionales de almacenamiento o procesamiento en la nube para datos de carácter personal deben contar con la autorización del titular de los datos. No se debe almacenar datos personales en servicios de computación en la nube sin la autorización del titular para la transmisión internacional de datos de acuerdo con la Ley 1581 de 2012.

7. Los responsables de procesos o dependencias a los que se autorice el uso de servicios de computación en la nube deben coordinar con la Mesa Técnica de TI, las acciones para garantizar la copia de respaldo de datos almacenados en servicios de computación en la nube.
8. Los responsables de procesos o dependencias a los que se autorice el uso de servicios de computación en la nube son responsables de exigir a sus subalternos y colaboradores el cumplimiento de las políticas de seguridad de la información institucionales cuando se les autorice el uso de servicios de computación en la nube.
9. Los eventos de seguridad de la información en los que estén involucradas plataformas de almacenamiento o procesamiento en la nube se tratan como incidentes de seguridad de la información, de acuerdo con los procedimientos del SGSI de la ANT.

7.3 Uso de controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad e integridad de la información pública reservada o pública clasificada mediante controles criptográficos

Obligaciones:

1. La Mesa Técnica de TI, es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de protección de la información de la Agencia Nacional de Tierras.
2. La Secretaría General es la responsable de la creación, activación, distribución y revocación de las llaves criptográficas a los usuarios autorizados y realizará seguimiento para que las llaves se encuentren activas en el período de tiempo previsto.
3. La selección de herramientas para cifrado de la información se realiza sobre la base de los resultados del análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información.
4. El uso de herramientas de cifrado es autorizado conforme a los roles o responsabilidades en el tratamiento de la información de los funcionarios, contratistas o partes interesadas de la ANT.
5. La solicitud de acceso o actualización al sistema o llaves de cifrado se debe efectuar de manera formal ante la Secretaría General.
6. Las personas autorizadas para uso de sistemas de cifrado de datos deben tener una gestión adecuada para conservar la disponibilidad, integridad y confidencialidad de las llaves, así como de la información a la cual se le haya aplicado algún proceso de cifrado.
7. La información cifrada o descifrada deberá ser tratada conforme a su nivel de calificación y su eliminación deberá realizarse a través de borrado seguro.
8. Las llaves o claves de cifrado se deshabilitan cuando existe riesgo de divulgación o cuando los funcionarios, contratistas o partes interesadas, usuarias de estas culminan la relación o vínculo contractual con la Entidad.
9. Los funcionarios, contratistas o partes interesadas tienen la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos de las herramientas de cifrado ante la Secretaría General.

7.4 Transferencia o intercambio de información

Objetivo: Definir las pautas y reglas generales para la protección de la información durante su intercambio entre los funcionarios, contratistas o partes interesadas de la Agencia Nacional de Tierras o entre la Entidad y partes externas, preservando las características de disponibilidad, integridad y confidencialidad.

Obligaciones:

1. La transmisión de la información bajo responsabilidad de la ANT se controla según los niveles de calificación de la información establecidos y las políticas de seguridad Institucionales.
2. En caso de que se requiera intercambiar información calificada como pública reservada o pública clasificada, se adoptan controles de cifrado de información de acuerdo con lo establecido en la política de uso de controles criptográficos.
3. Los intercambios de información con otras entidades o partes interesadas externas deben estar soportados por medio de contratos, convenios o acuerdos formalizados, determinando en ellos los medios y controles en el tratamiento de la información. Así mismo, se deben firmar acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.
4. El uso de la información transmitida o intercambiada se debe realizar conforme a las características del contrato, convenio o acuerdo suscrito con el tercero y cumpliendo la normatividad vigente en materia de protección de datos.
5. La transmisión de la información se debe realizar teniendo en cuenta la normatividad colombiana vigente, la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014 y sus decretos reglamentarios).
6. La información debe protegerse contra divulgación no autorizada conforme con el instructivo de Calificación y Etiquetado de la Información de la ANT.
7. Al transmitir información a partes interesadas se debe acordar entre las partes, que la información sólo podrá ser usada para las actividades autorizadas dentro de los acuerdos suscritos entre las partes.
8. El intercambio de información se debe efectuar según los acuerdos establecidos, en los cuales se describen: las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y procedimiento a seguir en caso de presentarse un incidente de seguridad y los niveles de calificación de la información a ser intercambiada.
9. Para la transferencia de información se deben tratar los riesgos relativos al uso de canales de comunicación de forma que se mantengan los niveles de seguridad aceptables para los responsables de los datos. En cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), se debe realizar a través de canales que preserven los niveles de confidencialidad e integridad de la información, conforme con el nivel de calificación de la información trasmitida.

10. Se deben garantizar acuerdos de confidencialidad con las partes interesadas que accedan o intercambien información bajo responsabilidad de la ANT, en donde se describan las responsabilidades de las partes y se garantice la reserva de la información.

7.5 Uso de dispositivos móviles

Objetivo: Garantizar la seguridad de la información en los dispositivos móviles cuando se administre, transmita o almacene información de la ANT.

Obligaciones:

1. Las redes de comunicaciones y acceso a Internet de la ANT cuentan con mecanismos de control de seguridad de la información de estricto cumplimiento por parte de los funcionarios, contratistas y partes interesadas para el acceso a la información a través de los dispositivos de tecnología móviles (computadores portátiles, Smartphone, tabletas, o cualquier equipo móvil electrónico con capacidad de acceso a las redes).
2. Los dispositivos móviles solo deben tener acceso a la información mediante accesos a redes inalámbricas diferentes a las redes de producción de los sistemas de información de la Entidad. La ANT cuenta con redes inalámbricas para permitir el acceso de visitantes ocasionales a sus dependencias.
3. Los dispositivos móviles propiedad de la ANT se deben proteger física y lógicamente para evitar el hurto, acceso o la divulgación no autorizada de la información cuando estén dentro o fuera de las instalaciones de la Entidad. El usuario del dispositivo móvil es enteramente responsable de aplicar los controles de seguridad recomendados por la Mesa Técnica de TI para la protección de dispositivos móviles.
4. De acuerdo con los niveles de calificación de la información almacenada en el dispositivo móvil, se determinará la necesidad de su cifrado, así como la ejecución de copias de respaldo.
5. En caso de extravió o hurto de un dispositivo móvil propiedad de la ANT, el funcionario, o contratista responsable del dispositivo será el responsable de informar de manera inmediata a la Secretaría General el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida o acceso a los sistemas de información desde el dispositivo.
6. Los funcionarios o contratistas de la Agencia a los que les hayan sido asignados dispositivos móviles institucionales no deben instalar software sin previa autorización y coordinación de la Mesa Técnica de TI.
7. No se deben realizar conexiones externas a redes públicas inseguras desde dispositivos móviles que sean propiedad de la Agencia Nacional de Tierras.
8. La Secretaría General tiene la potestad de realizar la desactivación, borrado y retiro de los accesos a los sistemas institucionales, cuando el dispositivo móvil haya sido extraviado o robado al funcionario o contratista responsable.
9. Los funcionarios o contratistas a los que se les autorice el uso de dispositivos móviles de la entidad deben seguir los siguientes lineamientos de seguridad para equipos móviles:

a) Los equipos, información o software de propiedad de la Agencia no deben salir sin autorización.
b) Para el retiro de los equipos de la Entidad se debe tramitar autorización ante la Secretaría General, aplicando los procedimientos definidos por la Entidad.
c) Cuando se autorice el retiro de equipos de propiedad de la Entidad se debe registrar el tiempo que se autoriza la salida del equipo. La fecha de salida y la fecha en que el equipo vuelve a las instalaciones de la Entidad, conforme el formato publicado en el Sistema Integrado de Gestión – SIG, ADMBS-F-032 FORMA SALIDA INDIVIDUAL DE ELEMENTOS V4.
d) Al retornar el equipo a las instalaciones se debe reportar a las áreas responsables de los mismos los eventos o incidentes que afectaron directa o indirectamente al equipo.
e) Los equipos propiedad de la Agencia no deberían ser retirados sin seguros que cubran hurto o daño parcial o total.
f) Al salir de las instalaciones de la Entidad, los equipos deben ser transportados en condiciones de seguridad que eviten impactos que puedan afectar su integridad.
g) Al llegar a las instalaciones en donde se usará el equipo se deben registrar ante el personal de vigilancia indicando marca, modelo, número de serie y siga las instrucciones del personal de vigilancia autorizado, igualmente registrar la salida del equipo ante el personal de vigilancia.

7.6 Relaciones con proveedores

Objetivo: Preservar los niveles de seguridad y privacidad de los activos de información que están bajo responsabilidad de la ANT cuando se autorice su uso por parte de proveedores.

Obligaciones:

1. Cuando se requiera otorgar acceso a los activos de información a los proveedores de la ANT, la Secretaría General y el responsable funcional del activo con apoyo de la Mesa Técnica de TI, deberá realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y la respectiva autorización de tratamiento en los casos que aplique conforme a los procedimientos legales y administrativos.
2. Antes de conceder los permisos de acceso se debe determinar por parte del responsable del activo: las necesidades del acceso, el acceso requerido (físico o lógico), el nivel de calificación de la información a acceder, la finalidad de uso, los controles mínimos a tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información.
3. Antes de conceder acceso a la información bajo custodia de la ANT a un proveedor o parte interesada se deben validar los antecedentes del proveedor o parte interesada conforme a los procedimientos establecidos por la Entidad, con el objeto de garantizar el adecuado manejo de la información.
4. En ningún caso se debe otorgar acceso a la información, sistemas de información o de procesamiento de información de la ANT a contratistas, proveedores o partes interesadas,

hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual y firmado el acuerdo de confidencialidad.

5. Dentro de los acuerdos, contratos o convenios formalmente firmados entre las partes se deberán definir claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de calificación, finalidad del tratamiento de la información, personal que está autorizado para el tratamiento de la información; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del contratista, proveedor o parte interesada.
6. Siempre que se otorgue acceso a la información bajo custodia de la ANT a contratistas, proveedores o partes interesadas, se deben establecer acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de la Entidad y cláusulas requeridas para proteger la información a acceder.
7. Todos los contratistas, proveedores o partes interesadas que tengan acceso a la información deben cumplir con las políticas de seguridad de la información de la ANT, así mismo, en caso de que identifiquen una amenaza que pueda llegar a vulnerar la información, deberán reportarla a Subdirección de Sistemas de Información de Tierras y/o a la Secretaría General.
8. El responsable del activo de información no permitirá el acceso a la información hasta no tener firmados y formalizados, por medio de un contrato, acuerdo o convenio con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

7.7 Teletrabajo

Objetivo: Definir las pautas y reglas generales para preservar la seguridad de la información de la ANT frente a riesgos asociados al teletrabajo.

Obligaciones:

1. Las actividades de teletrabajo sólo se podrán llevar a cabo siempre y cuando se establezcan controles de seguridad alineados con las políticas de seguridad y privacidad de la información de la entidad y frente al respectivo análisis del riesgo.
2. Una vez la ANT realice los análisis respectivos para la autorización de las actividades de teletrabajo por parte de sus funcionarios, la Mesa Técnica de TI evaluará la disponibilidad de los recursos tecnológicos y organizacionales para la adopción de un modelo de teletrabajo, que permitan cumplir con los intereses y necesidades de la entidad, considerando los requisitos que establezcan el Ministerio del trabajo y la seguridad social y el Ministerio de las Tecnologías de Información y las Telecomunicaciones.
3. Para el desarrollo de las actividades de teletrabajo se debe realizar un análisis de riesgos, a partir del cual se adopten los mecanismos de control para la protección de la información y los sistemas de información de la Entidad cuando sean utilizados mediante la modalidad de Teletrabajo.

4. Antes de llevar a cabo cualquier actividad de teletrabajo, se definirá entre la ANT y el funcionario, el alcance de las actividades a desarrollar y se determinarán como mínimo: la información a acceder, el horario de las actividades y los sistemas y servicios requeridos conforme con las necesidades de la ANT y la legislación colombiana vigente.
5. En caso de pérdida o hurto de un equipo en el cual se lleven actividades de teletrabajo, será responsabilidad del funcionario informar de forma inmediata a Secretaría General del evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información potencialmente afectada.
6. La oficina Jurídica con el apoyo de la Subdirección de Talento Humano y la Mesa Técnica de TI determinará las condiciones de seguridad de la información en los contratos o acuerdos con los funcionarios autorizados para laborar en la modalidad de teletrabajo, determinando las condiciones, responsabilidades conforme las necesidades de la ANT y la normatividad colombiana vigente.
7. La Secretaría General, con la información remitida por la Subdirección de Talento Humano, brindará el acceso a la información o sistemas de información que puedan ser utilizados a través de los equipos usados para las actividades de teletrabajo, de acuerdo con el análisis de riesgos realizado por la dependencia en la que labore el teletrabajador.
8. La Mesa Técnica de TI es la dependencia responsable de implementar los controles de seguridad necesarios para llevar a cabo las actividades de teletrabajo.
9. Los funcionarios que se encuentren autorizados para el desarrollo de actividades de teletrabajo deben cumplir con las responsabilidades y políticas de seguridad institucionales, así mismo reportar cualquier situación que pueda afectar el desarrollo de las actividades o ponga en peligro la información institucional.
10. La Mesa Técnica de TI y la Secretaría General en coordinación con la Subdirección de Talento Humano, realizará las campañas de sensibilización sobre las buenas prácticas de seguridad a aplicar durante las actividades de teletrabajo.
11. La Secretaría General es la responsable de establecer controles de seguridad en equipos de teletrabajo, coordinar la realización de copias de respaldo, tratamiento de malware, control de navegación por Internet, restricción de acceso a información entre otros.
12. La Secretaria General es la dependencia responsable de implementar protocolos que den respuesta a situaciones de alerta de riesgo de seguridad o falla en los equipos autorizados para actividades de teletrabajo.

7.8 Escritorio limpio, pantalla limpia

Objetivo: Establecer los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o por fuera de las horas laborales.

Obligaciones:

Para lograr un adecuado aseguramiento de la información los funcionarios y de la ANT deben adoptar buenas prácticas para el manejo y administración de la información física y electrónica que se

encuentra a su cargo, conforme a su calificación, con el fin de evitar que personas no autorizadas accedan a dicha información. Para ello, los funcionarios, contratistas o partes interesadas deben cumplir los siguientes lineamientos:

1. Guardar en forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) conforme los niveles de calificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.
2. Durante los lapsos de tiempo en los que se deja desatendidas las estaciones de trabajo, se debe bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida en el computador.
3. Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada de trabajo laboral o cuando una ausencia temporal supere las cuatro horas.
4. Al imprimir información reservada o pública clasificada, los documentos deben ser retirados de las impresoras de forma inmediata para evitar divulgación no autorizada de la información.
5. Los archivos que contengan información sensible o confidencial deberán ser almacenados en rutas que impidan el fácil acceso por terceros, evitando, guardarlos en el área de escritorio de la pantalla del computador.
6. La Secretaría General, es la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado.
7. El fondo del escritorio y protector de pantalla son de uso institucional y no deben ser modificados sin autorización.
8. Los funcionarios, contratistas o partes interesadas que tenga dentro de sus responsabilidades la atención al público, deben almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.
9. Todo funcionario, contratista o parte interesada debe aplicar todos los controles de seguridad pertinentes definidos por el Sistema de Gestión de Seguridad de la Información para prevenir el uso no autorizado de su estación de trabajo cuando esté desatendida, incluyendo:

    a) Bloqueo de sesión.
    b) Almacenamiento de información reserva o clasificada fuera del alcance de personal no autorizado.
    c) Apagado del equipo al finalizar la jornada laboral.
    d) Mantener en su puesto de trabajo únicamente la información con la que está trabajando en un momento determinado.
    e) Evitar la visualización de información física o electrónica a personal no autorizado desde su puesto de trabajo.

7.9 Respaldo de información

Objetivo: Definir los lineamientos generales para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información.

Obligaciones:

1. La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos de la ANT debe ser respaldada conforme a los lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como a los niveles de calificación de la información institucionales.
2. Los tiempos de preservación de las copias de respaldo deben ser definidos teniendo en cuenta los requerimientos de los procesos institucionales, así como también la tecnología requerida para la restauración de la información contenida en esas copias de respaldo.
3. Para la realización de las copias de respaldo, el responsable de la información debe formular un requerimiento a Secretaria General, determinando la necesidad de respaldo de información, el tipo de información a salvaguardar, frecuencia requerida para la toma de la copia de respaldo, niveles de calificación de la información y el tiempo de retención de las copias.
4. Las copias de respaldo se deben almacenar de forma segura para garantizar que no sean manipuladas por personal no autorizado.
5. Se deben registrar todas las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de estas.
6. El responsable de las copias de respaldo debe realizar las respectivas pruebas de restauración conforme a los propósitos para las cuales han sido recaudadas.
7. Las copias de respaldo deben ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información.
8. Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo, estos medios deben ser eliminados o sometidos a disposición final de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas. Los procesos de eliminación o disposición final deben cumplir con la normatividad vigente en materia de dispositivos de residuos electrónicos.
9. Los funcionarios, contratistas o partes interesadas responsables de la infraestructura, sistemas de información y bases de datos requeridas para la operación de los procesos institucionales, deben generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.
10. Los responsables de la información serán los encargados de evaluar que las copias de respaldo se realicen de acuerdo con lo estipulado y que las estrategias utilizadas se ajusten a las necesidades y requerimientos misionales.
11. Los funcionarios y contratistas de la ANT deben almacenar la información requerida para sus procesos operativos, en la ubicación establecida por la Mesa Técnica de TI, con el fin de garantizar la disponibilidad y copias de respaldo de cada una de las áreas, así mismo son responsables de depurar la información para la optimización de los recursos institucionales.

7.10 Ciberseguridad

Objetivo: Facilitar la aplicación de buenas prácticas y controles de ciberseguridad que permitan mejorar la resiliencia de la Entidad ante ataques cibernéticos. Fomentar la integración de las prácticas de gestión de ciberseguridad, seguridad digital y gestión de riesgos para reducir los impactos potenciales de amenazas o ataques cibernéticos.

A fin de lograr sus objetivos, la ciberseguridad de la ANT adopta los siguientes lineamientos:

a) La gestión de la ciberseguridad debe buscar el mejoramiento continuo de la seguridad digital.
b) Las actividades de ciberseguridad deben estar orientadas a reducir los impactos adversos de los incidentes de seguridad de la información.
c) El foco principal de la ciberseguridad es la prevención sobre la reacción.
d) En cuanto sea posible se debe buscar la preservación de las evidencias de los incidentes de seguridad de la información.
e) La gestión de la ciberseguridad debe apoyar las decisiones sobre uso de recursos y definición de los presupuestos en seguridad digital.
f) Los resultados de la gestión de la ciberseguridad deben permitir la actualización del análisis de riesgos.
g) La ciberseguridad debe apoyar el desarrollo de los programas de capacitación y toma de conciencia.
h) La ciberseguridad debe ser un insumo para el mejoramiento de las políticas y documentación de gestión de la seguridad digital.
i) La gestión de la ciberseguridad debe buscar el cumplimiento de las normas legales y regulaciones del sector Agricultura y Desarrollo Rural.
j) La gestión de la ciberseguridad debe alinearse con la gestión de las infraestructuras de TI y las estrategias de negocio.
k) Los roles y responsabilidades asociadas a la gestión de la ciberseguridad deben estar claramente definidas y aceptadas por los diferentes responsables.
l) Los resultados de la gestión de ciberseguridad se deben comunicar a todas las partes interesadas pertinentes, incluida la organización interna, organismos de control y terceras partes involucradas.
m) La gestión de la ciberseguridad debe contribuir a mantener la continuidad de las operaciones críticas misionales y mantener la disponibilidad de la información a un nivel aceptable ante el evento de una interrupción significativa.
n) Las respuestas ante incidentes deben estar soportadas en procesos y procedimientos planificados que aseguren su pertinencia y oportunidad.
o) Los procesos y procedimientos para la recuperación ante incidentes deben ser ejecutados en forma oportuna para garantizar la restauración oportuna de los sistemas afectados.
p) Los procesos de recuperación ante incidentes deben ser mejorados continuamente mediante las lecciones aprendidas.

Obligaciones:

Para impulsar el desarrollo de capacidades institucionales en materia de ciberseguridad, la Mesa Técnica de TI propenderá por:

1. Analizar y proponer las actualizaciones a la política de ciberseguridad institucional.
2. Analizar los incidentes de ciberseguridad que le son escalados y activa el procedimiento de contacto con las autoridades y grupos de interés especial, cuando lo estime necesario.
3. Realizar una gestión efectiva de la seguridad de la información y la ciberseguridad en la entidad.
4. Sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciber-amenazas.
5. Asesorar al comité institucional de gestión y desempeño en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia.
6. Realizar análisis de riesgo para los sistemas de información (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).
7. Sugerir anualmente los proyectos y/o presupuestos en materia de seguridad de la información y ciberseguridad.
8. Proponer los controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.
9. Definir y medir periódicamente los indicadores para evaluar la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.
10. Identificar y proponer, los controles para la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
11. Realizar análisis sobre la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos y presentar la evaluación y recomendaciones al comité institucional de gestión y desempeño.
12. Identificar y en la medida de lo posible, medir los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación.
13. Adoptar los procedimientos, así como los mecanismos que puedan identificar y analizar los incidentes de ciberseguridad que se presenten.
14. Preservar cuando sea posible las evidencias digitales para que las autoridades puedan realizar las investigaciones correspondientes.
15. Proponer ajustes a los sistemas de gestión de riesgo, de seguridad de la información y controles de seguridad como resultado de los incidentes presentados.
16. Socializar cuando sea pertinente, las lecciones aprendidas en materia de gestión de incidentes al interior de la Entidad y con las entidades de su sector.
17. Mantener dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.
18. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.

19. Mantener actualizadas y en operación las herramientas y/o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.
20. Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector agropecuario y a nivel nacional.
21. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
22. Monitorizar continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.
23. Aplicar el procedimiento de gestión de incidentes cuando se presenten estos para determinar los elementos de la red para identificar dispositivos que pudieran haber resultado afectados.
24. Reportar al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.
25. Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

7.11 Desarrollo Seguro

Objetivo: Definir e implementar todos los requisitos de Seguridad de la Información dentro del ciclo de vida de desarrollo de software.

Obligaciones:

1. Se deben identificar y acordar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se deben justificar, acordar y documentar.
2. Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
3. El cambio de versionamiento en el ambiente de producción debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso que se deba dar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
4. Se deben realizar pruebas de seguridad en el ambiente de pruebas, con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.
5. Los ambientes de desarrollo, pruebas y producción, deben estar separados.
6. Los usuarios y/o terceros que están involucrados en esta instancia, deben utilizar perfiles diferentes en el ambiente de desarrollo, pruebas y producción; además, asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente.
7. El ambiente de prueba debe simular el ambiente de producción. Sin embargo, los datos de prueba utilizados, a pesar de corresponder a una estructura similar a la de producción, deben utilizarse traslapados, para garantizar la seguridad y protección de los datos.
8. En caso de requerirse hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información se encuentra enmascarada, con el fin de que no se llegue a comprometer.

8 SENSIBILIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Conforme se establece en el Plan Operativo Anual de la ANT, las buenas prácticas frente a la seguridad de la información y la norma ISO27001 acerca de la seguridad ligada a los recursos humanos (A7), "*A.7.2.2 Concientización, educación y formación en seguridad de la información*"; la SSIT debe coordinar con la Subdirección de Talento Humano el desarrollo de programas o planes de capacitaciones periódicas sobre seguridad de la información a todos los colaboradores de la ANT. Cuando sea pertinente la SG y la SSIT deben informar sobre las políticas y los procedimientos de seguridad de la información a los colaboradores de la Agencia con el objetivo de concientizar y fomentar la cultura de la seguridad de la información.

9 NORMATIVIDAD APLICABLE A SEGURIDAD DE LA INFORMACIÓN

Constitución Política de Colombia, Artículos 15 y 20.
Ley 23 de 1982, Sobre derechos de autor.
Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.
Ley 850 de 2003, Por medio de la cual se reglamentan las veedurías ciudadanas.
Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 1336 de 2009, Por la cual se adiciona y robustece la ley 679 de 2001, de lucha contra la explotación, la pornografía y el Turismo sexual con niños, niñas y adolescentes.
Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC.
Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
Ley 1672 de 2013, Lineamientos para la Adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos.
Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1071 de 2015, Decreto Único Reglamentario del Sector Agricultura y Desarrollo Rural.

Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 1483 de 2015, Decreto Único Reglamentario del Sector Función Pública
Documento CONPES 3854, Política Nacional de Seguridad Digital.
NTC-ISO/IEC 27001:2013, Norma NTC ISO/IEC, Sistema de Gestión de Seguridad de la Información.
GTC-ISO/IEC 27002:2015, Es una guía que proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y la gestión de controles definidos en el Anexo A.

10 GLOSARIO

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (ejemplo: Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar su nivel de impacto en la organización.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: entorno complejo que resulta de la interacción de las personas, software y servicios a través de Internet por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna. ISO 27032.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano. Con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

Dato sensible: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado o personal: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: "… Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas; …". (Ley 1266 de 2008).

Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disco duro: Hard Disk Drive (HDD) corresponde a un disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos duros tienen una vida útil limitada. Las Unidades de Estado Sólido (SSD), son otro tipo de disco duro más veloz que los HDD, estas unidades de almacenamiento de información se basan en chips de memoria de acceso instantáneo.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Impacto: el costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

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

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (Stakeholder): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Responsable de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

Responsable del tratamiento: persona natural o jurídica, Pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Segregación de tareas: reparto de tareas sensibles entre distintos funcionarios para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Titular de la información: es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de la Ley de Hábeas Data y demás derechos y garantías a que se refiere la presente ley.

Teletrabajo: actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo.

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
14/09/2017	1	Primera versión del documento.
24/09/2018	2	Segunda versión del documento.
01/02/2019	3	Tercera Versión. Actualización del lineamiento para contemplar actualización de la política de gobierno digital de MINTIC
19/09/2022	4	Cuarta Versión. Se actualiza versión por cambios organizacionales y del entorno.

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