MANUAL DE POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso Información, Innovación y Tecnología
Subproceso Seguridad de la Información
VERSIÓN 5
MN-IIT-0072
Año 2023

El contenido de este documento corresponde a Información Pública

TABLA DE CONTENIDO

1. OBJETIVO

Proporcionar a los usuarios internos y externos de la **Unidad Administrativa Especial - Dirección de Impuestos y Aduanas Nacionales (DIAN)**, las políticas y lineamientos de obligatorio cumplimiento con el fin de gestionar la Seguridad y Privacidad de la Información en función de los principios de integridad, confidencialidad, disponibilidad y no repudio de la información.

2. ALCANCE

Este manual aplica a todos los usuarios internos y externos de la entidad, establece las políticas y lineamientos de carácter administrativo y técnico que deben ser consideradas en el manejo de cualquier tipo de información (física y digital de la **DIAN**), en los lugares donde la entidad tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio, transferencia y consulta de información, en el desarrollo de su misión institucional y cumplimiento de sus objetivos estratégicos.

Las políticas y lineamientos establecidos se encuentran enmarcados en El Modelo de Seguridad y Privacidad de la Información MSPI y la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), así como en la norma ISO/IEC 27001:2022, la Ley 1581 de 2012 de Protección de Datos Personales, la Ley 1712 de 2014 Transparencia y Acceso a la Información Pública y Reservada, entre otras, adoptadas por la entidad y que son necesarias para la protección de los activos de información de la **DIAN**.

3. DEFINICIONES Y SIGLAS

Todas las definiciones y siglas presentados en el contenido de este documento están exhaustivamente detallados y explicados en el Anexo Definiciones y Siglas de Seguridad y Privacidad de la Información, el cual, ha sido cuidadosamente elaborado para proporcionar una comprensión precisa y completa de los conceptos utilizados.

4. RESPONSABILIDAD Y CUMPLIMIENTO

Los siguientes documentos: (1) MSPI - El Modelo de Seguridad y Privacidad de la Información - OD-IIT-0001, (2) Manual para la Protección de Datos Personales - MN-IIT-0062, (3) Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información - MN-IIT-0072, (4) Procedimiento de Gestión de Activos de Información - PR-IIT-0366 y (5) Cartilla Gestión de Riesgos de Seguridad - CT-IIT-0132 deben ser aplicados con estricto cumplimiento por parte de todos por los directivos, funcionarios, contratistas, consultores, pasantes, proveedores y otros terceros que presten sus servicios o tengan algún tipo de vinculación con la **DIAN**, para el correcto cumplimiento de sus funciones y para conseguir un adecuado nivel de seguridad y protección de los activos de información.

El incumplimiento de lo estipulado en estos documentos acarreará las acciones disciplinarias a las que haya lugar, sin perjuicio de las acciones penales, administrativas o fiscales. Las acciones disciplinarias se regirán de acuerdo con el Código Disciplinario vigente.

5. LINEAMIENTOS Y POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se definen los lineamientos y políticas para los diferentes tipos de control los cuales son:

5.1 Organizacionales
5.2 De personas

5.3 Físicos
5.4 Tecnológicos
5.5 Adicionales (este último definido por la Entidad)

Establecidos en el ANEXO A de acuerdo con los controles de seguridad de la información de la norma ISO/IEC 27001:2022.

5.1 Controles organizacionales

Se describen los lineamientos que hacen referencia a los roles y responsabilidades en seguridad y privacidad de la información que establece la **DIAN**:

5.1.1 Políticas de seguridad de la información

A. Objetivo de control: Definir la idoneidad y adecuación de las políticas de seguridad y privacidad de la información de la **DIAN,** teniendo en cuenta requisitos legales y la misión institucional.

B. Alcance: El alcance de esta política aplica para todos los funcionarios y terceros de la **DIAN** (servidores públicos, funcionarios vinculados a la planta permanente y provisional, contratistas, consultores, pasantes, proveedores de bienes, entidades del estado, entes de control) que desempeñen alguna actividad con la **DIAN** o a nombre suyo.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad

D. Lineamientos:

1. La Oficina de la Seguridad de la Información debe:

    a. Emitir las políticas y lineamientos relacionados con la Seguridad y Privacidad de la Información en el campo de los datos y la información.
    b. Revisar una vez al año las políticas y lineamientos relacionados con la seguridad y privacidad de la información y determinar si es necesario ajustarlas según las necesidades y cambios de la entidad.
    c. Presentar ante el Comité Institucional Estratégico las políticas y lineamientos relacionados con la Seguridad y Privacidad de la Información para su aprobación.
    d. Solicitar la publicación de las políticas y lineamientos relacionados con la Seguridad y Privacidad de la Información para poder ser consultada por la ciudadanía en general.

E. Controles relacionados: No aplica.

5.1.2 Roles y responsabilidades para la seguridad de la información

A. Objetivo de control: Definir los roles y la asignación de responsables para cada acción establecida dentro de la planeación de seguridad de la información como aspecto fundamental para el correcto funcionamiento del MSPI.

B. ALCANCE: El alcance de este lineamiento aplica para todos los funcionarios y terceros con roles y responsabilidades relacionadas con la Seguridad y Privacidad de la Información.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Implementar y gestionar el Modelo de Seguridad y Privacidad de la Información en la entidad.
   b. Generar el gobierno de identidades, roles y responsabilidades, en seguridad y privacidad de la información.
   c. Revisar y actualizar la matriz de roles y responsabilidades de seguridad y privacidad de la información, mínimo una vez al año o cada vez que se requiera.
   d. Estructurar, diseñar y administrar el Programa Integral de Gestión de Datos Personales.
   e. Dar a conocer a los funcionarios y terceros de la **DIAN**, el Modelo de Seguridad y Privacidad de la Información establecido en la entidad.
   Efectuar el monitoreo al grado de implementación del Modelo de Seguridad y Privacidad de la Información.

2. Los jefes de las dependencias deben:

   a. Identificar los activos de información y conservar su seguridad. Los propietarios de los activos de información son los responsables de aplicar y cumplir los controles que mitiguen la afectación a la disponibilidad, confidencialidad e integridad de los activos de información.
   b. Designar a los enlaces de seguridad de la información, quienes deben dar cumplimiento a los lineamientos, políticas y demás reglamentación establecida con el fin de implementar el Modelo de Seguridad y Privacidad de la Información.
   c. Identificar los riesgos de seguridad de la información y dar cumplimiento a los planes de tratamiento y mitigación de estos.
   d. Crear la documentación que está bajo su responsabilidad para dar cumplimiento a las políticas definidas en este documento.

E. Controles relacionados:

1. 5.1 – Políticas de seguridad de la información

5.1.3 Segregación de funciones

A. Objetivo de control: Segregar las funciones clave para separar las responsabilidades de las dependencias de la entidad y permitir reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de información. Los lineamientos y las políticas están alineadas con las funciones definidas en el Decreto 1742 de 2020, el cual establece la nueva estructura y organización de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para todos los funcionarios y/o terceros que desarrollen funciones de acuerdo con las políticas de seguridad y privacidad de la información de la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Generar el gobierno de identidades (roles y responsabilidades) y monitorear las directrices relacionadas con el control y asignación de permisos para el acceso a las instalaciones, dependencias seguras y sistemas de información de la entidad.
   b. Actualizar la segregación de funciones de acuerdo con la matriz de roles y responsabilidades en seguridad y privacidad de la información, mínimo una vez al año o cada vez que se requiera.
   c. Revisar la segregación de funciones de seguridad de la información e incluirlo en la matriz de roles y responsabilidades del punto anterior.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Definir la segregación de funciones para los procesos y procedimientos que se definan para el cumplimiento de las políticas establecidas en este documento.
   b. Definir la segregación de funciones para el acceso y flujos de trabajo en los sistemas de información en la entidad, también para el personal que requiere ingreso a los *datacenters* o suscripciones de computación en la nube.
   c. Definir los respectivos controles para la segregación de funciones desde el inicio de desarrollo de los proyectos tecnológicos y acompañar los relacionados con desarrollos tecnológicos o adquisiciones de software de otras dependencias.

3. Los dueños de los Sistemas de Información deben:

   a. Definir los controles a implementar para evitar que una misma persona tenga acceso a dos o más responsabilidades dentro de un mismo sistema, para impedir realizar acciones o transacciones que ocasionen el uso indebido de los activos y/o cometer conductas fraudulentas.

4. Los jefes de las dependencias deben:

   a. Determinar los procedimientos y lineamientos a implementar para evitar que una persona pueda acceder, modificar o usar los activos de su competencia sin autorización ni detección.
   b. Aplicar controles compensatorios cuando la segregación de funciones sea difícil o imposible de conseguir. Entre estos controles, se encuentran:
      a) la revisión periódica de las actividades, lo que permite su supervisión mientras están en desarrollo, como una forma de validar que se lleven a cabo de manera correcta
      b) los rastros de auditoría
      c) la supervisión de la gestión.

5. Los funcionarios y terceros de la entidad deben:

    a. Conocer sus funciones y responsabilidades dentro de la entidad teniendo en cuenta para ello la matriz de roles y responsabilidades, los procesos y/o procedimientos y el manual de funciones, así como los lineamientos establecidos en este manual.

E. Controles relacionados: No aplica.

5.1.4 Responsabilidades de la dirección

A. Objetivo de control: definir responsabilidades de la dirección y comprender su papel en la seguridad y privacidad de la información, así como requerir a todo el personal que aplique las políticas establecidas en este documento.

B. Alcance: el alcance de este lineamiento aplica a los funcionarios de la entidad que ejecutan responsabilidades de la dirección en la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. El Comité Institucional Estratégico debe:

    a. Adoptar el presente documento como parte integral del Modelo de Seguridad y Privacidad de la Información.
    b. Requerir a todos los funcionarios y terceros el cumplimiento normativo interno de la entidad (políticas, directrices, lineamientos y procedimientos establecidos), así como la normatividad externa a la entidad relacionada con seguridad y privacidad de la información.
    c. Promover el compromiso de todos los niveles de responsabilidad y autoridad de la **DIAN** en la implementación del Modelo de Seguridad y Privacidad de la Información.
    d. Verificar el cumplimento de las políticas de seguridad y privacidad de la información y los objetivos definidos, alineados con las necesidades de la **DIAN**.
    e. Gestionar la integración de los lineamientos del Modelo de Seguridad y Privacidad de la Información con los procesos y procedimientos definidos en la **DIAN**.
    f. Comunicar la necesidad de definir y mantener una gestión de la seguridad y privacidad de la información representada por medio de los objetivos y las políticas de seguridad.
    g. Respaldar y promover a las personas para que contribuyan al desarrollo del Modelo de Seguridad y Privacidad de la Información y adquieran un rol de liderazgo en cada una de sus dependencias de responsabilidad.
    h. Gestionar los recursos requeridos para el mantenimiento del Modelo de Seguridad y Privacidad de la Información.

2. La Oficina de Seguridad de la Información debe:

    a. Divulgar y capacitar a los funcionarios de la entidad acerca de las políticas y lineamientos de seguridad y privacidad de la Información establecidos en este documento.

b. Definir y gestionar programas de capacitación, entrenamiento y educación que incluyan temas relevantes y pertinentes sobre seguridad y privacidad de la información.
c. Generar los lineamientos y políticas para la implementación del Modelo de Seguridad y Privacidad de la Información en la **DIAN** en concordancia con las políticas de seguridad y sus objetivos.
d. Verificar junto con las dependencias, la identificación y evaluación de los riesgos de seguridad de la información, identificación y valoración de activos y demás temas relacionados con la seguridad y privacidad de la información, para seleccionar y aplicar el plan de tratamiento de riesgos más adecuado.
e. Verificar que las dependencias realicen el análisis y evaluación de riesgos de seguridad de la información por lo menos una vez al año.
f. Establecer las herramientas y los procedimientos que permitan monitorear, hacer seguimiento y facilitar el reporte de eventos e incidentes de seguridad y/o privacidad de la información, que se consideren como incumplimiento de las responsabilidades establecidas en este numeral.
g. Realizar el monitoreo y el seguimiento de manera permanente al cumplimiento de las responsabilidades establecidas en los principios y lineamientos de este numeral.
h. Diseñar, implementar, supervisar y optimizar el Centro de Operación de Seguridad de la Información, aprovechando la información proporcionada para la toma de decisiones.
i. Definir y gestionar en coordinación con la Dirección de Innovación y Tecnología, o la dependencia que haga sus veces, los procedimientos de continuidad operativa y recuperación en caso de desastres, respecto de la infraestructura tecnológica de la **DIAN**.

3. Los jefes de las dependencias deben:

a. Promover el cumplimiento, por parte del personal bajo su responsabilidad, de las políticas, lineamientos, directrices y procedimientos de seguridad y privacidad de información.
b. Aplicar los controles establecidos por la **DIAN** para activar o desactivar, de manera temporal o permanente, el acceso a la información digital catalogada como pública clasificada, pública reservada y datos personales no públicos, por parte del personal que esté vinculado a la entidad utilizando DLP (prevención de pérdida de datos).
c. Clasificar los activos de información de su proceso de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.
d. Realizar mínimo una vez al año el análisis de riesgos de seguridad de la información para cada proceso con el apoyo de la Oficina de Seguridad de la Información y así determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de información de acuerdo con la guía de gestión de riesgos.
e. Definir los requerimientos de seguridad y privacidad de la información de cada proceso con el acompañamiento de la Oficina de Seguridad de la Información para los activos de información bajo su responsabilidad, para que se les proporcione un nivel adecuado de protección de conformidad con los estándares, políticas y lineamientos de seguridad y privacidad de la información.
f. Solicitar a la Oficina de Seguridad de la Información las capacitaciones sobre seguridad y privacidad de la información que le competa a la dependencia.
g. Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con su proceso, incluyendo los controles de seguridad y privacidad de la información.

h. Hacer seguimiento al cumplimiento de las obligaciones en materia de seguridad y privacidad de la información de su proceso.
i. Reportara la Oficina de Seguridad de la Información de los eventos o incidentes relacionados con el incumplimiento de las responsabilidades frente a la seguridad y privacidad de la información, descritos en los principios y lineamientos de este documento.
j. Incorporar la seguridad y privacidad de la información como parte de las actividades y tareas asignadas a su dependencia.

E. CONTROLES RELACIONADOS:

1. 6.3 - Concientización, educación y capacitación en seguridad de la información

5.1.5 Contacto con las autoridades

A. Objetivo de control: mantener contacto con las diferentes autoridades que puedan apoyar a solucionar incidentes de seguridad y privacidad de la información identificados en la **DIAN**.

B. Alcance: el alcance de este lineamiento aplica a la Oficina de Seguridad de la Información, dependencia encargada de establecer y mantener contacto con las autoridades pertinentes.

C. Características del control:

1. Tipo de control: preventivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Establecer los procedimientos y/o protocolos requeridos para contactar a las autoridades responsables de dar atención en caso de presentarse un incidente de seguridad y privacidad de la información.
b. Generar un documento (circular, instructivo, procedimiento, entre otros) que sea aplicado por los diferentes usuarios internos para reportar a esta oficina, ya sea de manera digital o manual, los incidentes de seguridad y privacidad de la información identificados y que a su vez deban ser gestionados de manera oportuna ante las autoridades nacionales.
c. Reportar a la Superintendencia de Industria y Comercio los incidentes relacionados con protección de datos personales, de acuerdo con el protocolo establecido por dicha entidad.
d. Establecer el canal de comunicación autorizado para contactar a las autoridades nacionales a las que se reportarán, en caso de ser requerido, los incidentes de cualquier índole que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información. Evaluar los eventos de violación de seguridad de la información presentados en la entidad y determinar las acciones que se deben adoptar, siendo una de ellas la de reportar a las autoridades nacionales competentes en la materia.
e. Mantener la relación con autoridades para contactarlas de manera oportuna en casos de presencia de un incidente de seguridad de la información, tales como Centro Cibernético Policial (CCP C4), Grupo de Respuesta a Emergencias Cibernéticas en Colombia (COLCERT), Centro de Coordinación Seguridad Informática Colombia

(CSIRT-CCIT), Policía Nacional, Superintendencia de Industria y Comercio y la Unidad Administrativa Especial Dirección de Bomberos de Colombia, entre otras autoridades.

E. Controles relacionados:

1. 5.24 – Planificación y preparación de la gestión de incidentes de seguridad de la información.
2. 5.28 – Recopilación de pruebas.
3. 5.29 – Seguridad de la información durante la interrupción.
4. 5.30 – Preparación de las TIC para la continuidad del negocio.

5.1.6 Contacto con grupos de interés especial

A. Objetivo de control: establecer y mantener contactos apropiados con grupos de interés especial u otros, foros y asociaciones profesionales especializadas en seguridad y privacidad de la información.

B. Alcance: el alcance de este lineamiento aplica a la Oficina de Seguridad de la Información, encargada de establecer y mantener contacto con los grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

C. Características del control:

1. Tipo de control: preventivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir mecanismos que permitan hacer mayor uso de las membresías en grupos o foros de interés especial en seguridad y privacidad de la información, impulsando de esta manera el desarrollo de competencias del talento humano en temáticas específicas de seguridad y privacidad de la información.
    b. Coordinar dentro de la **DIAN** las acciones requeridas para mantener contacto permanente con universidades, grupos de investigación, proveedores de tecnología, entre otros grupos de interés, que puedan ofrecer boletines, noticias, contenidos de formación y actualizaciones sobre temáticas relacionadas con seguridad y privacidad de la información, dirigidas a funcionarios que desempeñan funciones dentro del ámbito de la seguridad y privacidad de la información en la entidad.
    c. Mantener contacto con grupos especializados en seguridad y privacidad de la información, que ofrezcan recomendaciones ante incidentes que puedan vulnerar la confidencialidad, integridad y disponibilidad de la información en la entidad.

E. Controles relacionados:

1. 5.24 – Planificación y preparación de la gestión de incidentes de seguridad de la información
2. 5.28 – Recopilación de pruebas

5.1.7 Inteligencia de amenazas

A. Objetivo de control: recopilar y analizar la información relacionada con las amenazas a la seguridad y privacidad de la información de la entidad.

B. Alcance: el alcance de este lineamiento aplica a la Oficina de Seguridad de la Información de la **DIAN**, dependencia encargada de recopilar y analizar la información sobre amenazas existentes y emergentes relacionadas con la entidad.

C. Características del control:

1. Tipo de control: preventivo, detectivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir los mecanismos que faciliten las acciones informadas, para evitar que las amenazas causen daño a la entidad y reducir su impacto.
    b. Definir las herramientas, fuentes de información y metodologías para identificar las posibles amenazas cibernéticas que se puedan presentar en la entidad, con el fin de proporcionar una comprensión precisa y detallada del panorama de estas, y que agregue contexto a la información en el momento en que se pueda presentar un evento, para actuar de manera adecuada teniendo en cuenta experiencias previas en entidades similares.
    c. Recopilar la información y realizar el análisis de esta.
    d. Realizar un informe recopilando la información obtenida del análisis sobre las amenazas en la entidad, comunicarlo y socializarlo con personas y dependencias involucradas prevaleciendo los pilares fundamentales de integridad, disponibilidad y confidencialidad de la información.
    e. Implementar acciones correctivas resultado de los análisis de inteligencia de amenazas y tenerlas en cuenta en la gestión de riesgos de seguridad de la información en la **DIAN**.
    f. Utilizar y analizar la información sobre inteligencia de amenazas como entrada adicional a controles técnicos preventivos y de detección que debe implementar las diferentes dependencias de la entidad, como ejemplo: firewalls, sistemas de detección de intrusos o soluciones antimalware.
    g. Analizar y utilizar la información para los procedimientos y técnicas de pruebas de seguridad y privacidad de la información en la entidad.
    h. Compartir la información sobre inteligencia de amenazas con otras entidades de forma mutua para mejorar los conocimientos en relación con las experiencias obtenidas.

E. Controles relacionados:

1. 5.25 – Evaluación y decisión sobre eventos de seguridad de la información
2. 8.7 – Protección contra malware
3. 8.16 – Actividades de seguimiento
4. 8.23 – Filtrado web

5.1.8 Seguridad de la información en la gestión de proyectos

A. Objetivo de control: integrar la seguridad de la información en la gestión de proyectos de la entidad para tratar los riesgos de seguridad de la información.

B. Alcance: el alcance de este lineamiento aplica para todos los proyectos de tecnología que son ejecutados desde la Subdirección de Innovación y Proyectos.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Innovación y Proyectos o quien haga sus veces debe:

   a. Determinar la criticidad de la información que se utilizará en el proyecto, teniendo como base la clasificación de los activos de información.
   b. Definir en el proyecto, el tiempo que la información será utilizada, los periodos de conservación de la información y la accesibilidad a la información por parte de los funcionarios y terceros de la entidad.
   c. Incluir la privacidad de la información y los datos personales en el análisis de riesgos, previo al proyecto.
   d. Gestionar los respectivos acuerdos de confidencialidad y de entrega de información según la normatividad vigente en la entidad.
   e. Implementar las mejores prácticas relacionadas con el desarrollo seguro y pruebas de penetración para gestionar desde el inicio las debilidades de seguridad en los proyectos que incluyan desarrollo de sistemas de información.
   f. Determinar si en el proyecto van a participar terceros y si aplica gestionar las cláusulas de cumplimiento según las normas aplicables, la autorización de tratamiento de datos, la cláusula de confidencialidad de la información y de aceptación de las políticas de seguridad.
   g. Evaluar, tratar y hacer seguimiento a los riesgos de seguridad de la información y datos personales asociados a los proyectos, durante todo el ciclo de vida del proyecto (al inicio, durante la ejecución y al finalizar).

2. La Oficina de Seguridad de la Información debe:

   a. Acompañar a la Subdirección de Innovación y Proyectos en las actividades de definición de riesgos para cada uno de los proyectos que gestiona esta dependencia.

E. CONTROLES RELACIONADOS:

1. 5.12 - Clasificación de la información
2. 5.32 - Derechos de propiedad intelectual
3. 8.26 - Requisitos de seguridad de la aplicación

5.1.9 Inventario de información y otros activos asociados

A. Objetivo de control: desarrollar y mantener actualizado el inventario de activos de información. Los activos de información son el insumo principal de la entidad para la ejecución de la gestión de riesgos de seguridad de la información y adicionalmente, para generar el índice de Información Clasificada y Reservada y la matriz de Inventario de activos de Información.

B. Alcance: el alcance de este lineamiento aplica para todos los jefes de las dependencias de la **DIAN** que poseen facultades para identificar, clasificar y administrar activos de información con los que desarrollan sus funciones.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Información y Analítica debe:

    a. Ejercer gobierno teniendo en cuenta los activos de información definidos por las diferentes dependencias de la entidad, para tener autoridad y control sobre la información, a través de la implementación de procedimientos, circulares y otros instrumentos relacionados con la recolección, calidad, consistencia (limpieza de datos), y uso, en coordinación con otras dependencias de la entidad, en el marco de sus competencias.
    b. Definir los criterios para la identificación de activos de información junto con la Oficina de Seguridad de la Información.

2. La Oficina de Seguridad de la Información debe:

    a. Realizar capacitación y acompañamiento a todas las dependencias en lo referente a la Gestión de Activos de Información.
    b. Realizar seguimiento a la gestión de los activos de información, de acuerdo con los lineamientos referenciados en este documento (5.10, 5.12, 5.13 y 5.14) en la “sección E” de este control.
    c. Solicitar a las dependencias la actualización periódica del inventario para identificar cambios o eliminación de un activo.
    d. Definir la metodología para la gestión de activos de Información teniendo en cuenta lo relacionado con Datos Personales, el Manual para la Protección de Datos Personales, los lineamientos de MinTIC, la norma ISO 27001, los procedimientos de retención documental y demás legislación aplicable.
    e. Proporcionar la herramienta para la gestión de los activos de información y la facilitación de su identificación, registro, clasificación, valoración y tratamiento. Se deben tener en cuenta: los responsables, los tipos de activos, la ubicación y, la legislación aplicable.

3. Los jefes de las dependencias deben:

    a. Ejercer control sobre sus activos de información, administrar y mantener actualizado su inventario.

b. Realizar la gestión de los activos de información mediante el funcionario designado como “enlace de seguridad” de la Información en cada una de las dependencias.
c. Registrar los activos de información en la herramienta de gestión facilitada por la **DIAN,** siguiendo los lineamientos definidos en el procedimiento Gestión de Activos de Información. Para incluir los activos de información en los programas realizados por la Oficina de Seguridad de la Información dentro del marco del Sistema de Gestión de Seguridad y Privacidad de la Información.
d. Tener en cuenta los parámetros de las Tablas de Retención Documental de la **DIAN** para ser incluidos en los inventarios de información y otros activos asociados.
e. Realizar una revisión y actualización del inventario de activos de información cada vez que se requiera (por disposiciones internas o requerimientos de la Oficina de Seguridad de la Información) o como mínimo una vez al año.
f. Aprobar cualquier actualización realizada sobre los activos de información de la dependencia.
g. Aprobar los activos de información de su dependencia, una vez estén gestionados en su totalidad.
h. Diligenciar todos los campos que requiere la metodología de activos definida por la Oficina de Seguridad de la Información.

E. Controles relacionados:

1. 5.10 – Uso aceptable de la información y otros activos asociados
2. 5.12 – Clasificación de la información
3. 5.13 – Etiquetado de la información
4. 5.14 – Transferencia de información

5.1.10 Uso aceptable de la información y otros activos asociados

A. Objetivo de control: identificar, documentar e implementar reglas para el uso aceptable de la información y otros activos asociados con información e instalaciones de procesamiento de información.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios y/o terceros que hagan uso de la información y otros activos asociados propiedad de la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Generar un documento (circular, instructivo, procedimiento, entre otros) para ser aplicado por los diferentes usuarios internos para cumplir con el uso aceptable de los activos de información dentro de las diferentes dependencias de la entidad.
b. Capacitar a los funcionarios y/o terceros de la **DIAN,** en relación con los requisitos establecidos de seguridad de la información y privacidad, para la protección y el manejo adecuado de la información de la entidad.

c. Divulgar la política de uso aceptable de la información en la entidad a los funcionarios y/o terceros para que la conozcan y apliquen; así mismo, comunicar toda actualización de manera oportuna.
d. Incluir en la metodología de riesgos de seguridad de la información los riesgos asociados al uso aceptable de la información en la entidad.
e. Definir controles para la restricción de acceso no autorizado a los activos de información de la entidad.

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Implementar medidas cuando se utilicen entornos de trabajo colaborativos.
b. Implementar los controles para la restricción de acceso no autorizado a los activos de información definidos por la Oficina de Seguridad e la Información y realizar monitoreos periódicos para confirmar su funcionamiento correcto.
c. Establecer los mecanismos para proteger las copias temporales o permanentes de la información de los activos.
d. Conservar los activos de información (*Hardware* y *software*) de acuerdo con las recomendaciones de los fabricantes.

3. La Subdirección de Compras y Contratos debe:

a. Definir acuerdos de confidencialidad o compromisos de protección de los activos y su información de propiedad de terceros, incluyendo servicios de computación en la nube pública.
b. Vincular responsabilidad tanto civil como penal para el proveedor o la tercera parte contratada en lo relacionado al uso aceptable de los activos de la entidad.

4. Los jefes de las dependencias deben:

a. Hacer uso aceptable de los activos teniendo en cuenta la confidencialidad, integridad y disponibilidad de estos.
b. Cumplir con los requisitos de seguridad de la información que afectan a la información de la entidad, a otros activos asociados a la información y a los recursos de tratamiento de esta.
c. Gestionar, procesar y almacenar a información de acuerdo con la clasificación de los activos de información.
d. Utilizar los mecanismos establecidos por la Dirección de Gestión de Innovación y Tecnología que permitan proteger las copias temporales o permanentes de la información de los activos.
e. Suscribir los acuerdos de confidencialidad pertinentes en los formatos correspondientes, cuando exista intercambio o entrega de información a externos, contratistas o partes interesadas.

5. Los funcionarios y terceros deben:

a. Cumplir con los lineamientos y políticas establecidas sobre la responsabilidad del uso de las instalaciones de procesamiento de información en la **DIAN**.

E. Controles relacionados:

1. 5.12 – Clasificación de la información

2. 7.6. – Trabajar en áreas seguras
3. 7.8 – Ubicación y protección del equipo
4. 7.10 – Medios de almacenamiento
5. 8.10 – Eliminación de información

5.1.11 Devolución de bienes

A. Objetivo de control: devolver todos los activos de la entidad que se encuentren a cargo de los funcionarios y terceros de la **DIAN**, al terminar su contrato, empleo o acuerdo.

B. Alcance: el alcance de este lineamiento aplica a todos los funcionarios y/o terceros que posean activos físicos o electrónicos de la entidad y cambien o terminen su vinculación con la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Establecer procedimientos para la entrega y la recepción de bienes y activos físicos de la entidad por parte de los funcionarios y terceros.

2. La Subdirección de Soluciones y Desarrollo debe:

   a. Establecer lineamientos para realizar la entrega de bienes y activos de información de la entidad (dentro de estos se incluyen datos, equipos de cómputo, Hardware y Software).
   b. Identificar y documentar la información y otros activos tecnológicos asociados que deben ser devueltos en el momento de notificación de terminación vinculación, entre estos se encuentran:
   Equipo especializado.
   Hardware de autenticación (por ejemplo, llaves mecánicas, tokens físicos y tarjetas inteligentes para sistemas de información, sitios y archivos físicos).
   Copias físicas de la información.
   Equipos de cómputo.
   c. Implementar controles de restricción de copias de información no autorizadas en equipos de cómputo y dispositivos de almacenamiento, durante el período de notificación de terminación de contrato y/ o cesación de actividades temporales.

3. Los funcionarios y terceros deben:

   a. Devolver el activo de información que fue asignado para el desarrollo de sus funciones (documentos, datos, equipos de cómputo, hardware, Software, y todo elemento entregado o generado por la entidad), al finalizar su vínculo laboral o contractual, por cambio de dependencia o finalización de actividades.
   b. Hacer transferencia de la información que se haya trabajado o reproducido y efectuar su borrado general en el equipo usado.

E. Controles relacionados:

1. 5.18 – Derechos de acceso
2. 6.8. – Informes de eventos de seguridad de la información
3. 7.14 – Eliminación segura o reutilización de equipos
4. 8.24 – Uso de criptografía

5.1.12 Clasificación de la información

A. Objetivo de control: identificar y clasificar los activos de información de acuerdo con su criticidad teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información y requisitos legales.

B. Alcance: el alcance de esta política aplica a todos los propietarios que gestionan y administran activos de información de la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir los criterios y niveles para clasificar la información de acuerdo con su criticidad, donde se valorarán los activos, considerando sus atributos de confidencialidad, integridad y disponibilidad de la información.
    b. Comunicar los procedimientos definidos para la clasificación de la información y la guía para la identificación, creación, clasificación y/o actualización del inventario de activos de información.
    c. Disponer de una herramienta para la clasificación de los activos de información por parte de los propietarios de los activos.
    d. Definir controles para la protección de datos e información compartida con terceras partes.

2. Los jefes de las dependencias deben:

    a. Realizar la clasificación de la información de acuerdo con los procedimientos y guías definidas por la Oficina de Seguridad de la Información.
    b. Aprobar la entrega de información a una persona natural o jurídica.
    c. Monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar la actualización de las valoraciones de estos.
    d. Hacer cumplir los períodos de almacenamiento de información de acuerdo con lo establecido por el Programa de Gestión Documental (PGD) de la entidad, para la información física y electrónica manejada por la **DIAN.** Una vez cumplido el periodo, toda la información deberá ser eliminada adecuadamente.

3. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Implementar los controles para asegurar la protección de datos e información compartida con terceras partes, y que sean definidos por la Oficina de Seguridad de la Información. También deben realizar monitoreos periódicos para confirmar su correcto funcionamiento.

4. Los custodios de los activos de información deben:

    a. Aplicar los controles para la protección de la información, según su nivel de clasificación.
    b. Notificar a los propietarios sobre situaciones de riesgos en los activos de información.

E. Controles relacionados:

1. 5.1 – Políticas de seguridad de la información
2. 5.13 – Inventario de información y otros activos asociados

5.1.13 Etiquetado de la información

A. Objetivo de control: establecer procedimientos y/o lineamientos para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado por la entidad.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios y/o terceros que elaboran documentos para la entidad y también para los dueños de activos que etiquetan información de acuerdo con su clasificación.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado por la entidad.
    b. Divulgar los procedimientos para el etiquetado de información a todos los funcionarios y terceros de la entidad.
    c. Promover el uso del procedimiento de etiquetado de la información.
    d. Incluir dentro del esquema de etiquetado de la información los documentos de ofimática de la entidad.
    e. Incluir la clasificación de los activos como criterio para el etiquetado de la información en la entidad.

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Implementar mecanismos para la ejecución del etiquetado de la información en las herramientas tecnológicas de la entidad, de conformidad con los procedimientos establecidos por la Oficina de Seguridad de la Información.

3. Los jefes de las dependencias deben:

    a. Asegurar que el etiquetado de sus activos se realice según los criterios establecidos y de acuerdo con su clasificación.
    b. Etiquetar de la información de manera reconocible y de fácil utilización para evitar confusiones en el manejo y gestión de la información.
    c. Confirmar el etiquetado de información de los activos identificados en la matriz de activos de las dependencias.

4. Los funcionarios y terceros deben:

    a. Ser responsables del etiquetado de su información de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, las Tablas de Retención Documental (TRD) y debe estar alineado con lo ordenado por la Ley 1712 del 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional). Este etiquetado debe contemplar la información y los activos relacionados tanto en soporte físico como electrónico.
    b. Llevar a cabo el etiquetado de información de acuerdo con los procedimientos de etiquetado definido por la Oficina de Seguridad de la Información, teniendo en cuenta su clasificación.
    c. Realizar el etiquetado de la información en los documentos de ofimática de la entidad, de acuerdo con las guías definidas por la Oficina de Seguridad de la Información.

5. La Oficina de Tributación Internacional debe:

    a. Aplicar la metodología de etiquetado establecida por la Oficina de Seguridad de la Información para clasificar y marcar adecuadamente los documentos y datos obtenidos de los acuerdos internacionales.

E. Controles relacionados:

1. 5.12 – Clasificación de la información

5.1.14 Transferencia de información

A. Objetivo de control: definir mecanismos físicos o electrónicos para la transferencia de información con terceros y establecer los acuerdos requeridos para mantener la confidencialidad y no divulgación.

B. Alcance: el alcance de esta política abarca a todos los funcionarios y terceros que realicen transferencias (incluidas actividades de transferencia internacional) de información física, electrónica y verbal de la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

a. Conservar actualizado el inventario de toda la información electrónica que sea compartida; de igual manera debe contar con el requerimiento y la autorización de la dependencia dueña del activo de información, antes de compartirla o intercambiarla.
b. Implementar las medidas de seguridad necesarias para proteger la transmisión, transferencia o intercambio de información y así minimizar el riesgo de fuga, pérdida o modificación no autorizada de la información en las aplicaciones o equipos de comunicaciones.
c. Activar y remitir a la herramienta de análisis de eventos de la Oficina de Seguridad de la Información los logs generados por los servicios involucrados en la transferencia de información.
d. Contar con el inventario de conexiones, usuarios y la información a la que tienen acceso los terceros que hacen uso de este tipo de conexiones.
e. Utilizar medios seguros para la transferencia, transición e intercambio de información electrónica en medios físicos como cintas o discos.
f. Utilizar las mejores prácticas del mercado en el control de intercambio de información.
g. Limitar la transferencia de información mediante el uso de herramientas colaborativas vía web a información clasificada como “pública”.
h. Contar con una herramienta segura que permita la conexión entre las partes para compartir información con otras entidades o terceros, preservando la confidencialidad, integridad y disponibilidad de la información; lo anterior siempre y cuando exista un acuerdo con el tercero. Implementar y monitorear mecanismos de control sobre el envío de correos fuera de la entidad.
i. Implementar un sistema de etiquetado para la información sensible o crítica de la entidad, en caso de requerir transferencia de información.

2. La Dirección de Gestión de Fiscalización debe:

a. Gestionar la evidencia digital solicitada por un organismo de control y/o judicial competente que requiera información contenida en la misma, preservando la confidencialidad, integridad y disponibilidad de la información; dando cumplimiento a los acuerdos, convenios y normatividad vigente para tal fin.
b. Contar con la autorización de la Oficina de Seguridad de la Información para todas las entregas a los entes de control y/o judiciales de los archivos de evidencia física, digital o electrónica.
c. Utilizar y almacenar la huella digital o código *hash* que permita la integridad de la información suministrada en dos momentos diferentes, acorde con los estándares técnicos para el cifrado.
d. Cumplir con los procedimientos, lineamientos y formatos internos relacionados con el proceso de cadena de custodia.
e. Diligenciar los formatos de cadena de custodia vigentes para el proceso de entrega de evidencia digital a los entes de control y/o judiciales.
f. Solicitar al organismo de control y/o judicial los medios físicos necesarios para realizar el traslado, cumpliendo las especificaciones técnicas mínimas y procedimentales que se requieren para la entrega de evidencia digital.

3. La Subdirección de Asuntos Disciplinarios debe:

a. Solicitar a la Oficina de Seguridad de la Información las evidencias digitales recolectadas referente a información de los funcionarios para posterior envío a los Entes de Control.

b. Contar con la autorización de la Oficina de Seguridad de la Información para todas las entregas a los entes de control y/o judiciales de los archivos de evidencia física, digital o electrónica.
c. Utilizar y almacenar la huella digital o código *hash* que permita la integridad de la información suministrada en dos momentos diferentes, acorde con los estándares técnicos para el cifrado.
d. Cumplir con los procedimientos, lineamientos y formatos internos relacionados con el proceso de cadena de custodia.
e. Diligenciar los formatos de cadena de custodia vigentes para el proceso de entrega de evidencia digital a los entes de control y/o judiciales.
f. Solicitar al organismo de control y/o judicial los medios físicos necesarios para realizar el traslado, cumpliendo las especificaciones técnicas mínimas y procedimentales que se requieren para la entrega de evidencia digital.

4. La Oficina de Tributación Internacional debe:

a. Cumplir con la leyes y normas vigentes para la protección de datos personales en tratados internacionales.
b. Verificar el cumplimiento de los compromisos de la transferencia de información en acuerdo internacionales.
c. Tener en cuenta las directrices de la Circular Única de la Superintendencia de Industria y Comercio, modificada por la circular 002 del 23 de marzo de 2018, en el caso de compartir información con otros países, en donde se enuncian los países que cuentan con un nivel adecuado de protección de datos personales.
d. Verificar todos los documentos que contengan información sujeta a acuerdos internacionales, según los términos establecidos en los convenios firmados por la **DIAN**, etiquetar estos documentos de manera clara y visible con las marcas y categorías pertinentes según los estándares internacionales definidos en dichos acuerdos.

5. La Oficina de Seguridad de la Información debe:

a. Establecer medidas de seguridad y monitoreo para los canales de comunicaciones contratados con terceros, de tal manera que se minimice el riesgo de ataques o vulnerabilidades que expongan la información que se transmita, transfiera o intercambie.
b. Definir los compromisos de intercambio de información en los acuerdos internacionales.
c. Divulgar entre los funcionarios y terceros de la entidad, el uso adecuado de la transferencia de información (física, electrónica y verbal).

6. Los jefes de las dependencias que entregan información a terceros deben:

a. Cumplir los lineamientos establecidos por la Dirección de Gestión Jurídica (Circular No. 00026 de 2019 o la que la reemplace o sustituya), sobre la estandarización de la entrada y salida de información y la política de cifrado de datos e información, atendiendo los principios constitucionales y legales.
b. Aplicar los lineamientos del Manual para la Protección de Datos Personales para los casos donde se requiera el intercambio, transmisión y/o transferencia de la información tanto interna, como con terceros que contenga información asociada a datos personales.
c. Realizar un convenio entre las partes interesadas cuando se deba efectuar el intercambio de información con externos (entes de control, otras entidades nacionales o internacionales, empresas privadas, entre otros), teniendo en cuenta lo establecido en

el Manual para la Protección de Datos Personales y las leyes existentes que protejan la información.

d. Reportar a las partes interesadas todo incidente que ocurra con la información que sea intercambiada, transmitida y/o que se transfiera, a través de los medios que se tengan establecidos para tal fin.
e. Contar con la autorización del funcionario responsable del proceso institucional, en el caso de realizar extracción de información de las bases de datos corporativas, que es quien produce o administra la información y es el dueño del activo de información.

7. La Oficina de Comunicaciones Institucionales debe:

a. Dar buen manejo del correo electrónico asignado y de todas las actividades realizadas con el mismo y su contenido. Así mismo, el contenido de los mensajes enviados a través de correo electrónico debe contar con una firma institucional que permita identificar a la persona que lo envía, la dependencia, la Oficina, la Dirección de Gestión o Seccional a la que pertenece y la extensión telefónica. Esta medida debe aplicarse para el envío y el reenvío de mensajes.
b. Divulgar y recordar permanentemente los lineamientos para el uso correcto de la imagen institucional de la marca **DIAN**, en la referida firma. Los mensajes de correo electrónico están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva su mal uso.
c. Divulgar información a los funcionarios y/o terceros sobre la restricción de reenviar información masivamente, información no institucional, comunicaciones a dominios ajenos de la entidad.

8. La Subdirección Administrativa debe:

a. Implementar mecanismos de control para las actividades de transferencia de medios de almacenamiento físico (documentos, archivos, carpetas, entre otros).
b. Monitorear el correcto enrutamiento de la información física y/o electrónica y preservando la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito.
c. Prevenir el envío de información física, electrónica y verbal en las comunicaciones a la dirección o número equivocado.
d. Impedir el reenvío automático de correo electrónico a direcciones de correo externas.
e. Usar embalaje para envío de información física incluido el papel, que proteja el contenido de cualquier daño físico que pueda surgir durante el tránsito y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protegiendo contra cualquier factor ambiental que pueda reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o la radiación electromagnética. Utilizar normas técnicas mínimas para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos).
f. Usar controles para envío de información física a prueba de manipulaciones o inviolables (por ejemplo, bolsas, contenedores), dependiendo del nivel de clasificación de la información en los medios de almacenamiento a ser transportados.
g. Mantener registros de información de envío de información física para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar

la lista de destinatarios autorizados, los tiempos de transferencia a los custodios de tránsito y la recepción en destino.

h. Asegurar la implementación de controles adecuados en sala de reuniones (por ejemplo: insonorización, puertas cerradas).

9. Los funcionarios y terceros deben:

a. No revelar la información institucional importante o reservada de manera física, electrónica o verbal.
b. Firmar el compromiso de confidencialidad y de no divulgación de la información reservada o clasificada, según lo especificado en el Manual para el tratamiento de datos personales.
c. Comunicar a su jefe inmediato y a la autoridad competente cuando un usuario interno de la entidad reciba algún tipo de mensaje que contenga información inapropiada, amenazante, en contra de la imagen de la **DIAN** y/o cualquier contenido fuera de contexto, de acuerdo con lo previsto en el "Código General Disciplinario". Así mismo, se debe remitir a la Oficina de Seguridad de la Información el incidente reportado (Procedimiento PR-IIT-0458 Gestión de incidentes).
d. No realizar reenvío de correos electrónicos y agendas del correo electrónico institucional a cuentas personales.
e. No tener conversaciones verbales confidenciales en lugares públicos o por canales de comunicación inseguros, ya que pueden ser escuchadas por personas no autorizadas.
f. No dejar mensajes que contengan información confidencial en contestadores automáticos o mensajes de voz, ya que estos pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta.
g. Comenzar cualquier conversación delicada con un descargo de responsabilidad para que los presentes sepan el nivel de clasificación y los requisitos de manejo de lo que están a punto de escuchar.

E. Controles relacionados:

1. 5.10 – Uso aceptable de la información y otros activos asociados
2. 5.13 – Etiquetado de la información
3. 5.31 – Requisitos legales, estatutarios, reglamentarios y contractuales
4. 5.32 – Derechos de propiedad intelectual
5. 5.33 – Protección de registros
6. 5.34 – Privacidad y protección de la información de identificación personal (PII)
7. 8.7 – Protección contra malware
8. 8.24 – Uso de criptografía

5.1.15 Control de acceso

A. Objetivo de control: establecer los lineamientos generales para el acceso controlado a la información de la **DIAN**. Lo anterior, con el fin de minimizar afectación a la confidencialidad, integridad y disponibilidad de la información generada y procesada.

B. Alcance: el alcance de esta política aplica para todos los funcionarios y terceros de la **DIAN** que requieren acceder a la información, instalaciones de procesamiento de información y/o a la información de servicios informáticos y/o aplicaciones informáticas disponibles en la red.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Controlar el acceso a áreas seguras e instalaciones físicas de la **DIAN**, limitando el acceso del personal debidamente autorizado de acuerdo con sus necesidades.
   b. Definir controles para los accesos físicos de áreas restringidas.

2. La Oficina de Seguridad de la Información debe:

   a. Definir lineamientos para el control de acceso a las aplicaciones y servicios informáticos de la entidad.
   b. Adoptar legislación aplicable a la seguridad de la información y cualquier obligación contractual concerniente a la limitación de acceso para la definición de los lineamientos con respecto al control de acceso.
   c. Realizar monitoreo a través del Centro de Seguridad de la Operaciones para las actividades realizadas sobre los sistemas de información de la **DIAN** e informar a la Dirección de Gestión de Innovación y Tecnología si evidencia algún tipo de tráfico anómalo o de carácter riesgoso.
   d. Realizar la revisión de la segregación de funciones por las dependencias de la entidad.

3. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Implementar los controles de acceso para las aplicaciones y servicios informáticos definidos por la Oficina de Seguridad de la Información.
   b. Proveer un controlador de dominio que pueda establecer un sistema de Controladores de Dominio compuesto por uno o varios servidores de configuración idéntica que permita atender los requerimientos técnicos, geográficos o de servicio, siempre y cuando mantenga la sincronización en tiempo real.
   c. Mantener copias de respaldo de las credenciales de los usuarios con la periodicidad correspondiente a su criticidad e importancia.
   d. Monitorear y auditar las operaciones realizadas por los usuarios en los equipos, dispositivos o aplicaciones y/o servicios, sin requerir autorización expresa de las personas, cumpliendo las disposiciones vigentes sobre la materia.
   e. Mantener los registros donde cada uno de los lideres funcionales haya autorizado a usuarios (internos o externos) el acceso a los diferentes sistemas de información de la entidad.
   f. Realizar la revisión periódica de las actividades de los usuarios en los sistemas de información.
   g. Remover a los usuarios deshabilitados o redundantes en las aplicaciones y/o servicios prestados.
   h. Realizar monitoreo sobre las redes y los sistemas informáticos de la **DIAN.**
   i. Definir la segregación de roles de control de acceso, enmarcada en crear, modificar, eliminar, consultar e imprimir.

j. Definir matriz de roles para el control de accesos a los sistemas de información de la entidad.
k. Definir los accesos especiales sobre los activos de información para su adecuado acceso.
l. Divulgar y autorizarla información de acuerdo con el uso aceptable, la clasificación y el etiquetado de la información.
m. Realizar restricciones al acceso privilegiado.
n. Incluir segregación de funciones para los accesos a los sistemas de información.
o. Incluir manejo de registros en los sistemas de información.
p. Identificar la matriz de accesos de acuerdo con los roles establecidos para la entidad por los sistemas de información.

4. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Integrar los servicios y/o aplicaciones de la **DIAN** al controlador de dominio como fuente única de autenticación, si la aplicación o servicio técnicamente lo permite; el controlador de dominio debe poder gestionar la segregación de funciones de las aplicaciones y/o servicios.
b. Controlar el acceso a las áreas seguras e instalaciones de procesamiento de información y recursos tecnológicos, limitando éste al personal debidamente autorizado de acuerdo con sus necesidades para la operación.
c. Implementar controles para el acceso de usuarios remotos a los equipos en la red de la **DIAN**, el cual se debe realizar a través del servicio de escritorios remotos, escritorios virtuales o con la tecnología adoptada y apropiada para la entidad.
d. Retirar, de manera temporal o definitiva de la red de datos, los equipos que presenten tráfico, eventos o actividades que comprometan o puedan afectar el correcto funcionamiento de los sistemas de información de la **DIAN**.
e. Controlar todo acceso a la red de la entidad. En caso de que se requiera acceder a la red mediante elementos o recursos tecnológicos no institucionales, esto debe ser informado y autorizado.

5. La Subdirección de Gestión del Empleo Público debe:

a. Solicitar y autorizar a través de la herramienta asignada por la Dirección de Gestión de Innovación y Tecnología, por parte del responsable, el acceso a la información y a los recursos tecnológicos de la **DIAN** para funcionarios y terceros que laboren en la entidad o personal externo (empresa o entidad externa), basado en la premisa: “Todo está restringido, a menos de que esté expresamente permitido”.
b. Realizar el enrolamiento a los funcionarios y personal externo con los permisos y accesos a zonas no autorizadas (ejemplo: control de accesos que maneja el concesionario en el Aeropuerto el Dorado).

6. Los funcionarios y terceros deben:

a. Cumplir con la política establecida y seguir los procedimientos, instructivos, cartillas y demás documentos, definidos, relacionados con accesos a redes, gestión de usuarios, permisos de administrador, políticas de copias de respaldo (*backup)*, gestión de roles, desarrollo de sistemas de información y demás.
b. Solicitar por parte del jefe de la dependencia la aprobación a la Dirección de Gestión de Innovación y Tecnología, en caso de requerir una modificación a la configuración de las redes y equipos de infraestructura tecnológica según la necesidad de acceso.

c. Utilizar los usuarios asignados con los privilegios correspondientes para cada caso. Ningún usuario de la **DIAN** puede registrarse directamente en un equipo o servidor de la entidad como administrador con todos los privilegios de acceso.
d. Informar inmediatamente a la mesa de ayuda sobre cualquier novedad que afecte la operación normal de la infraestructura tecnológica de la entidad o acceso no requerido para la operación.

E. Controles relacionados:

1. 5.2 – Roles y responsabilidades para la seguridad de la información
2. 5.3 – Segregación de funciones
3. 5.10 – Uso aceptable de la información y otros activos asociados
4. 5.12 – Clasificación de la información
5. 5.13 – Etiquetado de la información
6. 5.16 – Gestión de identidad
7. 5.17 – Información de autenticación
8. 5.18 – Derechos de acceso
9. 5.31 – Requisitos legales, estatutarios, reglamentarios y contractuales
10. 5.32 – Derechos de propiedad intelectual
11. 5.33 – Protección de registros
12. 5.34 – Privacidad y protección de la información de identificación personal
13. 6.8. – Reporte de eventos de seguridad de la información
14. 7.2 – Entrada física
15. 7.3 – Aseguramiento de oficinas, salas e instalaciones
16. 7.4 – Supervisión de la seguridad física
17. 8.2 – Derechos de acceso privilegiado
18. 8.3 – Restricción de acceso a la información
19. 8.4 – Acceso al código fuente
20. 8.5 – Autenticación segura
21. 8.15 – Inicio de sesión
22. 8.18 – Uso de programas privilegiados de utilidad
23. 8.26 – Requisitos de seguridad de la aplicación

5.1.16 Gestión de identidad

A. Objetivo de control: definir y establecer lineamientos adecuados sobre sobre la gestión del ciclo de vida de las identidades.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios y terceros que utilizan identificación para acceder a la información de la entidad y otros activos asociados.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Definir lineamientos y controles para la gestión de identidades en la **DIAN,** que se encuentran definidos en este numeral. Monitorear de manera periódica las identidades asignadas a las personas y el cumplimiento de los lineamientos definidos en la gestión de identidad.

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Implementar los lineamientos y controles definidos por la Oficina de Seguridad de la Información respecto a la gestión de identidad.
b. Asignar un nombre único de cuenta a todos los funcionarios y terceros de la **DIAN** para hacer uso de los sistemas de información de la entidad.
c. Restringir las cuentas de administrador local de los equipos de los usuarios internos únicamente para labores de soporte técnico.
d. Verificar que todas las aplicaciones y sistemas de información tengan autenticación solo de cuentas administradas por el controlador de dominio y contar con la documentación de la gestión de identidades adoptada por la **DIAN**.
e. Asignar los roles a los usuarios internos únicamente si son aprobados por su jefe inmediato.
f. Establecer la gestión de identidades a través del controlador de dominio de la entidad o mediante la solución tecnológica adoptada por la **DIAN**.

3. Los funcionarios y terceros deben:

a. Cambiar la clave de acceso a los sistemas de información de la **DIAN** en forma periódica.
b. Cumplir los lineamientos y directrices sobre la gestión de identidad establecidas por la entidad.
c. Utilizar la identidad y la contraseña asignada para el acceso a los sistemas de información, estos son de uso personal e intransferible y es responsabilidad del usuario interno preservar su confidencialidad.
d. Notificar en caso de contar con roles o permisos que no son necesarios para el cumplimiento de sus funciones y obligaciones asignadas.

E. Controles relacionados:

1. 5.17 – Información de autenticación
2. 5.18 – Derechos de acceso
3. 5.19 – Seguridad de la información en las relaciones con los proveedores

5.1.17 Información de autenticación

A. Objetivo de control: Definir un proceso de gestión formal para la asignación de información de autenticación en la **DIAN** para el acceso a los recursos tecnológicos de la entidad.

B. Alcance: El alcance de este lineamiento aplica para que todos los funcionarios y terceros que hacen uso de información de autenticación. Adicionalmente, la Oficina de Seguridad de la Información, en apoyo con la Dirección de gestión de Innovación y tecnología, debe definir e implementar un sistema de gestión de contraseñas que permita mantener su calidad y controlar la asignación de información de autenticación.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir un proceso de gestión para la asignación de la información de autenticación en la **DIAN**, donde se incluyan criterios como:

        - El cambio de contraseñas solo puede ser solicitado por el titular de la cuenta o jefe/supervisor inmediato, este último solo cuando los colaboradores no tengan medios para realizarlo.
        - Cantidad de caracteres permitidos.
        - Tipos de caracteres permitidos.
        - Características diferenciales para administradores de servicios tecnológicos.
        - Impedir el reúso de contraseñas.
        - No enviar la contraseña por correo electrónico.
        - Definir lineamientos y controles para gestionar los requerimientos en la asignación de información de autenticación enmarcados en este numeral.
        - Promover buenas prácticas en el uso de la información de autenticación entre los funcionarios y terceros de la **DIAN**.

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Implementar los lineamientos y controles definidos por la Oficina de Seguridad de la Información para la asignación de la información de autenticación.
    b. Verificar la identidad del usuario antes de asignarle la información de autenticación ya sea nueva, de sustitución o provisional.
    c. Suministrar la información asociada a la autenticación a los usuarios de manera segura únicamente a través del correo institucional, evitando el uso correos electrónicos no autorizados.
    d. Implementar una herramienta para la gestión de contraseñas definiendo características de acuerdo con el sistema adoptado por la entidad.
    e. Renovar la autorización y solicitar el cambio de contraseña periódicamente para los usuarios externos que tengan autorización de acceso a la **DIAN**. Si la lista de usuarios con permisos no es renovada por los externos, serán bloqueados y luego de tres meses de estar bloqueados serán eliminados.
    f. Forzar el cambio de contraseñas periódicamente. Cuando un usuario sea nuevo en los sistemas se debe obligar a realizar su cambio.

3. La Subdirección de Soluciones y Desarrollo debe:

    a. Implementar los lineamientos de autenticación segura en los sistemas de información que desarrolle o desarrollos subcontratados en la entidad.

4. Los funcionarios y terceros de la entidad deben:

    a. Suscribir el compromiso de confidencialidad de la información, con el fin de mitigar el uso indebido de la información de autenticación entregada.
    b. Cumplir con lo establecido en los instructivos asociados a la creación de cuentas de usuario definido por la entidad.

E. Controles relacionados:

1. 6.2. – Términos y condiciones de empleo
2. 6.8. – Reporte de eventos de seguridad de la información
3. 8.24 – Uso de criptografía

5.1.18 Derechos de acceso

A. Objetivo de control: proporcionar, revisar, modificar y eliminar los derechos de acceso a la información y otros activos asociados, de acuerdo con reglas de control de acceso definidas por la entidad.

B. Alcance: el alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología, que asigna o revoca los derechos de acceso para todo tipo de usuarios en los sistemas de información y servicios de la entidad.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Realizar la configuración y/o instalación de los agentes correspondientes para la integración de ingreso, cambios y/o reinstalaciones de los sistemas de la **DIAN** a las plataformas de SIEM (*Security Information and Event Management* – Gestión de Eventos e Información de Seguridad), protección de bases de datos, identidades centralizadas e identidades de super usuarios internos.
    b. Contar con un sistema centralizado de identidades, por medio del cual se asignan los roles de acceso a los sistemas de información, de acuerdo con las funciones de cada usuario interno.
    c. Definir y establecer lineamientos y controles para la desactivación o bloqueo de los privilegios de acceso sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, teniendo en cuenta las siguientes situaciones administrativas:
        - Desvinculación.
        - Licencias.
        - Vacaciones.
        - Trasladados o ubicaciones entre dependencias o seccionales.
        - Cambio de cargo o proceso.
        - Sanción disciplinaria.

- Terminación de contrato de prestación de servicio o contrato con terceras partes o proveedores.
- En las situaciones anteriormente, los usuarios deben ser notificados a través de los canales dispuestos para tal fin.

2. La Subdirección de Gestión del Empleo Público debe:

   a. Notificar a los funcionarios de la entidad sobre la desactivación o bloqueo de los privilegios de acceso sobre los recursos tecnológicos, los servicios de red y los sistemas de información, de manera oportuna y a través de los canales dispuestos para tal fin.
   b. Reportar a la Dirección de Gestión de Innovación y Tecnología las novedades de desvinculación o cambio de rol del personal para proceder con los cambios de acceso en los recursos tecnológicos.

3. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Llevar el registro de las cuentas de super usuario interno de cada uno de los sistemas de la DIAN, con el fin de ser monitoreadas de manera permanente.
   b. Integrar al controlador de dominio los sistemas de la DIAN, para el manejo de los usuarios internos a través del sistema centralizado de identidades.
   c. Definir los tipos de usuario que tendrán acceso para cada tipo de información establecido de acuerdo con las funciones. Esta clasificación debe tener en cuenta los siguientes aspectos: funciones de la dependencia a la que pertenezca el funcionario, tipo de información a la que accede y las acciones permitidas sobre la información a la que se tiene acceso.
   d. Establecer un procedimiento que permita gestionar la creación, modificación, o borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso a las Apps, entre otros) indicando quién debe autorizarlo.
   e. Generar reportes de acceso y uso de los sistemas de información a los responsables de cada dependencia.
   f. Mantener actualizado y depurado el listado y los permisos de administración de los diferentes recursos tecnológicos de la entidad. Para tal efecto, se deben hacer por lo menos dos revisiones al año. Adicionalmente, se debe contar con un registro de cuentas con accesos privilegiados.
   g. Inactivar los derechos de acceso en la herramienta de gestión de identidades definida por la entidad. Los derechos de acceso se deben inactivar para ausencias temporales (vacaciones, incapacidades, licencias remuneradas, licencias no remuneradas, permisos, etc.) o en caso de sanción disciplinaria. Cuando se requiera la reactivación de los derechos de acceso para realizar actividades especiales inherentes al rol desempeñado por el funcionario o usuario, el jefe inmediato debe solicitar esta autorización. En caso de retiro, los derechos de acceso se inactivarán definitivamente.
   h. Gestionar las conexiones de los usuarios con roles sensibles (super usuarios internos, administradores y usuarios internos que manejan transacciones críticas, entre otros), utilizando la herramienta de gestión de Identidades privilegiadas que permita la conexión a los sistemas de la DIAN según las funciones del rol que desempeñe.
   i. Verificar que todas las aplicaciones y sistemas de información tengan autenticación solo de cuentas administradas por el controlador de dominio y contar con la documentación de la gestión de identidades que se realiza.
   j. Realizar monitoreo de todas las cuentas, incluidas las cuentas de super usuarios, administradores y también las cuentas genéricas o de servicio con privilegios especiales.

k. Eliminar las cuentas genéricas y duplicadas adicionales con permisos de administrador en los casos de pruebas suplementarias.

3. Los funcionarios y terceros de la entidad deben:

   a. Reportar oportunamente las novedades que originan el retiro o la inactivación de los derechos de acceso (cuentas de usuario) de manera temporal o definitiva, según sea el caso.

4. Los jefes de las dependencias deben:

   a. Verificar que sus funcionarios cuenten con los debidos roles para desempeñar sus funciones. Lo anterior se establece con base en el procedimiento PR-IIT-0455, Gestión de Accesos.
   b. Realizar validación de los roles en los sistemas de información y solicitar la inactivación en caso de identificar accesos no autorizados.
   c. Depurar los roles asignados y realizar acciones pertinentes para inactivar oportunamente el acceso a aquellos funcionarios que no requieren el acceso a sistemas de información externos.
   d. Reportar de manera oportuna las novedades de desvinculación o cambio de rol de sus funcionarios y terceros.

E. Controles relacionados:

1. 5.3. – Segregación de funciones
2. 5.9. – Inventario de información y otros activos asociados
3. 5.15. – Control de acceso
4. 5.20. – Abordar la seguridad de la información en los acuerdos con proveedores
5. 6.1. – Selección
6. 6.2. – Términos y condiciones de empleo
7. 6.3. – Concientización, educación y capacitación en seguridad de la información
8. 6.4. – Proceso disciplinario
9. 6.5. – Responsabilidades después de la terminación o cambio de empleo
10. 6.6. – Acuerdos de confidencialidad o no divulgación
11. 6.8. – Reporte de eventos de seguridad de la información

5.1.19 Seguridad de la información en las relaciones con los proveedores

A. Objetivo de control: facilitar y controlar las relaciones de la **DIAN** con los proveedores, con el fin de verificar y gestionar adecuadamente la información a la que tienen acceso para prestar los servicios y, asegurar el cumplimiento de las políticas y procedimientos de la seguridad y privacidad de la información emitidos por la entidad.

B. Alcance: el alcance de esta política aplica para todos los proveedores de servicios, hardware, software, redes, sistemas de comunicación y otros productos adquiridos por la **DIAN**, así como el personal a su cargo y demás terceros que tengan acceso a la información de la entidad, e incluye los proveedores en calidad de encargados del tratamiento de información a nombre de la entidad.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Establecer lineamientos relacionados con requisitos de seguridad y privacidad de la información con el fin de evitar su manipulación de ésta, accesos indebidos por parte de los proveedores, o utilización para una finalidad diferente a la acordada contractualmente o a través de la suscripción de acuerdos o convenios.
   b. Realizar seguimiento a la gestión de la seguridad de información asociada a las relaciones con los proveedores.
   c. Definir mecanismos de control de acceso a los activos de información (físicos, electrónicos o sistemas de información) que requieran los proveedores, en todo el ciclo de vida del dato, desde la recolección hasta la disposición final.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Definir y monitorear las necesidades y condiciones de conexión de los equipos de cómputo y dispositivos de procesamiento de información de los proveedores a través de acuerdos y niveles de servicio.
   b. Establecer y verificar las especificaciones y requerimientos para canales de comunicación segura en la transmisión e intercambio de información desde y hacia los proveedores.
   c. Establecer las configuraciones y requisitos de seguridad de la información pertinentes para los dispositivos de propiedad del proveedor en los que se almacene o procese información de la entidad, así como las herramientas de cifrado y controles técnicos requeridos para la comunicación segura, transmisión de información, medidas de respaldo y recuperación de la información a la cual tengan acceso los proveedores.
   d. Establecer cláusulas para el uso apropiado de la información en ambientes en nube. En caso de realizar la contratación a través de acuerdo marco de precios del SECOP, se deben verificar las cláusulas de seguridad allí definidas.

3. La Subdirección de compras y contratos debe:

   a. Definir en los contratos de la entidad la firma de acuerdos de confidencialidad o compromisos de uso de los servicios informáticos para proteger la información que será gestionada o a la cual tendrá acceso el proveedor, haciendo énfasis en los datos personales, para preservar la seguridad y privacidad de la información. Estos acuerdos y compromisos serán vinculantes y deben contener una responsabilidad tanto civil como penal para el proveedor o la tercera parte contratada.
   b. Verificar la suscripción de acuerdos de confidencialidad con los colaboradores del proveedor que intervienen en la gestión de la información objeto(finalidad) del contrato suscrito.
   c. Mantener actualizado el registro de todos los proveedores que hacen parte de la entidad y que tienen acceso a la información por la naturaleza de sus contratos.
   d. Definir los riesgos y obligaciones de seguridad y privacidad de la información para la suscripción de los contratos con terceros en la entidad.

e. Incluir cláusulas en los contratos para el cumplimiento de la Ley de Protección de Datos Personales por parte de los terceros involucrados en el proyecto o servicio, lo cual debe ser verificado por el supervisor de contrato.
f. Incluir en el manual de supervisión criterios de seguridad de la información asociados a los contratos que manipulen información institucional.
g. Incluir cláusulas dependiendo del tipo de información que maneje el proveedor, incluyendo obligaciones para la recuperación, la contingencia, la disposición final de la información, la eliminación y el borrado seguro de la información gestionada al finalizar la relación contractual, según la sensibilidad del contrato.

4. La Subdirección Administrativa debe:

   Incluir en los contratos de seguridad física actividades de concientización en seguridad de la información al personal de vigilancia.

5. La Subdirección de Soluciones y Desarrollo debe:

   Incluir en los contratos de desarrollo subcontratado cláusulas relacionadas con las buenas prácticas de desarrollo seguro, análisis de vulnerabilidades, derechos de autor y propiedad intelectual y revisión de cumplimiento de los lineamientos relacionados con desarrollo de software de este manual.

6. Los proveedores y terceros de la entidad deben:

   Adoptar las medidas de seguridad necesarias y adecuadas para la conservación, la protección, la custodia y la reserva de la información que reciba, produzca, procese o a la que tenga acceso para prevenir riesgos asociados con fuga, pérdida, manipulación o difusión no autorizada y el acceso no autorizado o fraudulento.
   Suscribir los acuerdos de confidencialidad o compromisos de uso de los servicios informáticos para proteger la información que será gestionada o a la cual tendrá acceso el proveedor, haciendo énfasis en los datos personales, preservando la seguridad y privacidad de la información, de acuerdo con lo establecido en el Formato FT-IIT-2748 (responsabilidad demostrada de terceros sobre la protección de los datos personales).
   Utilizar la información suministrada por la **DIAN** exclusivamente para la~~s~~ finalidades establecida~~s~~ en el objeto contractual.
   Suministrar a la **DIAN** la información relacionada con sus políticas, procedimientos y demás documentación asociada con la seguridad de la información y la protección de datos personales.
   Mantener la confidencialidad, integridad y disponibilidad de la información de la que haga uso o tenga conocimiento en el cumplimiento del objeto contractual, comprometiéndose a no utilizarla para provecho propio, ni divulgarla, comercializarla, publicarla, cederla, revelarla o reproducirla de manera directa e indirecta, o ponerla a disposición de terceros que no estén autorizados por la **DIAN** para conocerla.
   Evitar actos que comprometan o afecten a la **DIAN**, por lo que es su obligación como proveedor o contratista no utilizar la información institucional incluso después de terminada la relación contractual para su beneficio o el de terceros.
   Devolver o suprimir en los términos establecidos en el contrato toda la información entregada u obtenida de la **DIAN** en desarrollo de su objeto contractual, tales como documentos, soportes magnéticos y físicos, entre otros.

No acceder, copiar, reproducir, distribuir o transmitir por ningún medio conocido o por conocer la información confidencial, en todo o en parte, sin previo y escrito consentimiento de la **DIAN**.
Cumplir con el adecuado tratamiento de los datos personales de los titulares, recolectados por la entidad en virtud de la legislación vigente.
No transferir, ceder o divulgar el "usuario" y "contraseña" que le sean asignados (si aplica), teniendo en cuenta que se encuentran bajo su responsabilidad todas las acciones o tareas que se realicen con ellos.
Realizar actividades de concientización sobre seguridad y privacidad de la información al personal que tenga acceso a la información sensible de la **DIAN**.

7. Los supervisores de contratos deben:

   a. Custodiar y cuidar la documentación e información que en cumplimiento del objeto contractual sea entregada por la **DIAN**, así como a la que tenga acceso, e impedir o evitar su sustracción, destrucción, manipulación, ocultamiento o utilización indebida.
   b. Verificar la suscripción de acuerdos de confidencialidad con los colaboradores del proveedor que intervengan en la gestión de la información objeto (finalidad) del contrato suscrito.
   c. Interactuar coordinadamente con los enlaces de seguridad de la información designados por las diferentes dependencias de la entidad.
   d. Cumplir con la legislación vigente, así como con las medidas y protocolos de seguridad que la entidad ha implementado para mitigar la afectación a la confidencialidad de los datos de carácter personal, privados o sensibles.
   e. Reportar a la Oficina de Seguridad de la Información y a la Dirección de Gestión Innovación y Tecnología los incidentes de seguridad o privacidad de la información a través de los canales y medios destinados para tal fin.
   f. Gestionar el control de acceso a los activos de información que requieran los proveedores ya sean físicos, electrónicos o sistemas de información.
   g. Solicitar al proveedor la firma de los acuerdos de confidencialidad o compromisos de uso de los servicios informáticos para proteger la información que será gestionada o a la cual tendrá acceso el proveedor, haciendo énfasis en la que contenga datos personales, preservando la seguridad y privacidad de la información de la entidad.
   h. Identificar los riesgos de seguridad y privacidad de la información según el alcance del contrato o contratos bajo su supervisión.
   i. Tramitar las evaluaciones de seguridad y privacidad de la información solicitadas por la Oficina de Seguridad de la Información.
   j. En los reportes de supervisión de los contratos dejar constancia del seguimiento a los acuerdos de seguridad y privacidad de la información.

E. Controles relacionados: No aplica.

5.1.20 Abordar la seguridad de la información en los acuerdos con proveedores

A. Objetivo de control: establecer los requisitos de seguridad y privacidad de la información, pertinentes con cada proveedor que pueda procesar, almacenar, comunicar, suministrar y tener acceso a la información de la entidad.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios que requieren mantener un nivel acordado de seguridad y privacidad de la información en las relaciones con los proveedores, con el fin de establecer un entendimiento claro entre la entidad y el proveedor

en función de las obligaciones entre las partes para cumplir con los requisitos de seguridad y privacidad de la información. (incluyendo aquellos proveedores que actúen como encargados del tratamiento de información a nombre de la entidad; por ejemplo: mesa de ayuda, gestores de cobranza externos y *Call Centers*).

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la información debe:

   Validar que sean incluidas las políticas y procedimientos de seguridad de la información de la **DIAN** en los procesos de contratación.
   Verificar la inclusión en los acuerdos de las medidas de protección de todos los equipos requeridos para el procesamiento de información por parte de los proveedores.
   Verificar que se incluyan los procedimientos para la continuidad del negocio y la gestión de incidentes de seguridad y privacidad de la información, junto con los canales y medios destinados para tal fin.
   Validar que se incluya en los acuerdos las herramientas de cifrado y controles técnicos para la comunicación segura y transmisión de información desde y hacia los proveedores.

2. La Subdirección de compras y contratos debe:

   Diseñar acuerdos en los que se especifiquen las medidas de seguridad y privacidad de la información requeridas, de tal manera que se minimicen los riesgos por exposición indebida, difusión, adulteración o pérdida de información.
   Incluir en el manual de contratación las condiciones de los acuerdos con los proveedores en lo relacionado con seguridad y privacidad de la información.

3. Los supervisores de contratos deben:

   a. Validar los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
   b. Verificar que se incluyan en los acuerdos las medidas de respaldo y recuperación de la información a la cual tengan acceso los proveedores.
   c. Validar la inclusión de los mecanismos de control de acceso a los activos de información (físicos, electrónicos o sistemas de información) que requieran los proveedores.
   d. Validar la inclusión de las configuraciones y requisitos de seguridad de la información pertinentes para los dispositivos de propiedad de los proveedores, en los que se almacene o procese información de la entidad.
   e. Validar que se firmen, por parte de los proveedores, los acuerdos de confidencialidad y no divulgación de la información, así como verificar la suscripción de acuerdos de confidencialidad con los colaboradores/empleados de los proveedores que tengan acceso a la información de la entidad.

4. Los proveedores y terceros deben:

    a. Proteger la información calificada como pública clasificada y pública reservada que sea suministrada por la **DIAN**, para propender por la confidencialidad, integridad y disponibilidad de la información que se requiera para la ejecución de las actividades establecidas en los procesos contractuales.
    b. Tratar de manera adecuada los datos personales de los titulares en caso de tener accesos a ellos en el cumplimiento del contrato.
    c. Dar cumplimiento a las cláusulas asociadas con la seguridad de la información, a este manual y a los procedimientos asociados a seguridad y privacidad de la información.
    d. Reportar los incidentes de seguridad y privacidad de la información por los canales y medios destinados para tal fin.

E. Controles relacionados:

1. 5.10. – Uso aceptable de la información y otros activos asociados
2. 5.11. – Devolución de bienes
3. 5.12. – Clasificación de la información
4. 5.13. – Etiquetado de la información

5.1.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

A. Objetivo de control: Definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC en la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Compras y Contratos, la Oficina de Seguridad de la Información y la Dirección de Gestión de Innovación y Tecnología, las cuales deben incluir en sus acuerdos con proveedores requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos, servicios de tecnología de información y comunicaciones.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Compras y Contratos debe:

    a. Definir los requisitos de seguridad y privacidad de la información para los contratos suscritos para la adquisición de suministro de productos y servicios de tecnología de información y comunicaciones.
    b. Incluir dentro de los componentes de los contratos de TI garantías asociadas a la cadena de suministro de las TIC.

2. La Oficina de Seguridad de la Información debe:

    a. Definir los riesgos de seguridad de la información asociados a los requisitos y acuerdos establecidos para la cadena de suministro de productos y los servicios de tecnología de información y comunicaciones.

b. Verificar que se incluyan obligaciones para la cadena de suministro de tecnologías.

3. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Establecer en los contratos con sus proveedores de productos de tecnología de información y comunicaciones que estos apliquen las prácticas de seguridad adecuadas en la cadena de suministro.
   b. Establecer en los contratos con proveedores los requisitos de seguridad de la información y la gestión de riesgos, aplicables a la adquisición de productos o servicios de tecnología de la información y de comunicaciones.
   c. Tener la seguridad de que los servicios o los productos sean entregados de acuerdo con las especificaciones contractuales establecidas.
   d. Solicitar a los proveedores de servicios de TIC que transmitan, divulguen y comuniquen los requisitos de seguridad y privacidad a lo largo de su cadena de suministro.
   e. Identificar y documentar los componentes del producto o servicio que son críticos para la entidad.
   f. Verificar el aprovisionamiento de servicios en la nube, proveedores de servicios de telecomunicaciones y proveedores de hardware.

4. Los supervisores de los contratos deben:

   a. Notificar situaciones de riesgos a la Subdirección de Compras y Contratos novedades relacionadas con el suministro de productos y servicios de tecnología de información y comunicaciones.
   b. Monitorear las novedades relacionadas con el suministro de productos y servicios de tecnología de información y comunicaciones.

E. Controles relacionados: No aplica.

5.1.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores

A. Objetivo de control: monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad y privacidad de la información de los proveedores y prestación de servicios.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios que deban mantener el nivel acordado de seguridad y privacidad de la información y de prestación del servicio en línea con los acuerdos con los proveedores; adicionalmente se deben gestionar los cambios, incluyendo los asociados a la infraestructura, los aplicativos y los servicios tecnológicos, que son soportados por terceros, para permitir estándares de eficiencia, seguridad y calidad.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Compras y Contratos debe:

a. Definir procedimientos donde se establezcan las condiciones para el seguimiento, la revisión y la gestión de cambios en los servicios suministrados por los proveedores.
b. Establecer las acciones que deben tomar los supervisores cuando se observen deficiencias en la prestación del servicio por parte de los proveedores.

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Establecer lineamientos, procedimientos y/o mecanismos que permitan cumplir la gestión de cambios a nivel de infraestructura, sistemas de información y servicios tecnológicos que son soportados por proveedores, para confirmar eficiencia, seguridad y calidad en la gestión de cambios.
b. Monitorear la asignación de permisos de acceso de los proveedores a los sistemas de información de la entidad; lo anterior, teniendo en cuenta las condiciones que estos deben cumplir en cuanto a la gestión de usuarios y contraseñas definidos en este manual.
c. Incluir dentro de las cláusulas, cuando se considere necesaria, la identificación de vulnerabilidades en los contratos de tecnología.
d. Incluir dentro de las cláusulas contractuales la posibilidad de realizar auditorías a los proveedores cuando haya cambios en los servicios que suministra.
e. Involucrar al responsable del plan de recuperación de desastre con voto para los temas que puedan afectar la continuidad de la operación. Gestionar los cambios que se presenten en la ejecución de los contratos suscritos con los proveedores, los cuales pueden estar asociados con:

- Sistemas de información
- Políticas de seguridad de la información
- Mejoramiento de procedimientos
- Eficiencia de los controles de seguridad de la información
- Mantenimiento

3. Los supervisores de los contratos deben:

a. Realizar una revisión y actualización de sus proveedores, cada vez que se requiera, como mínimo una vez al año en cada inicio de período. Que se realiza con el apoyo por los enlaces de seguridad de la información designados.
b. Monitorear periódicamente el cumplimiento de los Acuerdos de Niveles de Servicio (ANS), acuerdos de confidencialidad y acuerdos de intercambio de información por parte de los proveedores.
c. Realizar seguimiento con regularidad a la prestación del servicio de los proveedores en los términos y condiciones de seguridad y privacidad de la información de los acuerdos se cumplan y que el manejo de incidentes de seguridad de la información se gestione adecuadamente.
d. Verificar que se cumplan los términos y condiciones de seguridad y privacidad de la información.

4. Los proveedores de la entidad deben:

a. Reportar a la Oficina de Seguridad de la Información y/o Dirección de Gestión de Innovación y Tecnología cualquier incidente de seguridad o privacidad de la información

que se presente en la relación con los proveedores, con el fin de tomar las medidas respectivas de acuerdo con los lineamientos, parámetros y procedimientos establecidos.

b. Respaldar y proteger los activos de información que sean utilizados por los proveedores, teniendo en cuenta la clasificación de la información. Cuando se requiera, se debe contar con el apoyo de la Dirección de Gestión de Innovación y Tecnología para preservar su conservación y resguardo.

E. Controles Relacionados:

1. 5.24. – Planificación y preparación de la gestión de incidentes de seguridad de la información
2. 5.29. – Seguridad de la información durante la interrupción
3. 5.30. – Preparación de las TIC para la continuidad del negocio
4. 5.35. – Revisión independiente de la seguridad de la información
5. 5.36. – Cumplimiento de políticas, normas y estándares de seguridad de la información
6. 6.8. – Reporte de eventos de seguridad de la información
7. 8.14. – Redundancia de las instalaciones de procesamiento de información

5.1.23 Seguridad de la información para el uso de servicios en la nube

A. Objetivo de control: establecer procesos de adquisición, uso, gestión y salida de los servicios en la nube, de acuerdo con los requisitos de seguridad y privacidad de la información definidos por la **DIAN**.

B. Alcance: el alcance de esta política aplica para la Oficina de Seguridad de la Información y la Dirección de Gestión de Innovación de Tecnología, encargadas de definir y comunicar una política sobre el uso de los servicios en la nube a todas las partes interesadas.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Definir los requisitos de seguridad y privacidad de la información asociados con el uso de los servicios en la nube, tales como IaaS, PaaS, SaaS y también lo definido en el Anexo Lineamientos Técnicos de Servicios en Nube.
   b. Definir los criterios de selección de los proveedores de servicios en la nube, teniendo en cuenta aspectos como la reputación, la fiabilidad, los mecanismos de protección de datos, las certificaciones de cumplimiento relevantes para el sector, la escalabilidad, la alta disponibilidad, el rendimiento y el modelo de costos.
   c. Definir las funciones y las responsabilidades relacionadas con el uso y la gestión de los servicios en la nube.
   d. Establecer un procedimiento para gestionar incidentes y cambios en los servicios en la nube.

2. La Subdirección de Compras y Contratos debe:

a. Establecer los lineamientos, procedimientos, manuales y/o mecanismos para la adquisición de servicios en la nube, tales como IaaS, PaaS, SaaS.
b. Especificarlas garantías que ofrecen los proveedores, en cuanto al cumplimiento de los principios de disponibilidad, confidencialidad e integridad de la información en los servicios en nube.

3. La Dirección de Gestión de Innovación y Tecnología debe:

a. Definir los riesgos de seguridad o privacidad de la información asociados con el uso de servicios en la nube, relacionados con la gestión de los servicios suministrados por terceros.
b. Solicitar y verificar la conformidad de los controles de seguridad y privacidad de la información con lo que cuenta el proveedor de servicios en la nube.
c. Dar cumplimiento a la Guía de Computación en la nube de MinTIC, donde se establecen los lineamientos de uso de las capacidades de las nubes en Colombia, teniendo en cuenta a su vez, el documento NIST *Special Publication* 800-145 y las características de las redes, los servidores, el almacenamiento, los sistemas informáticos y los servicios, que engloban: la demanda, los accesos a la red, la agrupación de recursos, la elasticidad de capacidades y la medición de los servicios.
d. Dar cumplimiento a la cartilla de protección en los servicios computación en la nube (*cloud computing*) emitida por la Superintendencia de Industria y Comercio de Colombia.
e. Establecer los criterios técnicos para evaluar o adquirir los servicios de cómputo en la nube.
f. Dar cumplimiento a la Directiva Presidencial 03 de 2021, mediante la cual se imparten lineamientos para el uso de los servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
g. Diseñar, definir y probar los procesos de continuidad operativa y recuperación en caso de desastres, respecto de la base tecnológica de la **DIAN**, proporcionando los procedimientos necesarios para tener accesibilidad a la información durante los mantenimientos programados y no programados.
h. Disponer de una herramienta para monitorear las capacidades de la nube, optimizando de manera periódica los recursos desplegados.
i. Definir con el (los) proveedor(es) de nube los ANS correspondientes a los tiempos de atención para fallas, nuevos requerimientos y demás que se requieran para la operación.
j. Incluir una cláusula en los contratos de nube donde indique que la **DIAN** tiene toda la propiedad de cualquier información agregada, creada, generada, modificada, almacenada o en cualquier otra forma asociada con la propiedad intelectual, la cual no podrá ser reclamada por el proveedor.
k. Incluir una cláusula en los contratos de nube para exigir al proveedor la eliminación segura de la información de la entidad al finalizar el contrato.
l. Incluir cláusula en los contratos de nube donde se indique que la **DIAN** tiene acceso a los reportes del proveedor asociados a: auditorías de seguridad de la información, continuidad y riesgos de seguridad y privacidad de la información, cuando la **DIAN** lo requiera.
m. Incluir los criterios de seguridad y privacidad para el aprovisionamiento y configuración de los recursos de nube.
n. Incluir en los ambientes en nube la misma configuración de segregación de ambientes tenidas en cuenta en los ambientes en *On-premise*.
o. Utilizar las condiciones de los ambientes de pruebas, desarrollo y producción al igual que se usan en *On-premise*.
p. Separar los ambientes y los servicios de seguridad en distintas cuentas o suscripciones.

q. Implementar segmentos de redes por roles de servidores a nivel de aplicaciones, bases de datos, y web hacia internet.
r. Implementar la gestión de identidades y acceso a los servicios que se utilizan en la nube, garantizando accesos basados en roles, autenticación multifactor, auditorías periódicas, depuraciones y la aplicación del principio de mínimo privilegio.
s. Configurar los grupos de seguridad de red o reglas de firewall para restringir el tráfico de red entrante y saliente a los recursos de la nube.
t. Adoptar el uso de herramientas y técnicas de infraestructura como código (IaC) para automatizar el aprovisionamiento de recursos, los procesos de configuración y mantener control de versiones sobre las plantillas o *scripts* utilizados.
u. Monitorear y optimizar el uso de los recursos en la nube.
v. Incluir los elementos de la nube, en los procesos de monitoreo de seguridad, generando alertas sobre eventos de seguridad.
w. Incluir criterios de segmentación de redes al igual que se realiza en *On-premise*.
x. Restringir el tráfico de red entrante y saliente a los recursos de nube, mediante reglas de firewall y/o grupos de seguridad de red.
y. Implementar redes privadas virtuales (VPN) o conexiones dedicadas entre entornos de nube y *On-premise*.
z. Incluir criterios de cifrado de datos confidenciales en tránsito y en reposo al igual que se realiza en *On-premise*.
aa. Incluir los aprovisionamientos y actualizaciones en los elementos de la nube, en el proceso de Gestión de cambios.
bb. Mantener un inventario de los recursos de nube de acuerdo con los criterios definidos en *On-premise*.
cc. Incluir los elementos de la nube en los análisis de vulnerabilidades, actualizaciones y aplicación de parches de seguridad.
dd. Implementar el etiquetado (*Tag*) de recursos en la nube para mejorar la administración e identificación de recursos y la asignación de costos

4. Los supervisores de los contratos deben:

a. Gestionar el manejo de los incidentes de seguridad y privacidad de la información que se presenten durante el uso de los servicios en la nube.
b. Monitorear y evaluar el uso continuo de los servicios en la nube para administrar los riesgos de seguridad y privacidad de la información.
c. Validar que el proveedor cuente con las mejores las prácticas y los procedimientos de seguridad de la información para el servicio prestado.
d. Validar que el país donde se aloje la información; especialmente la relacionada con datos personales, disponga de una seguridad jurídica similar a la colombiana para la transferencia o transmisión de estos, según la legislación en Colombia para la protección de datos personales.
e. Analizar periódicamente los gastos generados por los recursos desplegados en nube, buscando y reportando anomalías, para permitir optimizaciones en los consumos.

5. Los administradores de la nube deben:

a. Conservar los principios de seguridad de la información: confidencialidad, integridad y disponibilidad durante la operación del servicio.
b. Analizar qué información de la entidad puede migrarse a la nube.

c. Realizar un análisis de riesgos de seguridad y privacidad de la información con la metodología adoptada por la Oficina de la Seguridad de la Información para validar si la información puede o no ser migrada a la nube.
d. Generar los roles y responsabilidades de uso en la nube, desde el punto de vista tecnológico.
e. Reportar a la Oficina de la Seguridad de la Información los eventos o incidentes de seguridad o privacidad relacionados con la nube.

E. Controles relacionados:

1. 5.21. – Gestión de la seguridad de la información en la cadena de suministro de las TIC.
2. 5.22. – Seguimiento, revisión y gestión de cambios de servicios de proveedores.

5.1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

A. Objetivo de control: definir los roles, las responsabilidades y los procedimientos de gestión para la atención oportuna y eficaz de los incidentes de seguridad y privacidad de la información en la **DIAN**.

B. Alcance: el alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y las dependencias que definen e implementan los lineamientos para la gestión de incidentes de seguridad de la información, para el manejo de eventos o de los posibles incidentes de seguridad y privacidad de la información sobre los activos de información, a través de una oportuna identificación, atención, tratamiento y respuestas con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la **DIAN**.

C. Características del control:

1. Tipo de control: correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Elaborar en conjunto con la Dirección de Gestión de Innovación y Tecnología procedimientos, lineamientos o normatividad para evaluar los incidentes de seguridad de la información.
b. Coordinar los esfuerzos necesarios para dar atención a un incidente de seguridad y privacidad de la información dentro de la entidad, de igual manera, informar a los respectivos niveles administrativos de los incidentes y su grado de severidad dentro de la entidad, así como coordinar los esfuerzos con entidades externas (proveedores, ColCERT, Comando Conjunto Cibernético, Policía Nacional de Colombia, y la Superintendencia de Industria y Comercio) en caso de ser necesario.
c. Evaluar, clasificar y responder, de manera eficiente y adecuada, los incidentes de seguridad y privacidad de la información.
d. Gestionar los incidentes de seguridad y privacidad de la información que se presenten sobre los activos de información de la **DIAN**.

e. Consolidar las lecciones aprendidas, las cuales se realizan en conjunto con las dependencias involucradas en el incidente de seguridad y privacidad de la información y que serán documentadas en la herramienta definida por la entidad para este fin.
f. Generar una base de datos de conocimiento de incidentes de seguridad y privacidad de la información.
g. Realizar el escalamiento de los incidentes de seguridad y privacidad de la información a las partes que corresponden, tanto internas como externas.
h. Mantener los contactos apropiados con los grupos de interés especial de seguridad y privacidad de la información. En el caso de que se presente un incidente de seguridad y privacidad de la información y, ser requerido solicitar asesoría externa a los grupos como el ColCERT, las mesas de infraestructuras críticas cibernética el CSIRT Gobierno, el centro Cibernético Policial o a los foros de seguridad especializados y asociaciones profesionales.
i. Incluir en la clasificación de incidentes de seguridad y privacidad de la información, como mínimo: clasificación, prioridad, manera de contención, manera de recuperación, forma de erradicación, tiempos de respuesta (de acuerdo con el nivel de criticidad o impacto). Estas actividades se realizan para dar cumplimiento al ciclo de vida de la gestión y respuesta a un incidente de seguridad, de acuerdo con la Guía para la gestión y clasificación de incidentes de seguridad de la información (MINTIC).

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Coordinar los esfuerzos necesarios para dar atención a un incidente de seguridad o privacidad de información dentro de la entidad.
b. Gestionar los eventos de seguridad para detectar y tratarlos con eficiencia. Una vez identificados, clasificar o no como incidentes de seguridad y privacidad de la información.
c. Informar a los niveles administrativos los incidentes y su grado de severidad dentro de la entidad.
d. Recolectar la evidencia digital asociada con el incidente de seguridad o privacidad de la información.

3. Los funcionarios y terceros de la entidad deben:

a. Reportar los incidentes por los medios autorizados, teniendo en cuenta los procedimientos vigentes, y cualquier situación anormal que pueda llegar a convertirse en un incidente de seguridad y privacidad de la información, en donde se identifica su categoría y se direcciona a la Dirección de Gestión de Innovación y Tecnología y/o a la Oficina de Seguridad de la Información para su tratamiento y respuesta.

E. Controles relacionados:

1. 5.5. – Contacto con las autoridades
2. 5.6. – Contacto con grupos de interés especial
3. 5.25. – Evaluación y decisión sobre eventos de seguridad de la información
4. 5.26. – Respuesta a incidentes de seguridad de la información
5. 5.28. – Recopilación de pruebas
6. 6.8. – Reporte de eventos de seguridad de la información
7. 8.15. – Registro
8. 8.16. – Actividades de seguimiento

5.1.25 Evaluación y decisión sobre eventos de seguridad de la información

A. Objetivo de control: evaluar los eventos de seguridad presentados en la entidad, valorarlos y decidir si se clasifica como incidente de seguridad y privacidad de la información.

B. Alcance: el alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y la Dirección de Gestión de Innovación y Tecnología, encargadas de establecer un esquema de categorización y priorización de incidentes de seguridad y privacidad de la información para la gestión y respuesta.

C. Características del control:

1. Tipo de control: detectivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Evaluar, en conjunto con la Dirección de Gestión de Innovación y Tecnología, los eventos de seguridad para identificar si es necesario o no clasificarlos como incidentes de seguridad y privacidad de la información.
    b. Evaluar y clasificar los incidentes de seguridad de la información y privacidad de la información que se presenten sobre los activos de información de la **DIAN**.
    c. Crear un de grupo de monitoreo especializado en incidentes encargado de monitorear, clasificar, informar y gestionar a las dependencias o grupos correspondientes los incidentes de seguridad y privacidad de la información.
    d. Categorizar los incidentes de acuerdo con la Tabla de Impacto de Incidente (Guía para la gestión y clasificación de incidentes de seguridad de MINTIC).

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Adoptar los procedimientos, lineamientos o normatividad para la gestión de incidentes de seguridad y privacidad de la información.
    b. Clasificar el tipo de evento/incidente de acuerdo con los documentos, lineamientos o procedimientos establecidos por la entidad.
    c. Gestionar y responder a los eventos clasificados como incidente de seguridad y privacidad de la información, teniendo en cuenta los lineamientos o procedimientos definidos.
    d. Analizar, validar y documentar cada incidente de seguridad y privacidad de la información desde su identificación hasta la finalización de su tratamiento.
    e. Incorporar las lecciones aprendidas de la base de datos de conocimiento de incidentes de seguridad y privacidad de la información.

E. Controles relacionados: No aplica.

1. 6.8 - Reporte de eventos de seguridad de la información.

5.1.26 Respuesta a incidentes de seguridad de la información

A. Objetivo de control: verificar que se den respuesta de manera eficiente y eficaz a los incidentes de seguridad y privacidad de la información que se presenten en la entidad.

B. Alcance: el alcance de este lineamiento aplica para todos los funcionarios y terceros que deban dar respuesta a los incidentes de seguridad de la información que se presenten en la entidad, mediante el uso las herramientas y formatos definidos en los procedimientos vigentes.

C. Características del control:

1. Tipo de control: correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Generar respuesta a los incidentes de seguridad y privacidad de la información e incluir como mínimo la siguiente información:
      - Tipo de incidente.
      - Activo de información afectado.
      - Criticidad del incidente.
      - Descripción de las debilidades de seguridad de la información que se encontraron, causaron o contribuyeron al incidente.
      - Personas responsables en el tratamiento y respuesta del incidente.
      - Las actividades de tratamiento y respuesta involucradas en la gestión del incidente.
      - Duración de la solución del incidente.
      - Estado del incidente (Abierto: Sin dar una respuesta definitiva al incidente - Cerrado: Incidente tratado y manejado adecuadamente).
   b. Documentar un registro de las respuestas en la base de datos de conocimiento de incidentes de seguridad y privacidad de la información.
   c. Informar sobre el incidente de seguridad de la información a entes de control o autoridades competentes, teniendo en cuenta los procedimientos vigentes.
   d. Definir lineamientos respecto a respuesta de los incidentes para:
      - La contención del incidente.
      - Recopilación de evidencia.
      - Comunicación a las partes interesadas internas y externas.
      - Coordinar con partes internas y externas para mejorar la eficacia de la respuesta.
      - Analizar la causa raíz del incidente.
      - Identificar y gestionar las vulnerabilidades y debilidades en los controles relacionados con la causa del incidente de seguridad y privacidad de la información.
      - Establecer responsabilidades como el primer respondiente, vocero oficial dentro de la gestión de incidentes de seguridad o privacidad de la información.
   e. Informar o notificar a los propietarios de los activos de información afectados sobre el incidente de seguridad y privacidad de la información, así como de las medidas adoptadas para la remediación y/o solución del incidente.

E. Controles relacionados:

1. 5.24. – Planificación y preparación de la gestión de incidentes de seguridad de la información
2. 5.27. – Aprendiendo de los incidentes de seguridad de la información
3. 5.28. – Recopilación de pruebas
4. 5.29. – Seguridad de la información durante la interrupción
5. 5.30. – Preparación de las TIC para la continuidad del negocio

5.1.27 Aprendiendo de los incidentes de seguridad de la información

A. Objetivo de control: mantener y utilizar la base de datos de conocimiento para reducir la posibilidad o el impacto de futuros incidentes, utilizar las lecciones aprendidas para los planes de respuesta a los incidentes de seguridad y privacidad de la información.

B. Alcance: el alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, encargada de utilizar el conocimiento obtenido sobre los incidentes de seguridad y privacidad de la información, con el fin de fortalecer y mejorar los controles asociados.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Definir mecanismos que permitan cuantificar y hacer el seguimiento de todos los tipos, los volúmenes y los costos de los incidentes de seguridad y privacidad de la información.
   b. Utilizar la información obtenida de la evaluación de incidentes de seguridad y privacidad de la información para identificar los incidentes recurrentes o con impacto alto.
   c. Definir un esquema de formación y concienciación para los funcionarios y terceros de la entidad sobre las lecciones aprendidas para los planes de respuesta a los incidentes de seguridad y privacidad de la información.
   d. Documentar la base de datos de conocimiento para identificar las amenazas, las vulnerabilidades y las oportunidades de mejora con relación a los incidentes de seguridad y privacidad de la información que se presenten. Las lecciones aprendidas pueden incluir aspectos como:
      - Necesidades de controles adicionales o mejoras para limitar la frecuencia
      - Daños y costos de futuros sucesos
      - Mejoramiento de los contenidos de planes de sensibilización y toma de conciencia
      - Actualización de procedimientos y/o políticas de seguridad de la información
      - Actualización de registros de riesgos o causas de riesgos
      - Cambios en el procedimiento de gestión de incidentes
      - Identificación de acciones para reducir la probabilidad de nuevos incidentes
      - Identificación de activos de información más vulnerables
      - Identificación de posibles patrones de acción de ataques informáticos.
      - Escenarios de los incidentes
      - Monitoreo de riesgos de seguridad o privacidad de la información.
   e. Mantener un adecuado registro de lecciones aprendidas que permita conocer:

- Exactamente los hechos sucedidos, en qué momento y cómo se gestionó el incidente.
- Si se dio aplicación a los procedimientos documentados.
- Qué medidas o acciones se tomaron que podrían haber impedido la recuperación.
- Acciones correctivas que puedan prevenir incidentes similares en el futuro.
- Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

f. Informar, notificar o establecer reuniones con los propietarios de los activos de información afectados, donde se analicen y documenten la experiencia adquirida relacionada con la atención y solución del incidente.

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Implementar mecanismos que permitan cuantificar y hacer el seguimiento de todos los tipos, los volúmenes y los costos de los incidentes de seguridad y privacidad de la información que afecten la infraestructura tecnológica de la **DIAN.**
b. Documentar la base de datos de conocimiento para identificar las amenazas, las vulnerabilidades y las oportunidades de mejora de los incidentes de seguridad y privacidad de la información que se presenten en la infraestructura tecnológica de la entidad.

E. Controles relacionados:

1. 5.24. – Planificación y preparación de la gestión de incidentes de seguridad de la información.
2. 6.3. – Concientización, educación y capacitación en seguridad de la información.

5.1.28 Recopilación de evidencias digitales

A. Objetivo de control: Gestionar de manera eficaz y consistente la evidencia relacionada con incidentes de seguridad y privacidad de la información para efectos de acciones disciplinarias y legales.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información encargada de definir y aplicar procedimientos para la identificación, la recopilación, la adquisición y la preservación de la evidencia digital relacionada con eventos o incidentes de seguridad y privacidad de la información.

C. Características del control:

1. Tipo de control: correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de seguridad de la Información debe:

a. Cumplir con la normatividad vigente establecida y adoptada por la entidad y con la metodología general del procedimiento de Evidencia Digital (MINTIC), cumpliendo con los siguientes pasos:

- Aislamiento de la escena
- Identificación de fuentes de información
- Recolección y examinación de información
- Análisis de la información
- Reporte

b. Disponer de los elementos necesarios para la recolección de información como:
   - Dispositivos de recolección forense.
     - Dispositivos de backups.
     - Elementos de protección electromagnética y guantes.
     - Medios formateados y/o estériles.
     - Cámaras digitales.
     - Cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas.

c. Verificar las siguientes condiciones antes de iniciar el procedimiento de evidencia digital para el análisis, la evaluación y la decisión:
   - El evento debe estar previamente registrado como un incidente de confidencialidad, integridad y/o disponibilidad de la información y/o datos personales.
   - Se debe determinar si el incidente requiere o no un análisis forense.

d. Tener en cuenta las siguientes medidas al momento de realizar el procedimiento de identificación, recolección, procesamiento, análisis y manipulación de evidencia digital:
   - Verificar si ha ocurrido el incidente o no.
   - Verificar si existe la necesidad de ejecutar el procedimiento para la recolección de la evidencia digital al incidente reportado.
   - Minimizar la pérdida o alteración de datos.
   - Recolectar evidencia digital de medios volátiles como memoria RAM, conexiones de red o procesos.
   - Capturar imágenes de la evidencia digital.
   - Verificar que las copias de las pruebas electrónicas sean idénticas a las originales.
   - Documentar en las bitácoras todas las acciones, con fechas y horas precisas.
   - Analizar todos los datos recolectados.
   - Realizar un reporte de los hallazgos.

e. Cumplir, como mínimo, con las siguientes actividades cuando se maneje cadena de custodia:
   - Hacer un inventario y descripción de elementos.
   - Embalar las evidencias inventariadas en un contenedor, cerrado y etiquetado.
   - Etiquetar la fecha y hora del hallazgo, el número de evidencia, el número de registro (folio), la dirección exacta del lugar de los hechos, la descripción del material recolectado y las observaciones.
   - Nombre completo de los responsables de la recolección y el embalaje.
   - Documentar una hoja de ruta, en donde se registren los datos principales sobre descripción de la evidencia, las fechas, las horas, los custodios, las identificaciones, los cargos y las firmas de quién recibe y quién entrega.

E. Controles relacionados: No aplica.

5.1.29 Seguridad de la información durante la interrupción

A. Objetivo de control: Incluir en el plan de continuidad del negocio y el plan de recuperación ante desastres criterios de seguridad de la información.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, la Dirección de Gestión de Innovación y Tecnología, la Subdirección de Procesos y la Subdirección de Infraestructura Tecnológica y de Operaciones. Estas son las áreas encargadas de establecer, documentar, implementar y mantener los procesos, procedimientos y controles para cumplir el nivel de seguridad de la información durante una situación adversa.

C. Características del control:

1. Tipo de control: preventivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Participar en las pruebas que se realicen de los planes de recuperación ante desastres y validar requisitos de seguridad y privacidad en contingencia.
    b. Identificar, junto con la Subdirección de Procesos, los riesgos de seguridad y privacidad sobre la disponibilidad de los activos críticos de información relacionados con la continuidad del negocio. Para esto deben tener en cuenta los activos de información considerados como críticos para la entidad.

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Minimizar el impacto que se pueda derivar de cualquier situación de emergencia sobre los servicios de TI o el nivel de prestación de estos.
    b. Implementar el plan de recuperación ante desastres de forma adecuada, teniendo en cuenta la criticidad de los servicios, procesos y procedimientos.
    c. Elaborar un plan de mitigación o tratamiento para atender los hallazgos identificados en las pruebas, revisiones y/o monitoreos, asignando responsables y rango de fechas de ejecución.
    d. Definir, en conjunto con la Subdirección de Procesos, las aplicaciones y/o *software* de mayor impacto para la entidad. Lo anterior, preferiblemente a través de un Análisis de Impacto del Negocio (BIA por sus siglas en inglés).
    e. Desarrollar las estrategias de continuidad en las aplicaciones y sistemas de información (según el nivel de criticidad) que apoyan los procesos/procedimientos de la operación.
    f. Mantener actualizada la documentación del plan de recuperación ante desastres.
    g. Elaborar y ejecutar un plan de capacitación y sensibilización relacionado con la implementación plan de recuperación ante desastres y hacer seguimiento a dicho plan.
    h. Incluir en los planes de recuperación ante desastres controles de seguridad existentes durante la interrupción. En caso de no poderlos tener, establecer controles de compensación.
    i. Establecer un protocolo para la activación del plan de recuperación ante desastres. Alineado a los protocolos de Protocolo de Manejo de Incidentes e Identificación de Crisis - OD-PEC-0003 y Protocolo de manejo de crisis - OD-PEC-0004

j. Definir controles compensatorios en caso de que, en una situación de crisis, algún control tecnológico no se pueda implementar.

3. La Subdirección de Procesos debe:

a. Mantener actualizado el plan de continuidad del negocio. Para ello se realizan revisiones periódicas y cuando se produzca un cambio significativo que pueda afectar al mismo.
b. Alinear las estrategias de continuidad del negocio con el plan de recuperación ante desastres, definido por la Dirección de Gestión de Innovación y Tecnología.
c. Revisar por lo menos una vez al año, la alineación del plan de continuidad del negocio con el BIA actualizado.
d. Definir en conjunto con las direcciones de gestión de la **DIAN** por cada dependencia o sistema de información el tiempo RTO (*Tiempo Objetivo de Recuperación*), valor que establece el límite superior para la recuperación de los servicios de cada una de las aplicaciones que fueron identificadas en el punto anterior (preferiblemente a través del *Business Impact Analysis)*.
e. Elaborar y ejecutar un plan de capacitación y sensibilización relacionado con la implementación plan de continuidad del negocio y hacer seguimiento.
f. Identificar junto con la Dirección de Gestión de Innovación y Tecnología los riesgos sobre la disponibilidad de los activos críticos de información de TI que apoyan las operaciones.
g. Validar y actualizar, en conjunto con las direcciones de gestión de la **DIAN**, el nivel de criticidad del proceso, procedimiento o sistema de información y el tiempo de RTO, por lo menos una vez al año, esto preferiblemente a través Análisis de Impacto del Negocio (BIA por sus siglas en inglés).
h. Definir metodología para el plan de continuidad del negocio teniendo en cuenta: los tipos de interrupción, la metodología para Análisis de Impacto del Negocio e incluir como mínimo: las personas, los procesos, la infraestructura física y la tecnológica.
i. Realizar al menos una vez al año pruebas del plan continuidad del negocio y su alineación con el plan de recuperación ante desastres.
j. Supervisar el cumplimiento de los protocolos para la activación del plan de continuidad del negocio, incluidos en los documentos “Protocolo de Manejo de Incidentes e Identificación de Crisis” y “Protocolo de manejo de crisis” de la entidad.
k. Definir controles compensatorios en caso de que, en una situación de crisis, algún control no se pueda implementar.
l. Asegurar que las áreas operativas tengan actualizados los planes de operación alternos, en el evento de la perdida de los servicios de TI por encima de los RTO (*Tiempo Objetivo de Recuperación*) y RPO (*Punto Objetivo de Recuperación*).

E. Controles relacionados:

1. 5.30. – Preparación de las TIC para la continuidad del negocio

5.1.30 Preparación de las TIC para la continuidad del negocio

A. Objetivo de control: Planificar, implementar, mantener y probar la preparación de las TIC en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología, encargada de mantener la disponibilidad de la información en la **DIAN** y otros activos asociados durante la interrupción.

C. Características del control:

1. Tipo de control: correctivo.
2. Propiedades de seguridad: disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Verificar que el plan de recuperación ante desastres se desarrolle y se implemente de forma adecuada, teniendo en cuenta la criticidad de los servicios, procesos y procedimientos.
   b. Asegurar la autonomía de realizar revisiones y/o monitoreos a la metodología, estrategias, planes, procedimientos implementados y/o relacionados con resiliencia digital.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Identificar y establecer estrategias de continuidad de las TIC en las cuales se deben considerar opciones antes, durante y después de una posible interrupción o falla.
   b. Definir y documentar el plan de recuperación ante desastres.
   c. Incluir en los planes de continuidad TIC especificaciones de rendimiento y capacidad para cumplir con los requisitos y objetivos de continuidad de la entidad.
   d. Contar con herramienta como BIA (análisis de impacto del negocio) junto con RTO (Recovery Time Objective – Tiempo objetivo de recuperación) de cada servicio TIC priorizado y los procedimientos para restaurar esos componentes; así mismo RPO (Recovery Point Objective – Punto objetivo de recuperación) de los recursos TIC priorizados definidos como información y los procedimientos para restaurar la información.
   e. Establecer un plan de pruebas anual de las estrategias de recuperación de desastres definidos por la entidad.
   f. Capacitar a los involucrados en las estrategias de recuperación de desastres definidos por la entidad.
   g. Tomar las lecciones aprendidas de las pruebas de las estrategias de recuperación ante desastres definidos por la entidad e incluirlas en las futuras actualizaciones de los planes.
   h. Actualizar las estrategias de recuperación de desastres definidas por la entidad teniendo en cuenta los resultados de las pruebas realizadas y cambios que hayan surgido desde la última actualización del plan.
   i. Definir los objetivos, alcance y límites del plan de recuperación ante desastres.
   j. Desarrollar, entregar y actualizar los entregables del plan de recuperación ante desastres según la definición de la Guía para la preparación de las TIC en la continuidad del negocio del Modelo de Seguridad y Privacidad de la Información formulado por el MINTIC, con respecto a:
      - Planificación para la preparación de las TIC para la continuidad de negocio.
      - Implementación para la preparación de las TIC para la continuidad de negocio.
      - Evaluación de desempeño para la preparación de las TIC para la continuidad de negocio.
      - Mejora continua para la preparación de las TIC para la continuidad de negocio.

k. Cumplir con los objetivos de las siguientes prácticas profesionales de resiliencia definidas por el *Instituto Internacional de Recuperación de Desastres* (DRII, por sus siglas en inglés):
   - Inicio y administración del programa
   - Evaluación de riesgos
   - Análisis de impacto al negocio
   - Estrategias de continuidad de negocio
   - Respuesta a incidentes
   - Desarrollo e Implementación del plan
   - Programas de concientización y entrenamiento
   - Ejercicio, evaluación y mantenimiento del plan de continuidad del negocio
   - Comunicación de crisis
   - Coordinación con dependencias externas

l. Mantener actualizada la documentación del plan de recuperación ante desastres.
m. Elaborar y ejecutar un plan de capacitación y sensibilización relacionado con la implementación plan de recuperación ante desastres y hacerle seguimiento.
n. Incluir, en los planes de recuperación ante desastres, los controles de seguridad existentes durante la interrupción y en caso de no poderlos tener, establecer controles de compensación.
o. Definir las necesidades del plan de recuperación de desastres en los proyectos con soluciones de nuevas tecnológicas.
p. Incluir al comité en gestión de cambios en los procesos relacionados con el plan de recuperación de desastres.

3. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Probar de forma periódica el plan de recuperación ante desastres, para validar su adecuación a las necesidades de la entidad.
   b. Buscar que los centros de datos cumplan con los lineamientos definidos por la guía TIA-942 estándar - Diseño y Cableado de un Centro de Datos.
   c. Contar con la infraestructura requerida para el plan de recuperación ante desastres, como centros de datos alternos, sin importar las estrategias de continuidad definidas.
   d. Asignar, mantener y actualizar la infraestructura técnica (equipos, licencias, software, comunicaciones, centros de datos, entre otros) para la puesta en marcha de las estrategias definidas.

4. La Subdirección de Procesos debe:

   a. Mantener alineado el plan de continuidad del negocio y el plan de recuperación de desastres.

E. Controles relacionados:

1. 5.29. – Seguridad de la información durante la interrupción.

5.1.31 Requisitos legales, estatutarios, reglamentarios y contractuales

A. Objetivo de control: identificar la legislación y los registros contractuales en materia de seguridad y privacidad de la información, vigilar su cumplimiento y actualización de manera permanente.

B. Alcance: el alcance de este lineamiento aplica para Dirección de Gestión Jurídica y para todos los funcionarios y terceros que deben proteger la información de la **DIAN** evitando cualquier alteración, fuga o pérdida, preservando la confidencialidad, integridad y disponibilidad de esta.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión Jurídica debe:

   a. Mantener actualizado un catálogo normativo o normograma donde se identifiquen, documenten y actualicen todos los requerimientos de la legislación y la regulación nacional e internacional, con el fin de salvaguardar la información que se genere, obtenga, adquiera, transforme, controle, transfiera o se intercambie en la entidad.
   b. Dar cumplimiento de las leyes y normas reglamentarias y regulatorias establecidas, así como la normatividad interna en relación con seguridad y privacidad de la información.
   c. Definir la frecuencia de revisión, validación y pertinencia de los requisitos legales.
   d. Revisar periódicamente la legislación y los reglamentos identificados para mantener al día los cambios e identificar nueva legislación.
   e. Realizar la actualización del catálogo normativo de la entidad.

2. La Oficina de Seguridad de la Información debe:

   a. Realizar la verificación del cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con seguridad y privacidad de la información.

3. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Documentar y actualizar todos los requerimientos estatutarios, regulatorios y contractuales para cada sistema de información, una vez al año y/o cada vez que estos sean requeridos.

4. Los funcionarios y terceros de la entidad deben:

   a. Cumplir con las obligaciones legales, estatutarias, reglamentarios o contractuales relacionadas con seguridad y privacidad de la información.

E. Controles relacionados:

1. 5.20. – Abordar la seguridad de la información en los acuerdos con proveedores.

5.1.32 Derechos de propiedad intelectual

A. Objetivo de control: Implementar procedimientos apropiados para el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de software patentado.

B. Alcance: El alcance de esta política aplica para la Dirección de Gestión de Innovación y Tecnología, quien hace la adquisición de software en la **DIAN** y todos los funcionarios y terceros de la entidad que deben implementar y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Fortalecer la cultura en los usuarios internos de la **DIAN** sobre los derechos de propiedad intelectual.
    b. Definir una política y los procedimientos relacionados con los derechos de propiedad intelectual, incluyendo los requisitos legales, estatutarios, reglamentarios y contractuales aplicables.
    c. Incluir, dentro de las políticas de navegación de la entidad, el bloqueo de páginas que puedan infringir la ley de protección de derechos de autor.

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Definir controles con el objetivo de proteger adecuadamente la propiedad intelectual de la **DIAN**, tanto propia como la de terceros según aplique para los derechos de autor de software, licencias y código fuente.
    b. Validar que se use software autorizado por la entidad independiente si este es propietario, de licencia comercial o de software libre.
    c. Verificar que todo el software utilizado por la entidad, para trabajar o desarrollar esté licenciado y sea usado únicamente bajo los términos y condiciones definidos en las licencias.
    d. Verificar que no se exceda el número máximo de usuarios permitidos por las licencias o las capacidades, para tal efecto se deben realizar monitoreos periódicos de la utilización de software que se encuentren en el inventario.
    e. Reportar a la Oficina de Seguridad de la Información los eventos o incidentes relacionados con la violación de los derechos de propiedad intelectual.
    f. Mantener las evidencias de la propiedad de las licencias de software adquirido.
    g. Contar con un listado de licenciamiento de la entidad.
    h. Cumplir con los términos y condiciones del software libre.
    i. Registrar ante la entidad competente el software desarrollado por la entidad.

3. Los funcionarios y terceros deben:

    a. Utilizar software legalmente adquirido y/o autorizado por la entidad.

b. Cumplir con las políticas y lineamientos definidos para la utilización de software licenciado en los equipos de la entidad.
c. Referenciar la fuente de donde se extrajo la información para presentaciones, documentos, informes y demás documentos que utilicen los usuarios internos para funciones de su cargo.
d. Cumplir con la legislación de derechos de propiedad intelectual.
e. Evitar realizar descargas o almacenar o ejecutar en los equipos de la **DIAN** archivos de música, fotos, videos, software o material sujeto a propiedad intelectual.
f. Cumplir con la legislación vigente y/o requisitos legales aplicables a los derechos de propiedad intelectual, la protección de registros, la privacidad y la protección de datos personales y la reglamentación de controles criptográficos.
g. Cumplir con las leyes de derechos de autor y los acuerdos de licenciamiento, no duplicar y/o distribuir ningún software o su documentación sin permiso del propietario de los derechos de autor.
h. No copiar, total o parcialmente, estándares (por ejemplo: estándares internacionales ISO/IEC), libros, artículos, informes u otros documentos, salvo lo permitido por la ley de derechos de autor o las licencias aplicables.

E. Controles relacionados: No aplica.

5.1.33 Protección de registros

A. Objetivo de control: Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, reglamentarios y contractuales.

B. Alcance: El alcance de esta política aplica para todos los funcionarios y terceros de la entidad, con el fin cumplir los requisitos legales, estatutarios, reglamentarios y contractuales en la protección de registros.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

a. Establecer los lineamientos, procedimientos y/o instructivos para la protección de los registros en bases de datos, registros de transacciones (Logs) y registros de auditoría (Audit Logs).
b. Contar con sistemas de almacenamiento y manejo de datos, teniendo en cuenta como mínimo lo siguientes:
- Permitir el acceso a los datos (legibilidad de los medios y de formatos) durante todo el período de retención, para proteger la información contra pérdida debido a cambios futuros de la tecnología.
- Permitir recuperar los datos requeridos en un tiempo y formato aceptables, dependiendo de los requisitos que se deban cumplir.
- Identificar los registros y su período de retención.

- Permitir la destrucción apropiada de registros, luego del período de retención, si la entidad ya no los requiere.

c. Documentar procedimientos o instructivos sobre la retención, almacenamiento, manejo y disposición de registros e información electrónicos, en conformidad con el Programa de Gestión Documental de la **DIAN**.
d. Elaborar un programa de retención que identifique los registros electrónicos y el período de tiempo durante el cual se deberían retener los registros.
e. Definir un inventario de fuentes de información de acuerdo con la identificación y clasificación de activos de información.
f. Documentar lineamientos, procedimientos o instructivos, en conformidad con el Programa de Gestión Documental de la **DIAN**, sobre la retención, el almacenamiento y el manejo de registros e información electrónicos para cumplir con requisitos estatutarios, reglamentarios y contractuales o para el soporte de las actividades misionales de la entidad.
g. Establecer procedimientos y/o instructivos para conservar en un lugar seguro con acceso restringido al personal autorizado y con protección de acceso, los registros de eventos provenientes del hardware y el *software* de la infraestructura de seguridad de la **DIAN**.
h. Reportar a la Oficina de Seguridad de la Información los eventos o incidentes relacionados con la pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de registros de la **DIAN**.

2. Los funcionarios y terceros deben:

a. Cumplir con los lineamientos establecidos en el Programa de Gestión Documental de la **DIAN** y desarrollados en el instructivo IN-ADF-0132 - Manejo de los archivos en la UAE-**DIAN**.

E. Controles relacionados:

1. 8.24. – Uso de criptografía

5.1.34 Protección de la información de datos personales (identificación personal PII)

A. Objetivo de control: Mantener la protección y privacidad de la información de datos personales tal como lo estipula la legislación, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

B. Alcance: El alcance de esta política aplica para para todas las dependencias, funcionarios y terceros que deban cumplir los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información y de la protección de la información de identificación personal.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad, disponibilidad y privacidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Dar cumplimiento a los lineamientos y funciones establecidas en la Resolución 101 del 2020 “por la cual se designan las funciones del oficial de datos personales a la Oficina de Seguridad de la Información”, o la que la modifique con posterioridad.
b. Actualizar y verificar el cumplimiento de lo establecido en el Manual para la protección de datos personales MN-IIT 062 y la demás documentación relacionada.
c. Definir los lineamientos para la incorporación de instrumentos como compromisos de confidencialidad, control de acceso, definición de roles, anonimización o cifrado de la información, entre otros, que impidan que la información personal circule o se haga pública.

2. Los jefes de dependencias deben:

a. Dar cumplimiento a la Resolución 101 del 2020 “Por la cual se designan las funciones del oficial de datos personales a la Oficina de Seguridad de la Información y se fijan obligaciones de las dependencias frente a la protección de datos personales en la Unidad Administrativa Especial – Dirección de Impuestos y Aduanas Nacionales – **DIAN**”, o la que la modifique con posterioridad.
b. Identificar y gestionar los riesgos de seguridad de la información de los activos de información que contengan datos personales. Estos deben ser controlados para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información que contiene datos personales.
c. Adoptar, de carácter obligatorio, todos los lineamientos de protección de datos personales para el diseño, la implementación y/o la generación de nuevos servicios de la entidad como canales de atención, nuevos procesos, adecuación, renovación o disposición de espacios físicos, nuevas formas físicas o digitales de interoperabilidad o circulación de la información tanto interna o externamente.
d. Identificar en sus activos de información lo siguiente:
    - Cuáles contienen datos personales.
    - En qué medios se encuentran (físicos o electrónicos).
    - Qué medidas de seguridad aplican.
    - Si la recolección, tratamiento, circulación y disposición que se hace de esos activos se realiza conforme con las normas y políticas establecidas.
    - Si se trata de bases de datos con información personal, analizar y evaluar si debe ser registrada en el Registro Nacional de Bases de Datos dispuesto por la SIC y generar los reportes periódicos correspondientes.
e. Responsabilizarse directamente del tratamiento de datos personales manejados por su dependencia, y/o delegar a un tercero dicho tratamiento; en cualquiera de los casos se debe cumplir con los lineamientos y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de estos, de acuerdo con la normatividad vigente y lo establecido en este manual.
f. Realizar la recolección, el tratamiento, el almacenamiento y la disposición final de los datos, observando los principios de: legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
g. Recibir las bases de datos personales o información personal que, con ocasión de un mandato legal o el cumplimiento de un tratado, acuerdo, convenio, contrato o un mecanismo jurídico de igual naturaleza, la **DIAN** reciba de otra entidad u organismo en cumplimiento de sus funciones.

3. Todas las dependencias, funcionarios y terceros deben:

a. Cumplir la normatividad nacional vigente en materia de protección de datos personales. Proceder a la supresión de los datos personales en su posesión, una vez cumplida las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario. Esta supresión o disposición final de los datos personales se realiza de acuerdo con las políticas de gestión documental de la entidad.
b. Cumplir con la reglamentación y normatividad vigente de la **DIAN** en materia de protección de datos personales:
   - La circular externa No. 001 de 2019 "Política de Tratamiento de Datos Personales".
   - El Manual para la Protección de Datos Personales MN-IIT-0062 y sus respectivos anexos.
   - La Circular 26 de 2020 "*Mediante la cual se definen criterios para atender las solicitudes de acceso a la información pública, los lineamientos especiales dados por la SIC y las disposiciones internas del Manual de protección de datos personales*".

c. Cumplir con el adecuado tratamiento y protección a los datos personales de acuerdo de con Resolución 101 de 2020.Organizar y depurar los sistemas de información, las bases de datos o información personal que ya no están en uso.
d. Controlar y aplicar medidas de seguridad, técnicas y administrativas, para mantener actualizada la información personal.
e. Recolectar únicamente los datos personales necesarios para llevar a cabo las funciones de la entidad, con el objetivo de reducir o evitar el tratamiento de datos innecesarios.

E. Controles relacionados: No aplica.

5.1.35 Revisión independiente de la seguridad de la información

A. Objetivo de control: Revisar de forma independiente la gestión de la seguridad y privacidad de la información a intervalos planificados o cuando se produzcan cambios significativos.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Control Interno y/o terceros contratados para ejecutar la revisión a la entidad, en la gestión de la seguridad y privacidad de la información.

C. Características del control:

1. Tipo de control: preventivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Control Interno y/o quien haga sus veces debe:

   Revisar el cumplimiento de la implementación del Modelo de Seguridad y Privacidad de la Información de manera independiente y a intervalos planificados (objetivos de control, políticas, procesos, procedimientos de la seguridad de la información), o cuando ocurran cambios significativos. Las revisiones se realizan a manera de auditoría por personal especializado y serán acordadas con cada dependencia.
   Informar al jefe de cada dependencia sobre los resultados de las revisiones o auditorías y deben ser guardadas en un lugar específico de acceso propio para la dependencia y para la Oficina de Seguridad de la Información o quien haga sus veces.

Verificar las acciones correctivas propuestas por las dependencias para confirmar la eficiencia de estas.
Informar a la alta dirección del avance en la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.
Evaluar las oportunidades de mejora presentadas durante la revisión de la seguridad de la información.
Tener en cuenta la necesidad de cambios en el enfoque de la seguridad de la información.

2. Los jefes de las dependencias deben:

   a. Formular un plan de acción para corregir las deficiencias o falencias encontradas en las revisiones o auditorías. Así mismo, dicho plan y sus avances deben ser reportados en la herramienta o carpeta definida por la Oficina de Seguridad de la Información.

E. Controles relacionados:

1. 5.1. – Políticas de seguridad de la información.

5.1.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

A. Objetivo de control: Revisar el cumplimiento de todos los lineamientos, las políticas, lo procedimientos y las normas establecidas en materia de seguridad y privacidad de la información, con el fin de preservar los principios de privacidad, disponibilidad y confidencialidad.

B. Alcance: El alcance de este lineamiento aplica para los funcionarios y terceros de la entidad que deben aportar porque la seguridad de la información se implemente y opere de acuerdo con la política de seguridad de la información de la **DIAN**, las políticas, las reglas y los estándares específicos del tema.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   Evaluar el cumplimiento de la política de seguridad de la información y las acciones de mejora correspondientes, y llevar un registro de estas.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   Realizar análisis periódicos de seguridad en los sistemas de información con ayuda de herramientas automatizadas y generar informes técnicos de la verificación del cumplimiento con los estándares de implementación de la seguridad de la información.
   Realizar revisiones técnicas de los procedimientos de análisis, diseño, desarrollo y mantenimiento de las aplicaciones; se deben realizar revisiones técnicas y, en caso de

incumplimiento de algún control o lineamiento, se deben determinar las causas de este e implementar acciones de mejora.

3. Los jefes de las dependencias deben:

   a. Establecer los mecanismos de cumplimiento de todos los requisitos de seguridad de la información definidos en las políticas, las normas y los lineamientos aplicables en sus sistemas de información y en la información manejada.
   b. Cumplir con las normas de seguridad y privacidad de la información establecidas en este manual.
   c. Identificar las causas de incumplimiento de las políticas y normas de seguridad e implementar las acciones de mejora apropiadas para dar cumplimiento a estas.

E. Controles relacionados:

1. 5.35. – Revisión independiente de la seguridad de la información
2. 8.15. – Inicio de sesión
3. 8.16. – Actividades de seguimiento
4. 8.17. – Sincronización de reloj

5.1.37 Procedimientos operativos documentados

A. Objetivo de control: Documentar y disponer los procedimientos de operación para las instalaciones de procesamiento de información de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología, encargada del funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

C. Características del control:

1. Tipo de control: preventivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Procesos debe:

   a. Establecer las condiciones para la creación, la actualización y la eliminación de la documentación institucional.
   b. Promover en las dependencias la verificación y actualización de la documentación de cada una de estas.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Documentar y actualizar los procedimientos, instructivos y guías relacionados con la operación y administración de la plataforma tecnológica de la **DIAN**.
   b. Proporcionar a los funcionarios y terceros, de acuerdo con su rol o funciones: los manuales de proveedor, guía de uso, ficha técnica, e instructivos operativos de los servicios tecnológicos y sistemas de información que conforman la plataforma tecnológica de la **DIAN**.

c. Documentar los procedimientos de verificación, instalación, configuración y administración de los sistemas de información, el procesamiento y manejo de la información.
d. Documentar los procedimientos de gestión de respaldo de la información, incluidas las pruebas y la verificación de copias de seguridad.
e. Documentar, en conjunto con la Oficina de Seguridad de la Información, el manejo de errores y condiciones excepcionales que pueden definirse como incidentes de ciberseguridad, incidentes de seguridad informática y los incidentes de seguridad y privacidad de la información.
f. Documentar en conjunto con la Oficina de Seguridad de la Información las instrucciones especiales de manejo de medios para información confidencial, incluida la eliminación segura, la recuperación, el apagado o el reinicio del sistema.
g. Documentar los procedimientos con los requisitos de programación e interacción con otros sistemas y tener un registro de los cambios realizados en cada uno.
h. Contar con la documentación de monitoreo de red y monitoreo de los activos de información.

3. Los jefes de las dependencias deben:

a. Documentar y actualizar los procedimientos donde se relacionen aquellas actividades que puedan afectar el procesamiento de la información de la entidad, así como los procedimientos donde se relacionen las actividades para la protección de la confidencialidad, la integridad y la disponibilidad de la información de la **DIAN**.
b. Documentar y mantener actualizados todos los procedimientos de operación, teniendo en cuenta los ya existentes en la **DIAN**.

E. Controles relacionados:

1. 7.4. – Supervisión de la seguridad física
2. 7.10 – Medios de almacenamiento
3. 7.14. – Eliminación segura o reutilización de equipos
4. 8.6. – Gestión de capacidad
5. 8.15. – Inicio de sesión
6. 8.16. – Actividades de seguimiento
7. 8.17. – Sincronización de reloj
8. 8.18. – Uso de programas de utilidad privilegiados

5.2 Controles de personas

A continuación, se describen los lineamientos y políticas que hacen referencia a las responsabilidades que establece la **DIAN** para los funcionarios y terceros en términos de seguridad y privacidad de la información:

5.2.1 Selección

A. Objetivo de control: Verificar los antecedentes del talento humano de acuerdo con las leyes, los reglamentos, la ética y comprobar que cumpla con los requisitos de idoneidad, compromiso y responsabilidad inherentes al manejo de los activos de información a los que va a tener acceso y a los riesgos de seguridad y privacidad de la información.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión Corporativa y sus subdirecciones Gestión del Empleo Público y Compras y Contratos, que realizan vinculación de funcionarios y/o terceros en la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión Corporativa debe:

a. Establecer los mecanismos o controles en sus procesos de selección del personal tanto funcionarios como contratistas para verificar los antecedentes.
b. Incluir en las verificaciones de selección de personal tanto a funcionarios como a contratista en lo relacionado con confirmación de los soportes académicos y experiencias profesionales.
c. Incluir en la selección de funcionarios y contratistas la verificación de la identidad a través del documento de identidad y/o el pasaporte emitido por las autoridades competentes.
d. Incluir, en caso de que un funcionario cambie de cargo dentro de la entidad, la verificación de antecedentes.

2. La subdirección de Compras y Contratos debe:

a. Disponer de una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios, de acuerdo con lo que dicta la ley y la reglamentación vigente.
b. Establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales.
c. Ejecutar los procedimientos internos para la vinculación y retiro de contratistas, de conformidad con la normatividad vigente.

3. La subdirección Gestión del Empleo Público debe:

a. Incluir en los procedimientos de selección de personal de planta y los procesos contractuales la autorización para el tratamiento de los datos personales de acuerdo con la política de tratamiento de datos personales de la **DIAN** y conforme con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
b. Almacenar en la historia laboral de los funcionarios o en el expediente del contrato los documentos de verificación y los soportes correspondientes.
c. Dar cumplimiento a los mecanismos o controles establecidos por la Dirección de Gestión Corporativa para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
d. Establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales.
e. Ejecutar los procedimientos internos para la vinculación, ascenso, reubicación y retiro del talento humano de la entidad, de conformidad con la normatividad vigente.
f. Reportar a través de la mesa de servicio las novedades del personal para que, desde la Subdirección de Soluciones y Desarrollo, asigne o desasigne los usuarios en los sistemas de información y aplicativos, según sea necesario.

4. Los funcionarios de la entidad deben:

    a. Notificar a la Subdirección de Gestión del Empleo Público cuando haya novedades en su hoja de vida o en un título profesional nuevo adquirido posterior a su vinculación con la **DIAN**.

E. Controles relacionados:

1. 5.1 – Políticas de seguridad de la información

5.2.2 Términos y condiciones de empleo

A. Objetivo de control: Establecer acuerdos en la vinculación tanto de funcionario como de contratistas que manejen activos de información dentro de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión Corporativa y sus subdirecciones Gestión del Empleo Público y Compras y Contratos que realizan los términos y condiciones de la vinculación de funcionarios y/o terceros en la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión Corporativa debe:

    a. Establecer los lineamientos para los términos y las condiciones de contrato de los terceros y vinculación de funcionarios.
    b. Establecer las obligaciones contractuales sobre seguridad y privacidad de la información, las leyes de propiedad intelectual, protección de datos personales, transparencia y acceso a la información pública, y las acciones a tomar si no se cumplen estos términos.
    c. Promover la divulgación términos y condiciones en materia de la seguridad y privacidad de la información tanto en funcionarios como en contratistas.
    d. Definir para la firma, compromisos de confidencialidad de la información tanto en funcionarios como en contratistas.

2. La subdirección de Compras y Contratos debe:

    a. Definir los términos y condiciones para vinculación de terceros y funcionarios, en los cuales se establezcan las obligaciones contractuales en materia de seguridad y privacidad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública, así como las acciones a tomar si no se cumple con estos términos y condiciones.
    b. Dar a conocer a los candidatos los términos y condiciones del contrato y especificar las obligaciones en materia de la seguridad y privacidad de la información; aclarar que estas se extienden más allá de los límites de la **DIAN** y de ejecución del objeto contractual e informar las acciones a tomar si no se cumple con estos términos y condiciones.

c. Hacer firmar un documento de compromiso de confidencialidad de la información a los funcionarios; dicho documento debe reposar en la historia laboral.
d. Incluir dentro de las obligaciones contractuales condiciones ante el incumplimiento de las políticas de seguridad de la información o ante acciones irregulares relacionadas con los activos de información de la **DIAN**.

3. La subdirección Gestión del Empleo Público debe:

a. Incluir en las condiciones del empleo de los funcionarios a través de un acuerdo de confidencialidad donde se encuentren las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad y privacidad de la información que dicte la **DIAN**.
b. Definir los términos y condiciones del empleo de los funcionarios, en los cuales se establezcan las obligaciones del funcionario en materia de seguridad y privacidad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública, así como las acciones a tomar si no se cumple con estos términos y condiciones.
c. Dar a conocer a los candidatos los términos y condiciones del empleo y especificar las responsabilidades en materia de la seguridad y privacidad de la información. Se debe aclarar que estas responsabilidades se extienden más allá de los límites de la **DIAN** y del horario normal de trabajo y es necesario informar las acciones a tomar si no se cumple con estos términos y condiciones.
d. Hacer firmar un documento de compromiso de confidencialidad de la información a los contratistas; dicho documento debe reposar en el expediente contractual.

4. La Subdirección de Asuntos Disciplinarios debe:

a. Ejercer el control disciplinario y adelantar e instruir los procesos respecto a los funcionarios y ex funcionarios de la entidad que incumplan las políticas de seguridad de la información o cometan irregulares relacionadas con los activos de información de la **DIAN**.

E. Controles relacionados:

1. 5.9 - Inventario de información y otros activos asociados
2. 5.13 - Etiquetado de la información
3. 5.32 - Derechos de propiedad intelectual
4. 5.34 - Privacidad y protección de datos personales
5. 6.4 - Proceso disciplinario
6. 6.5 - Responsabilidades después de la terminación o cambio de empleo
7. 6.6 - Acuerdos de confidencialidad o no divulgación

5.2.3 Concientización, educación y capacitación en seguridad de la información

A. Objetivo de control: Promover conciencia, educación y capacitación en temas de seguridad y privacidad de la información, junto con las actualizaciones regulares de la política, procedimientos, instructivos y las buenas prácticas internacionales relacionadas con seguridad de la información.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, la Subdirección de la Escuela de Impuestos y Aduanas y Subdirección de Desarrollo del Talento Humano, que realizan actividades de conciencia, educación y capacitación en todos los funcionarios y terceros que tienen acceso a los activos de información de la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Establecer un programa de concientización, educación y capacitación en seguridad y privacidad de la información para el cumplimiento las responsabilidades de seguridad de la información en todos los funcionarios y terceros.
    b. Diseñar e implementar actividades de cultura, cambio y apropiación referentes a la seguridad y privacidad de la información dirigidas a los usuarios internos de la **DIAN** que tengan acceso a activos de información de la entidad.
    c. Incluir actividades de entrenamiento y actualización periódicas en materia de seguridad y privacidad de la información que permitan la comprensión del alcance y contenido de las políticas, lineamientos y directrices de seguridad y privacidad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.
    d. Evaluar la ejecución del programa de concientización, educación y capacitación de las actividades de cultura, cambio y apropiación referentes a la seguridad y privacidad de la información.
    e. Definir los contenidos a sensibilizar en toda la entidad, teniendo en cuenta riesgos comunes de seguridad y privacidad de la información, requerimientos, políticas, lineamientos, buenas prácticas, deberes y derechos en la materia y responsabilidades frente al incumplimiento, incluyendo el uso seguro de los activos de información.
    f. Definir contenido especializado para los funcionarios que realicen actividades específicas de seguridad y privacidad de la información como: tecnología, desarrollo de software, dependencias que manipulen datos personales.

2. La Subdirección de la Escuela de Impuestos y Aduanas debe:

    a. Establecer los mecanismos necesarios en sus procedimientos para que los programas de inducción, reinducción, capacitación y sensibilización incluyan y evalúen temas de seguridad y privacidad de la información.
    b. Verificar que los procedimientos y programas de capacitación y sensibilización pertinentes de la entidad, incluyan y evalúen temas de seguridad y privacidad de la información.
    c. Ofrecer los medios necesarios para que la Oficina de Seguridad de la Información pueda promover el programa de concientización, educación y capacitación en seguridad y privacidad de la información.

3. La Subdirección de Desarrollo del Talento Humano debe:

    a. Incluir en los programas y acciones requeridas por la entidad para lograr una transformación del talento temas relacionados con seguridad y privacidad de la información.

4. Los jefes de las dependencias deben:

    a. Propender porque los funcionarios internos de su dependencia y que tengan acceso a activos de información de la entidad se entrenen, capaciten y aprueben las capacitaciones para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar los usuarios sobre la correcta operación de los procedimientos y la adecuada protección de los activos de información de la entidad.
    b. Controlar que los funcionarios de su dependencia reciban la inducción o reinducción en el puesto de trabajo y/o bajo un esquema virtual.

5. Los supervisores de los contratos deben:

    a. Propender porque los contratistas bajo su supervisión y que tengan acceso a activos de información de la entidad se entrenen y reciban transferencia de conocimiento para las actividades que van a desempeñar, esto con el fin de sensibilizar los usuarios sobre la correcta operación de los procedimientos y la adecuada protección de los activos de información de la entidad.

6. Los funcionarios y terceros deben:

    a. Recibir las capacitaciones que suministra la Oficina de Seguridad de la Información y verificar que sus procesos y procedimientos incluyan los controles de seguridad y privacidad adecuados.
    b. Aprobar los cursos sobre seguridad y privacidad de la información que la Subdirección de la Escuela de Impuestos y Aduanas le asigne.

E. Controles relacionados:

1. 5.17 - Información de autenticación
2. 6.8 - Reporte de eventos de seguridad de la información

5.2.4 Proceso disciplinario

A. Objetivo de control: Cumplir con lo establecido en el Código General Disciplinario (CGD), Ley 1952 de 2019, que es la norma base para adelantar los procesos contra funcionarios y algunos particulares que ejercen funciones públicas de manera permanente o transitoria.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información que define lineamientos en materia de seguridad y privacidad y la Subdirección de Asuntos Disciplinarios y Subdirección de Compras y Contratos, que realizan actividades de verificación del cumplimiento del Código General Disciplinario en la **DIAN**.

C. Características del control:

c.

1. Tipo de control: preventivo y correctivo.

2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Asesorar a la Subdirección de Asuntos Disciplinarios en las acciones de traslado ante las instancias disciplinarias, administrativas o penales correspondientes, del resultado de los procesos derivados de los reportes y del análisis de los incidentes de seguridad y privacidad, teniendo en cuenta el impacto y las responsabilidades identificadas.

2. La Subdirección de Asuntos Disciplinarios debe:

   a. Investigar las conductas o violaciones a la seguridad de la información con relevancia disciplinaria, en las que se pueden ver inmersos funcionarios y exfuncionarios de la entidad, en el desarrollo de las funciones que les han sido encomendadas, o por su cargo, o por su sola condición de funcionario.
   b. Poner en conocimiento de los organismos competentes, la comisión de hechos presuntamente irregulares sobre seguridad y privacidad de la información de los que se tenga conocimiento dentro del proceso disciplinario.

3. Los funcionarios y terceros deben:

   a. Reportar cualquier comportamiento que esté relacionado con la violación de las normas, políticas, procedimientos o lineamientos de seguridad y privacidad de la información de la **DIAN** o, acerca de la ocurrencia de alguno de los delitos informáticos considerados en la Ley 1273 de 2009 si la conducta es cometida por algún funcionario o contratista.

4. Los supervisores de los contratos deben:

   a. Reportar cualquier comportamiento que esté relacionado con la violación de las normas, políticas, procedimientos o lineamientos de seguridad y privacidad de la información de la **DIAN** o, acerca de la ocurrencia de alguno de los delitos informáticos considerados en la Ley 1273 de 2009 si la conducta es cometida por un contratista bajo su supervisión.

5. Los funcionarios deben:

   a. Conocer las responsabilidades implícitas en los deberes definidos en el Código General Disciplinario (CGD), Ley 1952 de 2019, en particular el Artículo 38 numeral 6: “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”.
   b. Conocer lo pertinente a la violación de las políticas y lineamientos de seguridad y privacidad de la información de la entidad, con aplicación de lo establecido en la ley, particularmente en el Código General Disciplinario (CGD), Ley 1952 de 2019, el Estatuto Anticorrupción (Ley 1474 de 2011), junto con lo concerniente a delitos informáticos en la Ley 1273 de 2009, de ser el caso, y demás normas que las adicionen, modifiquen, reglamenten o complementen.

6. Los contratistas deben:

    a. Conocer lo pertinente a la violación de las políticas y lineamientos de seguridad y privacidad de la información de la entidad, con aplicación de lo establecido en la ley, particularmente en el Código General Disciplinario (CGD), Ley 1952 de 2019, el Estatuto Anticorrupción (Ley 1474 de 2011), junto con lo concerniente a delitos informáticos en la Ley 1273 de 2009, de ser el caso, y demás normas que las adicionen, modifiquen, reglamenten o complementen.

E. Controles relacionados:

1. 5.28 - Recopilación de pruebas

5.2.5 Responsabilidades después de la terminación o cambio de empleo

A. Objetivo de control: Definir responsabilidades y deberes de seguridad y privacidad que permanecen después de la terminación o cambio de empleo en la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, la Oficina de Tributación Internacional, la Dirección de Gestión de Innovación y Tecnología y la Dirección de Gestión Corporativa y sus subdirecciones Gestión del Empleo Público y Compras y Contratos, que realizan las actividades de en la terminación o cambio de empleo en la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Establecer mecanismos que permitan al jefe inmediato o supervisor de un contratista reportar eventos o incidentes que impliquen la pérdida, daño, robo o compromiso de activos de información de la **DIAN**, debido a la terminación o cambio de empleo del personal.

2. La Dirección de Gestión Corporativa debe:

    a. Establecer lineamientos a seguir en el caso de retiro, investigación, inhabilidades, o cambio de funciones de un funcionario, o así como con el personal contratado en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
    b. Establecer controles necesarios en sus procesos de terminación o cambio de empleo del personal de la **DIAN**.
    c. Verificar que los lineamientos establecidos en este numeral, ante la terminación o cambio de empleo del personal de la **DIAN**, se encuentren en procedimientos formales.

3. La subdirección Gestión del Empleo Público debe:

   a. Informar a los funcionarios que después de la terminación o cambio de empleo de la **DIAN**, las responsabilidades y deberes de seguridad y privacidad de la información permanecen válidos.
   b. Solicitar la desactivación del acceso a los servicios tecnológicos como: accesos VPN, cuentas de usuario, credenciales y demás accesos vinculantes y no necesarios para la OPEAC.
   c. Informar a la supervisión del contrato de vigilancia y seguridad privada para desactivar los accesos biométricos o de tarjetas de proximidad los sistemas de control de acceso.
   d. Definir un mecanismo para obtener el correcto diligenciamiento del Acta de Entrega por parte del funcionario, exceptuando que la desvinculación sea por fallecimiento:
   e. Recoger y custodiar la información de la **DIAN**.
   f. Transferir la información, de ser el caso.
   g. Verificar que se devuelvan todos los activos de información, se desactiven y/o eliminen los accesos físicos y lógicos y se transfiera la información pertinente a la **DIAN**.

4. La Subdirección de Compras y Contratos debe:

   a. Informar a los contratistas que después de terminación anticipada, definitiva, temporal o cesión del contrato de la **DIAN**, las responsabilidades y deberes de seguridad y privacidad de la información permanecen válidos.
   b. Definir un mecanismo para obtener el correcto diligenciamiento del Acta de Entrega por parte del contratista, exceptuando que la desvinculación sea por fallecimiento:
   c. Recoger y custodiar la información de la **DIAN**.
   d. Transferir la información, de ser el caso.
   e. Verificar que se devuelvan todos los activos de información, se desactiven y/o eliminen los accesos físicos y lógicos y se transfiera la información pertinente a la **DIAN**.
   f. Emitir un comunicado a los proveedores y demás personal con el que el usuario interno tenga contacto, indicándoles que esa persona ya no labora en la **DIAN** e informándoles quién asumirá sus funciones o responsabilidades.

5. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Establecer canales de comunicación y divulgarlos para que las dependencias que realizan vinculación de personal (tanto funcionarios como contratistas) notifiquen cuando el personal se desvincule de la entidad.
   b. Desactivar o deshabilitar el acceso a los servicios tecnológicos como: la cuenta de dominio, cuentas de administrador, cuentas privilegiadas, accesos a la VPN, perfiles y permisos de escritorio virtual, roles de sistemas de información y cuentas de usuario en aplicativos legados, entre otros, cuando se solicite formalmente a través de la herramienta de casos que utilice la dependencia.
   c. Crear una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con la **DIAN**. Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.
   d. Cambiar la contraseña inmediatamente y asignar un nuevo responsable cuando un funcionario o contratista se desvincule y esté a cargo de un buzón genérico (ejemplo: comunicaciones@dian.gov.co).
   e. Realizar el monitoreo sobre la gestión de roles y perfiles de acceso a la plataforma tecnológica de la **DIAN** en la terminación contractual o desvinculación de la entidad.

6. Las Subdirección Administrativa deben:

   a. Recoger los activos de información físicos, cuando la subdirección Gestión del Empleo Público notifique sobre la desvinculación definida de un funcionario.
   b. Recoger los activos de información físicos, cuando la Subdirección de Compras y Contratos notifique sobre la desvinculación definida de un contratista.

E. Controles relacionados:

1. 6.2 Términos y condiciones de empleo
2. 6.6 Acuerdos de confidencialidad o no divulgación

5.2.6 Acuerdos de confidencialidad o no divulgación

A. Objetivo de control: Proteger la información de la entidad y notificar a todos los usuarios internos, externos y proveedores de la **DIAN** sobre la responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada según lo especificado en el Manual para el tratamiento de datos personales y este manual.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, la Oficina de Tributación Internacional, y la Dirección de Gestión Corporativa y sus subdirecciones Gestión del Empleo Público y Compras y Contratos, que deben solicitar la firma del compromiso de confidencialidad y de no divulgación de los funcionarios y contratistas que se vinculan a la **DIAN**.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Incluir en el compromiso de confidencialidad y de no divulgación criterios como: duración del acuerdo, criterios después de la terminación, derecho a auditar y monitorear, notificación de incidentes, acciones ante un incumplimiento y similares.
   b. Definir un compromiso de confidencialidad y de no divulgación que incluya el tratamiento de los datos personales y los requisitos establecidos en este documento.

2. La Dirección de Gestión Corporativa debe:

   a. Establecer lineamientos para que tanto funcionarios como contratistas firmen el compromiso de confidencialidad y no divulgación.
   b. Revisar los requisitos de los acuerdos de confidencialidad y no divulgación, periódicamente o cuando ocurran cambios que influyan en los mismos.

3. La subdirección Gestión del Empleo Público debe:

    a. Supervisar que los funcionarios firmen el compromiso de confidencialidad y no divulgación cuando se vinculan a la entidad.
    b. Verificar que los funcionarios firmen el compromiso de confidencialidad y no divulgación cuando se vinculan a la entidad.
    c. Revisar los requisitos de los acuerdos de confidencialidad y no divulgación, periódicamente o cuando ocurran cambios que influyan en los mismos.

4. La Subdirección de Compras y Contratos debe:

    a. Hacer que todos los contratistas firmen el compromiso de confidencialidad y no divulgación cuando se vinculan a la entidad.
    b. Verificar que los contratistas firmen el compromiso de confidencialidad y no divulgación cuando se vinculan a la entidad.
    c. Incluir dentro del manual de contratación obligaciones para que los supervisores de los contratos soliciten la firma del compromiso de confidencialidad y no divulgación cuando el tercero tenga acceso a la información de la **DIAN**.
    d. Revisar los requisitos de los acuerdos de confidencialidad y no divulgación, periódicamente o cuando ocurran cambios que influyan en los mismos.

5. Los supervisores de los contratos deben:

    a. Solicitar y verificar la firma del compromiso de confidencialidad y no divulgación cuando el tercero bajo su supervisión tenga acceso a la información de la **DIAN**.

6. Los funcionarios y terceros deben:

    a. Firmar el compromiso de confidencialidad y no divulgación cuando se vinculen a la entidad.
    b. Verificar y entender el compromiso de confidencialidad y no divulgación.

E. Controles relacionados:

1. 5.31 - Requisitos legales, estatutarios, reglamentarios y contractuales
2. 5.32 - Derechos de propiedad intelectual
3. 5.33 - Protección de registros
4. 5.34 - Privacidad y protección de PII

5.2.7 Trabajo a distancia

A. Objetivo de control: definir las medidas de seguridad de la información que deben ser consideradas por los funcionarios de la entidad que trabajen en modalidad de teletrabajo, para que la información a la que se accedan se procese o almacene en los lugares según la modalidad asignada y esté protegida de accesos no autorizados, divulgación, pérdida o daño.

B. Alcance: el alcance de esta política aplica para la Oficina de Seguridad de la Información, la Dirección de Gestión Corporativa y su Subdirección de Gestión del Empleo Público, los funcionarios que se encuentren en modalidad de teletrabajo en la **DIAN** y la Dirección de Gestión de Innovación y Tecnología, que implementa controles tecnológicos en teletrabajo.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Socializar a los funcionarios que se encuentren en modalidad de teletrabajo las medidas de seguridad y privacidad, y las buenas prácticas para proteger la información.
   b. Dar a conocer a los teletrabajadores las medidas de seguridad de la información que estos deben cumplir.
   c. Concordar los lineamientos de las políticas de seguridad privacidad de la información con los requisitos relacionados en resolución 1247 del 2022 de la **DIAN**.

2. La Dirección de Gestión Corporativa debe:

   a. Establecer lineamientos para las condiciones de teletrabajo para todos los funcionarios de la **DIAN** incluyendo criterios para el uso adecuado de la información asignada.

3. La subdirección Gestión del Empleo Público debe:

   a. Implementar las condiciones de teletrabajo para todos los funcionarios de la **DIAN** incluyendo criterios para el uso adecuado de la información asignada.
   b. Establecer reglas y mecanismos de seguridad para el entorno físico para el teletrabajador.
   c. Establecer lineamientos asociados al uso apropiado de la información física de los teletrabajadores.
   d. Verificar que los elementos de información física o electrónica asignados al teletrabajador se encuentren en una ubicación apropiada que evite el daño o deterioro.
   e. Disponer de un acuerdo de teletrabajo para establecer las condiciones de seguridad en el teletrabajo.

4. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Llevar el registro e identificación de los equipos de cómputo que fueron asignados a los funcionarios que se encuentren en teletrabajo.
   b. Implementar controles de seguridad tecnológicos para proteger la confidencialidad, integridad y disponibilidad de la información en modalidad de teletrabajo.
   c. Verificar los controles tecnológicos establecidos y los parámetros de seguridad de la información para la realización de las funciones bajo teletrabajo.
   d. Implementar sistemas y protocolos de seguridad para la transmisión de la información en teletrabajo.
   e. Verificar periódicamente la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la **DIAN**.
   f. Instalar la misma línea base de software en los equipos de cómputo utilizados tanto para teletrabajo como en las instalaciones de la **DIAN**.
   g. Poner a disposición de los teletrabajadores las herramientas tecnológicas, instrumentos, equipos, conexiones, programas y demás elementos necesarios para la prestación y desarrollo de las labores.

h. Verificar que la conexión con la que cuenta el teletrabajador sea apta para realizar las labores.
i. Implementar una plataforma, software, programa, aplicación o cualquier herramienta tecnológica para facilitar las comunicaciones con el teletrabajador y realizar sus funciones.
j. Activar los registros de auditoría con el propósito, monitorear y/o controlar en los diferentes sistemas y aplicaciones de la entidad, y las actividades realizadas por los teletrabajadores.
k. Activas herramientas de cifrado en los equipos que se utilicen para teletrabajo con el fin de evitar la fuga de información en caso de robo fuga de información.
l. Instalar herramientas de borrado remoto en los equipos que se utilicen en para teletrabajo con el fin de prevenir la fuga de información en caso de robo.
m. Asignar un espacio de respaldo de la información en medios compartidos para los teletrabajadores con los debidos controles de acceso.

5. Los funcionarios en teletrabajo deben:

a. Prestar la debida custodia y el cuidado de sus cuentas de usuario y contraseñas de los equipos entregados, de acceso a las aplicaciones corporativas y las que permiten autenticarse en la red como usuarios **DIAN**.
b. Responder por todas las acciones que se realicen utilizando su cuenta de usuario y contraseña.
c. Responder por la información que genere, obtenga, adquiera o controle en el desempeño de sus funciones, especialmente si esta información es pública clasificada o pública reservada, independientemente del medio en el que esté disponible (físico o electrónico).
d. Preservar la seguridad de los equipos designados, en los que no se podrá instalar ningún software, programa o aplicativo que no se encuentre autorizado por la entidad.
e. Utilizar los equipos suministrados por la **DIAN** exclusivamente para el desarrollo y cumplimiento de las funciones propias del cargo o de las actividades adelantadas para la prestación de las labores encomendadas.
f. Utilizar la conexión a internet contratada para el sitio en el cual va a desempeñar sus labores y en ningún caso esta conexión puede ser pública o compartida.
g. Presentar y poner a disposición de la Dirección de Gestión de Innovación y Tecnología, los equipos asignados para teletrabajo, cuando sea requerido y en los tiempos establecidos por esta dirección o quien haga sus veces.
h. Evitar el uso compartido de los elementos de la **DIAN** suministrados por parte de la entidad.
i. Firmar el acuerdo con las condiciones de seguridad en el teletrabajo.

E. Controles relacionados:

1. 6.8 - Reporte de eventos de seguridad de la información

5.2.8 Reporte de eventos de seguridad de la información

A. Objetivo de control: Reportar por parte de los funcionarios y terceros que identifiquen eventos de seguridad de la información y privacidad tan pronto tengan conocimiento de estos a través de los canales de gestión definidos.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y todos los funcionarios y terceros que tengan acceso a la información de la **DIAN** e identifiquen posibles incidentes de seguridad y privacidad de la información.

C. Características del control:

1. Tipo de control: detectivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Definir procedimientos para el reporte de posibles eventos de seguridad y privacidad de la información incluyendo: responsables, canales de comunicación, tiempos de respuesta, clasificación de los posibles eventos.
    b. Socializar el procedimiento de incidentes de posibles eventos de seguridad y privacidad de la información.
    c. Hacer ejercicios de ingeniería social para verificar que el personal de la entidad haga uso de los canales dispuestos para el reporte de posibles eventos de seguridad y privacidad de la información.

2. Los funcionarios y terceros deben:

    a. Utilizar los canales de comunicación definidos por la Oficina de Seguridad de la Información para reportar los posibles eventos de seguridad y privacidad de la información, entre los cuales está el buzón de la oficina: seguridaddigital@dian.gov.co.
    b. Considerar que cualquier violación de la integridad, confidencialidad o expectativas de disponibilidad de la información de datos personales, según la Ley 1581 de 2012 debe ser reportada.
    c. Reportar cualquier posible evento de seguridad y privacidad de la información teniendo en cuenta al menos las siguientes situaciones:

        - Un control de seguridad ineficaz
        - Violación de la integridad, confidencialidad o expectativas de disponibilidad de la información
        - Errores humanos
        - Violaciones de acuerdos de seguridad física o digital
        - Daño o pérdida de información física o digital
        - Fuga o robo de información física o digital
        - Cambios no controlados en el sistema
        - Mal funcionamiento en el software o hardware
        - Violaciones de acceso
        - Suplantación de identidad
        - Uso indebido de imagen institucional

E. Controles relacionados:

1. 8.8 - Gestión de vulnerabilidades técnicas

5.3 Controles físicos

A continuación, se describen los lineamientos y políticas que hacen referencia a las responsabilidades que establece la **DIAN** para los funcionarios y terceros en términos de seguridad física:

5.3.1 Perímetros de seguridad física

A. Objetivo de control: Establecer los mecanismos o controles necesarios en los procedimientos de la entidad de forma que existan, funcionen y se apliquen adecuada y efectivamente los controles para los perímetros de seguridad física de la **DIAN**, teniendo en cuenta los principios y lineamientos de este numeral, con el fin de proteger las dependencias que contienen información de la entidad y otros activos asociados.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa, dependencia encargada de definir los lineamientos para los controles de perímetro de seguridad física de la entidad tanto en su sede principal como en todas las seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de Seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Definir junto con la Subdirección de Infraestructura Tecnológica y de Operaciones, el perímetro de las áreas seguras de tecnología que contienen la información y sus instalaciones de procesamiento sensible o crítico, las cuales deben estar cerradas y protegidas de accesos no autorizados (cerraduras, alarmas, construcciones sólidas, mecanismos de control).
   b. Validar que el perímetro de seguridad cuente con vigilancia mediante Circuito Cerrado de Televisión (CCTV) y ser monitoreado por el personal de vigilancia contratado por la **DIAN.**
   c. Validar que las puertas y ventanas de las oficinas, salas e instalaciones, que tienen bajo su custodia activos de información de alta criticidad, permanezcan cerradas con llave cuando estén desocupadas o no estén siendo supervisadas. Aquellas oficinas que no tengan puerta deben permanecer vigiladas o supervisadas, mientras se encuentre en ellas personal externo a la **DIAN.**
   d. Implementar alarmas, monitorear y efectuar pruebas periódicamente a todas las puertas contra incendios en los perímetros de seguridad que hayan definido la entidad.
   e. Efectuar un análisis de riesgos y planes de tratamiento específicos para cada una de las seccionales que permitan aplicar los lineamientos relacionados con la seguridad perimetral para estas instalaciones.
   f. Establecer los mecanismos o controles necesarios en sus procedimientos que permitan que existan, funcionen y se apliquen adecuada y efectivamente los controles físicos de entrada a las instalaciones y áreas seguras de la **DIAN**, teniendo en cuenta los principios y lineamientos de este literal y los que indique el Sistema de Gestión de Calidad.
   g. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN,** debido a inconvenientes en los perímetros de seguridad física.

2. Los funcionarios y terceros de la entidad deben:

    a. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN**, debido a inconvenientes en los perímetros de seguridad física.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal
2. 6.8 – Informes de eventos de seguridad de la información
3. 7.2 – Entrada física
4. 7.3 – Asegurar oficina, salas e instalaciones
5. 7.4 – Supervisión de la seguridad física

5.3.2 Entrada física

A. Objetivo de control: Evitar accesos físicos no autorizados que atenten contra la confidencialidad, integridad o disponibilidad de la información de la entidad. Así mismo, controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos a donde pueda entrar personal no autorizado a la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa, dependencia encargada de definir los lineamientos para los controles de entrada física de la entidad y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

    a. Implementar un sistema de control de acceso a las instalaciones de la **DIAN**, así como a las áreas seguras y a las demarcadas con acceso restringido dentro y fuera de las instalaciones principales de la entidad.
    b. Instalar mecanismos físicos (cerraduras, alarmas, sistemas lectores de tarjeta, muros y similares) con el objetivo de prevenir el acceso no autorizado a zonas que contengan activos de información de alta criticidad de la **DIAN**.
    c. Implementar en todos los puntos de acceso a áreas seguras, un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
    d. Contar con registro para el ingreso de funcionarios, contratistas y visitantes a las instalaciones de la **DIAN**, por parte del servicio de vigilancia ubicado en la recepción se debe registrar: nombre, número de identificación, fecha y hora de entrada, y nombre del funcionario que autoriza el ingreso.
    e. Implementar avisos de privacidad conforme a las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.

f. Implementar un mecanismo de identificación para los contratistas y visitantes de la **DIAN** que se debe portar en un lugar visible durante la estadía en la entidad, al igual que deben portar el carné o escarapela de la entidad de la cual provienen, si es el caso.
g. Mantener cerradas todas las puertas de acceso a cada una de las dependencias, oficinas, centros de cómputo, cableado y comunicaciones, salas de capacitación y similares en casos de ausencias temporales.
h. Establecer los mecanismos o controles necesarios en sus procedimientos que permitan que existan, funcionen y se apliquen adecuada y efectivamente los controles físicos de entrada a las instalaciones y áreas seguras de la **DIAN**, teniendo en cuenta los principios y lineamientos de este literal y los que indique el Sistema de Gestión de Calidad.
i. Establecer áreas de cargue, descargue y despacho de mercancías en zonas que no permitan el acceso a otras áreas de las edificaciones e implementar señalizaciones en estas.
j. Mantener las puertas externas de áreas de cargue, descargue y despacho vigiladas cuando las puertas internas estén abiertas.
k. Llevar un registro de los materiales que ingresan a instalaciones de la **DIAN**.
l. Inspeccionar y examinar los materiales que ingresan para determinar la presencia de componentes peligrosos o evidencias de alteración durante el transporte. Si hay componentes peligrosos o presentan alteraciones, se debe reportar de inmediato al personal de seguridad de la **DIAN**.
m. Portar el respectivo carné de identificación. En caso de ser personal que acceda a áreas de cargue, descargue y despacho debe estar identificado con información de la empresa para la que trabaja, así, confirmar que se cuenta con los permisos para transitar en estas áreas.
n. Establecer los mecanismos o controles necesarios en sus procedimientos para asegurar la existencia, funcionalidad y aplicación efectivade los controles físicos de acceso a las instalaciones y áreas seguras de la **DIAN**.

2. Los funcionarios y terceros de la entidad deben:

a. Enviar un comunicado por parte del funcionario responsable que autoriza el ingreso temporal de visitantes, indicando el motivo y duración de la autorización.
b. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN** debido a inconvenientes en los controles físicos de entrada o salida, así como los eventos e incidentes que se presenten en las áreas de despacho, cargue y descargue, que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN**.
c. Establecer y asignar permisos de acceso a las dependencias, oficinas, centros de cómputo, cableado y comunicaciones, salas de capacitación y similares únicamente a los Usuarios internos autorizados para su acceso.

E. Controles relacionados:

1. 5.9 – Inventario de información y otros activos asociados
2. 5.17 – Información de autenticación
3. 5.18 – Derechos de acceso
4. 5.33 – Protección de registros
5. 5.34 - Privacidad y protección de Información de Identificación Personal
6. 6.8 – Informes de eventos de seguridad de la información
7. 7.10 – Medios de almacenamiento

5.3.3 Asegurar oficinas, salas e instalaciones

A. Objetivo de control: Prevenir el acceso físico no autorizado a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa, dependencia encargada de administrar los recursos físicos de la **DIAN**, sus instalaciones y seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Implementar un sistema de detección de intrusos (sistema de alarmas físico) que debe permanecer activo en horario laboral.
   b. Realizar pruebas periódicas a los sistemas de detección de intrusos (sistema de alarmas físico) implementados, de forma que se pueda confirmar su correcto funcionamiento.
   c. Registrar todos los ingresos o salidas de las dependencias cada vez que entren o salgan los usuarios internos y visitantes, sin excepción. Este registro se debe realizar con la tarjeta de aproximación, mediante el sistema biométrico u otro sistema disponible para abrir las puertas. Por lo tanto, está prohibido “mantener abierta la puerta” para que ingresen o salgan otras personas diferentes a quien abrió la puerta con su mecanismo de ingreso. El personal de vigilancia de la **DIAN** debe estar atento al cumplimiento de este lineamiento.
   d. Acompañar a todos los visitantes por un funcionario de la **DIAN** cuando se encuentren en las dependencias donde se maneje información. Así mismo, los visitantes que requieran permanecer en las oficinas de la **DIAN**, por periodos superiores a dos días, deben ser presentados al personal de la dependencia donde permanecerán.
   e. Definir el horario autorizado para recibir visitantes en las instalaciones de la **DIAN**. En horarios distintos se requerirá de la autorización del jefe inmediato o superior jerárquico de la dependencia correspondiente.
   f. Clasificar e Identificar las instalaciones de la **DIAN** que se consideren críticas en relación con las actividades de procesamiento de información que son desarrolladas dentro de estas. Esta identificación debe ser discreta, sin señales obvias.
   g. Definir una ubicación específica para directorios, guías telefónicas internas y mapas, que no se encuentren al alcance del público o visitantes, permitiendo que el acceso a estos recursos sea únicamente a personal autorizado de la entidad.
   h. Efectuar un análisis de riesgos y planes de tratamiento específicos para cada una de las seccionales, que permita aplicar los lineamientos relacionados con la seguridad de oficinas, salas e instalaciones.
   i. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN** debido a fallas en la seguridad de oficinas, recintos e instalaciones.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal

5.3.4 Supervisión de la seguridad física

A. Objetivo de control: Verificar periódicamente el acceso físico de funcionarios y terceros con acceso a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones de la **DIAN**, para prevenir y detectar accesos no autorizados de forma oportuna a las instalaciones de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa, dependencia encargada de verificar de forma periódica el ingreso físico a las dependencias e instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Instalar circuito cerrado de televisión (CCTV) para la vigilancia de los equipos y usuarios internos o visitantes que realicen funciones con activos de información de alta criticidad, incluyendo las dependencias de cargue, descargue y despacho de mercancías con el objetivo de controlar y monitorear estas dependencias.
   b. Implementar avisos de privacidad conforme a las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.
   c. Monitorear y registrar periódicamente las actividades de los usuarios internos y visitantes en las instalaciones de la **DIAN** a través de un circuito cerrado de televisión.
   d. Notificar y presentar sin excepción al personal de cada dependencia, los visitantes que requieran permanecer en las oficinas de la **DIAN** por periodos continuos, definiendo con cada dependencia el tiempo mínimo para considerar obligatoria estas notificaciones en días.
   e. Implementar revisiones periódicas a los detectores de contacto, sonido o movimiento que permiten activar alarmas de intrusión en la entidad; estas revisiones deben considerar un cronograma de revisión que debe ser elaborado, aprobado y actualizado por la entidad.
   f. Activar alarmas de forma permanente en dependencias desocupadas dentro de las instalaciones de la **DIAN**, especialmente si se trata de secciones que contengan equipos tecnológicos o de comunicaciones.
   g. Mantener todos los diseños de cada uno de los sistemas de monitoreo, con clasificación “clasificada”, para evitar que existan posibilidades de divulgación no autorizada.
   h. Implementar, para cada panel de control de los sistemas de alarmas, mecanismos a prueba de manipulaciones no autorizadas.
   i. Implementar pruebas periódicas a los sistemas de alarmas y monitoreos que permitan confirmar que su funcionamiento se realiza de forma correcta acorde a lo definido por la entidad.

j. Efectuar un análisis de riesgos y planes de tratamiento específicos para cada una de las seccionales, que permita aplicar los lineamientos relacionados con la supervisión de la seguridad en estas instalaciones.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal.
2. 6.8 – Informes de eventos de seguridad de la información.

5.3.5 Protección contra amenazas físicas y ambientales

A. Objetivo de control: Diseñar e implementar la protección contra amenazas físicas y ambientales, considerando desastres naturales, ataques maliciosos, accidentes y otras amenazas físicas intencionales o no intencionales a la infraestructura de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, Oficina de Seguridad de la Información, Subdirección de Procesos, y la Subdirección Administrativa, dependencias encargadas de la gestión, control y pruebas de los Planes: Plan de Continuidad del Negocio y Plan de Recuperación de Desastres; así como la Subdirección de Desarrollo de Talento Humano por la facultad de capacitar a los funcionarios de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Alinear, revisar y actualizar los controles contra amenazas externas y ambientales, enmarcados en los planes de contingencia, de emergencia, de gestión de riesgo, planes de evacuación y de continuidad de la operación tecnológica.
   b. Monitorear las variables de temperatura y humedad de los centros de cómputo, cableado, comunicaciones y cuartos técnicos; y cuando estos se vean afectados por daño o falta de mantenimiento, reportar a la Subdirección Administrativa dichas eventualidades para que estos equipos sean cambiados o se haga el mantenimiento necesario para su debido funcionamiento.

2. La Subdirección Administrativa debe:

   a. Establecer los mecanismos o controles necesarios en sus procedimientos para permitir que existan, funcionen y se apliquen adecuada y efectivamente las acciones contra amenazas externas y ambientales, teniendo en cuenta los principios y lineamientos de este numeral y formen parte del Sistema de Gestión Ambiental de la entidad.
   b. Implementar mecanismos adecuados contra las amenazas ambientales (temperatura, humedad, fuego, etc.), especificados por los fabricantes de los equipos dispuestos en los centros de cómputo, cableado, comunicaciones y cuartos técnicos de la **DIAN**.
   c. Monitorear las variables de temperatura y humedad de los cuartos de archivo y, cuando estos se vean afectados por daño o falta de mantenimiento, se deben reportar dichas

eventualidades para que estos equipos sean cambiados o se haga el mantenimiento necesario para su debido funcionamiento.
d. Identificar las amenazas externas y definir acciones para prevenir o reducir las consecuencias de estas.
e. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN** debido a amenazas externas o ambientales.

3. La Oficina de Seguridad de la Información debe:

   a. Alinear, revisar y actualizar los procesos de continuidad operativa y recuperación en caso de desastres, respecto de la infraestructura tecnológica de la **DIAN**.

4. La Subdirección de Procesos debe:

   a. Coordinar la elaboración del Plan de Continuidad y Recuperación de Desastres, que mitigue la afectación la operación de la entidad; así mismo, implementar pruebas periódicas que confirmen operación adecuada de los controles contra amenazas externas y ambientales.

5. La Subdirección de Desarrollo de Talento Humano debe:

   a. Revisar, aprobar, actualizar y divulgar los documentos que relacionan los aspectos de prevención y atención de emergencias identificadas a nivel nacional, declaración del nivel de emergencia, alarmas y demás aspectos de seguridad física, que se encuentran contemplados en los procedimientos relacionados y que hacen parte del listado maestro.

6. Los funcionarios y terceros de la entidad deben:

   a. Conocer y aplicar los controles para la prevención y atención de emergencias identificadas a nivel nacional, declaración del nivel de emergencia, alarmas y demás aspectos de seguridad física, que se encuentran contemplados en los procedimientos relacionados y que hacen parte del listado maestro.
   b. Atender las recomendaciones sobre las medidas de seguridad del personal e instalaciones establecidas en el “Memorando 00092 del 30 de abril del 2021 “Recomendación sobre las medidas de seguridad del personal e instalaciones de la **DIAN**”.

E. Controles relacionados:

1. 5.29 – Seguridad de la información durante la interrupción
2. 5.30 – Preparación de las TIC para la continuidad del negocio

5.3.6 Trabajar en áreas seguras

A. Objetivo de control: Diseñar y aplicar medidas de seguridad para trabajar en áreas seguras de la **DIAN**, protegiendo la información y otros activos asociados contra daños e interferencias no autorizadas por parte del personal que trabaja en estas dependencias.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de

controlar la seguridad para trabajar en instalaciones de la **DIAN** y sus seccionales, así como la Oficina de Seguridad de la Información, encargada de gestionar y monitorear el acceso de ingreso a las áreas seguras.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Contar con mecanismos de protección física, ambiental, dispositivos y controles de acceso adecuados para la protección de la información que permitan el acceso solamente al personal autorizado.
   b. Restringir y/o resguardar elementos inflamables dentro de las áreas seguras, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.
   c. Implementar avisos que informen la restricción que existe en las áreas seguras, las cuales deben detallar que en ninguna circunstancia se puede fumar, comer o beber.
   d. Capacitar al personal de limpieza acerca de las precauciones a seguir durante el proceso de limpieza en cada una de las dependencias que la **DIAN** ha considerado como áreas seguras.
   e. Designar un funcionario específico para supervisar las actividades de limpieza en las áreas seguras. Con esta supervisión, a su vez, se impide el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.
   f. Implementar en las áreas seguras avisos relacionados con la Protección de Datos Personales en Sistemas de Videovigilancia que realiza la entidad.
   g. Monitorear periódicamente las áreas seguras, confirmando que estas cumplen como mínimo con lo siguiente:
      - Que estén vacías y cerradas con llave.
      - Restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte de la dependencia encargada.
      - Con apoyo de un CCTV, visualizar el trabajo realizado en estas áreas teniendo en cuenta que las cámaras no pueden apuntar directamente a la captura de información.
   h. Establecer los mecanismos o controles necesarios en sus procedimientos para permitir que existan, funcionen y se apliquen adecuada y efectivamente los controles de seguridad de las áreas seguras de la **DIAN**, teniendo en cuenta los principios y lineamientos de este numeral y que forman parte del Sistema de Gestión de Calidad.
   i. Reportar a la Oficina de Seguridad de la Información, los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN** en las dependencias seguras.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Contar con mecanismos de protección física y ambiental y dispositivos y controles de acceso adecuados para la protección de la información que permitan el acceso solamente al personal autorizado a las instalaciones seguras de los data center.

b. Restringir, almacenar, mantener y/o guardar elementos inflamables dentro de las dependencias seguras de los data center, y demás infraestructura de soporte a los sistemas de información y comunicaciones.
c. Implementar avisos que informen la restricción que existe en los data center, las cuales deben detallar que en ninguna circunstancia se puede fumar, comer o beber.
d. Designar a un funcionario específico para supervisar las actividades de limpieza en los datacenter. Con esta supervisión, a su vez, se impide el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.
e. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la **DIAN** en los data center.
f. Monitorear periódicamente los datacenter, confirmando que cumplen como mínimo con lo siguiente:
   - Que estén vacías y cerradas con llave.
   - Restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte de la dependencia encargada.
   - Con apoyo de un CCTV, visualizar el trabajo realizado en estas dependencias teniendo en cuenta que las cámaras no pueden apuntar directamente a la captura de información.

3. La Oficina de Seguridad de la Información debe:

   a. Gestionar los roles y responsabilidades que permiten el control y asignación de permisos para el acceso a áreas seguras ubicadas dentro de las instalaciones de la **DIAN**.
   b. Monitorear periódicamente la asignación de privilegios relacionados con la gestión de accesos que permiten ingreso a las áreas seguras de la **DIAN**.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal
2. 6.8 – Informes de eventos de seguridad de la información

5.3.7 Escritorio y pantalla despejados

A. Objetivo de control: Establecer la política de escritorio y pantalla despejada para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios removibles, dispositivos de impresión y digitalización de documentos.

B. Alcance: El alcance de esta política aplica para la Subdirección de Soluciones y Desarrollo y la Subdirección Administrativa, dependencias encargadas de mantener las estaciones y/o puestos de trabajo, escritorios físicos o virtuales limpios y libres de información sensible para la entidad en las instalaciones de la **DIAN** y sus seccionales. También aplica para la Oficina de Seguridad de la Información, encargada de divulgar y sensibilizar del buen uso y manejo de la información en los puestos de trabajo.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Mantener las estaciones o puestos de trabajo o escritorios, físicos o virtuales, limpios y estar libres de documentos, carpetas, archivos o medios que contengan información sensible para la entidad con el fin de proteger los documentos físicos o electrónicos y reducir los riesgos de acceso no autorizado, pérdida o daño de la información.
   b. Capacitar a los instructores y/o asistentes sobre recoger los materiales utilizados, borrar completamente los archivos y vaciar la papelera en los computadores disponibles en estos sitios y borrar cualquier información que se haya escrito en los tableros o carteleras, cuando salgan de dependencias de trabajo conjunto como auditorios, salas de reuniones o salones de capacitación.

2. La Oficina de Seguridad de la Información debe:

   a. Capacitar a los funcionarios y terceros con el objetivo de crear una cultura de seguridad en el uso de documentos de trabajo o archivos fuera de su lugar de conservación o almacenamiento, permitiendo que la utilización solo sea en función de su uso y de lo sensible de la información que contengan y permitiendo que, al alejarse del puesto de trabajo o escritorio y al finalizar la jornada de trabajo, la información quede bajo llave y protegida de cualquier acceso, uso o difusión indebida.

3. Los funcionarios y terceros de la entidad deben:

   a. Evitar dejar sesiones abiertas en los computadores y/o portátiles desatendidos, así como tabletas o teléfonos celulares.
   b. Apagar los equipos ante ausencias prolongadas y al final de cada jornada.
   c. Prevenir y no dejar, en el escritorio del computador, archivos de información ni accesos directos a estos archivos. Se deben almacenar los archivos en las carpetas virtuales habilitadas OneDrive y SharePoint de la dependencia destinadas para este fin.
   d. Verificar que todos los documentos físicos y electrónicos se resguarden, tanto al final de la jornada como cuando se aleje del puesto de trabajo.
   e. Ubicar los computadores personales y/o portátiles de forma que las pantallas no puedan ser visualizadas por personas no autorizadas.
   f. Evitar anotar las contraseñas en papeles, evitar colocarlas en el computador o debajo del equipo.
   g. Retirar del escritorio y guardar en una gaveta con llave los documentos, los medios y los dispositivos de almacenamiento removibles como CD, DVD, discos duros externos o memorias USB, autorizados en la **DIAN**, cuando no los estén utilizando y al final de la jornada de trabajo.
   h. Guardar en el archivo de gestión los expedientes físicos a cargo, al final de la jornada.
   i. Evitar dejar sobre los escritorios las llaves utilizadas para acceder a documentos de archivo (físico o electrónico).
   j. Eliminar documentos con información reservada o clasificada que no se utilice nuevamente, hacer uso de la máquina de picar y depositar los desechos en los recipientes de la máquina o de basura destinados para su recolección.
   k. Evitar retirar de las instalaciones de la **DIAN** información (física o electrónica) y cualquier activo de información de propiedad de la entidad; solo se deben retirar en casos excepcionales autorizados por el jefe de la dependencia.

l. Prevenir riesgos y amenazas de sustracción, destrucción, ocultamiento y/o utilización indebida de los recursos y la información contenida en ellos. Se deben mantener los escritorios virtuales limpios y libres de documentos, carpetas, archivos o medios que contengan información sensible para la entidad con el fin de proteger los documentos físicos o electrónicos y reducir los riesgos de acceso no autorizado, pérdida o daño de la información.

4. La Subdirección de Soluciones y Desarrollo debe:

a. Resguardar en debida custodia los dispositivos y medios removibles de almacenamiento (bajo llave).
b. Bloquear los computadores y/o portátiles cuando no estén en uso. Los computadores deben tener configurado el protector de pantalla, de forma que se active luego del tiempo de inactividad establecido por la Dirección de Gestión de Innovación y Tecnología.
c. Apagar correctamente los equipos de cómputo en las ausencias superiores a dos horas; se exceptúan las máquinas y equipos indispensables que permiten la operatividad y disponibilidad de los servicios tributarios, aduaneros y cambiarios (TAC) a cargo de la **DIAN**.
d. Fortalecer los mecanismos y controles sobre las pantallas limpias enumerados en este control.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal.
2. 5.36 – Cumplimiento de políticas, normas y estándares de seguridad de la información.
3. 6.8 – Informes de eventos de seguridad de la información.
4. 7.8 – Ubicación y protección del equipo.

5.3.8 Ubicación y protección del equipo

A. Objetivo de control: Ubicar y proteger los equipos para reducir los riesgos de amenazas, peligros del entorno y accesos no autorizados.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, y la Subdirección Administrativa, dependencias encargadas de gestionar los equipos y recursos de cómputo en las instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

a. Ubicar los equipos y dispositivos que son utilizados para soportar las funciones misionales y críticas de la entidad en las dependencias cuyo acceso sea restringido y esté supervisado.
b. Mantener durante horario no hábil o en horarios en los cuales el usuario interno no se encuentre en su sitio de trabajo, bajo seguridad, los dispositivos removibles, así como

toda información reservada y clasificada de la **DIAN**, independientemente del medio en que se encuentre.

c. Ubicar en locaciones protegidas los equipos de cómputo e impresoras para reducir el riesgo de amenazas ambientales y de acceso no autorizado.
d. Instalar sistemas de protección eléctrica en las instalaciones que brinden protección ante eventos del clima relacionados con rayos y tormentas eléctricas, que puedan sobrecargar o afectar la infraestructura tecnológica de las instalaciones.
e. Implementar medidas de protección física y eléctrica en la plataforma tecnológica (Hardware, software y comunicaciones) en las instalaciones, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
f. Monitorear de forma periódica el funcionamiento de los dispositivos de seguridad que permiten la detección temprana de incidencias en los centros de cómputo, cableado, comunicaciones y cuartos técnicos de la **DIAN**.
g. Proteger, a través de canaletas, el cableado de la energía y telecomunicaciones que llevan datos o sostienen los servicios de información, para evitar el deterioro e indisponibilidad del servicio.
h. Restringir el movimiento o retiro de equipos entre dependencias o fuera de la **DIAN**, sin previa autorización del responsable y sus registros de ingreso y salida pertinentes.
i. Restringir el uso de activos de información pública reservada, pública clasificada o datos personales no públicos (Carpetas, archivos de uso diario, accesos directos y similares) por parte de los usuarios internos, para evitar el fácil acceso a la información.
j. Establecer los mecanismos o controles necesarios en sus procedimientos que permitan que existan, funcionen y se apliquen adecuada y efectivamente, las acciones para la ubicación y protección de equipos de la **DIAN** y se encuentren en procedimientos formales del Sistema de Gestión de Calidad.
k. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por inconvenientes en la ubicación y protección de equipos.
l. Instalar sistemas de protección eléctrica en los centros de cómputo, cableado, comunicaciones y cuartos técnicos de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, e debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Proteger y monitorear el mantenimiento físico y lógico de los dispositivos y sistemas de la infraestructura de seguridad.
b. Implementar en los centros de cómputo, cableado, comunicaciones y cuartos técnicos de la **DIAN**, dispositivos de seguridad que permitan la detección temprana de incidencias consideradas como mínimas a controlar.
c. Restringir los equipos de cómputo cuando se detecte o sospeche que el equipo se encuentra contaminado por un software malicioso, un virus o por una falla física.
d. Implementar y monitorear frecuentemente en los centros de cómputo, cableado, comunicaciones y cuartos técnicos, un sistema de detección y prevención de incendios que minimice el impacto que puede generar la ocurrencia de un evento o situación de incendio en el lugar.
e. Autorizar el uso de equipos ajenos a la entidad, una vez se confirme que dicho equipo cumple con la legalidad del software instalado, antivirus licenciado y actualizado.
f. Implementar y monitorear un sistema de refrigeración que sea capaz de enviar alarmas vía correo electrónico en caso de mal funcionamiento o futuro mantenimiento de equipos pertenecientes a los centros de cómputo de la **DIAN**.

g. Notificar de forma oportuna las alarmas de eventos relacionados con la energía, provenientes del sistema de regulación y estabilización del fluido eléctrico en las instalaciones de la **DIAN**.
h. Implementar medidas de protección física y eléctrica en la plataforma tecnológica (Hardware, software y comunicaciones) en los datacenter, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
i. Reportar a la Oficina de Seguridad de la Información los eventos incidentes que se puedan provocar en los centros de datos a cargo de terceros, sean estos On-premise, en la nube o híbridos.
j. Mantener durante las actividades de mantenimiento preventivo o correctivo, la concordancia con los intervalos y especificaciones del proveedor; así mismo, generar los registros a que haya lugar en donde se permita realizar la trazabilidad de las fallas, personas involucradas y actividades desarrolladas.
k. Restringir los privilegios de configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla institucional, entre otros.
l. Implementar un bloqueo automático de las sesiones de usuario en todas las estaciones de trabajo después de cinco minutos de inactividad.
m. Restringir en los equipos de escritorio el almacenamiento de información que no se realice en carpetas compartidas de la dependencia o en repositorios como OneDrive o SharePoint.
n. Implementar y monitorear, en toda la infraestructura tecnológica, estándares de seguridad (hardening) para su funcionamiento.
o. Establecer los controles apropiados a los servicios de suministro que atenten contra los activos de información, así como identificarlos, clasificarlos, valorarlos, analizar sus riesgos y establecer los controles para mitigar la afectación a estos.
p. Ejecutar el procedimiento de borrado seguro antes de su reutilización o finalización de su vida útil, para cada uno de los equipos que contengan información pública reservada, pública clasificada o datos personales no públicos en sus medios de almacenamiento.
q. Capacitar a los usuarios internos responsables de computadores portátiles para que tengan los cuidados requeridos para el uso apropiado del equipo.

3. Los funcionarios y terceros de la entidad deben:

a. Utilizar los equipos de manera exclusiva bajo la completa responsabilidad, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.
b. No dejar descuidados ni desatendidos los equipos de cómputo o elementos que estén bajo su custodia.
c. Usar la guaya asignada para el uso de portátiles durante su uso, y si no se utilizan, resguardarlos bajo llave si no tienen guaya.
d. Bloquear la sesión al retirarse de su puesto de trabajo.
e. Apagar el equipo de cómputo y mantenerlo apagado en caso de que no se encuentre en la oficina por largos periodos o durante la noche, con excepción de la realización de actividades vía remota o la ejecución de procesos propios de las funciones asignadas.
f. Evitar realizar actividades o maniobras que pongan en riesgo los equipos de cómputo, impresoras y demás equipos electrónicos y la información que contienen, (consumir alimentos, bebidas o fumar, entre otros).
g. No realizar cambios directamente en los datos o por personas no autorizadas en los equipos de trabajo.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de Información de Identificación Personal
2. 6.8 – Informes de eventos de seguridad de la información

5.3.9 Seguridad de los activos fuera de las instalaciones

A. Objetivo de control: Aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad con el fin de mitigar la afectación a la confidencialidad, integridad y disponibilidad de los activos de información que sean retirados de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, y la Subdirección Administrativa, dependencias encargadas de gestionar la seguridad de los equipos fuera de las instalaciones de la **DIAN** o sus seccionales. así como la Oficina de Seguridad de la Información encargada de divulgar y sensibilizar del cuidado y resguardo de elementos de cómputo fuera de la entidad.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

    a. Notificar al jefe inmediato sobre la salida de los elementos de cómputo de las instalaciones de la **DIAN**.
    b. Registrar cualquier activo de información que sea retirado de las instalaciones de la **DIAN**, en el formato de salida temporal de bienes. En este se debe indicar las características y estado del activo, el nombre del funcionario responsable y el tiempo en el cual el activo será reintegrado.
    c. Aplicar medidas de seguridad adecuadas que minimicen los riesgos identificados en los entornos físicos que frecuentan los equipos y activos de información (entidades de orden local), comisión nacional (trabajo en campo), trabajo en la residencia del servidor público, entre otros), una vez están fuera de las instalaciones de la **DIAN**.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Implementar mecanismos de seguridad y protección requeridos (maletín, guaya, cargador, espumas, empaque, soportes, candado, entre otros.) en los equipos portátiles, tabletas, discos duros e implementos de comunicaciones (cámaras fotográficas, de video, etc.) previo a su retiro de las instalaciones.
    b. Deshabilitar los puertos de los equipos que cuenten con puertos de transmisión y recepción de infrarrojo y Bluetooth.
    c. Implementar controles de seguridad para fortalecer la confidencialidad de la información en los equipos portátiles que contengan información reservada, clasificada o datos personales no públicos.

d. Alinear los mecanismos de protección con las instrucciones dadas por los fabricantes de los equipos, de forma que la seguridad de estos equipos y activos fuera de las instalaciones sea la óptima.

3. La Oficina de Seguridad de la Información debe:

   a. Capacitar a los funcionarios y terceros (si aplica) sobre el cuidado de los activos de información que son retirados de las instalaciones de la **DIAN**, de forma que por ningún motivo estén desatendidos en sitios públicos, en su lugar de permanencia, y durante su traslado. Adicionalmente, deben estar resguardados con una guaya.
   b. Capacitar a los funcionarios sobre la importancia de resguardar los equipos portátiles, de forma que no estén a la vista en el interior de los vehículos y en caso de viaje, llevarlos como equipaje de mano.
   c. Verificar que los principios y lineamientos establecidos en este numeral, para la seguridad de equipos y activos, fuera de las instalaciones de la **DIAN**, se encuentren en procedimientos formales del Sistema de Gestión de Calidad.

4. Los funcionarios y terceros de la entidad deben:

   a. Informar inmediatamente a la Subdirección de Soluciones y Desarrollo, en caso de pérdida o robo de un computador portátil, adicionalmente se debe interponer la denuncia respectiva ante las autoridades competentes y hacer llegar copia de esta.
   b. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en la seguridad de equipos y activos fuera de las instalaciones de la **DIAN**.

E. Controles relacionados:

1. 5.14 – Transferencia de información
2. 6.7 – Trabajo remoto
3. 6.8 – Informes de eventos de seguridad de la información
4. 7.4 – Monitoreo de seguridad física
5. 7.5 – Protección contra amenazas físicas y ambientales
6. 8.1 – Dispositivos de punto final de usuario

5.3.10 Medios de almacenamiento

A. Objetivo de control: Establecer los procedimientos para la gestión de medios removibles para evitar posibles riesgos y fugas de la información y, con ello, proteger la información de usos no autorizados, robo, pérdida, uso indebido o corrupción de información en el proceso de transporte o transferencia de medios físicos.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo y la Subdirección Administrativa, dependencias encargadas de gestionar la seguridad de los equipos y dispositivos que funcionan como medios de almacenamiento de información en las instalaciones de la **DIAN** y sus seccionales. También aplica para la Oficina de Seguridad de la Información, encargada de divulgar y sensibilizar sobre el buen uso de los medios removibles y proveer el material necesario sobre el cifrado de la información.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Establecer procedimientos formales para la disposición segura de medios y minimizar el riesgo de fugas de información y datos personales sensibles.
   b. Disponer de un mecanismo de eliminación o residuos de aparatos electrónicos y debe dar cumplimiento a lo establecido en la política nacional de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos (RAEE). En el caso de la información almacenada en discos duros, debe hacerse eliminación de la información de forma segura con el fin de confirmar la pérdida de información. Cuando a un Disco Duro por su obsolescencia o con daños irreparables y sea imposible hacerle el borrado seguro, se debe certificar que la información no sea recuperable.
   c. Restringir la venta de documentos que hayan sido destruidos para reciclaje.
   d. Controlar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual).
   e. Realizar los registros de entradas y salidas de medios de almacenamiento en los casos de requerir transportes seguros. Estos registros deben considerar el detalle de los responsables durante el transporte la entrega, origen y destino del equipo o medio de almacenamiento, adicional, la protección aplicada, y las condiciones físicas que conserven la integridad, confidencialidad y disponibilidad de la información. Es obligatorio contar con la autorización formal para el retiro de equipos de cómputo, información o software de las instalaciones de la entidad.
   f. Revisar periódicamente los registros de retiro de activos para detectar los no autorizados y determinar cuáles de estos corresponden a medios de almacenamiento.
   g. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por inconvenientes en el retiro de equipos.

2. La Subdirección de Soluciones y Desarrollo debe:

   a. Implementar para cada requerimiento de uso de medios de almacenamiento, la documentación emitida en la entidad: procedimiento “PR-IIT-0460 Gestión de requerimientos”, formatos: “FT-IIT- 5264 Aceptación y autorización de uso de medios removibles”, “FT-IIT-2529 Registro de medios removibles entregados a terceros”.
   b. Restringir el uso y conexión de medios removibles como dispositivos de almacenamiento (celulares, memorias USB, discos duros externos, cintas, memorias flash, y otros medios de almacenamiento.) Sobre cualquier medio tecnológico de la entidad, salvo en casos en que los funcionarios, por su trabajo, requieran usar medios removibles.
   c. Implementar los controles requeridos para que los medios removibles sean utilizados solo por quienes están autorizados y para fines específicos.
   d. Restringir la ejecución de programas, software, o elementos que provengan de medios removibles; las personas autorizadas para la ejecución de programas en los equipos de la entidad son los funcionarios de la Dirección de Gestión de Innovación y Tecnología con esa responsabilidad o quien haga sus veces (Tanto en el nivel central como en las Direcciones Seccionales).

e. Cifrar la información que deba ser entregada a través medios removibles.
f. Restringir el uso de medios removibles para el manejo de información pública clasificada o publica reservada y que pueda afectar la protección de datos personales e información confidencial de la entidad. En caso de ser requerido, debe solicitarse la aprobación por parte del Oficial de Protección de Datos Personales para el manejo de este tipo de información y a su vez, utilizar técnicas de cifrado.
g. Llevar un registro de la eliminación de información en formato lógico o físico que se encuentre almacenada en medios removibles. Se debe incluir el motivo de la eliminación y el resultado de esta. Cuando se deba hacer la eliminación total de información, se debe contar con la aprobación del jefe inmediato; se debe hacer una copia de la información antes de eliminarla.
h. Monitorear la herramienta de antivirus implementada en la entidad, para confirmar que realiza un análisis de medios removibles detectando y evitando accesos de virus o malware en la plataforma de la entidad.
i. Confirmar la eliminación de la información de todo dispositivo antes de que sea asignado a otro funcionario.
j. Realizar un proceso de desmagnetización y sobreescritura segura (o similares), antes de hacerla eliminación física, para los casos de Discos Duros.
k. Utilizar para la destrucción de medios de almacenamiento algunos de los siguientes métodos si son físicos: desintegración, pulverización, fundición, incineración o trituración (o similares). En el caso de un medio óptico de almacenamiento, se debe realizar la pulverización, trituración de corte transversal o incineración.
l. Llevar un registro de la eliminación física, el motivo y el resultado de esta.

3. La Oficina de Seguridad de la Información debe:

a. Capacitar a los funcionarios y terceros de la **DIAN** en relación con el uso de medios removibles, conforme con las políticas, procedimientos y los demás documentos que se tengan contemplados por la entidad.
b. Proveer los manuales, software o herramientas para el cifrado de información en cualquier dependencia que lo requiera.

E. Controles relacionados:

1. 5.14 – Transferencia de información
2. 6.8 – Informes de eventos de seguridad de la información
3. 7.14 – Eliminación segura o reutilización de equipos
4. 8.10 – Eliminación de información

5.3.11 Utilidades de apoyo

A. Objetivo de control: Proteger los equipos de cómputo y procesamiento contra fallas de energía u otras interrupciones causadas por fallas en los servicios de suministro.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa, esta dependencia será la encargada de gestionar los recursos físicos y servicios públicos en las instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo y detectivo.

2. Propiedades de seguridad: integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Establecer los lineamientos para el uso de la red de energía regulada en los puestos de trabajo, en los cuales solo se deben conectar equipos como computadores de escritorio, computadores portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.
   b. Implementar mecanismos para regular el flujo de energía que permitan proteger a los equipos de cómputo y procesamiento de daños por interrupciones causadas por fallas en el soporte de los servicios públicos.
   c. Suministrar plantas eléctricas a las sedes de la **DIAN** y confirmar su mantenimiento preventivo y correctivo de forma periódica.
   d. Establecer los procedimientos, mecanismos o controles necesarios en sus procedimientos para la correcta prestación de los servicios de suministro en la **DIAN** y que se encuentren en el Sistema de Gestión de calidad.
   e. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por inconvenientes en la prestación de los servicios de suministro.
   f. Suministrar mecanismos de alarmas para detectar fallas en los servicios públicos.
   g. Proporcionar iluminación de emergencia y comunicaciones. Los interruptores y válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios públicos deben ubicarse cerca de las salidas de emergencia o las salas de equipos.
   h. Almacenar de manera segura el detalle de los contactos de emergencia, los cuales deben registrarse y estar disponibles para el personal en caso de un apagón. Así mismo, verificar que esta información no contenga datos personales más allá del nombre y número de teléfono del contacto.
   i. Inspeccionar periódicamente el correcto funcionamiento de los servicios públicos.
   j. Verificar que las empresas de servicios públicos tengan múltiples alimentaciones con diversas rutas físicas.
   k. Confirmar que el equipo de apoyo a los servicios públicos esté en una red separada de las instalaciones de procesamiento de información.
   l. Confirmar con el proveedor de servicio público el correcto funcionamiento de los equipos y que estos se encuentren operando correctamente, así como que estos cuenten con el mantenimiento de acuerdo con las especificaciones del fabricante.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información

5.3.12 Seguridad del cableado

A. Objetivo de control: Proteger el cableado de energía eléctrica y de telecomunicaciones contra interceptación, interferencia o daño.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección Administrativa y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de administrar y proteger el cableado de las instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

   a. Establecer los procedimientos, mecanismos o controles necesarios para la seguridad del cableado de la **DIAN**.
   b. Verificar que los principios y lineamientos establecidos para la seguridad del cableado, se encuentren en procedimientos formales del Sistema de Gestión de Calidad y se apliquen efectivamente.
   c. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en la seguridad del cableado.
   d. Mantener en buen estado la infraestructura física de los centros de cableado a nivel nacional (seccionales) y centro de datos de las sedes del nivel central, tales como puertas, cerraduras, paredes pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
   e. Realizar revisiones periódicas para confirmar el estado de los centros de cableado e informar cualquier novedad presentada a la Subdirección de Infraestructura Tecnológica y de Operaciones. Para los daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) deben ser gestionados directamente desde esta subdirección.
   f. Mantener organizado e identificado el cableado en los racks de los centros de cableado y centro de datos, al igual que del cableado estructurado, desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado a nivel nacional.
   g. Verificar que el cableado que transporta datos y de suministro de energía estén protegidos contra la interceptación, interferencia o daños.
   h. Separar los cables de comunicaciones y cables de energía eléctrica para evitar interferencia.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Administrar el ingreso y salida del personal a los centros de cableado y centros de datos de las seccionales.
   b. Autorizar y acompañar el ingreso y traslado de personal ajeno a la **DIAN** a los centros de cableado, responsabilizándose de las actividades realizadas durante la estadía de estas personas en el tiempo que permanezcan en las instalaciones.
   c. Controlar que los centros de cableado permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.
   d. Acompañar y evaluar el cumplimiento del protocolo de aseo en los centros de cableado y centro de datos, cuando se realice la actividad se debe contar con el acompañamiento de uno de los funcionarios de Subdirección de Infraestructura Tecnológica y de Operaciones.
   e. Establecer un plan de mantenimiento para los centros de cableado de tal manera que se corrijan fallas y/o se establezcan mejoras en estos.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 7.2 – Entrada física
3. 7.3 – Asegurar oficinas, salas e instalaciones
4. 7.4 – Supervisión de la seguridad física.
5. 7.5 – Protección contra amenazas físicas y ambientales
6. 7.6 – Trabajar en áreas seguras

5.3.13 Mantenimiento de equipos

A. Objetivo de control: Gestionar el correcto mantenimiento y funcionamiento de los equipos de la entidad para proteger su disponibilidad e integridad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, dependencia encargada de gestionar el mantenimiento de equipos y recursos de cómputo en las instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

    a. Autorizar el acceso a las instalaciones de procesamiento de la información o a la información de la **DIAN** y acompañar a un contratista o tercero, durante las actividades de mantenimiento a la infraestructura tecnológica.
    b. Llevar a cabo una evaluación de riesgos, la cual permita identificar los controles de seguridad requeridos para proteger la información conforme a la actividad que va a desarrollar el contratista o tercero.
    c. Determinar las instalaciones de procesamiento de información o la información de la **DIAN** a la cual el contratista o tercero necesita tener acceso, teniendo en cuenta los niveles de criticidad e importancia para las operaciones de la entidad.
    d. Identificar el tipo de acceso a la información que tendrá el contratista o tercero que realiza mantenimiento de equipos tecnológicos (computadores, switches, impresoras) y el acceso que tiene a las instalaciones de procesamiento de información e informar los riesgos de seguridad involucrados en:
        - Acceso físico.
        - Acceso lógico.
        - Conectividad a la red: Implica acceso, por medio de equipos conmutadores de red; por ejemplo, conexión permanente local, acceso remoto por canal dedicado, acceso por VPN en teletrabajo, etc.
    e. Identificar el personal del contratista o tercero involucrado en el manejo de la información de la **DIAN**.
    f. Conocer los diferentes medios y controles empleados por el contratista o tercero cuando almacena, procesa, comunica, comparte o intercambia información.

g. Disponer de una red destinada al uso del personal contratista o tercero de manera que se pueda controlar y monitorear el acceso a otras redes donde se maneja información confidencial para la **DIAN**.
h. Estipular en el contrato los requerimientos legales y reguladores y otras obligaciones contractuales asociadas a seguridad y privacidad de la información, para llevar cabo la labor del contratista o tercero.
i. Establecer los mecanismos de soporte y mantenimiento a los equipos.
j. Registrar todas las actividades de mantenimiento tanto preventivo como correctivo.
k. Programar con la debida anticipación las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio.
l. Programar con la debida anticipación las actividades de mantenimiento de los equipos de cómputo de la entidad.
m. Autorizar todos los equipos que requieran salir de las instalaciones de la **DIAN** para reparación o mantenimiento.
n. Reportar a la Oficina de Seguridad de la Información todos los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por inconvenientes en el mantenimiento de equipos.
o. Mantener el equipo de acuerdo con las especificaciones de servicio recomendadas por el proveedor.
p. Supervisar al personal que realice de mantenimiento de equipos cuando se encuentre en las instalaciones de la **DIAN**.
q. Autorizar y controlar el acceso para el mantenimiento remoto.
r. En caso de que el equipo que contiene información se retire de las instalaciones para su mantenimiento, aplicar medidas de seguridad para activos fuera de las instalaciones
s. Si se determina que el equipo debe desecharse, aplicar medidas para la eliminación segura o la reutilización de equipos.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 7.9 – Seguridad de los activos fuera de las instalaciones
3. 7.14 – Eliminación segura o reutilización de equipos

5.3.14 Eliminación segura o reutilización de equipos

A. Objetivo de control: Verificar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura, antes de su eliminación, disposición o reúso del equipo.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, dependencia encargada de gestionar la disposición final o el reúso de equipos y recursos de cómputo en las instalaciones de la **DIAN** y sus seccionales.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Realizar una copia de respaldo, y someter a procedimientos de borrado seguro de información y software instalado a los equipos de cómputo que vayan a ser reasignados o dados de baja, con el fin de evitar la pérdida de información o recuperación no autorizada de esta.
b. Utilizar las técnicas adecuadas para el borrado o sobre escritura segura de acuerdo con la tecnología del medio de almacenamiento.
c. Verificar que los principios y lineamientos establecidos en este literal, para la disposición segura o reutilización de equipos, se encuentren en procedimientos formales del Sistema de Gestión de Calidad y se apliquen efectivamente.
d. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en los procesos de disposición segura o reutilización de equipos.
e. Aplicar los anteriores lineamientos de seguridad a los medios de almacenamiento que contienen información antes de su eliminación o reutilización.

2. La Subdirección Administrativa debe:

a. Otorgar elementos para la destrucción de información física en las dependencias que procesen altos volúmenes de información de carácter público clasificado (incluyendo datos personales) e información pública reservada.
b. Establecer a través de Gestión Documental un procedimiento para la eliminación adecuada de información física.

1. Los funcionarios y terceros de la entidad deben:

a. Destruir los documentos físicos antes de arrojarlos a basura, en caso tal que se vayan a reutilizar, se deben tachar los datos allí presentes.
b. Impedir la reutilización de información física cuando esta contenga información de carácter público clasificado (incluyendo datos personales) e información pública reservada.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 7.10 – Medios de almacenamiento
3. 8.10 – Eliminación de información
4. 8.24 – Uso de criptografía

5.4 Controles tecnológicos

A continuación, se describen los lineamientos y políticas que hacen referencia a las responsabilidades que establece la **DIAN** para la seguridad en los recursos tecnológicos:

5.4.1 Dispositivos de punto final de usuario

A. Objetivo de control: Definir los parámetros y medidas de seguridad que deben implementar los funcionarios y terceros de la entidad para proteger los dispositivos de punto final de usuario y la información procesada y almacenada en estos, de tal manera que estén resguardados de pérdida, daño, acceso o divulgación no autorizada.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, la Subdirección Administrativa y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar la seguridad y protección de seguridad para los equipos de punto final de usuario en las instalaciones de la **DIAN**, sus seccionales y equipos personales que manejen información de la entidad.

C. Características del control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección Administrativa debe:

    a. Realizar la autorización, entrega y control del uso de dispositivos móviles, de acuerdo con el perfil del cargo, funciones, y necesidades específicas de cada dependencia, según la autorización definida por la Dirección de Gestión de Innovación y Tecnología.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Definir un control de cifrado para los dispositivos de punto final de usuario.
    b. Establecer lineamientos de ingreso y salida de las instalaciones de los dispositivos de punto final.
    c. Establecer lineamientos para la adecuada custodia, conservación, operación y mantenimiento de los dispositivos de punto final de usuario o que manejen información de la entidad en dispositivos personales.
    d. Definir controles lógicos para el acceso a diferentes aplicaciones y/o sistemas de la entidad a través de dispositivos de punto final de usuario.
    e. Revisar los requisitos de seguridad de los medios removibles que se utilicen para acceder a la información desde redes externas.
    f. Definir medidas de seguridad en cuanto software y antivirus de los dispositivos móviles utilizados para manejo de información, labores contractuales y funciones de la entidad, así como doble factor de autenticación.
    g. Establecer los lineamientos para conexiones de visitantes y usuarios internos que ingresen a la entidad dispositivos propios.
    h. Bloquear el acceso de los dispositivos de punto final de usuario en propiedad de terceros, contratistas y/o usuarios externos a el dominio de la **DIAN**: “dian.gov.co”; para conectarse a los servicios de la red de datos se debe realizar una solicitud a la mesa de ayuda y cumplir con los lineamientos referentes definidos por esta.
    i. Monitorear los dispositivos móviles institucionales y personales, que gestionen cualquier activo de información a través de las herramientas de gestión tecnológica definidas por la entidad.
    j. Realizar verificación de los dispositivos de punto final de usuario cuando se requiera de forma remota, sin que para ello se necesite la autorización de la persona a la que se le haya asignado y generar el reporte respectivo.
    k. Entregar elementos de seguridad -tipo guaya- para los dispositivos de punto final de usuario cuando sea necesario.

l. Brindar soporte a los usuarios internos responsables de los dispositivos de punto final únicamente en las instalaciones de la entidad, sobre los aplicativos y sistemas instalados en los equipos suministrados.
m. Registrar todos los casos de soporte de los dispositivos de punto final de usuario en la herramienta de gestión de mesa de ayuda.
n. Brindar el soporte a los equipos en modalidad de Teletrabajo y de acuerdo con lo establecido en la Circular 000496 de 9 mayo de 2022 o la que la sustituya.
o. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de los dispositivos de punto final.
p. Configurar en todos los computadores de la **DIAN** un protector de pantalla con tiempo máximo de cinco minutos para que se active cuando el equipo no esté en uso.

3. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Aplicar los procedimientos establecidos para la conservación de la información (copias de respaldo), formateo y reinstalación de las aplicaciones o servicios requeridos por el nuevo responsable del equipo.

4. Los funcionarios y terceros de la entidad deben:

a. Solicitar la autorización a la Subdirección de Soluciones y Desarrollo para el uso de aplicaciones dentro de los dispositivos de punto final de usuario que sean de su propiedad (computador portátil, celular Smartphone, Tablet y similares).
b. Permitir que se habiliten las funcionalidades de auditoría y control de la información almacenada en los dispositivos de punto asignados.
c. Tomar medidas y precauciones necesarias para la adecuada custodia, conservación, operación y mantenimiento de los dispositivos de punto final de usuario o que manejen información de la entidad en dispositivos personales; además, cumplir las disposiciones administrativas y técnicas aplicables definidas por la Oficina de Seguridad de la Información y la Dirección de Gestión de Innovación y Tecnología.
d. Responder por el cuidado, manipulación y seguridad en todo momento de los dispositivos de punto final de usuario que, por necesidades del servicio, requieran ser transportados fuera de las instalaciones de la entidad.
e. Dar cumplimientos a los lineamientos de ingreso y salida de los dispositivos de punto final estipulados por la Dirección de Gestión de Innovación y Tecnología.
f. Hacerse responsables de las llaves asignadas (llaves de guayas, llaves de cajones y similares) para el almacenamiento y cuidado de los dispositivos de punto final que se les asigne.
g. Utilizar las herramientas de cifrado cuando se requiere para el cuidado apropiado de la información pública clasificada y publica reservada que tenga a cargo.
h. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de los dispositivos de punto final asignados.
i. Bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, con el fin de impedir el acceso de terceros no autorizados a la información almacenada en el computador.
j. Evitar tener sobre el escritorio información propia de la entidad en medios de almacenamiento, en su lugar, se debe guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.

k. Evitar que, durante el uso de impresoras en la **DIAN**, se descuiden documentos con información clasificada y/o reservada que haya sido impresa.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 8.9 - Gestión de la configuración
3. 8.16 - Actividades de seguimiento

5.4.2 Derechos de acceso privilegiado

A. Objetivo de control: Restringir y controlar los accesos privilegiados, para la asignación y uso de derechos de acceso a los diferentes programas, servicios, aplicativos, bases de datos y cualquier acceso a actividades específicas de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar el aprovisionamiento de usuarios privilegiados y de administración en los sistemas e infraestructura de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Definir, aprobar y socializar un procedimiento de solicitud y autorización de derechos de acceso privilegiado de acuerdo con la política de control de acceso específica que maneja la entidad.
b. Autorizar, otorgar y confirmar que los privilegios para la administración de los sistemas de información sean asignados solamente a los funcionarios que tengan las competencias requeridas para cumplir sus funciones.
c. Mantener un listado actualizado de los funcionarios con accesos privilegiados y de administración en cada uno de los sistemas de información.
d. Establecer los controles para que los usuarios de los recursos tecnológicos, los servicios de red y los sistemas de información no puedan instalar programas o aplicar configuraciones críticas en sus equipos de cómputo utilitarios, que permitan escalar privilegios o evadir controles de seguridad informáticos.
e. Aprobar, actualizar y socializar con los grupos internos de trabajo de tecnología, el listado de programas utilitarios de uso autorizado para la operación de la plataforma tecnológica, los servicios de red y sistemas de información. Adicionalmente, se deben retirar o deshabilitar los programas utilitarios privilegiados no autorizados.
f. Restringir las conexiones remotas a los recursos de la plataforma tecnológica, permitiendo únicamente el acceso a los funcionarios autorizados.
g. Monitorear y deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, firmware y bases de datos, cuando los funcionarios hayan sido retirados de

sus funciones o se encuentren en una situación administrativa que los separe temporalmente de sus funciones; por ejemplo, en periodos de vacaciones.

h. Configurar, para el correcto uso, las carpetas de uso interno de la entidad preservando la integridad, confidencialidad y disponibilidad de la información.
i. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en los procesos de aprovisionamiento de usuarios privilegiados.

2. La Subdirección de Infraestructura tecnológica y de operaciones debe:

a. Mantener un listado actualizado de los funcionarios con accesos privilegiados y de administración en cada uno de los servidores, sistemas operativos, bases de datos y directorio activo de la entidad.
b. Aprovisionar los debidos accesos a los diferentes sistemas operativos y conexiones de bases de datos evitando el uso indebido de utilitarios que puedan afectar la seguridad los sistemas de información alojados sobre la plataforma tecnológica.
c. Restringir los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, permitiendo el acceso únicamente a los administradores de red.
d. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en los procesos de aprovisionamiento de usuarios privilegiados.

3. Los funcionarios y terceros de la entidad deben:

a. Permitir tomar el control remoto de sus equipos a la mesa de ayuda, para esto debe evitar tener archivos con información sensible a la vista y debe permanecer atento al equipo mientras el tercero tiene control sobre este.
b. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en los procesos de aprovisionamiento de usuarios privilegiados.

E. Controles relacionados:

1. 5.15 – Control de acceso.
2. 5.17 – Información de autenticación.
3. 5.18 – Derechos de acceso.
4. 6.8 – Informes de eventos de seguridad de la información.

5.4.3 Restricción de acceso a la información

A. Objetivo de control: Restringir el acceso a la información, sistemas de información y aplicaciones únicamente a personal autorizado, de acuerdo con la política de control de acceso establecida en este manual.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, dependencia encargada de gestionar los accesos a la información en los equipos de cómputo de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

   a. Segmentar, a través de roles, los privilegios de los usuarios dentro del sistema de información.
   b. Confirmar que se aplican los lineamientos de seguridad para el control de acceso a información electrónica teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.
   c. Prohibir el acceso a información sensible por parte de usuarios con identidades desconocidas.
   d. Proporcionar mecanismos para controlar el acceso a la información.
   e. Controlar a qué datos puede acceder un usuario de los sistemas de información.
   f. Controlar qué identidades o grupo de identidades tienen acceso a los sistemas de información.
   g. Establecer controles de acceso lógicos a los sistemas de información.

2. La Subdirección Administrativa debe:

   a. Restringir el acceso a información física teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

3. La Subdirección de Infraestructura tecnológica y de operaciones debe:

   a. Identificar, según los niveles de clasificación de información, cuáles sistemas son considerados sensibles y gestionar ambientes tecnológicos aislados e independientes.
   b. Aislar los sistemas de información clasificados como sensibles de otras fuentes de datos, con el objetivo de proteger la información desde los ambientes lógicos.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información

5.4.4 Acceso al código fuente

A. Objetivo de control: Restringir el acceso al código fuente de los sistemas de información, aplicaciones y software de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones y la Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar la seguridad del código fuente de los sistemas y aplicaciones de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura tecnológica y de operaciones debe:

   a. Autorizar, registrar y monitorear periódicamente todos los accesos al código fuente de los programas y sistemas de información de la entidad aplicando los principios de conservación de la información; el código fuente debe estar protegido mediante contraseñas con un alto nivel de cifrado.
   b. Restringir el acceso a los elementos asociados como diseños, especificaciones, planes de verificación y de validación, únicamente a personal autorizado y bajo supervisión de actividades.
   c. Ubicar en un equipo fuera de la red de la entidad y de accesos a internet, el código que se encuentre libre para pruebas específicas antes de ser enviado a producción.
   d. Inhabilitar puertos de USB, Bluetooth, RF (Radio Frecuencia) de los equipos utilizados para este tipo de pruebas, salvo que el jefe de la Oficina de Seguridad de la Información los autorice.
   e. Restringir el acceso directo al repositorio del código fuente a los desarrolladores, solo permitir el acceso a través de herramientas a los desarrolladores para el debido control de actividades y autorizaciones.
   f. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren acceso indebido al código fuente.

2. La Subdirección de Soluciones y Desarrollo debe:

   a. Utilizar el código que se encuentre libre de vulnerabilidades antes de ser enviado a producción.
   b. Restringir la actualización del código fuente, componentes asociados y otorgar el acceso al código fuente, únicamente con los procedimientos de control de cambios.
   c. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren acceso indebido al código fuente.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 8.32 – Gestión del Cambio

5.4.5 Autenticación segura

A. Objetivo de control: Permitir el ingreso a sistemas de información y aplicaciones de la **DIAN** mediante un inicio seguro de sesión.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar las características de autenticación en programas, sistemas de información e infraestructura de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

   a. Restringir la visualización de información por el sistema hasta que el proceso de inicio se haya completado satisfactoriamente.
   b. Inhabilitar mensajes de ayuda durante el proceso de autenticación.
   c. Validar los datos de acceso una vez se han diligenciado todos los datos de entrada.
   d. Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
   e. Bloquear la visualización de contraseñas digitadas.
   f. Implementar mecanismos de protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas en programas y sistemas de información.
   g. Generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión.
   h. Finalizar las sesiones inactivas después de un período definido de inactividad.
   i. Restringir los tiempos de duración de la conexión.
   j. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en el proceso de autenticación.

2. La Subdirección de Infraestructura tecnológica y de operaciones debe:

   a. Restringir la visualización de información de las bases de datos, sistema operativo, configuraciones de autenticación y Directorio Activo, hasta que el proceso de inicio se haya completado satisfactoriamente.
   b. Inhabilitar mensajes de ayuda durante el proceso de autenticación en los sistemas de información.
   c. Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
   d. Bloquear la visualización de contraseñas digitadas.
   e. Implementar mecanismos de protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas en bases de datos, sistema operativo y directorio activo.
   f. Generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión.
   g. Finalizar sesiones inactivas después de un período definido de inactividad en los sistemas de información.
   h. Restringir los tiempos de duración de la conexión en los sistemas de información.
   i. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en el proceso de autenticación.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información

5.4.6 Gestión de capacidad

A. Objetivo de control: Gestionar la capacidad, tanto de recursos humanos como de oficinas e instalaciones, con el fin de evitar pérdidas de disponibilidad o rendimiento de los sistemas de información.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura tecnológica y de Operaciones, Subdirección Administrativa y Subdirección de Desarrollo del Talento Humano, dependencias encargadas de gestionar la disposición de recursos físicos, tecnológicos y humanos de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de Seguridad: integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

    a. Planear y gestionar la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la **DIAN**, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.
    b. Optimizar los servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad.
    c. Realizar actividades de monitoreo, revisión, proyección y soporte oportuno para el uso y desempeño aceptable de capacidad de la infraestructura tecnológica.
    d. Realizar un plan de gestión de la capacidad para sistemas críticos de la entidad. Este plan debe ser formalizado en el Sistema de Gestión de Calidad.
    e. Definir si es necesario el uso de capacidades de computación en la nube.
    f. Definir si es necesaria la reducción de demanda de nuevos recursos tecnológicos.

2. La Subdirección Administrativa debe:

    a. Planear y gestionar la capacidad de los recursos físicos de la **DIAN**, efectuando proyecciones de crecimiento con una periodicidad definida y confirmar si existe la necesidad de espacios o instalaciones para el desarrollo de las actividades de la entidad.
    b. Realizar actividades de monitoreo, revisión y soporte de la capacidad sobre la infraestructura física de la entidad.

3. La Subdirección de Desarrollo del Talento Humano debe:

    a. Planear y gestionar la capacidad de los recursos humano de la **DIAN**, como parte de las actividades de administración del programa de desempeño de la entidad.
    b. Definir la necesidad de nuevo personal para apoyar las actividades de la entidad.

E. Controles relacionados: No aplica.

5.4.7 Protección contra malware

A. Objetivo de control: Proteger los equipos de cómputo para reducir los riesgos de amenazas, peligros del entorno y accesos no autorizados.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura tecnológica y de Operaciones y la Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar la seguridad lógica de los recursos tecnológicos de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo, detectivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura tecnológica y de operaciones debe:

    a. disponer de herramientas como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo ocasionado por software malicioso y que respalden la seguridad digital contenida y administrada en la plataforma tecnológica de la **DIAN** y los servicios que se ejecutan en la misma.
    b. Confirmar que el software de antivirus, antimalware, antispyware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad, posea las últimas actualizaciones y parches de seguridad y la posibilidad de actualización periódica de las ultimas bases de datos de firmas del proveedor de servicios, para mitigar las vulnerabilidades de la plataforma tecnológica.
    c. Confirmar que toda 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.
    d. Restringir la posibilidad a usuarios internos y externos de realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware.
    e. Restringir los cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por la Dirección de Gestión de Innovación y Tecnología o quien haga sus veces.
    f. Implementar listas de bloqueo para prevenir o detectar ante sitios web maliciosos.
    g. Diseñar e implementar revisiones periódicas al software y el contenido de los sistemas de información que apoyan los procesos críticos de la entidad.
    h. Mantener ambientes aislados para realizar pruebas en aplicaciones o programas que pueden afectar a la entidad.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Verificar que, en los casos en que los usuarios internos deban utilizar equipos que no pertenezcan a la entidad, cumplan con la legalidad del software instalado, antivirus licenciado y actualizado. Que solo puedan conectarse a la red una vez hayan obtenido en aval de la Dirección de Gestión de Innovación y Tecnología.
    b. Mantener actualizada una lista del software autorizado dentro de la **DIAN**.

c. Validar con la Oficina de Seguridad de la Información si el software solicitado para instalación está o no autorizado.

3. La Oficina de Seguridad de la Información debe:

   a. Concientizar de manera periódica a los servidores públicos, colaboradores y terceros de la **DIAN** sobre las falsas alarmas que se pueden generar, y las acciones a tomar en caso de que se presenten.
   b. Implementar y documentar lineamientos para verificar la información relacionada con el software malicioso y emitir comunicados informativos y de advertencia.
   c. Tomar acciones pertinentes para contener los incidentes asociados a software malicioso en caso de que se presenten, con el fin de evitar impactos catastróficos.

4. Los funcionarios y terceros de la entidad deben:

   a. Emplear los equipos y recursos de cómputo de manera exclusiva y bajo la completa responsabilidad del usuario interno al cual fueron asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no podrán ser utilizados con fines personales o por terceros no autorizados.
   b. Evitar la manipulación directa o por personas no autorizadas de los equipos a su cargo, y en caso necesario se deberá acudir a la Subdirección de Soluciones y Desarrollo a través de la mesa de ayuda para solicitar instalación de software en los equipos de la **DIAN**.
   c. Evitar cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware y antispam definida por la Subdirección de Soluciones y Desarrollo.
   d. Realizar tareas de escaneo de virus en diferentes medios previamente a su uso.
   e. Abstener el uso del equipo de cómputo cuando se detecte o sospeche que el equipo se encuentra contaminado por software malicioso, virus o por una falla física.
   f. Evitar descargar archivos de internet de fuentes desconocidas, abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
   g. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas en el equipo por motivos de rendimiento, errores y mensajes de alertas o por sospecha de algún daño o ataque por software malicioso.

E. Controles relacionados:

1. 6.3 – Concientización, educación y capacitación en seguridad de la información
2. 6.8 – Informes de eventos de seguridad de la información
3. 8.8 – Gestión de vulnerabilidades técnicas
4. 8.13 – Copia de seguridad de la información
5. 8.19 – Instalación de software en sistemas operativos
6. 8.32 – Gestión del cambio

5.4.8 Gestión de vulnerabilidades técnicas

A. Objetivo de control: Obtener oportunamente la información relacionada con las vulnerabilidades técnicas de los sistemas de información utilizados en la entidad, evaluar la

exposición a estas vulnerabilidades y tomar las medidas requeridas para tratar los riesgos que se pueden asociar.

B. Alcance: El alcance de esta política aplica para la Oficina de Seguridad de la Información, la Subdirección de Infraestructura Tecnológica y de Operaciones y la Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar pruebas de análisis de vulnerabilidades y aplicar de las correspondientes remediaciones en los sistemas e infraestructura tecnológica de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Realizar como mínimo una vez al año, según los recursos que le sean asignados, pruebas de vulnerabilidades sobre una muestra de los sistemas de la **DIAN**, las cuales serán programados en el cronograma anual.
    b. Definir indicadores para el monitoreo y toma de decisiones frente a las vulnerabilidades técnicas que se puedan presentar en la entidad.
    c. Mantener actualizados los inventarios de los sistemas de la **DIAN** a los cuales se le han hecho análisis de vulnerabilidades.
    d. Presentar a la Subdirección de Infraestructura tecnológica y de Operaciones y a la Subdirección de Soluciones y Desarrollo, los resultados obtenidos en las pruebas de vulnerabilidad para generar el cronograma de actividades necesarias para la implementación y/o remediación de las vulnerabilidades detectadas.
    e. Diseñar y aprobar controles mitigatorios, valorar el riesgo residual y hacer seguimiento al plan de acción de la dependencia dueña del activo de información, para los casos donde no se puedan realizar las remediaciones necesarias.
    f. Instar a los proveedores de sistemas de información, las evidencias de los análisis de vulnerabilidades sobre su sistema e infraestructura.

2. La Subdirección de Infraestructura tecnológica y de operaciones debe:

    a. Cumplir con las políticas y normas de seguridad de la información definidos para la entidad en todos los sistemas de información que se utilicen en la **DIAN**.
    b. Tener y mantener las herramientas y/o contratos de soporte necesarios que permitan realizar las actualizaciones de las distintas plataformas.
    c. Generar el cronograma de actividades necesarias para la implementación y/o remediación de las vulnerabilidades detectadas y presentar a la Oficina de Seguridad de la Información, quien se encarga del seguimiento y re-test según los recursos que se tengan disponibles.
    d. Implementar los controles mitigatorios, que ha sido diseñados y aprobados por la Oficina de Seguridad de la Información, para los casos donde se puedan realizar las remediaciones necesarias.
    e. Mantener los servicios tecnológicos actualizados en las últimas versiones seguras presentadas por los proveedores de las aplicaciones y/o infraestructuras.

f. Realizar pruebas antes de aplicar las nuevas versiones de software, firmware o a las actualizaciones (parches), para prevenir que estas nuevas versiones afecten el correcto funcionamiento de las aplicaciones en producción
g. Aplicar las actualizaciones en la infraestructura sea por necesidades del servicio en la Dirección de Gestión de Innovación y Tecnología o por una alerta informada por la Oficina de Seguridad de la Información y/o los fabricantes.
h. Realizar análisis periódicos de seguridad en los sistemas de información con ayuda de herramientas automatizadas y generar informes técnicos para la verificación del cumplimiento con los estándares de implementación de la seguridad de la información.
i. Realizar revisiones técnicas con los procedimientos de análisis, diseño, desarrollo y mantenimiento de las aplicaciones.
j. Realizar revisiones técnicas y en caso de incumplimiento de algún control o lineamiento, se deben determinar las causas de este e implementar acciones de mejora.
k. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas asociadas a vulnerabilidades.

3. La Subdirección de Soluciones y Desarrollo debe:

a. Tener y mantener las herramientas y/o contratos de soporte necesarias que permitan realizar las actualizaciones de los desarrollos subcontratados.
b. Generar el cronograma de actividades necesarias para la implementación y/o remediación de las vulnerabilidades detectadas en los desarrollos de la entidad o en desarrollos subcontratados y presentar a la Oficina de Seguridad de la Información, quien se encarga del seguimiento y re-test según los recursos que se tengan disponibles.
c. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de desarrollos internos o subcontratados por fallas asociadas a vulnerabilidades.

E. Controles relacionados:

1. 5.9 – Inventario de información y otros activos asociados
2. 5.14 – Transferencia de información
3. 5.20 – Abordar la seguridad de la información en los acuerdos con los proveedores
4. 5.26 – Respuesta a incidentes de seguridad de la información
5. 6.8 – Informes de eventos de seguridad de la información
6. 8.8 – Gestión de vulnerabilidades técnicas
7. 8.28– Codificación segura
8. 8.32– Gestión del Cambio

5.4.9 Gestión de la configuración

A. Objetivo de control: Establecer, documentar, implementar, socializar, monitorear y revisar las configuraciones de seguridad, de hardware, software, servicios y redes para permitir que el h*ardware, el software,* los servicios y las redes funcionen correctamente con la configuración de seguridad requerida y que la configuración no se altere por cambios no autorizados o incorrectos.

B. Alcance: El alcance de esta política aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones y la Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar las configuraciones de hardware, software, servicios y redes de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

   a. Definir y establecer plantillas de configuraciones de seguridad para los equipos de cómputo de la entidad y para sistemas recién instalados, así como para sistemas operativos durante su vida útil.
   b. Definir e implementar roles, responsabilidades y procedimientos para permitir un control satisfactorio de todos los cambios de configuración de los equipos de cómputo. Para ello, se debe considerar:
      - Minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador.
      - Deshabilitar identidades innecesarias, no utilizadas o inseguras.
      - Deshabilitar o restringir funciones y servicios innecesarios.
   c. Integrar la gestión de la configuración con los procesos de gestión de activos y las herramientas asociadas.
   d. Proteger las plantillas de configuraciones de seguridad como información confidencial, por lo cual debe resguardarse contra el acceso no autorizado.
   e. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas asociadas a configuraciones de seguridad.
   f. Realizar las mediciones de los indicadores para la gestión de vulnerabilidades de acuerdo con los niveles de severidad.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Definir y establecer plantillas de configuraciones de seguridad para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para sistemas recién instalados, así como para sistemas operativos durante su vida útil.
   b. Definir e implementar roles, responsabilidades y procedimientos para permitir un control satisfactorio de todos los cambios de configuración en los sistemas e infraestructura. Para ello, se debe considerar:
      - Minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador.
      - Deshabilitar identidades innecesarias, no utilizadas o inseguras.
      - Deshabilitar o restringir funciones y servicios innecesarios.
   c. Establecer las configuraciones y requisitos de seguridad de la información pertinentes para los dispositivos de propiedad del proveedor, en los que se almacene o procese información de la **DIAN**.

d. Revisar y actualizar las plantillas de configuraciones de seguridad, de forma preventiva o cuando los proveedores de los equipos indiquen actualizaciones de seguridad recomendadas.
e. Implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes.
f. Monitorear periódicamente las configuraciones de hardware, software, servicios y redes para confirmar que su funcionamiento este alineado con lo definido por la entidad en sus respectivas plantillas.
g. Restringir la posibilidad de realizar configuraciones únicamente a personal autorizado de la Subdirección de Infraestructura Tecnológica y de Operaciones y aplicar la gestión de cambios para efectuar modificaciones en las configuraciones.
h. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por fallas asociadas a configuraciones de seguridad.
i. Realizar las mediciones de los indicadores para la gestión de vulnerabilidades de acuerdo con los niveles de severidad.

E. Controles relacionados:

1. 5.32 – Derechos de propiedad intelectual
2. 6.8 – Informes de eventos de seguridad de la información
3. 8.32 – Gestión del Cambio

5.4.10 Eliminación de información

A. Objetivo de control: Eliminar de forma segura la información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento cuando ya no sea necesaria, con el fin de evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, dependencia encargada de gestionar las necesidades tecnológicas de los sistemas de información en las instalaciones de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Eliminar información sobre sistemas, aplicaciones y servicios que no sea de valor para los procesos de la entidad.
b. Eliminar versiones obsoletas, copias y archivos temporales dondequiera que se encuentren.

c. Usar un software de eliminación seguro y aprobado por la entidad para eliminar información de forma permanente, confirmando que no se pueda recuperar mediante el uso de herramientas forenses o de recuperación especializadas.
d. Usar proveedores aprobados y certificados de servicios de eliminación segura.
e. Utilizar mecanismos de eliminación apropiados para el tipo de medio de almacenamiento que se va a eliminar (desmagnetización de unidades de disco duro y otros medios de almacenamiento magnético).
f. Eliminar la información confidencial cuando el equipo se devuelve a los proveedores, eliminando los almacenamientos auxiliares (por ejemplo, unidades de disco duro) y la memoria antes de que el equipo abandone las instalaciones de la **DIAN**.
g. Elegir el método adecuado cuando se requiera eliminar de forma segura la información confidencial en algunos dispositivos (por ejemplo: teléfonos inteligentes) mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo: "restaurar la configuración de fábrica").
h. Destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene.
i. Oficializar las actividades de borrado de información, que permitan analizar la causa de un evento de fuga de información.
j. Reportar a la Oficina de Seguridad de la Información los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a fuga de información o por fallas en los procesos de disposición segura o reutilización de equipos.
k. Conservar la información confidencial por el tiempo necesario para su resguardo, para reducir el riesgo de divulgación no deseada.
l. Verificar si el método de eliminación proporcionado por el proveedor de servicios en la nube es adecuado. En caso afirmativo, determinar si la entidad debe usar el método o solicitar al proveedor de servicios en la nube elimine la información.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 7.14 – Eliminación segura o reutilización de equipos

5.4.11 Enmascaramiento de datos

A. Objetivo de control: Limitar la exposición de datos confidenciales, incluida la privacidad y protección de la información de identificación personal para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales por medio del enmascaramiento de datos.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, dependencia encargada de emitir las políticas y lineamientos relacionadas con la seguridad y privacidad de la información y la Subdirección de Soluciones y Desarrollo, encargada de coordinar y adelantar procesos de especificaciones técnicas, desarrollo interno o con terceros, procesos de calidad, actualización, mantenimiento, corrección y mejora de los sistemas de información y servicios digitales de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Promover técnicas como seudonimización o anonimización para ocultar la verdadera identidad de los titulares y desconectar el vínculo entre titular y datos.
    b. Verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados. La anonimización de datos debe considerar todos los elementos de la información sensible para ser efectivos.
    c. Seleccionar alguna de las técnicas adicionales para efectuar el enmascaramiento de datos: cifrado, anular o eliminar algunos caracteres, sustitución de valores, reemplazos con su hash u ofuscación de datos.
    d. Diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario consultante.
    e. Implementar acuerdos o restricciones en el uso de los datos procesados.
    f. Prohibir que sean cotejados los datos procesados con otra información para identificar al principal titular de la información personal.
    g. Realizar un seguimiento del suministro y recepción de los datos tratados.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Ocultar la verdadera identidad de los titulares de datos personales en casos donde se sospeche de situaciones de riesgo para la protección de la información personal.
    b. Implementar las consultas o máscaras de datos definidas por la Oficina de Seguridad de la Información en las bases de datos y todo repositorio de datos personales o sensibles.
    c. Implementar para los datos reemplazados con su hash, una función que permite evitar ataques de enumeración.
    d. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a identificación de titularidad en información personal.
    e. Aplicar las técnicas definidas por la Oficina de Seguridad de la Información para enmascarar los datos.

3. Los funcionarios y terceros de la entidad deben:

    a. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a identificación de titularidad en información personal.

E. Controles relacionados:

1. 5.34 – Privacidad y protección de información de identificación personal
2. 6.8 – Informes de eventos de seguridad de la información

5.4.12 Prevención de fuga de datos

A. Objetivo de control: Detectar y prevenir la divulgación y extracción no autorizadas de información por parte de individuos, sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, dependencia encargada de emitir las políticas y lineamientos relacionadas con la seguridad y privacidad de la información de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Monitorear los canales para detectar posibles amenazas de fuga de datos que tiene la **DIAN**: correo electrónico, transferencias de archivos, dispositivos móviles personales (que utilicen herramientas de la **DIAN**) y dispositivos portátiles de almacenamiento.
    b. Poner en cuarentena los correos electrónicos que contengan información confidencial para evitar la posible fuga.
    c. Seleccionar una herramienta que permita identificar y monitorear información sensible en riesgo de divulgación no autorizada, detectar la divulgación de información confidencial.
    d. Bloquear las acciones de los usuarios o las transmisiones de la red que expongan información confidencial.
    e. Analizar las situaciones en las que se requiere restringir la capacidad de determinados usuarios para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización.
    f. Requerir las autorizaciones por parte de los propietarios de los datos, para casos donde se requiera su exportación.
    g. Definir y divulgar los términos y condiciones de uso para la toma de capturas de pantalla o fotografías de la pantalla.
    h. Monitorear el uso y el movimiento de datos y tomar medidas para evitar la fuga de datos: alertar a los usuarios sobre su comportamiento de riesgo y bloquear la transferencia de datos a dispositivos portátiles de almacenamiento externo de la **DIAN**.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Implementar la herramienta seleccionada por la Oficina de Seguridad de la información que permite identificar y monitorear información sensible en riesgo de divulgación no autorizada y detectar la divulgación de información confidencial por servicios, dispositivos y medios de almacenamiento fuera de la organización.
    b. Implementar el cifrado, el control de acceso y la protección física a los medios de almacenamiento que contienen copias de seguridad que involucran datos sensibles o personales.

3. Los funcionarios y terceros de la entidad deben:

    a. Leer y aplicar los términos y condiciones de uso para la toma de evidencias bajo capturas de pantalla o fotografías a las pantallas.

b. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a fuga de información personal.
c. Identificar y clasificar la información para protegerla contra fugas y extracción no autorizada.

E. Controles relacionados:

1. 5.12 – Clasificación de la información
2. 5.15 – Control de acceso
3. 5.34 – Privacidad y protección de información de identificación personal
4. 6.8 – Informes de eventos de seguridad de la información

5.4.13 Copia de seguridad de la información

A. Objetivo de control: Respaldar la información, software e imágenes de los sistemas de la **DIAN**, por medio de copias de seguridad, siguiendo los procedimientos establecidos por la entidad.

B. Alcance: El alcance de esta política aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencia encargada de gestionar las copias de respaldo de los sistemas e infraestructura de la **DIAN**.

C. Características de control:

1. Tipo de control: correctivo.
2. Propiedades de seguridad: integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Formular, aprobar y socializar un plan y/o estrategia (documentada en un procedimiento formalizado) de copias de seguridad para la infraestructura, que permita realizar recuperación inmediata cuando se presente un daño por infecciones del sistema con ransomware, virus y malware, fallos de hardware (cortes de corriente y picos de tensión, excesos de temperatura y daños en los dispositivos), apagados incorrectos del equipo, problemas motivados por algún programa, daños del usuario al borrar archivos por error, entre otros. Para ello debe considerar:
- El tipo de información, software o imágenes de los sistemas; se les debe realizar respaldo.
- Las estrategias de copias de respaldo como: copia de seguridad completa, copia de seguridad incremental, copia de seguridad diferencial.
- Garantizar el funcionamiento del esquema de respaldos y de custodia.
- Los períodos de retención y frecuencia de las copias de respaldo, que permitan la continuidad de las operaciones y la consulta histórica de su información, validado previamente con el dueño del activo de información.
- El hardware, software y factor humano que interviene en cada etapa, con sus responsables.
- El almacenamiento de los datos (dónde / ubicación).

- El funcionamiento del plan de recuperación de datos.
- La disposición y control de la ejecución de las copias, así como la prueba periódica de su restauración.
- El proceso de recuperación ante desastres.
- La protección de las copias de respaldo aplicando cifrado a la información respaldada, en línea con la identificación de riesgos previa sobre la información respaldada.

b. Contar con un (Servicio Informático Electrónico) de copias de respaldo (herramientas, robots, aplicativos). Estas herramientas o sistemas deben ser de fácil uso y con escalabilidad, y deben considerar copias para:
   - Los servidores de archivos (carpetas con información de las dependencias)
   - Servidores que manejan aplicaciones web y aplicaciones locales
   - Información almacenada en servidores
   - Aplicaciones de los servidores
   - Información de aplicaciones contenida en servidores
   - Bases de datos de los servidores
   - Controladores de dominio y de DHCP (Configuraciones de elementos de red)
   - *Switches & Routers*
   - Equipos y/o estaciones de trabajo, siempre que cada responsable de cada dependencia considere necesario previa coordinación entre las dependencias y la Dirección de Gestión de Innovación y Tecnología.
c. Definir los requisitos para el almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site) de las copias de respaldo, teniendo en cuenta el volumen, capacidad y período de retención, en línea con los requisitos de los procesos.
d. Disponer de una plataforma web que permita hacer informes de copia de seguridad para verificar que las copias de respaldo se hayan realizado de manera correcta y así confirmar que si le pasa algo a algunos datos (borrado, infección por virus, entre otros) se pueda recuperar la versión más reciente de los datos.
e. Ejecutar y documentar el proceso de pruebas a las copias de respaldo y restauración de archivos, al menos una vez al semestre. Así mismo, verificar los responsables de las labores de restauración conforme con lo establecido en el procedimiento.
f. Implementar al menos dos copias de la información, una de las cuales debe permanecer fuera de las instalaciones de la entidad, excepto aquellos archivos de entidades externas o que, por cambios en la tecnología, no puedan duplicarse. Se debe evitar la replicación corrupta de las copias.
g. Realizar pruebas de tensión del hardware de backups (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de backups y unidades de dispositivo). Estas pruebas deben estar documentadas en el procedimiento de backups, así como sus responsables y los debidos documentos que soporten su elaboración. Estas pruebas deben hacerse como mínimo una vez al año o cuando se adquiera nueva infraestructura tecnológica para el almacenamiento de información de la entidad.
h. Realizar periódicamente un análisis de las necesidades del negocio para determinar, confirmar o actualizar el RPO de los sistemas de información.
i. Contar con las librerías e infraestructura necesarias para generar y restaurar las copias de respaldo; se debe establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente respecto a la información que contenga.
j. Contar con un sitio alterno de almacenamiento para las copias de respaldo con diferentes niveles de priorización.

k. Extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal y en el sitio alterno y/o otros sitios de procesamiento para cumplir con las medidas de protección y seguridad física apropiados.
l. Capacitar al Administrador de bases de datos, de la red y servidores, para que pueda:
   - Actualizar periódicamente las configuraciones de los servidores para la correcta ejecución de las copias de respaldo.
   - Efectuar las copias de información de los servidores conforme a la estrategia de copias de respaldo y cada vez que se realice un cambio significativo en los sistemas operativos o configuraciones básicas.
   - Realizar un respaldo diferencial semanalmente de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, dispositivos de red y de seguridad, conforme a la estrategia de copias de respaldo.
   - Realizar un respaldo full mensual de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, dispositivos de red y de seguridad, conforme a la estrategia de copias de respaldo.
   - Realizar un respaldo full anual de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, dispositivos de red y de seguridad, conforme a la estrategia de copias de respaldo.
m. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a copias de respaldo o restauración de información.

E. Controles relacionados:

1. 5.30 – Preparación de las TIC para la continuidad del negocio
2. 6.8 – Informes de eventos de seguridad de la información
3. 8.1 – Dispositivos de punto final de usuario
4. 8.10 – Eliminación de información

5.4.14 Redundancia de las instalaciones de procesamiento de información

A. Objetivo de control: Implementar suficiente redundancia para cumplir con los requisitos de disponibilidad de instalaciones de procesamiento de información.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar la redundancia de las instalaciones de procesamiento de información de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Asesorar todos los proyectos que se desarrollen en dentro de la entidad para confirmar que cuentan con un componente de resiliencia digital que apoye la disponibilidad de los servicios de TI.

2. La Subdirección de Infraestructura tecnológica y de operaciones debe:

   a. Cumplir con los lineamientos definidos por la guía “TIA-942 estándar - Diseño y Cableado de un Centro de Datos en los centros de datos”.
   b. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a la disponibilidad de servicios de TI.
   c. Contratar a dos o más proveedores de redes e instalaciones críticas de procesamiento de información, como proveedores de servicios de Internet.
   d. Utilizar dos centros de datos separados geográficamente (mínimo 20 km lineales) o servicios en la nube con sistemas duplicados, según la gestión de riesgos de seguridad de la información en la propiedad de disponibilidad.
   e. Tener componentes duplicados en los sistemas; por ejemplo: CPU, fuentes de alimentación discos duros, memorias o en redes (como cortafuegos, enrutadores, conmutadores).
   f. Implementar múltiples instancias paralelas de componentes de software con balanceo de cargas automático entre ellas.
   g. Plantificar y ejecutar pruebas para la activación de los componentes redundantes y las instalaciones de procesamientos.
   h. Contar con alertas sobre fallas en las instalaciones de procesamiento de información.
   i. Verificar el uso de tecnologías en nube para contar con redundancias de los recursos tecnológicos.
   j. Incluir y desarrollar lineamientos relacionados con el SOC (*Security Operation Center*).

E. Controles relacionados:

1. 5.30 – Preparación de las TIC para la continuidad del negocio.
2. 6.8 – Informes de eventos de seguridad de la información.

5.4.15 Inicio de sesión

A. Objetivo de control: Elaborar, conservar, proteger y revisar regularmente los registros de las actividades de los usuarios, fallas, excepciones y eventos de seguridad de la información (logs) contra alteraciones y accesos no autorizados.

B. Alcance: El alcance de esta política aplica para la Oficina de Seguridad de la Información, y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar los registros de eventos de los sistemas e infraestructura de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Definir, aprobar y socializar los procedimientos para proteger la información de registro (logs) de accesos o cambios no autorizados, de acuerdo con los siguientes parámetros:
   - Gestionar solo por los responsables (administradores y operadores) los logs a través de los roles y responsabilidades definidos.
   - Configurar accesos limitados (de solo lectura) a los logs para los procesos de auditoría.
   - Generar logs del sistema operativo (técnicos) y aplicaciones (funcional), y detallar las acciones y criterios de revisión.
   - Confirmar que todas las aplicaciones tengan activos los registros de las actividades realizadas por los funcionarios (se debe tener como mínimo la fecha, IP origen, IP destino, usuario, acción realizada y demás que se requieran).
   - Definir cuánto tiempo se conservan los logs de cada una de las aplicaciones, conforme a las TRD. En caso de no tener una clasificación se debe conservar como mínimo un año de los logs.
   - Detallar pruebas de aseguramiento para la recuperación de logs, del medio en el cual este almacenada.

b. Direccionar los logs en tiempo real de todos los sistemas de la **DIAN** al SIEM (Security Information and Event Management) de la entidad. Esta plataforma tendrá una retención de estos logs, según su capacidad.
c. Realizar copia de los logs de los sistemas operativos y aplicaciones en un medio diferente si el almacenamiento se llena, antes de ser eliminados de los servidores.
d. Alertar a la Oficina de Seguridad de la Información sobre eventos que puedan afectar la seguridad de la información de la entidad.

2. La Oficina de Seguridad de la Información debe:

   a. Confirmar que las bases de datos cuenten con el registro de las actividades realizadas por los usuarios internos y por los administradores de estos.
   b. Definir los umbrales de los eventos para determinar cómo y cuándo se debe actuar antes de que se presente un incidente de seguridad y privacidad de la información.

3. Los propietarios de los sistemas de información deben:

   a. Contar como mínimo con los siguientes archivos de registro de actividades (logs):
      - log de auditoría.
      - log de seguridad.
      - logs de aplicaciones.

   b. Estos logs deben tener una retención de mínimo un año. Estas actividades deben ser coordinadas con la Subdirección de Infraestructura Tecnológica y de Operaciones.

4. Los propietarios de los activos de información deben:

   a. Determinar los procedimientos a implementar para evitar que una persona pueda acceder, modificar o usar los activos de su competencia sin autorización ni detección.

5. Los funcionarios y terceros de la entidad deben:

    a. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados alertas en los registros de eventos.

E. Controles relacionados:

1. 5.25 – Evaluación y decisión sobre eventos de seguridad de la información
2. 5.28 – Recolección de evidencia
3. 5.34 – Privacidad y protección de información de identificación personal
4. 6.8 – Informes de eventos de seguridad de la información
5. 8.16 – Actividades de seguimiento
6. 8.17 – Sincronización de reloj.

5.4.16 Actividades de seguimiento

A. Objetivo de control: Monitorear las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y tomar medidas apropiadas de forma oportuna para evaluar posibles incidentes de seguridad de la información.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencias encargadas de gestionar los monitoreos a redes, los sistemas, aplicaciones e infraestructura de la **DIAN**.

C. Características de control:

1. Tipo de control: detectivo y correctivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

    a. Contar con un COSI (Centro de Monitoreo de Seguridad de la Información), para monitorear, identificar, correlacionar y alertar actividades de posible riesgo sobre los sistemas que registren los logs en el sistema SIEM de la entidad.
    b. Monitorear permanentemente los eventos de los sistemas de información de la **DIAN** que puedan generar un incidente de seguridad y privacidad de la información y que atente contra la confidencialidad, integridad o disponibilidad de los activos de información.
    c. Alertar a la Oficina de Seguridad de la Información sobre eventos que puedan afectar la seguridad de la información de la entidad.
    d. Definir y establecer una línea base para identificar el comportamiento normal (tanto en horas normales como en horas pico) de redes, los sistemas, aplicaciones e infraestructura, y así facilitar el identificar anomalías tales como:
        - Terminación no planificada de procesos o aplicaciones.
        - Actividad típicamente asociada con malware o tráfico que se origina en direcciones IP o dominios de red maliciosos conocidos (por ejemplo, aquellos asociados con servidores de comando.

- Características de ataque conocidas (por ejemplo, denegación de servicio y desbordamiento de memoria intermedia).
- Comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar).
- Cuellos de botella y sobrecargas (por ejemplo, colas de la red, niveles de latencia y fluctuaciones de la red).
- Acceso no autorizado (real o intentado) a sistemas o información.
- Escaneo no autorizado de aplicaciones comerciales, sistemas y redes.
- Intentos exitosos y fallidos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos).
- Comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

e. Monitorear tráfico de red, sistema y aplicación entrante y saliente.
f. Ejecutar acciones de revisión periódicas sobre archivos de configuración de red y sistema de nivel crítico o administrativo.
g. Registrar las revisiones a herramientas de seguridad, por ejemplo: antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos.
h. El software de monitoreo debe configurarse para generar alertas (por ejemplo, a través de consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) en función de umbrales predefinidos. También debe ajustarse y hacer capacitación en la línea de base de la organización para minimizar los falsos positivos.
i. Se deben establecer procedimientos para identificar y abordar los falsos positivos, incluido el ajuste del software de monitoreo para reducir la cantidad de falsos positivos en el futuro.

2. La Oficina de Seguridad de la Información debe:

a. Generar alertas necesarias ante actividades anómalas sobre los sistemas de información de la **DIAN** A su vez, realizar el plan e implementación de las actividades requeridas para corregir estos eventos.
b. Tener una plataforma para el monitoreo de las bases de datos que permita tener el registro detallado de las actividades que estas realicen e integrarán al sistema SIEM de la entidad, desde el que se realiza el monitoreo centralizado de las actividades realizadas a través del COSI.
c. Escalar a las diferentes dependencias de la entidad a través de los dueños de los activos de información, las actividades que puedan implicar un riesgo de seguridad de la información o un uso inadecuado de los sistemas de la **DIAN** y que puedan atentar contra de la confidencialidad, integridad o disponibilidad de la información, para que definan si las actividades corresponden a eventos anómalos.
d. Bloquear actividades o eventos identificados que no correspondan a una acción válida o acorde a las funciones de una dependencia, sin perjuicio de iniciar procesos legales internos o externos a que haya lugar.
e. Informar a la Dirección de Gestión de Innovación y Tecnología, la información relacionada con los riesgos, acciones y/o mitigaciones sugeridas, y con ello, acordar medidas para aplicar los controles y/o las acciones correspondientes para la mitigación de los eventos identificados y reportados.

f. Revisar la actividad asociada con malware o tráfico que se origina en direcciones IP o dominios de red maliciosos conocidos; por ejemplo, aquellos asociados con servidores de comando y control de botnet.
g. Revisar las características de ataque conocidas. Ejemplo: la denegación de servicio y el desbordamiento de memoria intermedia; el comportamiento inusual del sistema (registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar).
h. Capacitar al personal acerca de cómo responder a las alertas e interpretar con precisión los posibles incidentes.

3. Los funcionarios y terceros de la entidad deben:

a. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren la pérdida, daño, robo o compromiso de activos de información por incidentes asociados a alertas en los registros de eventos.

E. Controles relacionados:

1. 5.7 – Inteligencia de amenazas
2. 5.25 – Evaluación y decisión sobre eventos de seguridad de la información
3. 5.26 – Respuesta a incidentes de seguridad de la información
4. 5.28 – Recolección de evidencia
5. 6.8 – Informes de eventos de seguridad de la información

5.4.17 Sincronización de reloj

A. Objetivo de control: Sincronizar los relojes de los servidores, sistemas de procesamiento de información, equipos y servicios tecnológicos con una única fuente de referencia de tiempo, para obtener la exactitud de los registros de auditoría.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencia encargada de gestionar la configuración que permite la sincronización del tiempo legal en los sistemas y aplicaciones de la **DIAN**.

C. Características de control:

1. Tipo de control: detectivo.
2. Propiedades de seguridad: integridad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Documentar los requisitos necesarios para el cumplimiento de la sincronización de relojes de los servidores, sistemas de procesamiento de información, equipos y servicios tecnológicos.
b. Actualizar la hora de los servidores con la escala de tiempo internacional UTC, mediante sincronización a través del protocolo NTP v4, conforme al Instituto Nacional de Metrología (INM).

c. Realizar pruebas periódicas que permitan confirmar la correcta sincronización de la hora oficial de país provista por el Instituto Nacional de Metrología.
d. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren compromiso de activos de información por incidentes asociados a la hora que poseen los servidores, sistemas de procesamiento de información, equipos y servicios tecnológicos.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información

5.4.18 Uso de programas de utilidad privilegiados

A. Objetivo de control: Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, y la Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar el uso de programas de utilidad privilegiados de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Establecer una política, a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema.
b. Definir un lineamiento para que ningún usuario final tenga privilegios de administrador y que exista un número limitado de usuarios autorizados para el uso de programas utilitarios.
c. Definir un procedimiento de autorización para el uso de programas utilitarios por funcionarios y/o terceros.
d. Registrar y mantener actualizados todos los usos aprobados de los programas de utilidad.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Restringir el uso de las herramientas de administración licenciadas (herramientas propias de la **DIAN** usadas para administrar los equipos: instalación, desinstalación de software y similares) para el sistema, solo para usuarios administradores.
b. Implementar la política, a nivel del controlador de dominio, que impida la Instalación de software y cambios de configuración en los sistemas.
c. Confirmar que en los sistemas e infraestructura ningún usuario final tenga privilegios de administrador, conforme a lo establecido por la Subdirección de Soluciones y Desarrollo.

d. Bloquear la sesión después de cinco (5) minutos de inactividad del sistema, confirmando que se realice el bloqueo sin cerrar las sesiones de aplicación o de red.
e. Suspender y bloquear las estaciones de trabajo cuando la ausencia temporal de actividad supere las dos horas.
f. Limitar el número de usuarios autorizados para el uso de programas utilitarios.
g. Separar de forma lógica los programas de utilidad del software de aplicación.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información.
2. 8.2 – Derechos de acceso privilegiado.

5.4.19 Instalación de software en sistemas operativos

A. Objetivo de control: Establecer e implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos por parte de los usuarios, mitigando afectación la confidencialidad, integridad y disponibilidad de la información de la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones y Subdirección de Soluciones y Desarrollo, dependencias encargadas de gestionar el uso de software en los sistemas de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Prohibir el desarrollo y/o implementación de soluciones informáticas o herramientas de gestión no corporativas en lugares o ambientes diferentes a los dispuestos por la Dirección de Gestión de Innovación y Tecnología y que no sigan los procedimientos de desarrollo de software establecidos por la entidad.

2. La Subdirección de Soluciones y Desarrollo debe:

   a. Establecer restricciones y limitaciones para la instalación del software en los equipos de cómputo de la **DIAN**, según el licenciamiento que se tenga disponible.
   b. Contar con un inventario total de software de la entidad y avalar o realizar la adquisición de software para la **DIAN**.
   c. Cumplir con los procesos y procedimientos establecidos por la entidad para la construcción o adquisición de software.
   d. Validar si la entidad cuenta con soluciones que tengan las funcionalidades requeridas por alguna dependencia. De no existir estas soluciones, se debe escalar una solicitud de adquisición a la Dirección de Gestión de Innovación y Tecnología y cumplir con los procedimientos y requisitos para su adquisición e instalación.

e. Remitir a la Oficina de Seguridad de la información las solicitudes que se registren por la mesa de ayuda, relacionadas con requerimientos de instalación de software de uso libre.
f. Llevar el inventario de aplicaciones de uso libre que sean autorizadas por la entidad.
g. Instalar y mantener actualizados el software de seguridad de protección de punto final como antivirus, IDS/IPS, firewall, proxys y demás aplicaciones de seguridad informática que se instalen en los equipos de usuarios internos, de forma que cuenten con las últimas versiones de detección y control de nuevos vectores de ataques. Estos aplicativos no podrán ser manipulados o desactivados por los usuarios internos.
h. Restringir las posibilidades de copiar, vender y/o distribuir el software de la entidad.
i. Restringir el uso exclusivo de software especializado para realizar pruebas de vulnerabilidades, monitoreo de la red, explotación de vulnerabilidades, análisis de protocolos e intercepción o análisis de tráfico en la red, a funcionarios que hacen parte de la Oficina de Seguridad de la Información o de la Subdirección de Infraestructura Tecnológica y de Operaciones, bajo autorización y supervisión de la oficina antes mencionada.
j. Confirmar que las licencias instaladas en la **DIAN** corresponden en cantidad y versión licenciada con la que se adquirió.
k. Manejar un sistema de control de configuración para mantener el monitoreo e inventario de todo el software instalado en los equipos de cómputo de los usuarios.
l. Designar responsables y establecer instructivos y guías para controlar la instalación de software, tanto en las máquinas de los usuarios internos como en los servidores.
m. Confirmar que todo software instalado en la plataforma tecnológica de la **DIAN** cuente con soporte de los proveedores y fabricantes.
n. Conceder accesos temporales y supervisar a los fabricantes y terceros autorizados, para realizar actualizaciones sobre el software.
o. Generar un plan de actualizaciones para el software, aplicaciones y librerías de programas que se deben llevar a cabo por los administradores, bajo la autorización del Comité de Cambios.
p. Confirmar que las instalaciones de software se realizan siempre que se aprueben de forma satisfactoria.
q. Registrar de forma segura los eventos relacionados con actualizaciones de software operativo.
r. Archivar en repositorios seguros las versiones anteriores del(los) software(s) que han sido actualizados o cambiados.
s. Validar los riesgos que genera la migración hacia nuevas versiones del software. Se debe confirmar el correcto funcionamiento de los sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software es actualizado.
t. Restringir el uso de software o servicios de red que permitan el intercambio de información con terceras partes sin el debido aval o autorización por parte de la Oficina de Seguridad de la información.

3. La Oficina de Seguridad de la información debe:

a. Realizar el análisis del requerimiento de instalación de software de uso libre en términos de seguridad de la información y entregar el resultado a la Subdirección de Soluciones y Desarrollo para la toma de la decisión definitiva.
b. Enviar un mensaje al usuario interno e informar a su jefe inmediato, para que dé traslado a la autoridad disciplinaria, administrativa o judicial competente, informando sobre los

hechos que puedan ser constitutivos de violación a los reglamentos vigentes del uso de software.

c. Autorizar los accesos temporales y controlados a los fabricantes y terceros autorizados para realizar actualizaciones sobre el software.

4. Los funcionarios y terceros de la entidad deben:

a. Utilizar el software legalmente adquirido, desarrollado y/o autorizado por la entidad a través de la Subdirección de Soluciones y Desarrollo.
b. Enviar una solicitud a través de la mesa de ayuda a la Subdirección de Soluciones y Desarrollo en caso de requerirse la instalación de software de uso libre a través de la herramienta establecida para tal fin, relacionando el nombre de la aplicación, la versión, el tipo de licencia de uso, la casa de software productora, las referencias en internet, la justificación del requerimiento y el periodo de tiempo estimado de uso.
c. Abstener el uso de software o hardware que vulnere o evada los controles de seguridad informática o seguridad y privacidad de la información establecidos por la **DIAN**.
d. Informar a la Oficina de Seguridad de la información de eventos de violación a los reglamentos vigentes relacionados con software.

E. Controles relacionados:

1. 5.22 – Seguimiento, revisión y gestión de cambios de servicios de proveedores
2. 6.8 – Informes de eventos de seguridad de la información
3. 8.5 – Autenticación segura
4. 8.8 – Gestión de vulnerabilidades técnicas
5. 8.29 – Pruebas de seguridad en desarrollo y aceptación
6. 8.31 – Separación de los entornos de desarrollo, prueba y producción

5.4.20 Seguridad en redes

A. Objetivo de control: Proteger las redes y los dispositivos de red para mitigar la afectación a la información en los sistemas y aplicaciones de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura tecnológica y de Operaciones y la Oficina de Seguridad de la información, dependencias encargadas de gestionar la seguridad de las redes de la **DIAN** y sus seccionales.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Restringir las redes de datos alámbricas o inalámbricas de la **DIAN** a únicamente los funcionarios y terceros autorizados para conectarse y acceder a los sistemas de información de la entidad.

b. Restringir el acceso desde redes externas hacia plataformas informáticas de la entidad, e implementar el uso de IPSec (seguridad del protocolo de internet) para tal fin.
c. Supervisar las acciones de terceros autorizados por la Oficina de Seguridad de la Información para dar soporte, teniendo especial cuidado con los equipos que se conectan a la entidad utilizando herramientas seguras de conexión con las que se cuenta.
d. Monitorear accesos y uso de los servicios informáticos. En caso de evidenciar un mal uso del recurso informático por parte de un usuario interno, se debe suspender de forma parcial, temporal o total el acceso a este recurso y notificar a la Oficina de Seguridad de la Información.
e. Autorizar y monitorear la seguridad de la comunicación entre entidades públicas o privadas a través de accesos dedicados o a través de los servicios de computación en la nube.
f. Configurar los usuarios de las redes evitando la creación de comunidades, usuarios o contraseñas genéricas con acceso restringido.
g. Monitorear y, si no se requiere, deshabilitar los puertos físicos y lógicos de la plataforma tecnológica.
h. Establecer mecanismos para detectar intrusos para descubrir cualquier intento de acceso o ataque sobre plataformas informáticas.
i. Restringir el uso del servicio de internet solo para fines laborales e institucionales y realizar las funciones asignadas.
j. Restringir el uso de otros sistemas de comunicaciones alternos como Messenger, Yahoo! O cualquier otro medio de comunicación actual o futuro no autorizado por la Oficina de Seguridad de la información.
k. Contar con un procedimiento que permita controlar la publicación en los sistemas colaborativos de la información marcada o etiquetada como clasificada o reservada.
l. Restringir el acceso a los servicios de computación en la nube a través de dispositivos móviles. Dicho acceso solo está autorizado para usuarios internos que, por su rol, requieren movilidad entre diferentes sedes de la **DIAN** o ubicaciones externas.
m. Administrar las capacidades y accesos de los diferentes servicios disponibles en las herramientas de computación en la nube que contrate la entidad.
n. Integrar al SIEM de la entidad el registro de las actividades realizadas por los usuarios internos sobre los sistemas colaborativos.
o. Restringir el acceso a los servicios de computación en la nube desde equipos o redes de uso público.
p. Restringir la sincronización de información de la nube con cuentas personales.
q. Implementar sistemas que controlen la autenticación en la red.
r. Aislar temporalmente subredes clasificadas como críticas con apoyo de la Oficina de Seguridad de la información.
s. Deshabilitar protocolos de red que hayan sido identificados como vulnerables por parte de la Dirección de Gestión de Innovación y Tecnología y/o la Oficina de Seguridad de la información.
t. Mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos.

2. La Oficina de Seguridad de la información debe:

a. Validar y analizar las solicitudes de autorización de conexión de un tercero para realizar tareas de soporte en equipos de la entidad.

b. Evaluar los riesgos, costos, la disponibilidad de la información, su sensibilidad y su clasificación frente a los compromisos legales o contractuales que tenga la entidad por el uso de los servicios de computación en la nube.
c. Monitorear y revisar la información desarrollada, gestionada o almacenada en la nube, sin necesidad de contar con la autorización de su(s) autor(es) o generador(es).

3. Los jefes de las dependencias deben:

a. Determinar el tipo de información a almacenar en la nube de acuerdo con su clasificación y sensibilidad. De igual manera, establecer cuáles usuarios pueden tener acceso o permisos de modificación sobre la misma.
b. Coordinar con la Subdirección de Soluciones y Desarrollo el mecanismo un método para realizar la descarga de altos volúmenes de información, en la nube, a un sistema de carpetas públicas. Así mismo, se debe establecer el medio y la forma en que esta información sea recuperada en caso de ser necesario.

4. Los funcionarios y terceros de la entidad deben:

a. Solicitar a la Oficina de Seguridad de la información autorización cuando se requiera comunicación con un tercero para recibir soporte y que este requiera la conexión a equipos de la entidad.
b. Evitar, bajo el riesgo de sanción por parte de la entidad, el envío, recepción, descarga y visualización de páginas, archivos o adjuntos en cualquier formato digital, con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atente contra la integridad de las personas o instituciones.
c. Evitar, bajo el riesgo de sanción por parte de la entidad, colocar información de la **DIAN** (independientemente de su formato o su nivel de clasificación de confidencialidad) en sitios de internet públicos, privados o los denominados discos, carpetas virtuales o cualquier sistema de publicación de documentos, dentro o fuera de las instalaciones de **DIAN** que no sean aprobados por la entidad.
d. Especificar en sus redes sociales personales que sus opiniones, discusiones, expresiones y demás publicaciones son a nombre de quien las expresa y no se emiten a nombre de la entidad.
e. Evitar bajo sanción por la entidad publicar imágenes, opiniones, información o debates sobre la **DIAN** en sus redes sociales. Sin embargo, si algún usuario interno las publica, debe ser autorizado por la Oficina de Comunicaciones Institucionales y la Oficina de Seguridad de la información, para lo cual debe adicionar la siguiente frase en español e inglés:
    - "Las opiniones y publicaciones realizadas en este sitio corresponden a una opinión y no constituyen en ningún momento una posición oficial de la **DIAN"**.
    - "The opinions and publications made on this site correspond to a personal opinion and do not constitute at any time an official position by Colombian Tax and Customs Office, **DIAN**."
f. Sincronizar la información almacenada en su repositorio individual en la nube, con su equipo institucional, si está registrado en el dominio interno de la **DIAN**.
g. Mantener, depurar y/o actualizar la información almacenada en su repositorio individual creado en la nube.
h. Habilitar el control de cambios y las marcas de revisión activas cuando se utilicen herramientas de trabajo colaborativo o elaboración de archivos compartidos.

i. Evitar, bajo el riesgo de sanción por parte de la entidad, desactivar las funciones de seguimiento, revisión o auditoría que tengan configuradas las herramientas de computación en la nube.
j. Evitar, bajo riesgo de sanción por parte de la entidad, utilizar los servicios de colaboración en la nube para:
   - Procesar o almacenar información de tipo personal.
   - Distribuir software no seguro o de procedencia no permitida o ilegal.
   - Intentar obtener un acceso no autorizado o causar disrupción en cualquier dispositivo, dato, cuenta o red.
   - Obstaculizar el uso de las herramientas disponibles en la nube por parte de otras personas.
   - Copiar, adulterar o tratar de manipular el software disponible en la nube para provecho propio, usos no permitidos o ilegales.
   - Realizar acciones que pongan en riesgo la seguridad o aumenten la vulnerabilidad de los servicios o de la información disponible en la nube.
k. Reportar cualquier evento que pueda constituirse como un incidente de seguridad y privacidad de la información almacenada en los sistemas de colaboración.

E. Controles relacionados:

1. 5.3 – Segregación de deberes
2. 5.14 – Transferencia de información
3. 5.22 – Seguimiento, revisión y gestión de cambios de servicios de proveedores
4. 6.6 – Acuerdos de confidencialidad o no divulgación
5. 6.8 – Informes de eventos de seguridad de la información
6. 8.15 – Inicio de sesión
7. 8.16 – Actividades de seguimiento
8. 8.24 – Uso de criptografía

5.4.21 Seguridad de los servicios de red

A. Objetivo de control: Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura tecnológica y de operaciones, dependencia encargada de gestionar la seguridad de las redes de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Confirmar que todos los equipos, servicios propios o servicios que se contraten externamente, cuenten con los registros de auditoría de las labores realizadas en estos y que permita evaluar los riesgos de seguridad.

b. Monitorear permanente los canales de comunicación para identificar y establecer su desempeño y generar los mecanismos de control.
c. Brindar los niveles de servicio adecuados en las labores asociadas a los contratistas y a las necesidades propias de la entidad.
d. Contar con las características de seguridad que permitan controlar, monitorear, bloquear, segmentar y asignar los puertos para las diferentes redes que se utilicen.
e. Confirmar las medidas de seguridad que los proveedores implementan para mantener la seguridad de sus redes.
f. Establecer con apoyo de la Oficina de Seguridad de la información, los Parámetros técnicos requeridos para la conexión segura.
g. Establecer los únicos medios autorizados por la **DIAN** para el acceso a redes y servicios de red (como VPN).
h. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren compromiso de activos de información por incidentes asociados a la seguridad de los servicios de red.

E. Controles relacionados:

1. 6.8 – Informes de eventos de seguridad de la información
2. 8.20 – Seguridad en redes

5.4.22 Segregación de redes

A. Objetivo de control: Separar las redes, los grupos de servicios de información, sistemas de información y usuarios para controlar el tráfico entre ellos, en función de las necesidades misionales de la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencia encargada de gestionar la seguridad de las redes de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Diseñar y mantener la segregación en las redes de datos que permitan el aislamiento entre las diferentes aplicaciones y dependencias de la entidad.
b. Aislar el tráfico entre las zonas públicas y privadas de la entidad.
c. Configurar la red de datos para que se encuentre en segmentos físicos y lógicos independientes, separando como mínimo los usuarios internos, visitantes, las conexiones con terceros, la conexión a internet y las plataformas informáticas Para ello se puede implementar el uso de VLAN y equipos de enrutamiento o de seguridad tales como sistemas de firewall.
d. Establecer un perímetro externo llamado “DMZ internet (Delimitarized Zone)” en la red a través del cual se puedan limitar las conexiones desde internet hacia las plataformas

informáticas internas, permitiendo la seguridad de las últimas. De igual forma, las conexiones desde la red interna hacia la DMZ internet deben ser limitadas solamente a las necesidades operacionales de funcionamiento de las plataformas, bajo el principio de “acceso mínimo requerido”.

e. Aislar totalmente la DMZ internet de cualquier otra red interna, de forma que no se permitan accesos no autorizados a las redes internas.
f. Separar las redes alámbricas de las inalámbricas y se debe contar con redes inalámbricas públicas que están disponibles en casos especiales.
g. Configurar los dominios de red separados de la red pública (Internet) a través de firewall.
h. Implementar un portal cautivo de acceso inalámbrico para los invitados a las instalaciones de la entidad, el cual debe contar con las mismas restricciones establecidas para los funcionarios; este servicio no debe afectar la red interna, teniendo en cuenta que no es una prioridad en el cumplimiento de la misionalidad de la entidad
i. Implementar de forma segura la red de "Zona Wifi gratis para la Gente" según el Decreto 728 de 2017.
j. Implementar un servicio de red para los equipos de análisis forense, el cual debe estar aislado y solo puede ser utilizado por los responsables asignados en Fiscalización (TACI).
k. Reportar a la Oficina de Seguridad de la Información los eventos y/o incidentes que involucren compromiso de activos de información por incidentes asociados a la seguridad de los servicios de red.

E. Controles relacionados:

1. 5.15 – Control de acceso
2. 6.8 – Informes de eventos de seguridad de la información
3. 8.20 – Seguridad en redes

5.4.23 Filtros Web

A. Objetivo de control: Administrar el acceso a sitios web en los equipos de la entidad con el fin de reducir la exposición a contenido malicioso, afectación a los servicios de red, acceso a contenido ilegal y similares.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de seguridad de la información y Subdirección de Infraestructura Tecnológica y de Operaciones de la entidad, encargadas de proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la información debe:

a. Establecer y mantener actualizadas las reglas para el uso seguro y apropiado de los recursos en línea, incluyendo cualquier restricción a sitios web y aplicaciones basadas en la web indeseables o inapropiados.

b. Incluir, en las reglas de uso seguro y apropiado de los recursos en línea, las diferencias entre los equipos en la red de la entidad y los equipos que se encuentran en teletrabajo.
c. Identificar y documentar los tipos de sitios web a los que los funcionarios y terceros deben o no tener acceso.
d. Indicar si es válido o no el acceso a páginas o servicios de internet no permitidos que un funcionario o tercero solicite para el cumplimiento de sus actividades.
e. Definir lineamientos y controles para restringir el acceso a sitios web que contengan información ilegal o que se sepa que contiene virus o material que pueda afectar los equipos de la entidad, se debe considerar bloquear el acceso a los siguientes tipos de sitios web:
    - Con una función de carga de información, a menos de que esté permitido por razones misionales validas.
    - Maliciosos conocidos o sospechosos (por ejemplo, a aquellos que distribuyen *malware* o contenido de *phishing)*.
    - Servidores de mando y control.
    - Maliciosos identificados en la inteligencia de amenazas.
    - Que comparten contenido ilegal.

f. Verificar, al menos una vez al año, que los filtros web se están aplicando de acuerdo con los lineamientos establecidos.
g. Brindar capacitación a los funcionarios y terceros de la entidad sobre el uso seguro y apropiado de los recursos en línea, incluido el acceso a la web y los siguientes aspectos:

    - Las reglas definidas en este tema.
    - El punto de contacto para plantear problemas de seguridad.
    - El proceso de excepción cuando se necesita acceder a recursos web restringidos por razones comerciales.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Implementar los controles definidos por la Oficina de Seguridad de la Información, bloqueando la dirección IP o el dominio de los sitios web identificados que requieren restricción de acceso.
b. Direccionar a la Oficina de Seguridad de la Información las solicitudes de funcionarios o terceros que soliciten el acceso a páginas o servicios de internet no permitidos.
c. Restringir la posibilidad de escuchar música, ver videos, televisión y sitios de streaming, tales como Netflix, HBO GO, prime video, entre otros, a los que se acceda utilizando la red de datos y el servicio de internet institucional, salvo que por las funciones asignadas sea necesario su acceso y sea debidamente autorizado por la Oficina de Seguridad de la información.
d. Restringir el acceso a redes sociales (Facebook, Twitter, YouTube, Tik Tok y similares) dentro de la red de datos de la **DIAN**. Solamente la Oficina de Comunicaciones podrá tener acceso a páginas y redes sociales para el monitoreo y/o la realización de sus funciones.
e. Prohibir el acceso a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la Oficina de Seguridad de la Información a través de la política de navegación.

3. Los funcionarios y terceros de la entidad deben:

    a. Solicitar a la Oficina de Seguridad de la Información a través de jefe inmediato, acceso a páginas o servicios de internet no permitidos cuando estos sean requeridos para el cumplimiento de sus actividades.

E. Controles relacionados:

1. 5.7. – Inteligencia de amenazas.

5.4.24 Uso de criptografía

A. Objetivo de control: Establecer un esquema para el uso adecuado y eficaz de las técnicas criptográficas para gestionar la confidencialidad, integridad, y disponibilidad de la información pública reservada y pública clasificada y datos personales administrada por la **DIAN** que sea transportan, transmiten y/o almacenan en los diferentes medios digitales y/o electrónicos disponibles en la entidad.

B. Alcance: El alcance de esta política aplica para todas las dependencias de la **DIAN** que tratan información pública reservada, pública clasificada y datos personales, para el personal encargado de implementar los controles de cifrado en los servicios de red, en las plataformas informáticas y en los sistemas de información de la entidad, en el momento de almacenarse o transmitirse por cualquier medio digital o electrónico utilizado.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Validar el cumplimiento de la política para que la información pública reservada y pública clasificada, datos personales sensibles o privados, semiprivados y de menores, se cifre en el momento de almacenarse o transmitirse por cualquier medio.
    b. Definir lineamientos sobre el uso de criptografía para la protección de la información en la entidad.
    c. Establecer condiciones de cifrado para los correos electrónicos de la entidad cuando estos cuenten con información pública reservada o pública clasificada.

2. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Controlar que la información y/o las aplicaciones que contengan contraseñas de usuario o claves para el control de acceso a los sistemas de información no sea almacenada en texto plano y debe hacer uso de mecanismos criptográficos.
    b. Identificar todo sistema de información o aplicación requerido para transmitir información pública reservada y clasificada, para que cuente con mecanismos de cifrado de datos.
    c. Cifrar los discos duros de los equipos de cómputo que contengan información pública reservada o pública clasificada.

d. Definir protocolos o certificados de cifrado en los canales de comunicación a nivel de red interna y externa.
e. Controlar y establecer los mecanismos de seguridad para las comunicaciones cifradas con terceros que se realicen a través del uso de conexiones de VPN.
f. Adelantar las acciones pertinentes para la implementación del mecanismo de firma electrónica en los siguientes servicios: cifrado de documentos y comunicaciones, sede electrónica, portal del funcionario, buzón del ciudadano, business process management, automatización de procesos y procedimientos, gestión de expedientes electrónicos, archivo electrónico, gestión documental electrónica, movilidad, seguridad e identidad digital, entre otros.
g. Cifrar la información en los procesos de recepción, almacenamiento, transmisión y/o consulta de los activos de información catalogados como información pública reservada y pública clasificada de la **DIAN**, con el propósito de proteger su confidencialidad, integridad.
h. Utilizar herramientas, mecanismos y técnicas criptográficas para realizar operaciones como cifrado, firma digital, firma electrónica, para asegurar el principio de no repudio de las transacciones electrónicas.
i. Aplicar controles criptográficos en todo el ciclo de vida de los documentos o archivos digitales, cuando contengan información pública reservada y pública clasificada, datos personales sensibles o privados, semiprivados y de menores de edad.
j. Aplicar controles criptográficos para la información de intercambio con fines tributarios, aduaneros y cambiarios. También se deben aplicar controles en la recepción, almacenamiento, consulta y/o transmisión de información y emplear esquemas de seguridad exclusivos e independientes.
k. Utilizar y almacenar la huella digital o código hash que mitiguen la afectación sobre la integridad de la información suministrada en dos momentos diferentes.
l. Utilizar técnicas criptográficas para autenticar a los usuarios o entidades externas que requieran hacer uso de los sistemas de información de la **DIAN**. Su implementación se realizará según los lineamientos establecidos en este manual.
m. Manejar esquemas de cifrado “desde el arranque” (PBA) para los discos de almacenamiento interno de los equipos portátiles, de manera que el inicio del sistema operativo se realice con el disco ya cifrado.
n. Configurar y administrar las herramientas, sistemas y mecanismos de cifrado.
o. Implementar métodos de cifrado a nivel de dispositivo de almacenamiento, base de datos, table-space para la información pública reservada y pública clasificada.
p. revisar que en los sistemas de información y/o aplicaciones construidas por terceros o internos, se apliquen controles criptográficos a la información pública reservada y pública clasificada, datos personales sensibles o privados, semiprivados y de menores de edad.
q. Controlar que los métodos criptográficos implementados sean interoperables y portables.
r. Administrar y controlar las llaves criptográficas.
s. Definir roles y responsabilidades para la implementación de reglas para el uso de criptografía y la gestión de las claves.
t. Definir las soluciones criptográficas y las prácticas de uso que se aprueben o se requieren para su uso en la entidad.
u. Emitir y obtener certificados de clave pública.
v. Definir lineamientos para la distribución de claves y recuperación de claves perdidas o dañadas, y también para la destrucción de llaves que se requieran en la entidad.
w. Utilizar y almacenar el cálculo de sumas de verificación o código hash para la integridad de la información suministrada en dos momentos diferentes.

x. Requerir como mínimo el uso de mecanismos de identificación basados en llave pública o su equivalente para los procedimientos de cargue automático de archivos provenientes de terceros.
y. Definir y establecer restricciones de importación hardware y software informático que esté diseñado para tener funciones criptográficas no permitidas.
z. Regular los controles criptográficos mediante un esquema de cifrado de datos que utilice algoritmos, protocolos, mecanismos y técnicas con estándares nacionales y/o internacionales.
aa. Utilizar algoritmos, protocolos, mecanismos y técnicas de cifrado con estándares nacionales y/o internacionales.
bb. Utilizar herramientas, mecanismos y técnicas criptográficas para la protección de la información en operaciones como el cifrado, firma digital, firma electrónica y con el fin evitar el no repudio de las transacciones electrónicas.
cc. Utilizar herramientas, mecanismos y técnicas criptográficas para la protección de la información, acorde con los estándares técnicos, la guía de referencia de BlockChain para la adopción e implementación de proyectos en el estado colombiano y los estándares de BlockChain.

3. Los funcionarios y terceros deben:

a. Notificar a la Dirección de Gestión de Innovación y Tecnología la información que requiere sea cifrada según la información pública reservada y clasificada, datos personales sensibles o privados, semiprivados y de menores.
b. Solicitar a la Dirección de Gestión de Innovación y Tecnología la disposición de controles criptográficos, de manera total o parcial, sobre las bases de datos donde se encuentre almacenada información pública reservada y pública clasificada, datos personales sensibles o privados, semiprivados y de menores de edad.
c. Cumplir con los lineamientos de cifrados definidos en esta política y emplear las herramientas adoptadas por la Dirección de Gestión de Innovación y Tecnología para este fin.
d. Cifrar previamente y generar una huella digital o código hash cuando se requiere enviar información pública reservada o publica clasificada, datos personales sensibles o privados, semiprivados y de menores de edad, a través de la herramienta de correo electrónico institucional.
e. Almacenar las claves de forma segura y comprometerse a restringir el acceso solo a los usuarios autorizados. De igual forma, una copia de las claves, si esta existe, deberá ser almacenada en sitio seguro para su recuperación en caso de que esta se extravíe.
f. Cumplir las condiciones de cifrado definidas por la Oficina de Seguridad de la Información para el envío de correos electrónicos de la entidad, cuando estos cuenten con información pública reservada o pública clasificada.
g. Dar cumplimiento de la presente política con el fin de que la información pública reservada y pública clasificada, datos personales sensibles o privados, semiprivados y de menores de edad, se cifre en el momento de almacenarse o transmitirse por cualquier medio.

E. Controles relacionados:

1. 5.22. – Seguimiento, revisión y gestión de cambios de servicios de proveedores
2. 5.31. – Requisitos legales, estatutarios, reglamentarios y contractuales
3. 8.24. – Uso de criptografía

5.4.25 Ciclo de vida de desarrollo seguro

A. Objetivo de control: Definir los lineamientos y directrices de desarrollo seguro de software y gestionar la seguridad y privacidad de la información, como parte integral del ciclo de vida de desarrollo seguro del software de los sistemas de información de la **DIAN**, el cual incluye la adquisición, desarrollo, ajustes y mantenimiento de software.

B. Alcance: El alcance de este lineamiento aplica para los proveedores de software, contratistas, terceros, la Dirección de Gestión de Innovación y Tecnología y la Subdirección de Soluciones y Desarrollo, por cuanto son las que adquieren, reciben, instalan y/o desarrollan software para la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Definir y documentar detalladamente los lineamientos para la trasferencia de software desde desarrollo hacia producción y para los desarrollos contratados.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Establecer en lo posible las últimas metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.
    b. Gestionar el correcto funcionamiento y separación de ambientes de desarrollo, pruebas, integración y producción.
    c. Implementar los lineamientos y los controles establecidos por la Dirección de Gestión de Innovación y Tecnología en relación con lo definido en este control.
    d. Confirmar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información se encuentren actualizados con los últimos parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
    e. Certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
    f. Gestionar el cumplimiento del manual de políticas y lineamientos de seguridad de la información, normatividad y lineamientos vigentes en la **DIAN** durante todo el ciclo de desarrollo.
    g. Proteger el código fuente del software construido, para que personal no autorizado no pueda descargarlo ni modificarlo.
    h. Certificar que la información a ser entregada para sus pruebas esté enmascarada o anonimizada, no se revele información confidencial de los ambientes de producción y que no contiene datos personales reales de acuerdo con lo establecido en la Ley 1581 de 2012.

3. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

    a. Implementar el correcto funcionamiento y separación de ambientes de desarrollo, pruebas, integración y producción.

E. Controles relacionados:

1. 5.8. – Seguridad de la información en la gestión de proyectos
2. 5.32. – Derechos de propiedad intelectual
3. 8.4. – Acceso al código fuente
4. 8.9 – Gestión de la configuración
5. 8.27. – Principios de arquitectura e ingeniería de sistemas seguros
6. 8.28. – Codificación segura
7. 8.29. – Pruebas de seguridad en desarrollo y aceptación
8. 8.30. – Desarrollo subcontratado
9. 8.31. – Separación de los entornos de desarrollo, prueba y producción
10. 8.32. – Gestión del cambio

5.4.26 Requisitos de seguridad de la aplicación

A. Objetivo de control: Identificar, especificar y aprobar los requisitos de seguridad de la información al desarrollar o adquirir aplicaciones.

B. Alcance: El alcance de este lineamiento aplica la Dirección de Gestión de Innovación y Tecnología y la Subdirección de Soluciones y Desarrollo, encargados de verificar la protección de la información y que todos los requisitos de seguridad de la información de identifiquen y aborden al desarrollar o adquirir aplicaciones.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

    a. Identificar y especificar los requisitos de seguridad de las aplicaciones, estos requisitos se pueden determinar a través de una evaluación de riesgos.
    b. Incluir en los requisitos de seguridad de las aplicaciones, como mínimo, los siguientes aspectos:

        - Nivel de confianza en la identidad.
        - Identificar el tipo de información y nivel de clasificación a ser procesado por la aplicación.
        - Necesidad de segregación de acceso y nivel de acceso a datos y funciones en la aplicación.
        - Resiliencia contra ataques maliciosos o interrupciones no intencionales (por ejemplo, protección contra desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL)).

- Requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción.
- Necesidad de privacidad asociada con todas las partes involucradas.
- Los requisitos de protección de cualquier información confidencial.
- Protección de datos en proceso, en tránsito y en reposo.
- Necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas.
- Controles de entrada, incluidas verificaciones de integridad y validación de entrada.
- Controles automatizados (por ejemplo, límites de aprobación o aprobaciones duales).
- Controles de salida, considerando también quién puede acceder a las salidas y su autorización.
- Restricciones en torno al contenido de los campos de "texto libre", ya que pueden coincidir al almacenamiento no controlado de datos confidenciales (por ejemplo, datos personales).
- Requisitos derivados del proceso de negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio.
- Requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para registro y monitoreo o sistemas de detección de fuga de datos).
- Manejo de mensajes de error.

c. Identificar requisitos de seguridad en los servicios transacciones que puedan realizar en desarrollos de la entidad o desarrollos subcontratados.
d. Incluir en las cláusulas contractuales para los desarrollos subcontratados los lineamientos mencionados en el presente control.
Ejecutar como mínimo las prácticas referenciadas en OWASP o en s*ecure software development lifecycle*, así mismo, validar la inclusión de buenas prácticas como: *SANS CIS Controls version 8, Web Application Security Consortium, Common Weakness Enumeration (CWE), Department of Homeland Security: Build Security In Porta, CERT Secure Coding y MSDN Security Developer Center.*
e. Incluir en los desarrollos de la entidad una lista de validación de entradas, verificando: fuentes de datos, datos de entradas, fallas de entrada, tipos de datos no esperados, rangos de datos, largos de datos, caracteres considerados peligrosos.
f. Se debe sanear todas las salidas de datos no confiables hacia consultas SQL, XML y LDAP en los sistemas de información que desarrolle la entidad; así mismo las salidas de datos no confiables hacia un comando del sistema operativo.
g. Administrar la autenticación y las contraseñas de los sistemas de información de la entidad, teniendo en cuenta al menos lo siguiente: autenticación en todos los sistemas, servicios de autenticación estándar, centralizar los controles de autenticación, falla segura de autenticación, cifrar las contraseñas, no enviar contraseñas por correo cuando se solicite "olvido contraseñas".
h. Administrar las sesiones de los sistemas de información que se desarrollen en la entidad, incluyendo mínimos los siguientes criterios: deshabilitar logueos persistentes, generar un nuevo identificador de sesión luego de cada re-autenticación, no permitir logueos concurrentes con el mismo usuario.
i. Implementar un control de acceso desde los desarrollos de la entidad, teniendo en cuenta como mínimo lo siguiente: restringir el acceso a URL (Uniform Resource Locator) protegidas, limitar el acceso a funciones protegidas, evitar las referencias directas a objetos, restringir el acceso a servicios y limitar el número de transacciones que un usuario común o un dispositivo puede desarrollar en determinado período.

j. Incluir prácticas de criptografía en los sistemas que desarrolle la entidad, teniendo en cuenta el FIPS 140-2 o un estándar equivalente, se sugiere (Ver http://csrc.nist.gov/groups/STM/cmvp/validation.html).
k. Configurar los errores y los logs de los sistemas de información desarrollados en la entidad que permitan identificar como mínimo lo siguiente: a) registrar log de fallas de validación, b) registrar intentos de autenticación, c) registrar log de fallas en los controles de acceso y d) registrar los eventos de intento de evasión de controles.
l. Proteger los datos implementando el mínimo privilegio, restringiendo el acceso de los usuarios solamente a la funcionalidad, datos y sistemas de información que son necesarios para realizar sus tareas.
m. Remover cualquier aplicación que no sea necesaria y la documentación de los sistemas que pueda revelar información útil para los atacantes.

E. Controles relacionados:

1. 5.17. – Información de autenticación
2. 5.31. – Requisitos legales, estatutarios, reglamentarios y contractuales
3. 5.32. – Derechos de propiedad intelectual
4. 5.33. – Protección de registros
5. 5.34. – Privacidad y protección de la información de identificación personal (PII)
6. 5.35. – Revisión independiente de la seguridad de la información
7. 5.36. – Cumplimiento de políticas, normas y estándares de seguridad de la información
8. 8.2. – Derechos de acceso privilegiado
9. 8.5. – Autenticación segura
10. 8.24. – Uso de criptografía

5.4.27 Principios de arquitectura e ingeniería de sistemas seguros

A. Objetivo de control: Establecer, documentar y mantener principios para la construcción de sistemas seguros y la aplicación a cualquier actividad de implementación de sistemas de información y/o software.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología y la Subdirección de Soluciones y Desarrollo encargadas de verificar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Definir y documentar lineamientos para la construcción, mantenimiento y/o ajustes de los sistemas de información y/o software aplicando los principios de construcción de seguridad.

b. Incluir el tema de seguridad en el diseño en todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de la información y el manejo de datos personales de acuerdo con lo establecido en la Ley 1581 de 2012.
c. Realizar el análisis de patrones de ataques conocidos y tenerlos en cuenta en la construcción y/o ajustes de los sistemas de información y/o software.
d. Revisar y actualizar con regularidad los lineamientos, principios y procedimientos establecidos para la construcción de software y/o sistemas de información, teniendo en cuenta la mejora continua para contribuir a los estándares de seguridad y poder combatir nuevas amenazas potenciales. Las actualizaciones que se realicen deben cumplir el versionamiento documental establecido en el Sistema de Gestión Documental.
e. Verificar que se cumplan los lineamientos, principios y /o procedimientos establecidos para el ciclo de desarrollo de seguro software, cuando se contrate con un tercero la construcción y/o mantenimiento de sistemas de información y/o software para la entidad.
f. Crear capacidades de los controles de seguridad para prevenir, detectar y responder a eventos de seguridad en los sistemas de información.
g. Incluir principios de "confianza cero" y establecer principios de desarrollo tales como: "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación predeterminada", "fallo seguro", "desconfiar de la entrada de aplicaciones externas", "seguridad en implementación", "asumir incumplimiento", "privilegio mínimo", "facilidad de uso y administración" y "funcionalidad mínima".

2. La Dirección de Gestión de Innovación y Tecnología debe:

a. Verificar que los operadores de tecnologías de la información incluyan las siguientes consideraciones de seguridad de la información, para las transacciones por redes de telecomunicaciones:
   - El uso de mecanismos criptográficos por parte de cada una de las partes involucradas en la transacción.
   - Todos los aspectos de las transacciones deben validar que:
     i. La información de autenticación privada y confidencial del usuario, de todas las partes, sea validada y verificada.
     ii. La transacción permanezca confidencial y se mantenga la privacidad asociada con todas las partes involucradas.
     iii. La trayectoria de las comunicaciones entre todas las partes involucradas esté cifrada.
     iv. Los protocolos usados para comunicarse entre todas las partes involucradas sean seguros.
     v. El almacenamiento de los detalles de la transacción se realice en un entorno que no sea accesible públicamente y no sea retenido ni expuesto en un medio de almacenamiento accesible directamente desde la Web.
b. Donde se utilice una autoridad confiable (por ejemplo, para los propósitos de emitir y mantener firmas o certificados digitales), la seguridad debe estar integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

E. Controles relacionados:

1. 5.12. – Clasificación de la información
2. 5.15. – Control de acceso
3. 5.16. – Gestión de identidad
4. 5.17. – Información de autenticación

5. 5.18. – Derechos de acceso
6. 8.2. – Derechos de acceso privilegiado
7. 8.5. – Autenticación segura

5.4.28 Codificación segura

A. Objetivo de control: Aplicar los principios de codificación segura al desarrollo de software en la entidad.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información y la Subdirección de Soluciones y Desarrollo, encargadas de verificar que el software se escriba de forma segura y definir controles para reducir las posibles vulnerabilidades de seguridad de la información en el software.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

    a. Monitorear las posibles amenazas con el fin de mantener actualizada la base de conocimiento sobre las vulnerabilidades del software y poder asesorar y guiar acerca de los principios de codificación segura en la entidad a través de la mejora y aprendizaje continuos.

2. La Subdirección de Soluciones y Desarrollo debe:

    a. Definir y documentar la codificación segura en el desarrollo de software (en la planificación, en la ejecución y en la revisión y mantenimiento de software en la entidad).
    b. Implementar la codificación segura en el desarrollo de software en la entidad.
    c. Establecer y aplicar las líneas base seguras aplicables para el desarrollo de software, estas definiciones deben extenderse a los componentes de software de terceros y el software de código abierto.
    d. Planificar los requisitos previos antes de la codificación segura, los cuales deben incluir los siguientes aspectos:
        - Configuración de herramientas de desarrollo, como entornos de desarrollo integrados para ayudar a hacer cumplir la creación de código seguro.
        - Seguir la orientación emitida por los proveedores de herramientas de desarrollo y entornos de ejecución.
        - Mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores).
        - Calificación de los desarrolladores en la escritura de código seguro.
        - Diseño y arquitectura seguros.
        - Normas de codificación seguras.
        - Uso de ambientes controlados para el desarrollo.

    e. Realizar actividades de capacitación en codificación segura en el equipo de desarrollo.

f. Evitar el uso de técnicas inseguras en las diferentes fases del desarrollo de software.
g. Realizar análisis de vulnerabilidades de código para los sistemas que se consideren críticos. Incluyendo todos los desarrollos de software.
h. Realizar análisis de errores de codificación comunes, documentarlos y promover su mitigación en el personal de desarrollo de software.
i. Incluir en las buenas prácticas de desarrollo de software el control de versiones para administrar el código por versiones, historial de cambios para facilitar la revisión y la recuperación del código.

E. Controles relacionados:

1. 8.8. – Gestión de vulnerabilidades técnicas
2. 8.29. – Pruebas de seguridad en desarrollo y aceptación

5.4.29 Pruebas de seguridad en desarrollo y aceptación

A. Objetivo de control: Llevar a cabo pruebas de funcionalidad de la seguridad durante el ciclo de desarrollo de sistemas de información y/o software, para las actualizaciones, ajustes, nuevos sistemas de información, nuevos desarrollos propios de la **DIAN** y/o software, así como establecer criterios de aceptación relacionados.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo encargadas de validar el cumplimento de los requisitos de seguridad de la información cuando las aplicaciones o el código se implementen en el entorno de producción.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

a. Definir el alcance de las pruebas, las cuales deben ser proporcionales a la importancia y naturaleza del sistema, aplicación y/o software.
b. Realizar pruebas durante los ciclos de desarrollo de los sistemas, elaborando un programa detallado de las actividades, entradas de las pruebas y las salidas esperadas bajo diferentes condiciones.
c. Incluir en las pruebas los siguientes requisitos de seguridad de la información:
   - Cumplir con el diligenciamiento de los formatos vigentes para pruebas funcionales por parte de los funcionarios dueños de los sistemas de información y/o software antes de cualquier puesta en producción, documento(s) que certifica(n) la realización de estas pruebas.
   - Certificar la ejecución de pruebas no funcionales y de seguridad por parte de la Dirección de Gestión de Innovación y Tecnología por medio del diligenciamiento del formato vigente para este fin y anexar las evidencias consolidadas.

- Evidenciar la certificación y aceptación por parte de las dependencias funcionales sobre las pruebas realizadas.

d. Llevar a cabo las pruebas de aceptación en un ambiente stanging, para verificar la conformidad del sistema y evitar introducir vulnerabilidades al ambiente de producción de la **DIAN**.
e. Verificar que el entorno de prueba, en la medida de lo posible, coincida con el entorno de producción, teniendo en cuenta la separación de los entornos de desarrollo, prueba y producción.
f. Establecer la ejecución de pruebas automáticas en los sistemas de información en la entidad.
g. Realizar pruebas para detectar errores en los sistemas de información en ambientes de pruebas y producción.
h. Establecer pruebas de rendimiento automáticas para identificar rápidamente los problemas de rendimiento de los sistemas de información.
i. Incluir pruebas de capacidad de los sistemas de información, definiendo límites de uso y capacidad máxima esperada, incluyendo pruebas cuando se superen los limites definidos.
j. Establecer pruebas de seguridad automáticas dinámicas (DAST) y estáticas (SAST) incluyendo pruebas de penetración automatizadas del proceso de compilación e implementación de los sistemas de información.

E. Controles relacionados:

1. 5.32. – Derechos de propiedad intelectual
2. 8.25. – Ciclo de vida de desarrollo segur.
3. 8.26. – Requisitos de seguridad de la aplicación
4. 8.27. – Principios de arquitectura e ingeniería de sistemas seguros
5. 8.28. – Codificación segura
6. 8.29. – Pruebas de seguridad en desarrollo y aceptación
7. 8.31. – Separación de los entornos de desarrollo, prueba y producción

5.4.30 Desarrollo subcontratado

A. Objetivo de control: Supervisar y efectuar seguimiento de la actividad de desarrollo de sistemas de información y/o software contratado externamente.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo, la cual debe asegurar que sean implementadas las medidas de seguridad de la información requeridas por la entidad en el desarrollo de sistemas subcontratados.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y tecnología debe:

a. Suministrar al desarrollador externo el modelo de amenazas debidamente aprobado.

b. Incluir en las cláusulas contractuales de los desarrollos subcontratados obligaciones relacionadas con el cumplimiento de buenas prácticas de desarrollo, entrega de pruebas y resultados de análisis y remediación de vulnerabilidades realizadas al desarrollo subcontratado.
c. Incluir en las cláusulas contractuales de desarrollos subcontratados, que en caso de que la entidad realice un análisis de vulnerabilidades e identifique en el software subcontratado alguna vulnerabilidad, el tercero debe realizar la remediación sin incurrir en costos adicionales.
d. Verificar y certificar las evidencias suministradas por el desarrollador externo, considerando como mínimo que:
   - Se haya realizado las pruebas suficientes para determinar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.
   - Se haya realizado pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas.
   - Se haya realizado las pruebas de seguridad estáticas y dinámicas de software.
   - Se haya entregado la documentación, componentes y artefactos creados.
   - Todo desarrollo ejecutado por un tercero debe usar como mínimo las prácticas referenciadas en OWASP o en Secure software development lifecycle.

E. Controles relacionados:

1. 5.32. – Derechos de propiedad intelectual
2. 8.25. – Ciclo de vida de desarrollo seguro
3. 8.26. – Requisitos de seguridad de la aplicación
4. 8.27. – Principios de arquitectura e ingeniería de sistemas seguros
5. 8.28. – Codificación segura
6. 8.29. – Pruebas de seguridad en desarrollo y aceptación
7. 8.31. – Separación de los entornos de desarrollo, prueba y producción

5.4.31 Separación de los entornos de desarrollo, prueba y producción

A. Objetivo de control: Reducir los riesgos de acceso o cambios no autorizados en los ambientes utilizados para el desarrollo de aplicaciones en la entidad, con la separación de ambientes de desarrollo, pruebas y producción.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología y la Subdirección de Infraestructura Tecnológica y de Operaciones, ambas encargadas de establecer y proteger adecuadamente los ambientes para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas de información y/o software.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad e integridad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

a. Definir los procedimientos, mecanismos o controles necesarios para reducir los riesgos de accesos o cambios no autorizados en ambientes utilizados en el ciclo de vida del desarrollo.
b. Proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Validar que todos los desarrollos de software que sean realizados por funcionarios, usuarios o contratistas dentro de la entidad, sean llevados a cabo en las plataformas de desarrollo de la entidad dispuestas para estas funciones.
b. Realizar la instalación de nuevas aplicaciones misionales o nuevas plataformas de forma tal que se integren al correcto funcionamiento de la red o de las aplicaciones en producción.
c. Definir y documentar las reglas para la transferencia de software del ambiente de pruebas a producción.
d. Verificar que todo cambio que se realice en los sistemas información en producción sea probado en un ambiente de pruebas antes de aplicarlo en los sistemas en producción, salvo que sean cambios de emergencia y que no afecten la continuidad del negocio.
e. Verificar que los compiladores, editores y otras herramientas de desarrollo y utilitarios del sistema, no sean accedidos desde sistemas de producción.
f. Verificar que en los ambientes de pruebas y producción los usuarios usen perfiles diferenciados; igualmente debe verificar que los menús desplieguen mensajes de identificación apropiados para reducir el riesgo de error.
g. Restringir el uso de datos personales en ambientes de desarrollo, conforme con lo establecido en la Ley 1581 de 2012.
h. Implementar y controlar el acceso a los ambientes de desarrollo seguro.
i. Realizar monitoreo, documentación y seguimiento a los cambios de estos ambientes y en los repositorios donde se almacena el código fuente.
j. Realizar las copias de respaldo en lugares seguros y fuera del entorno de desarrollo.
k. Monitorear y controlar los datos que se generen desde y hacia los ambientes de desarrollo seguro.

3. La Subdirección de Soluciones y Desarrollo debe:

a. Verificar que todo cambio que se realice en los sistemas información en producción sea probado en un ambiente de pruebas antes de aplicarlo en los sistemas en producción, salvo que sean cambios de emergencia y que no afecten la continuidad del negocio.
b. Validar que todos los desarrollos de software que sean realizados por funcionarios, usuarios o contratistas dentro de la entidad, sea llevados a cabo en las plataformas de desarrollo de la entidad dispuestas para estas funciones.

E. Controles relacionados:

1. 8.29. – Pruebas de seguridad en desarrollo y aceptación.
2. 8.33. – Información de prueba.

5.4.32 Gestión del cambio

A. Objetivo de control: Controlar los cambios que se presenten sobre los sistemas de información, aplicativos y/o servicios de la entidad a través de la definición de procedimientos formales de control de cambios a la infraestructura tecnológica de la entidad y dentro del ciclo de vida de desarrollo.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología, la Subdirección de Soluciones y Desarrollo y la Subdirección de Infraestructura Tecnológica y de Operaciones encargadas de controlar y reducir, al mínimo, el impacto sobre los cambios normales o de emergencia que se presenten sobre los sistemas de información, aplicativos, servicios y/o infraestructura de la entidad.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, integridad y disponibilidad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Evitar las modificaciones a los paquetes de software suministrados por los proveedores, los cuales se deben limitar a los cambios necesarios; y todos los cambios se deben controlar estrictamente.
   b. Definir y mantener actualizado el procedimiento de gestión de cambios de TI.
   c. Implementar un software para la administración de la gestión de los cambios de TI.
   d. Definir indicadores de gestión para el monitoreo de la gestión de cambios y toma de decisiones.
   e. Verificar que los paquetes suministrados por el vendedor-proveedor no hayan sufrido modificaciones antes de ser instalados.
   f. Incluir criterios de seguridad en los procedimientos de cambios de TI que implementen en la entidad.
   g. Cumplir las prácticas de gestión de cambios de TI, como es: registrar, planear, evaluar, autorizar, probar, implementar y cerrar todos los cambios de TI.

2. La Subdirección de Soluciones y Desarrollo debe:

   a. Registrar las solicitudes de cambio en el Formato de Requerimiento de Cambio (FRC), ya sea físicamente o en una herramienta diseñada para tal fin.
   b. Realizar un documento con las solicitudes programadas y la fecha/hora propuesta, de igual manera anexar un documento de interrupción planeada del servicio, donde se detallen los activos que están indisponibles y el tiempo previsto de inactividad.
   c. Evaluar los cambios desde la perspectiva de la misionalidad y de TI conforme a su nivel de riesgo. Los criterios para tener en cuenta, entre otros, son: seguridad, complejidad, experiencia, capacidad, disponibilidad, continuidad y criticidad.
   d. Verificar el cambio en ambientes de pruebas preparados para dicha actividad y obtener la aprobación técnica y funcional.
   e. Implementar los cambios autorizados a través del grupo técnico correspondiente, conforme a la fecha aprobada. En lo posible realizarlo a través de órdenes de servicio

para poder ser rastreadas. Se debe revisar el plan de reversión que debe estar explícitamente en la aprobación del cambio.

f. Revisar y cerrar los cambios para su evaluación en post implementación, donde se verifique si el cambio logró sus objetivos, si el solicitante y las partes interesadas están satisfechos, si no hay efectos secundarios inesperados y si se documentaron las lecciones aprendidas (cuando aplique).
g. Certificar en conjunto con los funcionarios dueños de los sistemas de información que los cambios implementados en los sistemas de información y/o software, y/o infraestructura, se hayan realizado en los tiempos definidos y no afectaron los procesos de negocio involucrados.
h. Mantener un registro actualizado de todos los sistemas de información y/o software, versión de estos, fecha de última compilación y responsable(s) de su mantenimiento y soporte.
i. Restringir el acceso a la documentación de sistemas de información, bibliotecas de códigos fuentes y programas ejecutables, solo a funcionarios autorizados. La excepción a este lineamiento son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios del o los sistemas de información.
j. Revisar los procedimientos de integridad y control de aplicaciones para que no estén comprometidos debido a los cambios en las plataformas de operaciones.
k. Verificar que los cambios en la plataforma operativa se hagan a tiempo para permitir las pruebas y revisiones apropiadas antes de cualquier implementación.
l. Considerar los siguientes aspectos, en caso de que un paquete de software necesite modificaciones:
    - Los niveles de riesgo en materia de integridad y afectación de controles de seguridad. En caso de verse comprometidos se deben tomar las medidas requeridas.
    - Si el paquete de software es suministrado por un proveedor externo, la Dirección de Gestión de Innovación y Tecnología debe solicitar el permiso de modificación y obtener el certificado para no perder su integridad.
    - Cualquier ajuste realizado debe ser documentado y debidamente aprobado por la Dirección de Gestión de Innovación y Tecnología a través del comité de cambios.
    - La Dirección de Gestión de Innovación y Tecnología, debe realizar una evaluación del impacto en caso de ser responsable del mantenimiento futuro del software como resultado de los cambios.
    - Revisar la compatibilidad con otros sistemas de información y/o software.

m. Probar y documentar los cambios completamente, de manera que se puedan aplicar de nuevo, si es necesario, a futuras actualizaciones de software.

3. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Verificar que todo cambio en los servicios de infraestructura y/o sistemas de información de la **DIAN**, cuenten con una solicitud de cambio y se deberán realizar siguiendo el procedimiento de gestión de cambios.
b. Seguir procesos formales de documentación, especificación, pruebas, control de calidad y gestión de la implementación, para todos los nuevos desarrollos, funcionalidades y cambios importantes a los sistemas y software existentes.
c. Cumplir con los lineamientos de gestión de cambios de este manual.
d. Evitar usar actualizaciones automáticas de software en los activos de información críticos, ya que algunas actualizaciones pueden hacer que fallen aplicaciones importantes.

e. Revisar las aplicaciones críticas del negocio y tras cambios que se presenten realizar pruebas, para que no haya impacto adverso en las operaciones o seguridad de los activos de información críticos de la **DIAN**.

E. Controles relacionados:

1. 5.30 – Preparación de las TIC para la continuidad del negocio
2. 5.37 – Procedimientos operativos documentados
3. 8.29 – Pruebas de seguridad en desarrollo y aceptación
4. 8.31 – Separación de los entornos de desarrollo, prueba y producción

5.4.33 Información de prueba

A. Objetivo de control: Realizar la selección, protección y control de los datos utilizados en las pruebas de los sistemas de información y efectuarlas de manera cuidadosa.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Soluciones y Desarrollo y la Subdirección de Infraestructura Tecnológica y de Operaciones quienes hacen uso de los ambientes de pruebas y el uso de los datos de pruebas en los sistemas de información de la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad e integridad.

D. Lineamientos:

1. La Subdirección de Soluciones y Desarrollo debe:

   a. Solicitar autorización por parte de usuario funcional cada vez que se copie información operacional de producción a un ambiente de desarrollo y/o pruebas.
   b. Borrar del ambiente de desarrollo y/o pruebas inmediatamente después de finalizar las pruebas, la información operacional que haya sido copiada.
   c. Registrar el copiado y uso de la información operacional para ejecutar auditorías, en los casos que sea requerido.
   d. Certificar que no se revele información confidencial de los ambientes de producción.
   e. No usar, durante la ejecución de pruebas en ambientes de desarrollo, datos que contengan información personal o información sensible que esté contenida en el ambiente de producción de los sistemas de información. Cuando se vayan a utilizar se deben anonimizar.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

   a. Aplicar los procedimientos de control de acceso, tanto a los ambientes de producción, como a los ambientes desarrollo y/o pruebas.
   b. Enmascarar la información entregada para las pruebas.
   c. Certificar que no se revela información confidencial de los ambientes de producción.

E. Controles relacionados:

1. 8.11 - Enmascaramiento de datos
2. 8.31 - Separación de los entornos de desarrollo, prueba y producción

5.4.34 Protección de los sistemas de información durante las pruebas de auditoría

A. Objetivo de control: Planificar y acordar los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos para minimizar las interrupciones en los procesos misionales.

B. Alcance: El alcance de este lineamiento aplica para la Dirección de Gestión de Innovación y Tecnología quien gestiona los mecanismos para que los sistemas tengan logs de auditoría y a la Oficina de Control Interno que dentro de los planes de auditoría incluye el análisis de logs en sistemas misionales.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad e integridad.

D. Lineamientos:

1. La Dirección de Gestión de Innovación y Tecnología debe:

    a. Definir los requisitos de auditoría para acceso a sistemas y datos y mecanismo de solicitud.
    b. Ofrecer el acceso al software y datos únicamente sea en modo de lectura para los procesos de auditoría.
    c. Otorgar acceso de solo lectura a los archivos file systems y si se requiere un acceso diferente se debe proveer copias aisladas, las cuales serán borradas una vez terminada la visita.
    d. Definir el alcance de las pruebas técnicas y los requisitos para solicitudes especiales y hacer el seguimiento de estas.
    e. Llevar a cabo el procedimiento de cambios las pruebas de auditoría en producción que se vayan a realizar.
    f. Verificar que las pruebas de auditoría en producción se realicen fuera del horario laboral, para evitar la indisponibilidad o lentitud de los sistemas de información y afectación de los servicios.
    g. Revisar logs para las operaciones de la auditoría.
    h. Establecer la relación de responsabilidades que tienen los usuarios que tengan acceso a los logs de auditoría.
    i. Incluir protocolos de autenticación en la red para los usuarios que tengan acceso a los logs de auditoría.
    j. Fortalecer la seguridad y optimizar los dispositivos de red y los controles asociados cuando un usuario realice acceso a los logs de auditoría de los sistemas.
    k. Validar y, si es necesario, aislar temporalmente subredes críticas para los procesos de auditoría de los sistemas.
    l. Deshabilitar protocolos de red vulnerables para el acceso a los logs de auditoría de los sistemas, esta actividad se debe realizar en toda la red.

2. La Oficina de Control Interno debe:

    a. Solicitar a la Dirección de Gestión de Innovación y Tecnología los accesos de solo lectura a los sistemas operativos que desee hacer auditoria de los sistemas dentro del plan de auditoría que disponga para el año.
    b. Indicar a la Dirección de Gestión de Innovación y Tecnología los tiempos requeridos de accesos a los logs de auditoría. En caso de que se vayan a utilizar herramientas para este propósito, se debe notificar y planificar su ejecución; las herramientas no pueden afectar el funcionamiento de los sistemas.
    c. Hacer uso adecuado y bajo las condiciones que indique la Dirección de Gestión de Innovación y Tecnología de los accesos que sean otorgados en los sistemas.

E. Controles relacionados:

1. 5.2 - Roles y responsabilidades de seguridad de la información

5.5 Controles adicionales

5.5.1 Analítica de datos

A. Objetivo de control: Hacer recolección, almacenamiento y procesamiento de inmensas cantidades de datos digitales y usar adecuadamente técnicas para la analítica de datos en la **DIAN**.

B. Alcance: El alcance de este lineamiento aplica para la Subdirección de Información y Analítica, encargada del gobierno de datos de la entidad. También aplica para la Subdirección de Infraestructura Tecnológica y de Operaciones, dependencia encargada de gestionar los accesos a grandes volúmenes de información en la **DIAN**.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad e integridad.

D. Lineamientos:

1. La Subdirección de Información y Analítica debe:

    a. Definir roles, responsabilidades y accesos requeridos para salvaguardar la seguridad de la información utilizada en los procesos y/o procedimientos de analítica de datos.
    b. Definir lista de datos requeridos para la analítica de datos, esta lista debe evitar el uso de datos que no sean requeridos para los propósitos de la dependencia.
    c. Definir métodos para el abastecimiento y recolección de los datos utilizados para la analítica de datos a través de métodos seguros que eviten la fuga de esta información.
    d. No utilizar de datos personales de ningún tipo. Los datos personales son de carácter estadístico, pero no pueden ser utilizados para hacer referencia a un titular en particular.
    e. Definir los lineamientos de transferencia de información, cuando se vaya a realizar trasferencia de los datos con otros posibles sistemas de analítica de datos.

f. Definir los modelos de analítica de datos con criterios de seguridad y privacidad de la información con el propósito que todos los involucrados tengan en cuenta estos criterios.
g. Definir en la evaluación y calibración de los datos para analítica de datos con criterios asociados a seguridad y privacidad de la información.
h. Incluir en el despliegue y monitoreo de la analítica de datos criterios de seguridad y privacidad de la información.
i. Identificar, tratar y hacer seguimiento de riesgos de seguridad de la información que involucren la analítica de datos.
j. Revisar la clasificación de la información utilizada, implementando los controles necesarios para mitigar la afectación a su confidencialidad, integridad y disponibilidad.
k. Definir procesos y/o procedimientos de analítica de datos con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

2. La Subdirección de Infraestructura Tecnológica y de Operaciones debe:

a. Disponer de espacios para la consulta de información para analítica de datos con los controles de acceso definidos en este manual.
b. Entregar únicamente la información solicitada por la dependencia de analítica de datos. Se debe evitar entregar información que no sea requerida para este propósito.

E. Controles relacionados:

1. 5.34 - Privacidad y protección de PII
2. 8.5 - Autenticación segura

5.5.2 Inteligencia artificial

A. Objetivo de control: Adelantar acciones requeridas para mitigar la afectación de la integridad, disponibilidad y confidencialidad de la información cuando se requiera gestionar alguna información de los procesos misionales de la **DIAN** a través del uso de la inteligencia artificial (IA).

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información, la cual debe promover el uso seguro de las tecnologías y a los jefes de las dependencias que inicien proyectos utilizando tecnología asociadas con inteligencia artificial.

C. Características de control:

1. Tipo de control: preventivo.
2. Propiedades de seguridad: confidencialidad, disponibilidad e integridad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

a. Asesorar los proyectos, tecnologías y/o procesos que utilicen capacidades de Inteligencia Artificial sobre la protección de la confidencialidad e integridad de la información que sea utilizada.

b. Incluir capacidades de soporte tecnológico para la gestión y monitoreo de riesgos de seguridad en Inteligencia Artificial, incluyendo respuesta a emergencias.
c. Incluir evaluaciones de seguridad en Inteligencia Artificial y crear capacidades de evaluación en seguridad de terceros y en las dependencias que utilicen estas tecnologías.

2. Los jefes de las dependencias deben:

a. Realizar previamente la revisión de la clasificación de la información que será utilizada en proyectos de inteligencia artificial, implementando los controles necesarios para mitigar la afectación a su confidencialidad, integridad y disponibilidad de la información que sea utilizada.
b. Aplicar los controles necesarios para el manejo de datos personales que sean recolectados, utilizados y analizados en los proyectos, tecnología y/o procesos de Inteligencia Artificial, teniendo en cuenta lo especificado en el "Manual para la protección de datos personales - MN-IIT-0062".
c. Aplicar un enfoque de gestión de riesgos de seguridad de la información en cada fase del ciclo de vida del proyecto.
d. Utilizar estándares internacionales, reglamentación nacional y de la industria para los requisitos de seguridad en el uso de Inteligencia Artificial.
e. Verificar que al iniciar un proyecto de Inteligencia Artificial se incluyan componentes para educar y capacitar al personal involucrado, promoviendo el desarrollo seguro y sostenible de estas tecnologías.
f. Verificar que la entidad esté alineada con las recomendaciones y sugerencias para abordar la formulación y gestión de los proyectos que incluyan el uso de Inteligencia Artificial (IA) detalladas en la guía: "Marco Ético para la Inteligencia Artificial en Colombia".

E. Controles relacionados:

1. 5.30 - Preparación de las TIC para la continuidad del negocio
2. 5.31 - Requisitos legales, estatutarios, reglamentarios y contractuales
3. 6.3 - Concientización, educación y capacitación en seguridad de la información
4. 8.8 - Gestión de vulnerabilidades técnicas

5.5.3 Amenaza interna

A. Objetivo de control: Promover la inclusión de loa análisis y gestión de amenazas internas en la seguridad y privacidad de la información para la promoción, protección e identificación de posibles incidentes.

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información quien debe promover la gestión de riesgos de seguridad de la información, la Dirección de Gestión de Innovación y Tecnología que debe promover la seguridad en ambientes digitales y a todo el personal de la **DIAN** que tenga acceso a la información institucional.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad, disponibilidad e integridad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Verificar que los sistemas informáticos y de telecomunicaciones que dispone la entidad posean el adecuado nivel de ciberseguridad ante amenazas internas, mediante el cumplimiento de las políticas, procedimientos y lineamientos de la **DIAN**, para realizar estas verificaciones se deben usar técnicas como análisis de vulnerabilidades (se recomienda utilizar sistemas de métricas para vulnerabilidades como CVSS1 y para aplicaciones ser encomienda OWASP) y las herramientas de seguridad informática que posee la entidad.
   b. Promover una cultura de uso seguro de la información y del ciberespacio para los usuarios internos de la entidad; mediante la ejecución periódica de campañas, programas de capacitación y/o sensibilización acerca de los riesgos de ciberseguridad, ciber amenazas, políticas de seguridad y acciones a seguir en caso de presentarse incidentes de seguridad de la información.
   c. Desarrollar actividades para la gestión y respuesta de incidentes relacionados con amenazas internas.
   d. Incluir dentro de la gestión de riesgos de seguridad de la información criterios relacionados con amenazas internas.

2. La Dirección de Gestión de Innovación y Tecnología debe:

   a. Definir los controles de seguridad en el proceso del ciclo de vida de desarrollo de software, para la creación y mantenimiento de software más seguro teniendo en cuenta amenazas internas.
   b. Implementar y cumplir las políticas, procedimientos, controles y lineamientos establecidos por la entidad relacionados con amenazas internas, con el fin de proteger y mantener disponibles los activos de información expuestos en el ciberespacio por medio de los sistemas informáticos y de telecomunicaciones.

3. Los funcionarios y terceros deben:

   a. Reportar mediante los canales de comunicación autorizados, cualquier evento o incidente interno de seguridad relacionado con la información y/o los recursos tecnológicos, para que se registre y se le dé el trámite necesario.

E. Controles relacionados:

1. 6.3 - Concientización, educación y capacitación en seguridad de la información
2. 6.8 - Reporte de eventos de seguridad de la información

5.5.4 Seguridad en diseño

A. Objetivo de control: Integrar la seguridad de la información en el diseño de las actividades que realice la entidad, para mitigar riesgos de seguridad de la información desde las primeras fases de cualquier iniciativa institucional.

[1] CVSS: Common Vulnerability Scoring System

B. Alcance: El alcance de este lineamiento aplica para la Oficina de Seguridad de la Información quien debe promover la gestión de riesgos de seguridad de la información y los jefes de las dependencias que inicien actividades en las que involucren información.

C. Características de control:

1. Tipo de control: preventivo y detectivo.
2. Propiedades de seguridad: confidencialidad, disponibilidad e integridad.

D. Lineamientos:

1. La Oficina de Seguridad de la Información debe:

   a. Promover una cultura de criterios de seguridad y privacidad de la información en el diseño de todas las iniciativas que se tengan en la entidad, siempre y cuando estas utilicen información, aunque no se lleve un proceso formal de proyectos en estas iniciativas.

2. Los jefes de las dependencias deben:

   a. Identificar los activos de información que puedan intervenir en los proyectos, clasificarlos, valorarlos y usarlos para la identificación de riesgos del proyecto.
   b. Contemplar los componentes de seguridad de la información, riesgos de seguridad de la información, en las iniciativas desde la fase del diseño de estos, aunque no se lleve un proceso formal de proyectos en estas iniciativas.
   c. Determinar la criticidad de la información que se utiliza en las iniciativas desde el diseño de estas, aunque no se lleve un proceso formal de proyectos en estas iniciativas.
   d. Incluir la privacidad de la información y los datos personales en el análisis de riesgos previo al diseño de las iniciativas, aunque no se lleve un proceso formal de proyectos en estas iniciativas.
   e. Gestionar los respectivos acuerdos de confidencialidad y de entrega de información de acuerdo con la normatividad vigente en la entidad, en el caso de participación de terceros.

E. Controles relacionados:

1. 5.8 - Seguridad de la información en la gestión de proyectos
2. 5.9 - Inventario de información y otros activos asociados

5 MARCO LEGAL Y NORMATIVO

Para el marco legal y normativo, se puede consultar el Normograma de la Oficina de Seguridad de la Información, el cual contiene las leyes, decretos, resoluciones y demás documentos aplicables como políticas, manuales, circulares, documentos CONPES y, en general, toda la normatividad relacionada con los temas tratados en este Manual de Políticas y Lineamientos de Seguridad de la Información. Consulte el normograma aquí.

https://diancolombia.sharepoint.com/sites/diannetpruebas/Areas/OSI/Paginas/Normograma.aspx

Los procedimientos, instructivos y formatos relacionados en este Manual de Políticas y Lineamientos de Seguridad de la Información se encuentran en este listado maestro de documentos de la entidad:

https://diancolombia.sharepoint.com/sites/diannetpruebas/procesos/Paginas/Listado-Maestro-VI.aspx

6 ACCIONES DE IMPLEMENTACIÓN

Las dependencias de la **DIAN** que tengan asignadas responsabilidades relacionadas en este manual deben definir un plan de acción y hacer seguimiento, para dar cumplimiento a éste.

Este Plan deberá ser elaborado y entregado a la Oficina de Seguridad de la Información, dentro de los seis (6) meses siguientes a la publicación del presente Manual. La Oficina de Seguridad de la Información puede realizar verificación de este cumplimiento.

7 CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	13/01/2022	31/07/2022	Versión inicial	Información Pública
2	1/08/2022	28/09/2022	Versión 2 que reemplaza lo establecido en la versión 1. Actualiza los lineamientos establecidos en los numerales: "20. Inteligencia Artificial "y, "20.1 Analítica de Datos".	Información Pública
3	28/09/2022	17/11/2022	Versión 3 que anexa la identificación de los controles de seguridad digital en los numerales: 14.1.1 Análisis y especificación de los requisitos de seguridad de la información. 14.2.5 Principios de construcción de sistemas seguros.	Información Pública
4	18/11/2022	22/10/2023	Se derogan las siguientes circulares: Circular de Uso del servicio de impresión No.000033 del 08 de sept 2015 Circular de Teletrabajo No.000496 mayo 2022 Circular de Uso de computadores portátiles No.000026 del 08 de agosto de2016 Circular de Cifrado de datos - No.00013 del 4 abril 2017 Circular de Uso de medios removibles - No. No.00017 del 30 de agosto de 2019.	Información Pública

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
5	23/10/2023		Actualización de la Norma ISO 27001 y 27002 en la versión 2022. Se modifica la plantilla del documento.	Información Pública

Elaboró:	*Oficina de Seguridad de la Información* ***Elaboración Técnica***		*Oficina de seguridad de la información*
	Tito Alejandro Menjura Murcia ***Elaboración metodológica***	*Gestor II*	*Coordinación de Procesos y Riesgos Operacionales*
Revisó:	*Fanny Constanza Hernández Arias*	*Gestor IV*	*Oficina de seguridad de la información*
Aprobó:	*Hugo Alcides Pérez Pinilla*	*Jefe (E)*	*Oficina de seguridad de la información*