



Departamento Nacional de Planeación



**MANUAL OPERATIVO DEL COMPONENTE DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
(GSI)**

**DEPARTAMENTO NACIONAL DE PLANEACIÓN
BOGOTÁ, 2025**



TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
2. ARTICULACIÓN CON LA POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN.....	4
3. OBJETIVOS	5
3.1. Objetivo General	5
3.1.1. Objetivos específicos.....	5
3.1.2. Objetivos estratégicos del DNP	5
3.1.3. Alineación con los objetivos estratégicos	6
4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	6
5. NORMATIVA RELACIONADA CON SEGURIDAD DE LA INFORMACIÓN.....	7
6. MARCO DE REFERENCIA DEL COMPONENTE DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN.....	7
7. DEFINICIONES.....	7
8. CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD	8
9. ALCANCE/APLICABILIDAD.....	8
10. MODELO DE GOBERNANZA DE LA SEGURIDAD DIGITAL	9
10.1. Alta Dirección	10
10.2. Comité Institucional de Gestión y Desempeño.....	10
10.3. Secretaría General	11
10.4. Oficina de Control Interno Disciplinario	11
10.5. Subdirección de Gestión del Talento Humano	12
10.6. Subdirección de Contratación	12
10.7. Subdirección Administrativa y Relacionamiento con la Ciudadanía.....	13
10.8. Oficina Asesora de Comunicaciones.....	14
10.9. Oficina de Control Interno	14
10.10. Oficina Asesora de Planeación	14
10.10.1. Profesional continuidad de negocio – en el marco del Modelo de Operación por Proceso	15
10.11. Oficina Asesora Jurídica	15
10.12. Jefes de dependencia, coordinadores de grupo y/o supervisores	15
10.13. Gestores SIG.....	16
10.14. Líderes funcionales, técnicos y administradores de los sistemas de información.....	17
10.15. Colaboradores (funcionarios, contratistas, pasantes)	18
10.16. Oficina de Tecnología y Sistemas de Información	18
10.16.1.1. Asesor seguridad de la información.....	19
10.16.1.2. Oficial de seguridad de la información.....	20
10.16.2. Grupo de Planeación y Gestión de TIC	20
10.16.2.1. Especialista continuidad de negocio del componente tecnológico	20
10.16.3. Grupo de Infraestructura tecnológica.....	21
10.16.3.1. Especialista WAF y DRP.....	21
10.16.4. Grupo de soporte a usuarios.....	21
10.16.5. Grupo de Gestión de Sistemas de Información	22



10.16.6.	Centro de servicios	22
10.16.6.1.	Gerente de Proyecto Centro de Servicios.....	22
10.16.6.2.	Analista y Especialista de Infraestructura de Procesamiento y Almacenamiento	23
10.16.6.3.	Operador Infraestructura de Backup.....	23
10.16.6.4.	Operador Infraestructura Eléctrica	24
10.16.6.5.	Especialista y Operador de Infraestructura de Redes.....	24
10.16.6.6.	Especialistas Seguridad Informática	25
10.16.6.7.	Especialista en balanceador/firewall de aplicaciones (WAF)	25
10.16.6.8.	Centro de operaciones SOC	25
10.16.6.9.	Gestor de Calidad	26
10.16.6.10.	Líder gestor de Aplicaciones	26
10.16.6.11.	Mesa de ayuda y soporte	26
10.17.	Proveedores	27
10.18.	Usuarios externos sistemas de información	27
1.	SANCIONES	28
11.	ESTRUCTURA DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN	28
11.1.	Premisas básicas de seguridad de la información	28
11.1.1.	Confidencialidad	28
11.1.2.	Disponibilidad	29
11.1.3.	Integridad.....	29
11.1.4.	Autenticidad	29
11.1.5.	Auditabilidad	29
11.1.6.	No repudio	29
12.	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30
12.2.	Seguridad organizacional.....	30
12.3.	Seguridad del recurso humano	31
12.4.	Gestión de los activos de información	34
12.5.	Control de acceso	43
12.6.	Criptografía.....	46
12.7.	Seguridad física y ambiental	47
12.8.	Gestión de operaciones	51
8.2.	Políticas Scraping	58
12.9.	Gestión de comunicaciones	62
12.10.	Adquisición, implementación y mantenimiento de sistemas.....	62
12.11.	Políticas relación con proveedores.....	65
12.12.	Administración de incidentes de seguridad de la información.....	68
12.13.	Administración de la seguridad de la información en la continuidad del negocio.....	69
12.14.	Cumplimiento	71
12.15.	Protección de datos.....	71
13.	CAPACITACIÓN E INDUCCIÓN EN SEGURIDAD DE LA INFORMACIÓN.....	71
14.	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL CGSI	72
15.	APROBACIÓN Y REVISIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	74



1. INTRODUCCIÓN

El presente manual contiene las políticas de seguridad de la información y directrices que deben cumplir las personas usuarias del DNP, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en la información digital.

Las políticas están orientadas a proteger los activos de información en los ambientes relacionados con TIC, en los cuales se procesan, operan, almacenan, transmiten o usan información institucional a los que les aplican los controles correspondientes para su adecuada protección, para fomentar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como Internet y el correo electrónico mitigando los riesgos que puedan afectar los activos de información digital institucionales.

Por lo anterior, se establecen las siguientes políticas generales en seguridad de la información, basados en la norma NTC ISO 27001:2013 y el [Modelo de Seguridad y Privacidad de la Información \(MSPI\)](#) de MINTIC, las cuales ayudarán a ofrecer servicios seguros, confiables y oportunos en la Entidad, como lo dictan las directrices de la [Política Gobierno Digital](#) y la [Política de Seguridad Digital](#), para brindar mayor confianza de los ciudadanos hacia las instituciones del estado. La Entidad está en el proceso de la transición a las normas ISO 27001:2022 e ISO 27002:2022.

Las políticas están definidas con un código que describe el número de capítulo y el estándar así: [PL02-ES1] corresponde al estándar número uno (1) de la política número dos (2).

2. ARTICULACIÓN CON LA POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

El componente de seguridad de la información (GSI) está alineado con la [Política del Sistema Integrado de Gestión](#) *“El Departamento Nacional de Planeación, está comprometido con el desarrollo sostenible e incluyente del país, a través del ciclo de planeación, cuyos productos atienden las necesidades de la nación y consideran las características de los territorios. Esto lo logra y consolida a través de su Sistema Integrado de Gestión, el cual cumple normativamente y articula los elementos de planeación y gestión institucional, con un enfoque preventivo basado en riesgos, alta capacidad técnica, compromiso de su talento humano, gestión del conocimiento clave, **información confiable y segura**, recursos tecnológicos, financieros y de infraestructura, en un entorno de trabajo seguro, saludable, responsable con las personas y el ambiente; que contribuyen a una cultura organizacional íntegra y transparente que trasciende hasta nuestros grupos de valor y que impacta en la satisfacción de sus necesidades, el mejoramiento continuo de la gestión institucional y el aumento de valor público”*.

La política del SIG incluye el componente de seguridad de la información, expresamente en el compromiso frente a *“..., información confiable y segura”*

Así mismo, el objetivo general del componente de seguridad de la información se encuentra articulado con:

- El [propósito No. 2 de la Política del Sistema Integrado de Gestión](#) definida como: *“Gestionar el tratamiento y acceso a la información institucional, el manejo adecuado de los activos de información, protegiendo su integridad, disponibilidad, confidencialidad y privacidad.”*
- El [Manual del SIG](#): Establece que la Oficina de Tecnología y Sistemas de información es el responsable operacional del componente de seguridad de la información.



- [Resolución interna 442 de 2009](#): Acto administrativo de creación del Sistema de Gestión de Seguridad de la Información en el DNP.
- [Resolución interna 0923 de 2022](#): Acto administrativo del Comité Institucional de Gestión y Desempeño y establece sus funciones respecto a las políticas de gobierno y seguridad digital.
- El [Plan de Seguridad y Privacidad de la Información](#), el [Plan estratégico de Seguridad y Privacidad de la información](#) y el [Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información](#).

Para el Departamento Nacional de Planeación, la protección de la información busca la mitigación del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad acorde con las necesidades de los diferentes grupos de interés identificados.

3. OBJETIVOS

3.1. Objetivo General

Gestionar la [confidencialidad](#), [integridad](#) y [disponibilidad](#) de la información digital de software, hardware, servicios tecnológicos, servicios de información (aplicativos, portales, sistemas de información) bajo un enfoque tecnológico de seguridad informática de acuerdo con las disposiciones normativas establecidas por las Entidades rectoras en la materia y los lineamientos del Sistema Integrado de Gestión (SIG).

3.1.1. Objetivos específicos

El componente de seguridad de la información ha definido cuatro objetivos específicos identificados con la sigla OECS para fortalecer la implementación de la protección de la información digital, la gestión de la seguridad informática protegiendo la confidencialidad, integridad y disponibilidad de la información digital institucional.

- **OECS1:** Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de las personas usuarias de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.
- **OECS2:** Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información.
- **OECS3:** Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.
- **OECS4:** Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.

El compromiso del DNP para satisfacer los requisitos aplicables relacionados con la seguridad de la información está descrito en el primer objetivo específico y el compromiso con la mejora continua del componente de gestión de la seguridad de la información está descrito en el segundo objetivo específico.

3.1.2. Objetivos estratégicos del DNP

Los objetivos estratégicos (OE) del DNP pueden ser consultados en la [sede electrónica](#):

Este documento es fiel copia del original que reposa en la Oficina Asesora de Planeación. Su impresión se considera copia no controlada



- **OE1:** Articular y coordinar el diseño y fortalecimiento de los lineamientos de política y los instrumentos de planeación de largo y mediano plazo, con un enfoque integral entre el territorio y los sectores Inversión Pública.
- **OE2:** Diseñar e implementar estrategias que mejoren la calidad de la inversión pública. Redefinir la planeación y gestión de la inversión pública considerando la concurrencia de fuentes con un enfoque de impacto y eficiencia Capacidad Territorial.
- **OE3:** Fortalecer las capacidades técnicas de los sectores y territorios que promuevan la productividad, la competitividad, la sostenibilidad y la equidad. Posicionar al DNP como referente en gestión institucional articulada, innovadora y efectiva.
- **OE4:** Mejorar el desempeño institucional que garantice el cumplimiento de los objetivos y metas definidos por la Entidad. Promover la transformación regional con enfoque del territorio, hacia la productividad, la competitividad y la sostenibilidad en el mediano y largo plazo Gestión Integral Institucional.

3.1.3. Alineación con los objetivos estratégicos

La alineación de los objetivos representa la estrategia y requisitos del negocio que aplican al componente de seguridad de la información.

Tabla 1: Alineación de Objetivos estratégicos con los objetivos del Componente de Seguridad de la Información

OE/ OECS	OECS1	OECS2	OECS3	OECS4
OE1	X			X
OE2	X			
OE3	X			X
OE4	X	X	X	X

Fuente: Elaboración OTSI

El OE2 está alineado al OECS1 al implementar controles enfocados a la protección de la confidencialidad, integridad, disponibilidad de la información. Promover la mejora continua de los procesos y del servicio a las personas usuarias, mediante la identificación y tratamiento de los riesgos sobre los activos de información que puedan afectar la respuesta oportuna de sus requerimientos.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La Entidad ha adoptado los principios de seguridad incluidos en el Modelo de Seguridad y Privacidad de la Información de MINTIC:

1. Las responsabilidades frente a la seguridad de la información están definidas en el M-PG-07 Manual Operativo de seguridad de la información, compartidas y publicadas en la [intranet](#) y en la [sede electrónica](#) del DNP y aceptadas por cada uno de las personas colaboradoras proveedoras o terceros. Para las personas colaboradoras la aceptación se realiza en el Manual de Funciones de la Entidad porque en los conocimientos básicos o esenciales está incluido el Sistema Integrado de Gestión y el componente de seguridad de la información es parte de éste y para los proveedores y terceros la aceptación se realiza en las cláusulas contractuales.
2. El DNP protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos de negocio.



3. El DNP controla la operación de sus procesos del [Sistema Integrado de Gestión](#) garantizando la seguridad de los recursos tecnológicos y las redes de datos.
4. El DNP implementa los controles de acceso para la información digital, sistemas y recursos de red.
5. El DNP vela porque la seguridad informática sea parte integral del ciclo de vida de los sistemas de información institucionales.
6. El DNP realiza una adecuada gestión de los eventos de seguridad informática.
7. El DNP vela por el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas relacionadas con seguridad digital, seguridad de la información y seguridad informática.

5. **NORMATIVA RELACIONADA CON SEGURIDAD DE LA INFORMACIÓN.**

El DNP como Entidad Pública cumple con normativa legal vigente que incluye leyes, decretos y resoluciones, que se han tenido en cuenta para la implementación del componente de gestión de seguridad de información se encuentran identificadas y documentadas en el Normograma y otros documentos de Origen Externo en el [Anexo 1 - Normograma y otros documentos de origen externo](#). La relación de la norma y los controles se seguridad está en la [declaración de aplicabilidad](#).

Los contratos asociados al componente de seguridad de la información están publicados en el [SECOP II](#)¹.

6. **MARCO DE REFERENCIA DEL COMPONENTE DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN**

Marco de referencia interno normativo incluye que la Oficina de Tecnología y Sistemas de la Información (OTSI) tiene la responsabilidad de implementar el Modelo de Seguridad y Privacidad de la información (MSPI) y gestionar incidentes informáticos en materia de seguridad de la información y es el responsable operacional del componente de gestión de seguridad de la información conforme está incluido en el Manual del SIG. La evaluación periódica del cumplimiento de las políticas de Gobierno Digital y Seguridad Digital se realiza a través del Formulario Único Reporte de Avances de la Gestión (FURAG) del Modelo Integrado de Planeación y Gestión de la Función Pública, el Índice de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el autodiagnóstico del MSPI.

Los marcos de referencia normativos están incluidos en el [Anexo 1 - Normograma y otros documentos de origen externo](#), las amenazas actuales y proyectadas se encuentra incluidas en el [Anexo 6 - Contexto Departamento Nacional de Planeación](#) y [Anexo 6a - Resumen de Contexto DNP](#).

7. **DEFINICIONES**

- **CGSI:** Es el Componente de Seguridad de la información, es el mismo Sistema de Gestión de Seguridad de la información (SGSI) que menciona la norma ISO 27001:2013.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la Entidad antes de crear nuevas políticas.
- **Filtro de contenido:** Programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

¹ El SECOP II funciona como una plataforma transaccional con cuentas para las Entidades Estatales y los Proveedores. Fuente <https://www.colombiacompra.gov.co/secop-ii/que-es-el-secop-ii>



- **Firewall:** Aplicación utilizada para controlar las comunicaciones, permitiéndolas o prohibiéndolas.
- **Incidente grave:** El incidente de seguridad digital debe atenderse de en un tiempo menor a 6 horas, contadas a partir del reporte al CSIRT de Gobierno.
- **Incidente muy grave:** El incidente de seguridad digital debe atenderse de forma inmediata y menor a 2 horas, contadas a partir del reporte al CSIRT de Gobierno.
- **Licencias de Software:** Es el derecho a perpetuidad de uso del Software sin tiempo de caducidad establecido, la Entidad lo adquiere y/o renueva para uso en la plataforma tecnológica (equipos de cómputo y servidores). El derecho de uso es para una versión en específico y se renueva periódicamente el soporte, mantenimiento y actualización con el fin de tener acceso a las últimas versiones disponibles.
- **Plataforma tecnológica:** Infraestructura, software base, comunicaciones, etc.
- **Política:** Declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.
- **Seguridad de la información:** Este principio de la Política de Gobierno Digital busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las Entidades del Estado, y de los servicios que prestan al ciudadano.
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Seguridad informática:** se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.
- **Servicios de Información:** Representan los portales (páginas web) y sistemas de información desarrollados a la medida para el Departamento Nacional de Planeación (DNP).
- **Servicios de Office 365:** Correo electrónico, One Drive, SharePoint, Teams, Forms, Power BI, Viva Engage.
- **Suscripción de Software:** Es el derecho de uso del Software con tiempo de caducidad establecido, donde las suscripciones implican para el DNP un pago inicial y el pago de renovaciones periódicas. Mientras la suscripción esté activa, se tiene derecho de uso sobre los productos y servicios contratados.
- **Tercero:** Entidades externas al DNP.
- **Usuarios:** Personas funcionarias, contratistas, pasantes, proveedores y terceras partes del DNP.

El [Glosario Manual Operativo](#) contiene la definición de los términos, siglas y abreviaciones usadas en el presente manual.

8. CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

La [declaración de aplicabilidad](#) contiene la clasificación de las políticas del Manual Operativo de Gestión de Seguridad de la Información de acuerdo con lo solicitado en el control 5.1.1 (Políticas para la seguridad de la Información) de la Norma ISO 27001:2013.

9. ALCANCE/APLICABILIDAD

El presente manual operativo aplica para las personas funcionarias, contratistas, pasantes y terceros del Departamento Nacional de Planeación los cuales se encuentran ubicados en Bogotá y en sus sedes país, así



como para los todos los procesos del [Sistema Integrado de Gestión](#), información digital y tecnológica de la Entidad.

El cumplimiento de lo estipulado en el M-PG-07 Manual Operativo de seguridad de la información es obligatorio para todas las personas usuarias incluyendo terceros, y en caso de que se incumplan o infrinjan las políticas de seguridad por negligencia o intencionalmente, el DNP tomará las acciones disciplinarias y legales correspondientes.

Las responsabilidades frente a la seguridad de la información están definidas en el presente Manual Operativo de seguridad de la información, compartidas y publicadas en la [intranet](#) y en la [sede electrónica](#) del DNP y aceptadas por cada uno de las personas colaboradoras, proveedoras, o terceros.

10. MODELO DE GOBERNANZA DE LA SEGURIDAD DIGITAL

El modelo de gobernanza contiene la estructura operacional de los roles que participan en la gestión de la seguridad de la información. Los niveles de gobernanza que enmarcan las acciones para la implementación seguridad digital en el DNP son los siguientes:

- **Nivel estratégico:** Es el nivel en el que se definen las políticas y las prioridades estratégicas de seguridad de la información y seguridad digital. Determina los objetivos a largo plazo y el modo en que las múltiples partes interesadas han de interactuar entre sí.
- **Nivel táctico:** Es el nivel en el que se elaboran los planes, procesos y procedimientos para coordinar las actividades de seguridad digital. Efectúa el control de la gestión realizada por el nivel operacional y soporta las decisiones que se toman y que afectan a las múltiples partes interesadas.
- **Nivel operacional:** Es el nivel en el que se implementan, ejecutan actividades y tareas rutinarias definidas por el nivel táctico.

Gráfica 1: Modelo de Gobernanza de Seguridad digital en DNP



Fuente: Elaboración OTSI



10.1. Alta Dirección

La Alta Dirección es la máxima autoridad en el sistema. Está conformada por Director(a) General, Subdirector(a) General de Prospectiva y Desarrollo Nacional, Subdirector(a) General de Inversiones, Seguimiento y Evaluación, Subdirector(a) General de Descentralización y Desarrollo Territorial, Subdirector(a) General del Sistema General de Regalías y Secretario(a) General, quienes aseguran la orientación y estructura estratégica y táctica del SIG, la definición y comunicación de las responsabilidades y autoridades requeridas, y realizan las revisiones al desempeño del SIG y aseguran la disponibilidad de recursos².

Las responsabilidades de la Alta Dirección en el componente de seguridad de la información son:

- Fomentar el cumplimiento de las políticas y lineamientos definidos en materia de seguridad de la información en los colaboradores de la Entidad.
- Apoyar la difusión y sensibilización de la seguridad de la información en la Entidad.
- Propender por la asignación de recursos económicos que permitan el cumplimiento de los objetivos del componente de seguridad de la información y la gestión de la continuidad de negocio.
- El [Manual del SIG](#) en el numeral “*Compromiso de la Alta Dirección*” describe los compromisos transversales de la Alta Dirección.

10.2. Comité Institucional de Gestión y Desempeño

El Comité Institucional de Gestión y Desempeño está conformado por el/la Director(a) General o su delegado, el/la Secretario(a) General, quien lo presidirá; el/la Subdirector(a) General de Prospectiva y Desarrollo Nacional o su delegado, el/la Subdirector(a) General de Inversiones, Seguimiento y Evaluación o su delegado, el/la Subdirector(a) General de Descentralización y Desarrollo Territorial o su delegado, el/la Subdirector(a) General del Sistema General de Regalías Territorial o su delegado, el/la Subdirector(a) de Gestión del Talento Humano, el/la Subdirector(a) Administrativo y de relacionamiento con la Ciudadanía, el/la Subdirector(a) Financiero, el/la Subdirector(a) Contractual, el/la Jefe de la Oficina de Tecnología y Sistemas de Información, el/la Jefe de la Oficina Asesora de Comunicaciones, el/la Jefe de la Oficina Asesora Jurídica, el/la Jefe de la Oficina Asesora de Planeación quien será el Secretario Técnico, el/la Jefe de la Oficina de Control Interno, con voz y sin voto.³

Las responsabilidades del Comité Institucional de Gestión y Desempeño en el componente de seguridad de la información son:

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de gobierno digital, seguridad digital y de la información.
- Evaluar las situaciones que hayan dado lugar a un incumplimiento de seguridad de la información y las recomendaciones presentadas por la Oficina de Tecnología y Sistemas de Información.
- Aprobar las dadas de bajas de software.
- Autorizar los ejercicios de Ethical hacking e ingeniería social propuestos por la Oficina de Tecnología y Sistemas de Información.
- Aprobar y realizar seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.

² Fuente Manual del SIG

³ Fuente Manual del SIG



- Aprobar acciones, mejores prácticas y resultados previstos que contribuyan al mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información de MINTIC.
- Promover adopción de las políticas de seguridad de la información en la cultura organizacional y procesos de la Entidad.
- Vigilar el cumplimiento de la normatividad relacionada con la mejora continua de la seguridad de la información.
- Adoptar las decisiones que permitan la gestión y mitigación de riesgos críticos de seguridad de la información.

Gestión de crisis y continuidad del negocio con la finalidad asegurar la capacidad de recuperación ante incidentes graves de acuerdo [Manual para la Gestión de Continuidad del Negocio](#). Seguimiento a los indicadores de desempeño para medir la efectividad en la gestión de la seguridad de la información y los resultados de monitoreo de la eficacia de las políticas establecidas.

10.3. Secretaría General

La Secretaria General formula y hace seguimiento a las acciones necesarias para cumplir las normas y disposiciones que regulan los procedimientos y trámites de carácter administrativo y presupuestal de los planes, programas y proyectos de la Entidad, del Fondo Nacional de Regalías en liquidación y del Sistema General de Regalías según la normatividad vigente⁴.

Las responsabilidades de la Secretaria General en el componente de seguridad de la información son:

- Evaluar las situaciones que hayan dado lugar a un incidente de seguridad de la información reportados por la Oficina de Tecnología y Sistemas de Información.
- Liderar la continuidad de negocio en la Entidad.

10.4. Oficina de Control Interno Disciplinario

En el marco de lo ordenado en el artículo 12 del Código General Disciplinario, el Decreto 1893 de 2021, dispuso la creación entre otras, de la Oficina de Control Interno Disciplinario, adscrita a la Secretaría General, encargada del ejercicio de la acción disciplinaria contra las personas funcionarias y ex funcionarias de la Entidad, así como, de la promoción de políticas, planes y programas de prevención, enfocados en la sensibilización respecto de comportamientos generadores de falta disciplinaria. Así las cosas, la Oficina de Control Interno Disciplinario - OCID, adelanta la etapa de Juzgamiento del proceso disciplinario, la cual inicia con la notificación del pliego de cargos o auto de citación a audiencia, según corresponda, hasta la notificación del fallo de primera instancia. En ese sentido, las funciones de la oficina se sustentan en dos pilares, el ejercicio de la potestad disciplinaria como autoridad en la materia y en las gestiones propias de prevención y corrección.⁵

Las responsabilidades de la Oficina de Control Interno Disciplinario en el componente de seguridad de la información son:

- Evaluar las situaciones que hayan dado lugar a un incidente de seguridad de la información reportados por la Oficina de Tecnología y Sistemas de Información.
- Participar en las actividades relacionadas con la continuidad de negocio en la Entidad.

⁴ https://www.dnp.gov.co/LaEntidad/_equipo-directivo/Paginas/secretaria-general.aspx

⁵ https://www.dnp.gov.co/LaEntidad/_secretaria-general/oficina-control-interno-disciplinario/



10.5. Subdirección de Gestión del Talento Humano

La Subdirección de Gestión del Talento Humano planea, organiza, dirige, supervisa y controla las actividades relacionadas con el desarrollo y administración del Recurso Humano del Departamento Nacional de Planeación (DNP), según las disposiciones legales, normativas, institucionales y los criterios técnicos relacionados⁶.

Las responsabilidades de la Subdirección de Gestión del Talento Humano en el componente de seguridad de la información son:

- Gestionar las actividades relacionadas con teletrabajo.
- Informar a la Oficina de Tecnología y Sistemas de Información y a las personas con el rol de [líderes de técnicos](#) de los sistemas de información, portales y aplicativos el ingreso, retiro y rotación de personas funcionarias y/o pasantes.
- Hacer uso adecuado de las listas de distribución para envíos masivos correos.
- Informar a la Oficina de Tecnología y Sistemas de Información las personas funcionarias autorizados para firmar digitalmente.
- Participar en las actividades relacionadas con la continuidad de negocio en la Entidad.
- Realizar la gestión de vinculación, capacitación, desvinculación de las personas funcionarias y pasantes dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.
- Implementar procesos de selección que incluyan verificación de antecedentes y evaluaciones de confiabilidad con criterios de seguridad de la información.
- Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación.
- Integrar el entrenamiento en seguridad de la información dentro del proceso de inducción y reintroducción del personal
- Apoyar al responsable de Seguridad de la Información en la implementación del plan de concientización y sensibilización en seguridad y privacidad de la información.

10.6. Subdirección de Contratación

La Subdirección de Contratación asesora a la Secretaria General en relación con los procesos de contratación en sus diferentes etapas y en los cuales sea parte el Departamento Nacional de Planeación (DNP), según las disposiciones normativas vigentes⁷.

Las responsabilidades de la Subdirección de Contratación en el componente de seguridad de la información son:

- Informar a la Oficina de Tecnología y Sistemas de Información y a los [líderes de técnicos](#) de los sistemas de información, portales y aplicativos el ingreso, retiro y rotación de personas contratistas.
- Apoyar a las dependencias en la cesión de derechos patrimoniales del software.
- Participar en las actividades relacionadas con la continuidad de negocio en la Entidad.

⁶ https://www.dnp.gov.co/LaEntidad/_secretaria-general/subdireccion-gestion-talento

⁷ https://www.dnp.gov.co/LaEntidad/_secretaria-general/Subdireccion-contratacion/contratacion/Paginas/default.aspx



- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Apoyar los lineamientos de seguridad para la gestión con proveedores
- Realizar la gestión de vinculación, capacitación, desvinculación de las personas contratistas dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.
- Implementar procesos de selección que incluyan verificación de antecedentes y evaluaciones de confiabilidad con criterios de seguridad de la información.
- Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación.
- Integrar el entrenamiento en seguridad de la información dentro del proceso de inducción y reintroducción del personal
- Apoyar al responsable de Seguridad de la Información en la implementación del plan de concientización y sensibilización en seguridad y privacidad de la información.

10.7. Subdirección Administrativa y Relacionamento con la Ciudadanía

La Subdirección Administrativa y Relacionamento con la Ciudadanía dirige y guía la prestación de los servicios de apoyo logístico a las diferentes dependencias del Departamento Nacional de Planeación (DNP), brindando las condiciones físicas adecuadas, de calidad y confort a todas las personas funcionarias y colaboradores para el desarrollo eficiente de sus actividades misionales⁸.

Las responsabilidades de la Subdirección Administrativa y Relacionamento con la Ciudadanía en el componente de seguridad de la información son:

- Ingresar a la póliza de seguridad los bienes adquiridos, transferidos y/o donados al DNP.
- Gestionar los tokens de firma digital y capacitar a las personas usuarias en el uso de la firma en el sistema de información ORFEO⁹.
- Garantizar que los equipos de los centros de datos y de las sedes cuenten con fuentes ininterrumpidas de poder y estabilizadores de potencia.
- Garantizar el funcionamiento del control de acceso biométrico al centro de datos.
- Coordinar con la Oficina de Tecnología y Sistemas de Información la limpieza del centro de datos.
- Garantizar que la Entidad cuente con alarmas de detección de humo y sistemas automáticos de extinción de fuego.
- Revisar que los equipos de cómputo estén conectados a la red regulada.
- Garantizar la actualización de los planos conexiones del cableado (voz y eléctricos) en conjunto con el Centro de Servicios.
- Gestionar la devolución, traslado de los equipos de cómputo.
- Aprobar el ingreso y salida de equipos de cómputo.
- Atender las PQRDS (Peticiónes, Quejas, Reclamos, Denuncias y Solicitudes) relacionadas con datos personales.

⁸ https://www.dnp.gov.co/LaEntidad_/secretaria-general/subdireccion-administrativa-relacionamiento-ciudadania/

⁹ Sistema encargado de controlar de un modo eficiente y sistemático la creación, la recepción, el mantenimiento, la utilización y la disposición de los documentos



- Entregar a las dependencias el mensaje para notificación automática sobre los canales autorizados para radicar las PQRDS en los buzones que reciban y envíen mensajes a los ciudadanos.

10.8. Oficina Asesora de Comunicaciones

La Oficina Asesora de Comunicaciones contribuye con la difusión en los círculos académicos, políticos y noticiosos del país, de las actividades adelantadas por el Departamento Nacional de Planeación (DNP)¹⁰.

Las responsabilidades de la Oficina Asesora de Comunicaciones en el componente de seguridad de la información son:

- Mantener actualizado la relación de delegados web de las dependencias.
- Entregar las contraseñas de las redes sociales a la Oficina de Tecnología y Sistemas de Información.
- Velar por el cumplimiento de las políticas de redes sociales.
- Administrar el grupo de WhatsApp asignado a su dependencia (sí aplica).
- Hacer uso adecuado de las listas de distribución para envíos masivos correos.
- Participar en las actividades relacionadas con la continuidad de negocio en la Entidad.

10.9. Oficina de Control Interno

La Oficina de Control Interno tiene como misión fortalecer el mejoramiento continuo de la gestión institucional, a través de la asesoría multidisciplinaria a las directivas para el adecuado funcionamiento del sistema de control interno fundamentado en el autocontrol, la planeación y la autoevaluación de la gestión¹¹.

Las responsabilidades de la Oficina de Control Interno en el componente de seguridad de la información son:

- Definir responsables de planificar, ejecutar y reportar las auditorías de seguridad de la información, asegurando que cuenten con la competencia y formación necesarias para evaluar la efectividad de los controles del MSPI.
- Establecer la efectividad de los controles para asegurar el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales, a través de sus procesos de seguimiento y evaluación.
- Proporcionar una evaluación independiente y objetiva sobre la eficacia del sistema de gestión de seguridad de la información, identificando áreas de riesgo y proponiendo mejoras para garantizar el cumplimiento de los objetivos y la normativa aplicable.
- Participar en las actividades relacionadas con la continuidad de negocio en la Entidad.

10.10. Oficina Asesora de Planeación

La Oficina Asesora de Planeación es la encargada de coordinar la gestión en los temas de plan de acción, proyectos, presupuesto de inversión y desarrollo organizacional para promover la eficiencia y eficacia del desempeño institucional, según las disposiciones legales, normativas, institucionales y los criterios técnicos relacionados¹².

¹⁰ https://www.dnp.gov.co/LaEntidad_/Direccion-general/oficina-asesora-comunicaciones/Paginas/default.aspx

¹¹ https://www.dnp.gov.co/LaEntidad_/Direccion-general/oficina-control-interno/Paginas/default.aspx

¹² https://www.dnp.gov.co/LaEntidad_/Direccion-general/oficina-asesora-planeacion/Paginas/default.aspx



Las responsabilidades de la Oficina Asesora de Planeación en el componente de seguridad de la información son:

- Asesorar metodológicamente a las dependencias en las herramientas transversales para la planeación, evaluación y mejora del SIG.
- Gestionar la aprobación de los cambios en las políticas de seguridad de la información solicitadas por la Oficina de Tecnología y Sistemas de Información.
- Administrar el grupo de WhatsApp asignado a su dependencia (sí aplica).

10.10.1. Profesional continuidad de negocio – en el marco del Modelo de Operación por Proceso

- Articular el desarrollo del plan de articulación de la Gestión de Continuidad del Negocio a nivel de procesos propuesto por la Oficina Asesora de Planeación para el DNP.
- Generar los insumos y recomendaciones para la mejora en la fase de implementación de la Gestión de Continuidad de Negocio.
- Gestionar las actividades de articulación de la Gestión de Continuidad del Negocio con los componentes del SIG.

10.11. Oficina Asesora Jurídica

- Brindar asesoría a los procesos, dependencias y al Comité Institucional de Gestión y Desempeño en temas jurídicos, legales que involucren acciones y la interpretación de las nuevas regulaciones y normativas que impacten el componente de seguridad y privacidad de la información.
- Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada y el Registro de activos de información de acuerdo con la regulación vigente.

10.12. Jefes de dependencia, coordinadores de grupo y/o supervisores

Son los conductores operativos de un procedimiento, responsable de velar por la ejecución de las actividades, métodos y documentos descritos, así como de su seguimiento, medición, análisis y mejora¹³.

Las responsabilidades de la persona que ejerza la jefatura del área responsable, coordinador de grupo y/o supervisor de contrato en el componente de seguridad de la información son:

- Garantizar que las personas colaboradores a su cargo conozcan, cumplan las políticas y participen en las sensibilizaciones de seguridad de la información de conformidad con el [M-CT-02 Manual de Supervisión e Interventoría](#).
- Verificar que los contratos y/o convenios con componente tecnológico que realice la dependencia incluyan los lineamientos en seguridad de la información del [M-CT-01 Manual de contratación](#).
- Reportar al centro de servicios las violaciones sobre el uso adecuado de software, incidentes y/o requerimientos.

¹³ Manual del SIG <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL%20DEL%20SIG.Pu.pdf>



- Informar a la Subdirección de Gestión del Talento Humano, Subdirección de Contratación y a las personas [líderes de los sistemas de información](#) cuando se registre el ingreso, retiro y/o traslado de una persona colaboradora para que se realice la creación, inactivación de usuario en los activos de información.
- Verificar la entrega de la información almacenada en los equipos de cómputo, correo electrónico y servicios de Office 365 cuando una persona colaboradora se retire y/o traslade de dependencia.
- Verificar la devolución de los activos a la Subdirección Administrativa y Relaciónamiento con la Ciudadanía cuando una persona colaboradora se retire y/o traslade de dependencia.
- Supervisar el traslado de activos en su dependencia.
- Velar por el cumplimiento de las políticas de Whatsapp, confidencialidad, datos personales, continuidad de negocio (sí aplica).
- Liderar la actualización, clasificación de los [activos de información](#) asignados a la dependencia.
- Liderar la identificación de [riesgos de seguridad de la información](#).
- Solicitar concepto técnico a la Oficina de Tecnología y Sistemas de Información para la contratación de servicios profesionales, el licenciamiento, la adquisición, adaptación, construcción y/o mantenimiento de sistemas de información o plataformas digitales.
- Velar por el cumplimiento [Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información](#) en el diseño y desarrollo de sistemas de información, aplicativos y portales desarrollados en la dependencia.
- Gestionar ante la Subdirección de Contratación la cesión de derechos patrimoniales del software, sistemas de información, aplicativos y portales desarrollados en la dependencia.
- Informar a la Oficina de Tecnología y Sistemas de Información sobre los hardware y software que vaya a adquirir, conectar a la plataforma tecnológica del DNP.
- Velar porque el software adquirido o licenciado por los proyectos y/o programas sea entregado a la Oficina de Tecnología y Sistemas de Información y quede a nombre del DNP.
- Solicitar al centro de servicios la actualización de las listas de distribución de correo electrónico, las actualizaciones en las restricciones de acceso a páginas de Internet de acuerdo con las necesidades de la dependencia.
- Aprobar las solicitudes de autorización de software, los permisos de administrador, solicitudes de acceso remoto de su dependencia.
- Verificar la organización, contenido, permisos y custodia de los discos de red asignados a la dependencia.
- Ejercer control de las impresiones realizadas en su dependencia.
- Informar a Oficina Asesora de Comunicaciones la actualización de los delegados web.
- Informar a Subdirección de Gestión del Talento Humano la terminación del teletrabajo de las personas colaboradoras de su dependencia.
- Gestionar que la dependencia configure el mensaje de notificación automática que la Subdirección Administrativa y Relaciónamiento con la Ciudadanía definió sobre los canales autorizados para radicar las PQRDS para los buzones que reciben y envían mensajes a los ciudadanos.

10.13. Gestores SIG

Son los facilitadores designados en cada dependencia, que actúa como enlace directo entre el Administrador del Sistema, los jefes y demás integrantes de la dependencia a la cual pertenecen. Se encargan de difundir todo lo relacionado con el sistema; realizar los requerimientos al Administrador, y mantener actualizados los reportes de indicadores, riesgos, acciones de mejora, entre otros¹⁴.

¹⁴ Manual del SIG <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL%20DEL%20SIG.Pu.pdf>



Las responsabilidades de los gestores SIG en el componente de seguridad de la información son:

- Fomentar al interior de la dependencia la participación de las personas colaboradoras en las sensibilizaciones de seguridad de la información.
- Articular al interior de su dependencia la actualización de los [activos de información](#) y la gestión de [riesgos de seguridad de la información](#).
- Alinear los productos de los planes institucionales con las líneas de acción estratégica del proceso de gestión TIC y clasificadores de productos (1. Seguridad digital. 2. Gobierno Digital. 3. PETI.4. Compromisos estratégicos instituciones).
- El [Manual del SIG](#) en el numeral “responsabilidad y autoridad” describe los compromisos transversales de los gestores SIG.

10.14. Líderes funcionales, técnicos y administradores de los sistemas de información

El rol de líder de los servicios de información (sistemas de Información, aplicativos y portales), líder de servicios tecnológicos, personal de sitio e infraestructura del Centro de servicios y/o la Oficina de Tecnología y Sistemas de Información, proveedores con contratos vigentes que apoyen la gestión de la plataforma tecnológica.

Las responsabilidades de los líderes funcionales, técnicos y administradores de los sistemas de información en el componente de seguridad de la información son:

- Activar y desactivar cuentas de usuarios en los activos de información (sistemas, aplicativos, y portales) a su cargo de acuerdo con los reportes de las dependencias.
- Cumplir con los permisos asignados en los servidores y estaciones cliente relacionados con los activos de información.
- Cumplir con las políticas de software, derechos de autor, confidencialidad, datos personales, continuidad de negocio.
- Dar cumplimiento a lo establecido en el [Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información](#) en el diseño y desarrollo de sistemas de información, aplicativos y portales desarrollados en la dependencia.
- Implementar el [lineamiento de desarrollo seguro de aplicaciones](#) para los activos de información a su cargo
- Gestionar la mitigación de las vulnerabilidades en los activos de información a su cargo reportadas por la Oficina de Tecnología y Sistemas de Información.
- Implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información en los activos de información a su cargo.
- Gestionar los cambios en los en los activos de información a su cargo de acuerdo con los [procedimientos establecidos](#).
- Realizar la sesión de derechos patrimoniales.
- Reportar las violaciones sobre el uso inadecuado de software, incidentes y/o requerimientos.
- Gestionar la recolección de evidencia de los incidentes de seguridad de la información.
- Realizar la gestión de [riesgos de seguridad de la información](#) para los [activos de información](#) a su cargo.
- Realiza la actualización de los catálogos y hojas técnicas de servicios de los [activos de información](#) a su cargo.
- Entregar a la Oficina de Tecnología y Sistemas de Información las claves de los [activos de información](#) a su cargo.
- Incluir parámetros de seguridad basado en usuarios, perfiles y roles de los activos de información a su cargo.



- Velar porque los ambientes productivos de los activos de información a su cargo no tengan versiones de backup.
- Coordinar pruebas de recuperación de los activos de información a su cargo.
- Cambiar las contraseñas establecidas por defecto en los activos de información a su cargo.
- Almacenar el código fuente en Microsoft DevOps Server.

10.15. Colaboradores (personas funcionarias, contratistas, pasantes)

Son los encargados de mantener y mejorar el SIG, con el cumplimiento de sus funciones y obligaciones, según corresponda¹⁵.

Las responsabilidades de las personas colaboradoras en el componente de seguridad de la información son:

- Conocer, cumplir el [Manual Operativo de seguridad de la información](#), el [Manual Datos Personales](#), [Código Único Disciplinario](#) y el [Código de Integridad](#).
- Presentar las evaluaciones de conocimiento de seguridad de la Información.
- Dar uso apropiado a los recursos entregados, al usuario y/o claves asignadas.
- Cumplir con las políticas de correo electrónico, redes sociales, Whatsapp, puesto de trabajo, software, derechos de autor, confidencialidad, datos personales, continuidad de negocio, acceso remoto, conexión a la red, teletrabajo.
- Almacenar la información institucional en la plataforma tecnológica del DNP.
- Entregar a su jefe inmediato y/o supervisor la información almacenada en los equipos de cómputo, correo electrónico y servicios de Office 365 al retirarse y/o trasladarse de dependencia.
- Devolver los activos a su cargo, gestionar los traslados, salidas de activos y reportar el extravió o hurto a Subdirección Administrativa y Relaciónamiento con la Ciudadanía.
- Reportar al [Centro de Servicios](#) cualquier novedad, requerimiento y/o incidente de seguridad en la prestación de algún servicio de TIC.
- Informar a su jefe inmediato y/o supervisor los incumplimientos en el uso de software y/o derechos de autor
- Los delegados web deben mantener la información actualizada.
- Participar en la actualización, clasificación de los [activos de información](#) asignados a la dependencia y la gestión de [riesgos de seguridad de la información](#).
- Usar el antivirus institucional y herramientas autorizadas por la Oficina de Tecnología y Sistemas de Información recolectar y/o compartir información.
- Registrar en la portería de los edificios los equipos de su propiedad.

10.16. Oficina de Tecnología y Sistemas de Información

La Oficina de Tecnologías y Sistemas de Información (OTSI) lidera los aspectos relacionados con tecnologías y sistemas de información en el Departamento Nacional de Planeación (DNP), para el apoyo del cumplimiento de la misión y objetivos de ésta, alineando la tecnología con los procesos de la organización, para ser habilitador del desarrollo de estrategias institucionales de mayor valor agregado para la entidad y el país¹⁶.

Las responsabilidades de la Jefatura de la Oficina de Tecnología y Sistemas de Información como responsable de Seguridad de la Información en el componente de seguridad de la información son:

¹⁵ Manual del SIG <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL%20DEL%20SIG.Pu.pdf>

¹⁶ https://www.dnp.gov.co/LaEntidad/_Direccion-general/oficina-tecnologia-sistemas-informacion/



- Ejecutar las funciones descritas en el artículo 10 de [Decreto 1893 de 2021](#).
- Liderar las responsabilidades operacionales del componente de seguridad de la información de acuerdo con numeral “*responsabilidad y autoridad*” del [Manual del SIG](#).
- Presentar al Comité institucional de Gestión y Desempeño las situaciones que hayan dado lugar a un incumplimiento de seguridad de la información y las recomendaciones en el componente de seguridad de la información.
- Presentar al Comité institucional de Gestión y Desempeño los ejercicios de Ethical hacking e ingeniería social para aprobación.
- Reportar a Oficina de Control Interno Disciplinario y la Secretaría General los incidentes de seguridad que requieran investigación disciplinaria.
- Presentar junto con Subdirección Administrativa y Relacionamento con la Ciudadanía las dadas de bajas de software.
- Apoyar a la Entidad en las actividades de continuidad de negocio.
- Realizar la creación, modificación y cancelación de las cuentas de las personas usuarias en los servicios a su cargo previa solicitud.
- Analizar las solicitudes de uso de nuevas herramientas de recolección de información.
- Implementar medidas de seguridad para la protección de la plataforma tecnológica.
- Gestionar los cambios de acuerdo con el procedimiento de control de cambios.
- Mantener actualizada la documentación de los servicios tecnológicos.
- Implementar acuerdos de niveles de servicio con los proveedores de TIC.
- Establecer los procedimientos tecnológicos para el teletrabajo.
- Atender las auditorías realizadas por la Oficina de Control Interno.
- Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos de seguridad de la información, implementación de controles y definición de actividades de planes de tratamiento.

La Oficina de Tecnología y Sistemas de Información (OTSI) está conformada por cuatro (4) grupos, de acuerdo con lo establecido en la [Resolución 0530 de 2022](#).

10.16.1.1. Asesor seguridad de la información

Las responsabilidades del rol de Asesor seguridad de la información en el componente de seguridad de la información son:

- Coordinar las actividades relacionadas con el componente de Gestión de Seguridad de la Información, que incluyen actualización y sensibilización de las Políticas de Seguridad de la Información.
- Realizar junto con la Oficina de Tecnología y Sistemas de Información la actualización de las políticas del M-PG-07 Manual Operativo de seguridad de la información.
- Participar en el seguimiento y recomendaciones para mejoramiento del Componente de Seguridad de la Información.
- Apoyar la gestión de incidentes de seguridad de la información.
- Realizar la custodia de las contraseñas de seguridad de los servicios tecnológicos.



10.16.1.2. Oficial de seguridad de la información

Las responsabilidades del rol de Oficial de Seguridad de la Información en el componente de seguridad de la información son:

- Asistir en la supervisión de las actividades relacionadas con los Especialistas de Seguridad Informática del Centro de Servicios (CDS) y el Centro de Operaciones de Seguridad (SOC).
- Elaborar insumos técnicos y de seguridad para aconsejar y orientar la toma de decisiones en relación con la seguridad de la información de los proyectos informáticos, peticiones, solicitudes y demás requerimientos.
- Realizar la actualización de los manuales, procedimientos, y/o formatos del Componente de Seguridad de la información de acuerdo con las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC, la estrategia de ciberseguridad del Ministerio de Defensa, la política de seguridad digital de la Presidencia de la República, la normativa de protección de datos personales de la Superintendencia de Industria y Comercio y la implementación de la norma ISO 27001:2022.
- Brindar acompañamiento a las dependencias en la identificación de los activos de información e identificación de los riesgos de seguridad de información con el fin de velar por la integridad, disponibilidad y confidencialidad.
- Llevar a cabo las actividades de divulgación y promoción de la importancia del componente de Gestión de Seguridad de la Información y los temas relacionados en la normativa aplicable.
- Actuar como enlace sectorial de seguridad digital ante el Coordinador Nacional de Seguridad Digital de la Presidencia de la República, y elaborar insumos que permitan la gestión de requerimientos e incidentes relacionados con seguridad de la información para el reporte periódico al CSIRT de Gobierno.
- Asesorar a la Oficina de Tecnología y Sistemas de Información en procesos para la inclusión de requisitos, cláusulas de seguridad e identificación de riesgos para los contratos de TIC.
- Apoyar las auditorías de seguridad de la información.
- Realizar la custodia de las contraseñas de seguridad de los servicios tecnológicos.
- Realizar la aprobación de los perfiles especiales.

10.16.2. Grupo de Planeación y Gestión de TIC

Grupo de la OTSI que lidera Políticas de Gobierno y Seguridad Digital, licenciamiento, Seguridad de la Información, Sistema Integrado de Gestión, Presupuesto TI.¹⁷

10.16.2.1. Especialista continuidad de negocio del componente tecnológico

Las responsabilidades del rol de Especialista continuidad de negocio del componente tecnológico en el componente de seguridad de la información son:

- Brindar acompañamiento técnico a las dependencias en la estructuración del cronograma para el desarrollo de las pruebas de DRP, documentando mediante actas e informes los resultados de las pruebas con sus recomendaciones.
- Actualizar el análisis de riesgos de continuidad enfocado a la indisponibilidad de instalaciones físicas, recurso humano y proveedor con el apoyo de la Oficina Asesora de Planeación.

¹⁷ PETI <https://colaboracion.dnp.gov.co/CDT/GrupoPlaneacion/M-TI-02%20Manual%20del%20Plan%20Estrat%C3%A9gico%20de%20TI.Pu.pdf>



- Acompañar, construir y documentar las actividades relacionadas con el diagnóstico e implementación de arquitectura de seguridad de la información de MINTIC y su relación con la continuidad del negocio en el componente tecnológico, Plan de recuperación de Desastres (DRP), la norma ISO 22301 y las guías de MINTIC.
- Articular junto con la Oficina Asesora de Planeación y la Oficina de Tecnología y Sistemas de Información la estructuración e implementación del Plan de Continuidad de Negocio en el componente tecnológico.
- Adelantar actividades en coordinación con las dependencias del DNP relacionadas con la identificación de los tiempos de recuperación, los componentes tecnológicos críticos y los procedimientos necesarios para mitigar la afectación de la operación de la Entidad ante eventos catastróficos y lo relacionado con los sistemas de información en el Catálogo de Servicios TI asociado al plan de restauración de servicio.

10.16.3. Grupo de Infraestructura tecnológica

Grupo de la OTSI que administra la plataforma física y lógica, conectividad, seguridad, Comunicaciones Unificadas¹⁸.

Las responsabilidades del Grupo de Infraestructura tecnológica en el componente de seguridad de la información son:

- Supervisar las actividades administración de copias de seguridad, la red, el centro de datos y plataforma tecnológica realizadas por el centro de servicios.

10.16.3.1. Especialista WAF y DRP

Las responsabilidades del rol de Especialista WAF y DRP en el componente de seguridad de la información son:

- Planear, implementar y documentar las pruebas correspondientes al plan de recuperación de desastres de la plataforma tecnológica.

10.16.4. Grupo de soporte a usuarios

Grupo de la OTSI que apoya el servicio técnico de estaciones cliente, portátiles y Workstation, servicios de videoconferencia, apoyo a sistemas de información.¹⁹

Las responsabilidades del Grupo de soporte a usuarios en el componente de seguridad de la información son:

- Realizar el alistamiento de equipos.
- Generar los reportes de impresión.
- Establecer las fichas técnicas de impresoras de los procesos contractuales.
- Administrar el software.

¹⁸ PETI <https://colaboracion.dnp.gov.co/CDT/GrupoPlaneacion/M-TI-02%20Manual%20del%20Plan%20Estrat%C3%A9gico%20de%20TI.Pu.pdf>

¹⁹ PETI <https://colaboracion.dnp.gov.co/CDT/GrupoPlaneacion/M-TI-02%20Manual%20del%20Plan%20Estrat%C3%A9gico%20de%20TI.Pu.pdf>



10.16.5. Grupo de Gestión de Sistemas de Información

Grupo de la OTSI que asesora y administra los temas de Arquitectura empresarial y de aplicaciones, Gestión de proyectos de TI, soporte, mantenimiento y prueba sobre Sistemas de Información.²⁰

Las responsabilidades del Grupo de Gestión de Sistemas de Información en el componente de seguridad de la información son:

- Gestión de los Tokens de firma digital.
- Emitir concepto técnico para la contratación de servicios profesionales, el licenciamiento, la adquisición, adaptación, construcción y/o mantenimiento de sistemas de información o plataformas digitales.
- Asesorar a las dependencias sobre la sesión de derechos patrimoniales del software, sistemas de información construidos.
- Asesorar a las dependencias para la implementación del Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información.
- Custodiar el código fuente de los sistemas de información.

10.16.6. Centro de servicios

El centro de servicios realiza la gestión, mantenimiento, administración, soporte técnico, monitoreo y disponibilidad de la infraestructura tecnológica que provee servicios de tecnologías de la información de las comunicaciones (TIC), asegurando la continuidad en la operación e implementando el servicio de Centro de Operación de Seguridad (SOC).

Las responsabilidades del Centro de Servicios en el componente de seguridad de la información son:

- El Centro de Servicios no responsable de prestar servicio de soporte técnico en equipos externos y personales.
- El Centro de Servicios no presta el servicio de configuración de las redes sociales en los dispositivos móviles.
- Cumplir con los acuerdos de niveles de servicio (ANS) establecidos.

10.16.6.1. Gerente de Proyecto Centro de Servicios

Las responsabilidades del Gerente de Proyecto Centro de Servicios Centro de Servicios en el componente de seguridad de la información son:

- Cumplir los Acuerdos de Niveles de Servicio (ANS) establecidos.
- Supervisar la gestión de la infraestructura, mantenimiento, gestión de cambios, gestión de los centros de datos institucionales, Gestión de incidentes.
- Conservar la confidencialidad de la información.
- Interlocutor principal del Contratista con el DNP
- Coordinar el recurso humano Especialistas, Operadores, técnicos y demás que el proyecto conlleve con su respectiva documentación y seguimiento a servicio

²⁰ PETI <https://colaboracion.dnp.gov.co/CDT/GrupoPlaneacion/M-TI-02%20Manual%20del%20Plan%20Estrat%C3%A9gico%20de%20TI.Pu.pdf>



- Coordinar, actualizar y consolidar la documentación asociada con el desarrollo del contrato y elaborar los informes de gestión requeridos.
- Coordinar el seguimiento a las solicitudes de servicios registradas en la herramienta de gestión de servicios TIC (ITSM) con su respectiva documentación.
- Hacer seguimiento de la gestión de casos registrados en la herramienta de gestión de servicios de TIC (ITSM).
- Gestionar la presentación de cotizaciones asociadas con la Bolsa de Repuestos.
- Asegurar el cumplimiento de los acuerdos de niveles de servicio (ANS) establecidos
- Generar y presentar propuesta de mejoramiento de la infraestructura tecnológica a administrar.
- Dirigir la prestación de los servicios de infraestructura y conectividad del DNP, gestionando la operación continua y la seguridad de la información en procesos, tecnología y gente, apoyando el cumplimiento de los objetivos de DNP.
- Identificar, analizar, priorizar y gestionar los riesgos de seguridad información, implementando los controles necesarios viables desde el punto de vista técnico, operacional y de costos.
- Verificar el funcionamiento de las medidas de seguridad, así como, el cumplimiento de las normas y leyes aplicables.

10.16.6.2. Analista y Especialista de Infraestructura de Procesamiento y Almacenamiento

Las responsabilidades del Analista y Especialista de Infraestructura de Procesamiento y Almacenamiento del Centro de Servicios en el componente de seguridad de la información son:

- Administrar y gestionar el antivirus institucional, los centros de datos institucionales, el correo electrónico institucional, el Directorio activo, discos de red.
- Instalar los certificados de sitio web seguro (SSL), Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Activar y desactivar cuentas de usuarios en el Directorio activo
- Generar copia de backup sólo se entrega al titular
- Administrar Office 365
- Configurar copias de respaldo en Servidores (Shadow copies)
- Mantener inventario actualizado de infraestructura
- Implementar MFA
- Instalar certificados SSL
- Administración del antivirus
- Configurar registros de auditoria en los servidores
- Mantener actualizada la información a su cargo
- Realizar actualizaciones de seguridad de Windows y Linux(trimestral)
- Cambiar contraseñas por defecto
- Configurar cambio de contraseña en el siguiente inicio de sesión

10.16.6.3. Operador Infraestructura de Backup

Las responsabilidades del Operador Infraestructura de Backup del Centro de Servicios en el componente de seguridad de la información son:



- Gestionar la copia de seguridad.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Realizar pruebas de recuperación de las copias de respaldo.
- Administrar backup Office 365.
- Mantener inventario actualizado de Backup.
- Mantener actualizada la información a su cargo.
- Cambiar contraseñas por defecto.
- Realizar actualizaciones de seguridad de veeam.
- Dos backup de los discos de red fuera del DNP.

10.16.6.4. Operador Infraestructura Eléctrica

Las responsabilidades del Operador Infraestructura Eléctrica del Centro de Servicios en el componente de seguridad de la información son:

- Administrar la plataforma eléctrica.
- Gestionar los planos eléctricos.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Usar software y herramientas TIC autorizados por la OTSI.
- Mantener inventario actualizado de red.
- Cambiar contraseñas por defecto.
- Monitoreo de UPS, aires acondicionados.
- Configurar registros de auditoria en dispositivos UPS, aire acondicionado.
- Realizar actualizaciones de seguridad de dispositivos de UPS.

10.16.6.5. Especialista y Operador de Infraestructura de Redes

Las responsabilidades del Especialista y Operador de Infraestructura de Redes del Centro de Servicios en el componente de seguridad de la información son:

- Administrar la red de datos.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Usar software y herramientas TIC autorizados por la OTSI.
- Mantener inventario actualizado de red.
- Cambiar contraseñas por defecto.
- Cableado protegido por interferencias.



- Configurar registros de auditoria en dispositivos de red.
- Realizar actualizaciones de seguridad de dispositivos de red.
- Administración de la Redes Lan, Wifi, WAN.

10.16.6.6. Especialistas Seguridad Informática

Las responsabilidades del Especialista Seguridad Informática del Centro de Servicios en el componente de seguridad de la información son:

- Administrar y Gestionar Firewall institucional.
- Gestión de políticas de navegación.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Usar software y herramientas TIC autorizados por la OTSI.
- Mantener inventario actualizado de seguridad.
- Cambiar contraseñas por defecto.
- Configurar registros de auditoria en dispositivos de seguridad.
- Realizar actualizaciones de seguridad de dispositivos de seguridad.
- Administración de equipos de seguridad.
- Monitorear navegación, bloquear sitios web maliciosos.
- Realizar análisis de vulnerabilidades.
- Gestionar la mitigación de vulnerabilidades

10.16.6.7. Especialista en balanceador/firewall de aplicaciones (WAF)

- Administración de WAF.
- Mantener inventario actualizado de las configuraciones de WAF.
- Cambiar contraseñas por defecto.
- Monitoreo del WAF.
- Configurar registros de auditoria en dispositivos WAF.
- Configurar WAF para remediar vulnerabilidades.
- Configurar WAF a demanda para nuevos sitios.
- Realizar actualizaciones de seguridad de dispositivos de WAF.

10.16.6.8. Centro de operaciones SOC

Las responsabilidades del Centro de operaciones SOC del Centro de Servicios en el componente de seguridad de la información son:

- Monitoreo de la infraestructura tecnológica.
- Diseño y ejecución de las pruebas de Ethical hacking e ingeniería social.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.



- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.
- Mitigar los ataques de denegación de servicio distribuido que puedan ser realizados contra las publicaciones web y la plataforma tecnológica.
- Monitoreo de Fraude de los dominios, fraude vía email, fugas de información en Deep y dark web, nuevos sitios phishing monitoreo de perfiles falsos en redes sociales, uso no autorizado de imágenes, logos, marca del DNP y los sitios web institucionales.
- Monitoreo 7x24x365 de la Plataforma tecnológica del DNP.
- Detectar, responder y mitigar las amenazas informáticas recolectando todos los eventos y alertas de seguridad de la plataforma tecnológica.
- Identificar, analizar, realizar el escalamiento, reporte de los casos, acciones de tratamiento e indicadores de compromiso y seguimiento de las alarmas, eventos e incidentes detectados.

10.16.6.9. Gestor de Calidad

- Velar porque el CDS tome las capacitaciones impartidas por la OTSI.
- Verificar que los servicios administrados por el CDS se encuentren documentados y actualizados.
- Verificar que los cambios sean gestionados.
- Actualización de la CMBD.
- Actualizar la matriz de proveedores y contratos.

10.16.6.10. Líder gestor de Aplicaciones

- Gestionar el adecuado funcionamiento de las aplicaciones y portales del DNP que se encuentran instaladas dentro de la infraestructura del DNP.
- Gestión de cambios en sistemas de información, portales y aplicaciones.
- Gestión de la capacidad en sistemas de información, portales y aplicaciones.
- Apoyo a los líderes técnicos y funcionales en el monitoreo en sistemas de información, portales y aplicaciones.

10.16.6.11. Mesa de ayuda y soporte

Es el primer punto de contacto para todas las solicitudes e incidentes de soporte realizada por las personas colaboradoras del DNP.

Las responsabilidades de la mesa de ayuda y soporte del Centro de Servicios en el componente de seguridad de la información son:

- Implementación MFA.
- Creación de contraseñas.
- Gestionar los equipos de usuario final.
- Instalar software.
- Conservar la confidencialidad de la información.
- Custodiar la información institucional.
- Garantizar la gestión de los centros de datos institucionales, mantenimientos y cambios, incidentes de la plataforma a su cargo.



10.17. Proveedores

Un proveedor es una entidad o individuo externo que proporciona productos, servicios, o soluciones que contribuyen a la protección, gestión, y seguridad de la información de una organización. Estos proveedores pueden ofrecer una variedad de servicios, como soluciones de software de seguridad (antivirus, firewalls, sistemas de detección de intrusos), servicios de consultoría en ciberseguridad, auditorías de seguridad, formación en seguridad, o incluso servicios de recuperación de datos.

Las responsabilidades de los proveedores en el componente de seguridad de la información son:

- Conocer, cumplir el M-PG-07 Manual Operativo de seguridad de la información, el M-PG-12 Manual Datos Personales.
- Cumplir las políticas de confidencialidad, acceso remoto.
- Gestionar los cambios en los en los activos de información a su cargo de acuerdo con los procedimientos establecidos.
- Registrar en la portería de los edificios los equipos de su propiedad.
- Solicitar autorización a la Oficina de Tecnología y Sistemas de Información conectarse a la red.
- Cumplir los acuerdos de niveles de servicio.
- Gestionar los riesgos de los servicios ofrecidos.
- Gestionar incidentes de seguridad e informar de forma oportuna.
- Identificar áreas de mejora y recomendaciones en el servicio ofrecido.
- Asegurarse que las personas que hace parte del servicio o soporte cumplan con los requisitos de seguridad establecidos en el contrato.
- Atender auditorías internas solicitadas por la Oficina de Tecnología y Sistemas de Información evaluar la eficacia de los controles de seguridad relacionados con proveedores.
- Gestionar la recolección de evidencia de los incidentes informáticos relacionados con la infraestructura tecnológica.
- Gestionar la mitigación de las vulnerabilidades reportadas por la Oficina de Tecnología y Sistemas de Información.

10.18. Usuarios externos sistemas de información

Una persona usuaria externa es cualquier persona o entidad que no hace parte del DNP y que interactúa con los sistemas de información, aplicativos y/o portales institucionales, para realizar tareas específicas o acceder a la información que estos proporcionan.

Las responsabilidades de las personas usuarias externas de los sistemas de información en el componente de seguridad de la información son:

Gestionar e implementar los controles de seguridad de la información en su ambiente personal y/o laboral que incluyen la activación y desactivación de usuarios, protección de las contraseñas, actualización del software y dispositivos, conexión segura, identificación de amenazas potenciales, uso de herramientas de seguridad, navegación segura, protección de los dispositivos (equipo de cómputo, dispositivo móvil), medidas de seguridad para equipos compartidos, controles de seguridad física, notificación de incidentes de seguridad, anonimización de datos personales.



11. SANCIONES

Cualquier violación a las políticas de seguridad de la información debe ser sancionada de acuerdo con el [PT-ED-06 Procedimiento Instrucción Disciplinaria](#), el [PT-ED-07 Procedimiento Juzgamiento](#), normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de esta.

12. ESTRUCTURA DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

12.1. Premisas básicas de seguridad de la información

Los siguientes principios básicos fundamentan las políticas de seguridad de la información, con el fin de preservar la gestión integral de esta, protegiéndola desde la plataforma tecnológica, infraestructura física y recurso humano que la soporta.

12.1.1. Confidencialidad

La siguiente tabla describe la relación entre la clasificación de información determinada por la Ley de Transparencia, Ley de Protección de Datos Personales, la Corte Constitucional y el DNP.

Tabla 2: Clasificación de información determinada por la Ley de Transparencia y Ley de Protección de Datos Personales

Clasificación Ley de Transparencia	Relación otras clasificaciones
Información pública (P)	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
Información pública clasificada (C)	Es la información que no debe ser divulgada debido a que se pueden vulnerar los derechos de las personas naturales o jurídicas. Contiene información con alguna de las siguientes temáticas: a) derecho de las personas a la intimidad, b) derecho a la vida, salud o seguridad, c) los secretos comerciales, industriales, profesionales y d) datos personales. Esta información es clasificada de acuerdo con el artículo 18 de la Ley 1712 de 2014 y la normativa de datos personales Ley 1581 de 2012, Ley 1266 de 2008 y Decreto 1377 de 2013
Información pública reservada (R)	Es la información que no debe ser divulgada debido a que esto puede causar daño a intereses públicos. Solamente la Constitución o la ley pueden definir qué información es de carácter reservado. Contiene información con alguna de las siguientes temáticas: a) Defensa y seguridad nacional, b) Seguridad pública, c) Relaciones internacionales, d) Prevención, investigación y persecución de los delitos y las faltas disciplinarias, e) Debido proceso y la igualdad de las partes en los procesos judiciales, f) Administración efectiva de la justicia, g) Derechos de la infancia y la adolescencia, h) Estabilidad macroeconómica y financiera del país, i) Salud pública, j) Opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, l) Es Documento en construcción. Esta información es reservada de acuerdo con el artículo 19 de la Ley 1712 de 2014.

La información digital se encuentra almacenada en los sistemas de información y aplicativos, por lo tanto, es importante determinar la clasificación de esta teniendo en cuenta el artículo 6 de la Ley 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y los artículos 3,5,7 de la Ley 1581 de 2012 por medio de la cual se dictan disposiciones generales para la protección de datos personales y el artículo 3 del Decreto 1377 de 2013.



12.1.2. Disponibilidad

La información debe estar disponible en cualquier momento.

Tabla 3: Disponibilidad de información en el DNP

Calificación		Explicación
Baja	5x8	El activo tiene que estar disponible en horario laboral entre semana
Media	6x8	El activo tiene que estar disponible en horario laboral entre semana, e incluyendo los sábados
Alta	7x24	El activo tiene que estar disponible tiempo completo, todos los días y todas las horas.

Tabla 4: Impacto Disponibilidad de información en el DNP

Calificación	Explicación
Alta	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
Media	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
Baja	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen

12.1.3. Integridad

La información debe estar adecuadamente protegida para asegurar que no sea alterada.

Tabla 5: Integridad de la información en el DNP

Calificación	Explicación
Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos
Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a personas funcionarias, contratistas y pasantes de la entidad.
Alta	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.

12.1.4. Autenticidad

Los activos de información digitales solo pueden estar disponibles verificando la identidad de un sujeto o recurso.

12.1.5. Auditabilidad

Los activos de información digitales deben tener controles que permitan su revisión.

12.1.6. No repudio

Los activos de información digitales deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.



13. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

13.2. Seguridad organizacional

El DNP gestiona la seguridad de la información con los roles definidos en el modelo de gobernanza, autorizaciones, acuerdos, manejo con terceros.

[PL02-ES1]

El Comité Institucional de Gestión y Desempeño evaluará las situaciones que hayan dado lugar a un incumplimiento del M-PG-07 Manual Operativo de seguridad de la información presentadas por la OTSI, aprobará las recomendaciones de las acciones a seguir para mantener el componente de Gestión de Seguridad de la información del SIG. La Oficina Asesora de Planeación como rol de secretaria técnica guardará las actas de las reuniones en el expediente correspondiente y dará copia a los integrantes del Comité para su seguimiento.

[PL02-ES2]

La OTSI promoverá la sensibilización y divulgación del M-PG-07 Manual Operativo de seguridad de la información, para lo cual se apoyará en las personas que ejerzan los roles de jefaturas de dependencia, coordinación de grupo y/o supervisión, el Oficina Asesora de Planeación y los gestores SIG.

[PL02-ES3]

Todos las personas [usuarias](#) del DNP, deberán conocer y cumplir el M-PG-07 Manual Operativo de seguridad de la información, el [Código de Integridad](#) y dar uso apropiado a los recursos entregados conforme a lo establecido en el [Código Único Disciplinario](#).

El M-PG-07 Manual Operativo de seguridad de la información y sus políticas de la Gestión de Seguridad de la información hace parte del SIG y se encuentra en los repositorios de información definidos.

Las personas que ejerzan jefaturas de dependencia, coordinación de grupo y/o supervisión, y que tengan personal a su cargo son responsables de que dicho personal conozca, acepte y cumpla las políticas de seguridad de la información.

Para ello en cada vigencia las personas funcionarias, contratistas, pasantes deberán presentar la evaluación de conocimiento de Seguridad de la Información de las sensibilizaciones realizadas por la OTSI, hasta que el resultado sea aprobado con mínimo el 70%²¹.

[PL02-ES4]

Todas las personas usuarias que identifiquen cualquier novedad, requerimiento y/o incidente de seguridad en la prestación de algún servicio de TIC deberán reportarlo al Centro de Servicios al correo electrónico centrodeservicios@dn.gov.co. El Centro de Servicios son los únicos autorizados para la realización de procedimientos técnicos en los equipos institucionales.

²¹ Este porcentaje se define de acuerdo con el indicador relacionado con el plan de sensibilización de seguridad de la información.



[PL02-ES5]

La Oficina de Tecnología y Sistemas de Información podrá utilizar herramientas para identificar problemas y mejorar el uso adecuado de las tecnologías de información y comunicaciones - TIC del DNP, sin infringir las políticas relacionadas con el software y/o derechos de autor.

[PL02-ES6]

La elaboración y revisión de las políticas de seguridad es realizada por las personas que ejercen los roles de Oficial y el Asesor de Seguridad de la información con el apoyo técnico de quienes colaboran y poseen conocimiento en las temáticas correspondientes, los cambios en las políticas de seguridad de la información son aprobados por la persona que ejerce la jefatura de la Oficina de Tecnología y Sistemas de la Información como responsable operacional del componente de seguridad de la información y son revisadas por la Oficina Asesora de Planeación de acuerdo con lo establecido en el Manual [M-PG-03](#) Manual para la elaboración y control de documentos del Sistema Integrado de Gestión y el formato [F-PG-04 Solicitud para la actualización, creación o eliminación de documentos](#).

13.3. Seguridad del recurso humano

El DNP busca asegurar que las personas usuarias, entiendan sus responsabilidades en relación con las políticas de seguridad institucional y actúen de manera consistente con las mismas.

[PL03-ES1]

Cuando persona usuaria que termine su relación laboral o finalice su relación contractual, y/o sea trasladado de dependencia, las personas que ejerzan los roles de Jefes de dependencia, coordinadores de grupo y/o supervisores, debe informar a la Subdirección de Gestión del Talento Humano y/o al Subdirección de Contratación, para que se realicen los trámites de creación, modificación y cancelación de las cuentas de Las personas usuarias al centro de servicios, la OTSI y las personas [líderes funcionales, técnicos y administradores de los sistemas de información](#).

[PL03-ES2]

Cuando persona usuaria se encuentre ad- portas de terminar su relación laboral o contractual con la Entidad, las personas que ejerzan los roles de Jefes de dependencia, coordinadores de grupo y/o supervisores, deberán informar con una antelación mínima de 8 días hábiles a la fecha de finalización del referido vínculo, a [los líderes funcionales y técnicos, administradores de los sistemas de información](#) según corresponda y a la OTSI; con el fin de proceder al retiro de los accesos lógicos a los activos de información a los a los que la persona usuaria tenía acceso.

Para permitir un tiempo de entrega del cargo e información, empalme o presentación de informes del estado de las actividades realizadas por personas contratistas y dar continuidad a los procesos misionales, se tendrán en cuenta las siguientes excepciones, cuyos términos deberán coincidir con el plazo máximo que se tiene para hacer entrega del cargo, y proceder así a deshabilitar la cuenta usuario una vez éste sea efectivamente legalizado:

- Las cuentas de acceso de los directores, subdirectores, y jefes de oficina deberán establecerse en estado inactiva, máximo a los quince días (15) días calendario de finalizar la relación laboral.
- Las cuentas de acceso para las personas funcionarias deben establecerse en estado inactiva, máximo a los diez (10) días calendario de finalizar la relación laboral.



- Las cuentas de acceso para las personas contratistas que no tienen entre sus actividades contractuales administración de sistemas de información deben establecerse en estado inactiva máximo a los ocho (8) días calendario de finalizar su vínculo contractual.
- Las cuentas de acceso para las personas contratistas que tienen entre sus actividades contractuales administración de sistemas de información y se encuentren en trámite del proceso de contratación tendiente a la suscripción del nuevo contrato; la inactividad de la cuenta de usuario se dará dentro de los quince (15) días calendario siguientes a la finalización de la relación contractual.
- Las cuentas de acceso para las personas contratistas que tienen entre sus actividades contractuales administración de sistemas de información y no se tenga previsto adelantar un proceso de contratación para la suscripción de contrato, deben establecerse en estado inactiva a los ocho (8) días calendario de finalización de la relación contractual.
- Las cuentas de acceso de las personas contratistas que pertenezcan a la Subdirección Financiera, Subdirección de Contratación, Oficina de Control Interno, Oficina Jurídica, Subdirección Administrativa y Relación con la Ciudadanía, Oficina Asesora de Planeación y Oficina de Tecnología y Sistemas de información, el Jefe de la respectiva Dependencia, deberá solicitar la extensión de las cuentas, para aquellas personas colaboradoras que se encuentren en trámite del proceso de contratación tendiente a la suscripción del nuevo contrato; las cuentas solicitadas deberán establecerse en estado inactiva máximo a los quince (15) días calendario de haber finalizado la relación contractual. La solicitud de extensión de las cuentas de usuario de estas dependencias deberá hacerse a la OTSI, con mínimo ocho (8) días calendario de anticipación a la finalización del contrato.
- Cuando una persona usuaria sea trasladado de dependencia, la persona que ejerza la jefatura del área responsable y/o la supervisión deberá informar a las personas líderes funcionales, técnicas y administradora de los sistemas de información según corresponda y a la OTSI, con una antelación mínima de ocho (8) días calendario, para retirar los accesos lógicos de ingreso a los activos de información a los que la persona usuaria tenía acceso y realizar la respectiva reasignación.
- La persona que ejerza la jefatura del área responsable y/o la supervisión jefe de área y/o supervisor del contrato, deberán dar cumplimiento estricto a los términos y excepciones que se han dejado indicados; lo anterior, a efectos de solicitar con la suficiente antelación la entrega de los productos a que haya lugar en virtud del contrato y/o la renovación ante el vencimiento de este, así como prever los tiempos requeridos para el proceso de inactivación de las cuentas de dichos usuarios.
- Las cuentas inactivas sólo serán habilitadas si la persona usuaria se vincula nuevamente a la Entidad mediante una resolución de nombramiento y/o contrato.

[PL03-ES3]

Cuando una persona usuaria termine su relación laboral o contractual, y/o sea trasladado de dependencia, persona que ejerza la jefatura del área responsable, coordinación de grupo y/o la supervisión deberán verificar la entrega de la información (equipo de cómputo, servicios office 365, entre otros), su organización en los discos de red y/o SharePoint institucional para garantizar su preservación y conservación, para la verificación de la información se debe tener en cuenta el [M-AD-03 Manual para la Gestión de Documentos y Administración de Archivo](#).

Con el propósito de no saturar los discos de red, las dependencias podrán almacenar en el One Drive de la secretaria de la dependencia, los backups de correos o pst.

[PL03-ES4]

Cuando una persona usuaria termine su relación laboral o contractual, y/o sea trasladado de dependencia, la persona que ejerza la jefatura del área responsable, coordinación de grupo y/o la supervisión deberá verificar que los activos asignados a las personas funcionarias, contratistas, pasantes o proveedores sean devueltos a



la Subdirección Administrativa y Relacionamento con la Ciudadanía para el control de inventarios en las condiciones y estado en que le fueron entregados de conformidad con el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#) y posterior alistamiento de los equipos de cómputo por parte de la Oficina de Tecnología y Sistemas de Información.

[PL03-ES5]

El traslado entre dependencias del DNP de todo activo informático, está bajo el control de la Subdirección Administrativa y Relacionamento con la Ciudadanía y se realiza conforme a la solicitud realizada en el aplicativo establecido para este fin.

Cuando una persona usuaria requiera retirar de las instalaciones de la Entidad activos informáticos, se deberá solicitar autorización a la Subdirección Administrativa y Relacionamento con la Ciudadanía, con el fin de registrar, controlar y hacer seguimiento a los mismos. La persona usuaria que retire el activo será el responsable de la custodia, salvaguarda de la información que allí este almacenada.

Las personas funcionarias, contratistas y pasantes que tengan activos informáticos a su cargo, son responsables de la pérdida o daño que sufran, cuando lo anterior no se ocasione por el deterioro natural, por su uso normal o por otra causa justificada. Cuando se presenten eventos de pérdida o daño de activos se procederá a realizar la reclamación a la compañía de seguros.

El traslado, retiro y reporte de pérdida de bienes del DNP debe realizarse de conformidad con el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#).

[PL03-ES6]


Para acceder a la información del correo electrónico institucional y/o la estación de trabajo, se debe contar con la autorización expresa de la persona usuaria titular de la cuenta y la persona que ejerza la jefatura del área responsable. En caso de investigación, previa orden judicial se accederá a la información con base en los protocolos que defina la autoridad competente. En caso de fallecimiento de la persona usuaria el acceso será entregado la persona que ejerza la jefatura del área responsable y/o supervisor previa solicitud la cual se adjuntará al ticket asignado.

[PL03-ES7]

Cuando una persona usuaria termine su relación laboral o contractual, y/o sea trasladado de dependencia, la persona que ejerza la jefatura del área responsable, coordinación de grupo y/o la supervisión deberá verificar que la persona usuaria entregue copia de los mensajes electrónicos institucionales almacenados en su buzón de correo, para que estos puedan ser consultados posteriormente.

[PL03-ES8]

En el proceso de selección de las personas funcionarias, pasantes o contratistas, se verificarán antecedentes disciplinarios de los candidatos sin importar el cargo o posición al que se postulen. Los antecedentes de las personas contratistas están incluidos en el formato Documentos para la suscripción de contratos con persona natural F-CT-02 serán verificados por la Subdirección de contratación, los antecedentes del personal de planta y pasantes incluidos en Lista de chequeo de documentos para la toma de posesión de un cargo público F-TH-21 serán verificados por la Subdirección de Gestión de Talento Humano.

 Departamento Nacional de Planeación	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 34 de 75 VERSIÓN: 14

13.4. Gestión de los activos de información

El DNP establece los lineamientos que se relacionan con el mantenimiento y protección apropiados de todos los activos de información.

[PL04-ES1]

La OTSI mantendrá los listados de software incluyendo el Software Específico, Software Free Permitido y No Permitido, los cuales pueden ser consultados en la [intranet](#).

En caso de requerir la instalación del software se debe realizar la solicitud a través del Centro de Servicios, para así validar si el software está autorizado y se cuenta con las licencias disponibles.

En caso de requerir un software que no esté incluido en los listados, la persona usuaria deberá gestionar la solicitud con la OTSI, enviando la siguiente información: nombre software, área usuaria, persona funcionaria a quien se asigna la licencia, justificación de uso, aplicación en la Entidad, nombre y cargo del solicitante. Nombre y cargo del jefe inmediato que aprueba la solicitud, para su respectivo análisis de viabilidad. La solicitud no garantiza la asignación del software ya que depende de procesos contractuales, seguridad, pertinencia, entre otros.

En los equipos del DNP sólo se podrá instalar y/o utilizar el software autorizado por la OTSI. El software proporcionado por el DNP no puede ser copiado o suministrado a terceros, o instalado en equipos personales de las personas usuarias.

Las personas usuarias a los cuales les sean autorizados permisos de administrador mediante el formato [Compromiso perfiles especiales F-TI-19](#) se comprometen a no instalar software sobre los equipos y servidores del DNP que no se encuentre debidamente autorizado por la OTSI del DNP.

La solicitud de cuentas con permisos de administrador en los equipos y servidores del DNP será permitida para las personas usuarias que lo requieran de acuerdo con sus funciones previa autorización por parte de la OTSI.

[PL04-ES2]

El software instalado en los equipos y servidores del DNP, así como los datos creados, almacenados y recibidos, son propiedad del DNP su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución serán sancionadas de acuerdo con las normas vigentes.

[PL04-ES3]

La OTSI periódicamente efectuará la revisión del software instalado en los equipos institucionales de cada dependencia. El hallazgo de software no autorizado se considerará como un incumplimiento al presente M-PG-07 Manual Operativo de seguridad de la información.

[PL04-ES4]

Las personas usuarias deben de solicitar a través del Centro de Servicios los requerimientos de aplicativos, equipos informáticos, software de acuerdo con el Procedimiento [P-TI-01 Atención a Requerimientos de Servicios TIC](#).



[PL04-ES5]

Los documentos de las licencias de uso de software, las claves para descarga desde las páginas de los fabricantes u otros medios que vengan originalmente en las versiones y sus respectivos manuales estarán bajo custodia de la OTSI.

[PL04-ES6]

El DNP es propietario de todos los activos de información tecnológicos y los administradores de estos activos son las personas usuarias, responsables por la información de sus procesos y del hardware o sistemas de información según corresponda el tipo de activo.

[PL04-ES7]

Los activos de Información del DNP no deben ser utilizados, para divulgar, propagar o almacenar contenido personal, comercial de publicidad, promociones, ofertas, programas destructivos (virus), o cualquier otro que afecte la disponibilidad de la plataforma tecnológica, la reputación de la Entidad o que su uso no esté autorizado.

[PL04-ES8]

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales. Las personas usuarias no deben realizar intencionalmente actos que impliquen mal uso de los recursos tecnológicos, como el envío de correos electrónicos masivos con fines no institucionales, la práctica de juegos en línea, navegación a sitios de alto riesgo, sitios con contenido pornográfico, chistes, terroristas, hackers, racistas, publicación de videos en línea, divulgación de cualquier contenido que represente riesgo para la red de la Entidad, que afecte la imagen y el buen nombre del DNP.

La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afectar la conexión a Internet, y la red interna.

[PL04-ES9]

Se encuentra prohibido el uso, e instalación de juegos, almacenar archivos con contenido pornográfico, software ilegal, software malicioso, música, videos, información de carácter personal o no institucional en los equipos del DNP, en los discos de red, SharePoint institucional y/o [servicios de Office 365](#). La OTSI realizará el monitoreo e informará a las dependencias para su respectiva eliminación.

[PL04-ES10]

Las personas usuarias no deberán realizar las siguientes labores sin previa autorización de la OTSI:

- Instalar software en cualquier equipo del DNP.
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del DNP.
- Modificar, revisar, transformar o adaptar cualquier software.
- Descompilar o realizar ingeniería de reverso en cualquier software.

[PL04-ES11]

La persona usuaria deberá informar a su jefe inmediato acerca de cualquier conocimiento que tenga de alguna violación sobre el uso adecuado o legal del software o sobre los derechos respectivos de autor.

[PL04-ES12]

La persona usuaria es responsable de todas las transacciones o acciones efectuadas con la cuenta asignada.



[PL04-ES13]

Cada persona usuaria es responsable de asegurar que el uso de redes externas, tal como internet, no comprometa la seguridad de los activos de información del DNP. Esta responsabilidad incluye, pero no se limita a, prevenir que intrusos tengan acceso los recursos de informáticos y de prevenir la introducción y propagación de virus.

El DNP procura la seguridad de su infraestructura, más no se hace responsable por el resultado de transacciones financieras personales que se realicen desde los equipos institucionales.

[PL04-ES14]

Todo archivo o material recibido a través de medio magnético, óptico, descargado de Internet o de cualquier red externa, deberá ser revisado para detección de virus y antes de ser colocados en la plataforma tecnológica del DNP.

[PL04-ES15]

Todo cambio a la plataforma tecnológica informática deberá ser formalizado a través del formato [F-TI-18 Solicitud de cambios](#) y será realizado de acuerdo con el procedimiento PT-TI-04 Control de Cambios de Tecnologías de la Información.

[PL04-ES16]

Es responsabilidad de las personas usuarias del DNP almacenar la información institucional en la plataforma tecnológica del DNP (discos de red o sistemas de información o aplicativos o portales o One Drive o SharePoint empresariales) según corresponda y que tenga relación con el ejercicio de sus funciones o actividades contractuales. En las estaciones cliente la información debe almacenarse en One Drive.

La Alta Dirección propenderá por la asignación de recursos económicos que permitan el cumplimiento de esta política.

[PL04-ES17]

En caso de requerir apoyo en la realización del backup o copia de seguridad de la información almacenada en las estaciones cliente la persona usuaria puede solicitarlo al Centro de Servicios.

Antes de autorizar cualquier acceso a la estación cliente (para servicios de mantenimiento, actualizaciones o cambios de equipos), la persona usuaria debe garantizar que ha realizado la copia de seguridad de su información.

[PL04-ES18]

El préstamo de portátiles se debe tramitar a través del Centro de Servicios con 48 horas de anticipación y se proveerán de acuerdo con la disponibilidad. Es responsabilidad de la persona usuaria la custodia y salvaguarda de la información almacenada y realización de la copia de seguridad de la información almacenada en el equipo prestado antes de su devolución al DNP. En caso de salida de los equipos fuera del DNP se deben seguir los procedimientos establecidos en el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#) de la Subdirección Administrativa y Relaciónamiento con la Ciudadanía.

[PL04-ES19]

Todos los bienes que son adquiridos, transferidos y/o donados al DNP son ingresados a una póliza de seguro de acuerdo con los procedimientos establecidos en el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#) de la Subdirección Administrativa y Relaciónamiento con la Ciudadanía.



[PL04-ES20]

Los equipos que ingresan temporalmente al DNP que son de propiedad de terceros, deben ser registrados por Las personas usuarias en la portería de los edificios donde están las oficinas del DNP, para controlar su respectiva salida; en caso de pérdida de los equipos el DNP no se hace responsable.

No es responsabilidad de la OTSI, ni del Centro de Servicios prestar servicio de soporte técnico (revisión, mantenimiento, reparación, configuración, creación de documentos y manejo e información), ni el suministro de elementos adicionales que posibilite la utilización de cualquier equipo que sea propiedad de terceros.

Si la persona usuaria utiliza equipos de su propiedad, la OTSI, solo asignará acceso a Internet a través de la red invitados.

[PL04-ES21]

Las claves de acceso a los activos de información son estrictamente confidenciales, personales e intransferibles.

Los responsables de cada servicio o activo de información deberán tomar las medidas necesarias para proteger la confidencialidad de las claves. Los servicios incluyen las redes sociales institucionales. Para coordinar la entrega de las claves en sobre sellado los responsables de cada servicio deben escribir al correo seguridad.ciber@dnpp.gov.co. Las contraseñas asignadas a los activos de información deben ser entregadas en sobre sellado e identificadas con el nombre del servicio o servidor, la fecha y quién las entrega.

[PL04-ES22]

Los delegados de las dependencias se denominan “*Webmaster de Edición de Contenido*” tienen las siguientes responsabilidades: Preparar la información de su dependencia, mantenerla actualizada, informar al Webmaster de Administración de contenido del Oficina Asesora de Comunicaciones lo relacionado con las nuevas publicaciones, actualizaciones y retiros realizados en la intranet, y portales del DNP.

[PL04-ES23]

El correo electrónico debe ser utilizado con propósitos laborales. El uso de mensajería masiva sólo está autorizado para el Oficina Asesora de Comunicaciones, la Subdirección de Gestión del Talento Humano y la OTSI, teniendo en cuenta las funciones de comunicación que cumplen.

No se permite el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red. El tamaño máximo del correo masivo interno para el DNP es de 35 MB.

La OTSI se reserva el derecho de filtrar los tipos de archivo que vengán anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus, malware, spam, phishing, programas destructivos o software. Si el virus, malware, u otro programa destructivo, phishing no puede ser eliminado, el mensaje será borrado.

[PL04-ES24]

En caso de pérdida de la información de los mensajes electrónicos almacenados en el buzón del servidor, la recuperación solamente se garantizará mientras La persona usuaria este activo en la Entidad, exceptuando los correos que la persona usuaria haya eliminado directamente en el servidor.



[PL04-ES25]

Las personas usuarias no deben usar el correo institucional para la creación de cuentas en redes sociales como Twitter, Facebook, Instagram, LinkedIn, YouTube, Flickr y similares. Con excepción del Oficina Asesora de Comunicaciones que tiene asignado un correo institucional para el manejo de redes sociales.

Para el uso de las redes sociales institucionales se debe tener en cuenta que el contenido publicado (gráfico, texto, video o cualquier otra forma) debe corresponder a la línea gráfica del Gobierno Nacional conceptualizada en la guía de sistema gráfico, cumplir con la normativa de derechos de autor, propiedad intelectual, normas constitucionales sobre privacidad y habeas data. El material publicado debe pertenecer a las Entidades del Gobierno de Colombia, o contar con la autorización para su uso. El contenido publicado tendrá como referencia el enlace de las Páginas Web de la Entidad.

El administrador de las redes sociales institucionales debe cerciorarse de que el mensaje se publique desde la cuenta institucional y no desde una cuenta personal, cuando haga uso de dispositivos móviles, como celulares.

Para la red social Whatsapp las dependencias enviarán los mensajes desde los números telefónicos autorizados y administradores de los grupos institucionales.

Las publicaciones no deben reflejar las opiniones o sentimientos personales del administrador de las redes sociales institucionales.

Las redes sociales institucionales deben ser utilizadas para la difusión de mensajes relacionados netamente con asuntos gubernamentales y avances de sus temáticas particulares de carácter institucional. En ningún caso el contenido publicado podrá ser utilizado por los administradores de estas para beneficios personales o de terceros. Está prohibido revelar [información clasificada, reservada](#) privada y confidencial de las Entidades del Gobierno, de conformidad con la normativa aplicable a la materia.

El administrador de las redes sociales institucionales dará respuesta oportuna a los comentarios de las personas usuarias de la red según los tiempos de respuesta establecidos por la Entidad.

[PL04-ES26]

La OTSI no presta el servicio de configuración de las redes sociales en los dispositivos móviles. Es responsabilidad del propietario del dispositivo móvil.

Para el uso de redes sociales, Las personas usuarias deben utilizar su correo personal no institucional, con la finalidad de reducir el riesgo de atribuciones erróneas al DNP sobre opiniones. Para la red social Whatsapp Las personas usuarias están autorizados a utilizar su número telefónico y dispositivo personal.

Las personas usuarias deben dejar expreso, y de manera visible en los perfiles de sus cuentas, que su comunicación es personal y no representa los puntos de vista de la Entidad, deben abstenerse de revelar información de carácter clasificada, reservada, confidencial de la Entidad para la que laboren.

En caso de que un jefe requiera la suspensión del acceso a redes sociales deberá manifestarlo a la OTSI a través del Centro de Servicios centrodeservicios@dnpc.gov.co.

[PL04-ES27]

Los correos electrónicos que salen de la Entidad tienen de forma automática la sentencia de confidencialidad con el siguiente contenido:



CONFIDENCIALIDAD: Este correo electrónico es correspondencia confidencial del DEPARTAMENTO NACIONAL DE PLANEACION, si Usted no es el destinatario le solicitamos informe inmediatamente al correo electrónico del remitente o a centrodeservicios@dnp.gov.co así mismo por favor bórralo y por ningún motivo haga público su contenido, de hacerlo podrá tener repercusiones legales.

Si Usted es el destinatario, le solicitamos tener absoluta reserva sobre el contenido, los datos e información de contacto del remitente o la quienes le enviamos copia y en general la información de este documento o archivos adjuntos, a no ser que exista una autorización explícita a su nombre.

CONFIDENTIALITY: This electronic mail is confidential correspondence of the DEPARTAMENTO NACIONAL DE PLANEACION, if you are not the addressee we ask you to report this to the electronic mail of the sender or to centrodeservicios@dnp.gov.co also please erase it and by no reason make public its content, on the contrary it could have legal repercussions.

If you are the addressee, we request from you not to make public the content, the data or contact information of the sender or to anyone who we sent a copy and in general the information of this document or attached archives, unless exists an explicit authorization on your name.

[PL04-ES28]

La OTSI se reserva el derecho de monitorear las cuentas de correo electrónico institucional que presenten un comportamiento sospechoso, sin que ello infrinja lo establecido por la Ley.

[PL04-ES29]

Las personas usuarias que requieran permisos de acceso, modificación, o eliminación en los discos de red, deben diligenciar el formato "[Cuadro actualización accesos y permisos al disco de red](#)" F-TI-01. El formato debe ser enviado por el jefe de la dependencia, y/o responsable de la información del área y remitir la solicitud al Centro de Servicios a través de correo electrónico.

Ante la imposibilidad de firmarlo el jefe de la dependencia, y/o responsable de la información del área debe enviar la solicitud a través de correo electrónico.

Los tipos de permisos que se pueden otorgar a las personas usuarias están dados por los siguientes Grupos:

Tabla 6: Tipos de permisos para cuentas de usuario en el DNP

GRUPOS	GRUPO DISCO O:\	GRUPO DISCO S, R, T, U
Grupo A	Dependencia Grupo _AO. Crea, modifica, elimina o lee carpetas y archivos.	Dependencia Grupo _AS Crea, modifica, elimina o lee carpetas y archivos.
Grupo G		Dependencia Grupo _GS Lee, escribe archivos. NO borra archivos, NO borra carpetas NO crea carpetas.
Grupo L	Dependencia Grupo _LO Lee y lista carpetas y archivos.	Dependencia Grupo _LS Lee y lista carpetas y archivos.

Para facilitar la administración de los permisos de las carpetas, se recomienda no crear subcarpetas superiores al séptimo nivel, los nombres de las carpetas deben ser máximo de veinticinco (25) caracteres y los nombres de los archivos de máximo treinta (30) caracteres.



[PL04-ES30]

Toda información, ya sea física o digital, que sea generada, almacenada o transformada por personas funcionarias, contratistas, pasantes o proveedores de la entidad, utilizando los recursos proporcionados por el DNP o en el ejercicio de sus funciones o servicios contratados, constituye un activo de información propiedad del Departamento Nacional de Planeación (DNP). Se prohíbe extraer, divulgar y/o publicar información física, digital, y/o almacenada en los discos de red, SharePoint y/o sistemas de información propiedad del DNP, sin expresa autorización de su jefe inmediato.

[PL04-ES31]

Se prohíbe el uso indebido de la información institucional con fines lucrativos o comerciales.

[PL04-ES32]

La responsabilidad de la organización, y contenido de los discos de red y/o SharePoint corresponde a cada una de las dependencias del DNP propietarias de la información, por lo tanto, es necesario revisarlo continuamente para evitar el uso inadecuado de espacio en disco. Cada dependencia es responsable del manejo y [clasificación de la información](#).

[PL04-ES33]

La responsabilidad de generar las copias de respaldo de la información de los discos de red está a cargo de la OTSI. La recuperación de la información solamente se garantizará los últimos doce (12) meses anteriores a la fecha de la solicitud.

[PL04-ES34]

La responsabilidad de custodiar información institucional fuera de las instalaciones del DNP está a cargo de la OTSI.

[PL04-ES35]

Ninguna persona usuaria debe manipular las impresoras, equipos de cómputo, u otro elemento tecnológico propiedad del DNP, en caso de presentarse problemas y/o fallas se deben reportar al Centro de Servicios centrodeservicios@dnpp.gov.co.

[PL04-ES36]

Es responsabilidad de la persona usuaria verificar que las hojas a utilizar en las impresoras no tengan ningún elemento como ganchos, clips, plásticos entre otros, que puedan afectar su funcionamiento.

[PL04-ES37]

Los documentos impresos deben ser de carácter institucional. Es responsabilidad de la OTSI publicar mensualmente en el disco O los reportes de impresión por pisos, dependencias y las cuentas de usuario para que todos las personas usuarias del DNP y la persona que ejerza la jefatura del área responsable pueda ejercer control en cada una de sus direcciones. La Información puede ser consultada en O:\Sistemas\Reportes Informaticos\Impresion.

[PL04-ES38]

Se debe dejar establecido en las fichas técnicas de impresoras de los procesos contractuales y de los convenios que suscriba el DNP, que dichas máquinas deben ser impresoras multifuncionales a blanco y negro y que tengan habilitada la función de impresión a doble cara (dúplex) de forma automática.



Está permitido para la Alta Dirección contar con impresoras a color para el desempeño de sus funciones misionales. Tales dependencias son: Dirección General, Subdirección General de Prospectiva y Desarrollo Nacional, Subdirección General de Descentralización y Desarrollo Territorial, Subdirección General de Inversiones, Seguimiento y Evaluación, Subdirección General del Sistema General de Regalías, Secretaría General.

[PL04-ES39]

Es responsabilidad de la Oficina de Tecnología y Sistemas de Información la gestión de puntos de red.

[PL04-ES40]

El DNP reconoce que la información es uno de sus principales activos intangibles, por tal razón promoverá a través de campañas de sensibilización a las personas usuarias la importancia de su protección y mitigar el riesgo de error humano, fraude o mal uso de estos.

[PL04-ES41]

La Oficina de Tecnología y Sistemas de Información debe ofrecer mecanismos de seguridad a los servicios de tecnología de información y comunicación, TIC.

[PL04-ES42]

En caso de que una dependencia del DNP necesite dar información [clasificada y/o reservada](#) a un [tercero](#), deberá hacerlo de acuerdo con los documentos de confidencialidad establecidos por el DNP, en cumplimiento de la ley de protección de datos.

[PL04-ES43]

Cualquier tipo de información del DNP no debe ser vendida, transferida, intercambiada con terceros para ningún propósito diferente a cumplir con la misión del DNP, teniendo en cuenta que se debe contar con una autorización previa por parte del Jefe Inmediato.

[PL04-ES44]

La información del DNP debe ser clasificada en términos del valor, de los requisitos legales y de su sensibilidad e importancia para el DNP de acuerdo con el criterio de cada dependencia y a las [premisas de básicas de seguridad de confidencialidad](#) adoptado por el DNP en este documento.

[PL04-ES45]

Los administradores de infraestructura deben contar con un inventario actualizado de los dispositivos en producción y stock. Adicionalmente deben contar un mapa topológico actualizado.

[PL04-ES46]

La creación de grupos institucionales en WhatsApp debe realizarse con fines exclusivamente institucionales y laborales. El uso está autorizado para la Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación, considerando sus funciones de comunicación y gestión integral de la continuidad de negocio.

[PL04-ES47]

Los administradores de los grupos institucionales en WhatsApp de la Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación son los responsables de la gestión, administración y respuesta oportuna a las personas colaboradoras según los tiempos de respuesta del procedimiento [PT-PG-05 Atención a peticiones, quejas, reclamos, sugerencias y denuncias establecido por la Entidad.](#)



Es responsabilidad de la Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación mantener actualizados los datos de contacto de los administradores de los grupos institucionales en WhatsApp. En caso de que un administrador se retire de la Entidad, el jefe de la dependencia correspondiente debe garantizar la entrega adecuada de la administración del grupo institucional al nuevo responsable designado.

[PL04-ES48]

La Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación se reservan el derecho de monitorear las conversaciones de los grupos institucionales en WhatsApp, aquellas personas colaboradoras que presenten un comportamiento sospechoso serán retirados de los grupos sin que ello infrinja lo establecido por la Ley.

[PL04-ES49]

Las personas colaboradoras son responsables de tener instalado un antivirus en sus dispositivos personales, se recomienda la instalación del provisto por la Entidad, tomando en cuenta que Whatsapp es un canal de comunicación abierto y pueden recibir mensajes sospechosos desde otro chat y/o canales que no son del DNP. El DNP no se hace responsable de los mensajes, la interpretación individual de los mismos y las posibles afectaciones que éstos puedan generar.

[PL04-ES50]

La información divulgada a través de los grupos institucionales en WhatsApp tiene carácter institucional y es de acceso público. Por lo tanto, la dependencia solicitante de la divulgación es responsable de revisar que la información compartida no contenga datos personales, [información clasificada, reservada](#) y/o recolecte datos institucionales. Para tales fines, se deben utilizar los canales oficiales como el correo electrónico y/o la intranet.

[PL04-ES51]

Las dependencias que requieran divulgación a través de los grupos institucionales en WhatsApp deben seguir los procedimientos establecidos en el [proceso PR-GC Gestión de las comunicaciones](#).

[PL04-ES52]

La divulgación de información a través de los grupos institucionales en WhatsApp se llevará a cabo exclusivamente durante el horario laboral, de acuerdo con la Ley 2191 de 2022 (Ley de desconexión laboral), a menos que se trate de situaciones de emergencia o continuidad del negocio, que son excepciones permitidas.

[PL04-ES53]

Las personas colaboradoras tienen el derecho de revocar su autorización en conformidad con la Ley de Protección de Datos Personales, retirándose voluntariamente de los grupos institucionales en WhatsApp en cualquier momento. En caso de que deseen ser incluidos nuevamente, deben ponerse en contacto con la Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación.

[PL04-ES54]

Los colaboradores tienen la opción de actualizar y corregir su número de contacto notificando a la Oficina Asesora de Comunicaciones y la Oficina Asesora de Planeación, quienes se encargarán de hacer las modificaciones necesarias en los grupos institucionales en WhatsApp.

[PL04-ES55]

Las dependencias que requieran crear, actualizar buzones institucionales para envío y/o recepción de información (interna y/o externa) deben solicitarlo al centro de servicios a través [del portal](#), indicando la persona funcionaria responsable, dependencia de este. Al buzón se le asignará una vigencia de máximo un año a partir



de su creación después de ese periodo se desactivará automáticamente. En caso de que la dependencia requiera su habilitación, modificación y/o eliminación el jefe de la dependencia debe realizar la solicitud. Si el buzón solicitado recibe información externa la dependencia solicitante es responsable de configurar el mensaje de notificación automática que la Subdirección Administrativa y Relaciónamiento con la Ciudadanía definió sobre los canales autorizados para radicar las PQRDS.

[PL04-ES56]

Las dependencias son responsables de identificar, actualizar y clasificar los activos de acuerdo con el [M-PG-13 Manual para la identificación de activos de información](#), durante la actualización de la información las dependencias pueden solicitar apoyo a la persona con el rol de Oficial de Seguridad de la información para la solución de inquietudes sobre el manual mencionado.

13.5. Control de acceso

El DNP implementara controles para la protección de los activos de información (red, sistemas de información, aplicativos, portales, servicios tecnológicos e infraestructura física (Instalaciones))

[PL05-ES1]

La identificación de las personas usuarias ante cada sistema de información será única y confidencial.

[PL05-ES2]

Las personas colaboradoras, proveedoras y usuarias externas son responsables de seguir una buena política para la selección de las claves de acceso y deben garantizar que su “*contraseña*” se conserva personal e intransferible. Por lo que se dan las siguientes recomendaciones:

- La “*contraseña*” debe cambiarse con periodicidad; por lo menos cada dos meses.
- Cuando se cambie la clave de acceso no se debe utilizar las que se hayan usado previamente.
- No debe escribir la “*contraseña*” en papel o en una agenda al alcance de otras personas.
- No preste su contraseña es personal e intransferible.

[PL05-ES3]

Todas las personas colaboradoras, proveedoras y usuarias externas deben garantizar que su “*contraseña*” es fuerte, es decir, difícil de deducir, por lo tanto, la contraseña debe seguir las siguientes recomendaciones:

- Debe tener al menos ocho (8) caracteres.
- No utilizar nombres propios de personas, mascotas, equipos deportivos ni fechas, ni similares.
- No utilizar caracteres repetidos (por ejemplo: AAAA, xxx, etc.).
- No utilizar “*contraseñas*” con caracteres incrementales, por ejemplo: MARIA1, MARIA2.
- Usar “*contraseñas*” no pronunciables y sin significado obvio.
- Ser significativamente diferente de otras contraseñas anteriores.
- Usar combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales como:
! " # \$ % & & / () = ? ; > < [*]

[PL05-ES4]

Toda creación de usuario debe ser asociado directrices de duración y permisos de acceso a los activos de información asignados por sus funciones y/o actividades contractuales, solicitados por la dependencia al centro de servicios y/o personas que ejerzan el rol de líderes funcionales, técnicos y administradores de los sistemas



de información. Los líderes funcionales, técnicos deben realizar la depuración periódica de usuarios previo reporte de las áreas que consolidan el ingreso y/o retiro de personal y/o la información proporcionada por la OTSI.

[PL05-ES5]

Las cuentas pertenecientes a usuarios que ya no tengan vínculo alguno con el DNP deben ser retiradas de todos los servicios informáticos previa solicitud del jefe de área y/o supervisor del contrato.

[PL05-ES6]

La asignación de cuentas o identificadores de usuario se debe realizar bajo el estándar para nombrar usuarios del DNP.

[PL05-ES7]

Las cuentas de usuario se asignarán con privilegios de usuario normal, es decir sin privilegios de administración. Las personas usuarias que requieran permisos de administrador (servidores y/o estaciones cliente) deberán diligenciar el formato [Compromiso perfiles especiales F-TI-19](#), el cual debe ser solicitado por los jefes de dependencia, coordinadores de grupo y/o supervisores y validado por la OTSI.

[PL05-ES8]

Las contraseñas predefinidas que traen los elementos nuevos tales como servidores, bases de datos, aplicaciones, routers, switches, etc., deben cambiarse inmediatamente antes de colocarla en producción.

[PL05-ES9]

Cuando el Centro de Servicios asigne cuentas de usuario y una nueva contraseña, esta debe ser segura evitando así la implementación clásica de claves genéricas, la persona usuaria la utilizará solo en el primer inicio de sesión obligándolo a realizar el cambio para acceder al servicio.

Para facilitar el cambio de las contraseñas, las personas usuarias pueden consultar el [instructivo de cambio de contraseña disponible en la intranet](#), adicionalmente la persona usuaria puede contactar al [Centro de Servicios](#) para su acompañamiento en la recuperación.

[PL05-ES10]

En los Servidores Windows y estaciones cliente se debe habilitar el control automático de bloqueo con contraseña, para las sesiones que permanecen más de cinco (5) minutos inactivos. Esta política no aplica para los equipos de las salas de reuniones con el fin de evitar interrupciones en las mismas. Durante el bloqueo de pantalla se mostrarán las imágenes provistas por el sistema operativo.

[PL05-ES11]

Las personas usuarias no deben dejar sus estaciones de trabajo con la sesión abierta.

[PL05-ES12]

En los puestos de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de las labores.

- Mantener organizado y en orden el puesto de trabajo. Los archivadores y escritorios que tienen cerradura deben permanecer cerrados.
- No dejar documentos confidenciales (como contraseñas, información con datos personales, [información clasificada o reservada](#) de la dependencia) a la vista de otras personas en documentos, post-it, etc.



- Los documentos confidenciales deben ser destruidos antes de ser arrojados a la basura.
- Al finalizar las labores diarias o si la persona usuaria se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.

[PL05-ES13]

Las personas usuarias son responsables de no ingerir alimentos ni bebidas en el puesto de trabajo.

[PL05-ES14]

Las personas usuarias son responsables de apagar los activos de información tecnológicos (estaciones cliente, portátiles, televisores e impresoras) al finalizar la jornada.

[PL05-ES15]

Las personas usuarias deben recoger los trabajos de impresión que contengan [información confidencial, clasificada, reservada](#) de forma inmediata.

[PL05-ES16]

Mostrar una advertencia indicando la responsabilidad que asume la persona usuaria en el momento que accede a los activos de información.

[PL05-ES17]

No mostrar la contraseña que se introduce.

[PL05-ES18]

El DNP compartirá información con Entidades con las cuales establezca convenios de intercambio de información. Dicho intercambio estará protegido mediante las conexiones con certificados de sitio web seguro (SSL), para garantizar la seguridad de la información entre las Entidades participantes.

[PL05-ES19]

Los activos de información dispuestos por el DNP para el apoyo de las labores desempeñadas por las personas funcionarias, pasantes, o algunos contratistas y/o proveedores deben ser usados con propósitos laborales.

[PL05-ES20]

Las personas usuarias deben mantener la configuración establecida por la OTSI (Ej.: mecanismos de protección antivirus y la activación de un firewall en el equipo portátil).

[PL05-ES21]

Las personas usuarias deben reportar el extravío o hurto de los equipos del DNP a la Subdirección Administrativa y Relacionamento con la Ciudadanía forma inmediata de acuerdo con el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#).

[PL05-ES22]

Las personas usuarias podrán solicitar al Centro de Servicios la implementación de autenticación doble factor para proteger el acceso a la cuenta de correo electrónico.

[PL05-ES23]

El acceso a los datos, aplicaciones y servicios multimedia almacenados en la plataforma Office 365 (One Drive institucional, SharePoint, Correo Electrónico, Power BI, Forms, Stream, etc.) sólo serán otorgados por la



persona usuaria propietaria, en caso de que la cuenta de usuario este desactivada al momento de la solicitud se requiere a autorización de la persona que ejerza la jefatura de la dependencia.

[PL05-ES24]

Para la creación de formularios de recolección de información, las herramientas institucionales son SharePoint o Forms de Office 365, lo anterior con el fin de garantizar que la información este en la plataforma tecnológica del DNP. El uso de otras herramientas online, requieren el aval y acompañamiento de la OTSI para evitar incidentes de seguridad de la información.

[PL05-ES25]

Cuando las personas usuarias requieran compartir información con usuarios internos y externos, las herramientas institucionales son SharePoint y One Drive. El uso de otras herramientas para compartir información, requieren el aval y acompañamiento de la OTSI para evitar incidentes de seguridad de la información.

13.6. Criptografía

El DNP implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información y determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

[PL06-ES1]

Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basado en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación según las necesidades.

[PL06-ES2]

Cuando se creen nuevos aplicativos, portales, sistemas de información las dependencias responsables deben solicitar a la OTSI la configuración de los certificados de sitio web seguro (SSL), a fin de garantizar que las comunicaciones sean seguras.

[PL06-ES3]

Se utilizarán controles criptográficos en los siguientes casos:

- 1) Para la protección de claves de acceso a sistemas, datos y servicios.
- 2) Para la transmisión de [información clasificada, reservada](#), fuera del ámbito del DNP.
- 3) Para el resguardo de información, cuando así se determine a partir de la evaluación de riesgos realizada por el dueño del activo de información, o por el área responsable de la seguridad de la información.
- 4) Para los activos de información que, a partir de la evaluación de riesgos requieran la implementación de este control.

[PL06-ES4]

La OTSI será el responsable de la gestión administrativa de los tokens relacionados con firma digital. La Subdirección de Gestión del Talento Humano será el responsable informar a la OTSI quienes son las personas usuarias autorizados para firmar, para que esta oficina realice la instalación de estos.

La Subdirección Administrativa y Relacionamiento con la Ciudadanía será responsable de la capacitación en el uso de la firma digital en el Sistema de Gestión Documental del DNP.



La persona usuaria que este autorizado para realizar el proceso de firma digital será responsable de todas las transacciones y acciones efectuadas con el token. Ninguna persona usuaria podrá firmar utilizando el token de otra persona.

En caso de pérdida de token de firma digital u olvido de la contraseña la persona usuaria debe informar a la OTSI, para ejecutar el proceso administrativo respectivo.

[PL06-ES5]

Se debe almacenar y/o transmitir la información digital clasificada como [reservada o clasificada](#) bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

[PL06-ES6]

Los sistemas de información o aplicativos que requieran realizar transmisión de información reservada o restringida, deberán implementar mecanismos para cifrado de datos.

[PL06-ES7]

Se debe contar con un procedimiento para el manejo y la administración de los certificados de sitio web seguro (SSL),²² y para la aplicación en las publicaciones que lo requieran.

[PL06-ES8]

Los líderes técnicos de TIC (internos o externos) deben cifrar la [información reservada y/o clasificada](#) y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

De igual manera deben asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los procedimientos y estándares adoptados por la Entidad.

13.7. Seguridad física y ambiental

El DNP adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

[PL07-ES1]

El líder de proyectos del Centro de Servicios es el responsable de velar por el cumplimiento de las políticas del centro de datos.

[PL07-ES2]

No se permite el ingreso al centro de datos a personal no autorizado.

[PL07-ES3]

La Subdirección Administrativa y Relacionamiento con la Ciudadanía debe garantizar que el control de acceso al centro de datos del DNP, cuente con dispositivos electrónicos de autenticación y/o sistema de control biométrico de acuerdo con el [M-AD-02 Manual para la Administración Logística](#).

[PL07-ES4]

La Subdirección Administrativa y Relacionamiento con la Ciudadanía debe garantizar que todos los equipos de los centros de datos y de las sedes cuenten con fuentes ininterrumpidas de poder y estabilizadores de potencia.

²² El procedimiento es de uso interno para la OTSI.



[PL07-ES5]

La limpieza y aseo del centro de datos y afines está a cargo de la Subdirección Administrativa y Relacionamiento con la Ciudadanía y debe efectuarse en presencia de una persona funcionaria o un contratista autorizado. Dicho personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sirvan para su labor de limpieza aseo.

[PL07-ES6]

Por ningún motivo se debe fumar, comer o beber en el área de centro de datos.

[PL07-ES7]

El centro de datos debe estar provisto de piso elaborado con materiales no combustibles.

[PL07-ES8]

Se debe contar con instrumentos capaces de registrar las condiciones de humedad y temperatura.

[PL07-ES9]

El centro de datos debe tener un sistema de refrigeración por aire acondicionado. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la prestación del servicio.

[PL07-ES10]

El centro de cómputo debe tener unidades de potencia ininterrumpida UPS que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea, de acuerdo con la autonomía de los equipos que prestan el respaldo.

[PL07-ES11]

Eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego.

[PL07-ES12]

La Subdirección Administrativa y Relacionamiento con la Ciudadanía debe garantizar que se cuente con alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectados a un sistema central.

[PL07-ES13]

Los detectores deberán ser probados de acuerdo con las recomendaciones del fabricante, por lo menos una vez al año y esta prueba deberá estar prevista con su respectiva documentación.

[PL07-ES14]

Se deben tener extintores de incendios o un sistema contra incendios debidamente probados, y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

[PL07-ES15]

El cableado de la red del centro de datos debe ser protegido de interferencias.

[PL07-ES16]

Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.



[PL07-ES17]

Está prohibida la grabación de video en las instalaciones del centro de datos por personal externo al DNP.

[PL07-ES18]

Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por una persona funcionaria o contratista autorizado del DNP.

[PL07-ES19]

Las puertas del centro de datos deben permanecer cerradas y con las luces apagadas en los momentos en los que no se realicen actividades.

[PL07-ES20]

Cuando se requiera realizar alguna actividad sobre algún centro de cableado (Rack), este debe quedar ordenado, sus puertas frontales deben quedar cerradas y con llave cuando se finalice la actividad.

[PL07-ES21]

El centro de datos debe estar monitoreado para controlar las fallas que puedan presentarse.

[PL07-ES22]

En el centro de datos tiene una planilla, donde se registran la(s) actividad(es), los responsables y los tiempos de actividad.

[PL07-ES23]

A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos de cómputo como computadores, monitores. Los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por la Subdirección Administrativa y Relaciónamiento con la Ciudadanía.

[PL07-ES24]

Los cables de red deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

[PL07-ES25]

Deben existir planos que describan las conexiones del cableado (voz y eléctricos) custodiados por el Coordinador asignado de la Subdirección Administrativa y Relaciónamiento con la Ciudadanía y de datos custodiados por el líder del centro de servicios.

[PL07-ES26]

El acceso a los centros de cableado (Racks) debe estar protegido, sus puertas deben permanecer cerradas y la llave de acceso debe ser custodiado por el centro de servicios.

[PL07-ES27]

El DNP debe mantener contratos de soporte 7x24 y mantenimiento de los equipos críticos, de acuerdo con la disponibilidad de recursos.

[PL07-ES28]

Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.



[PL07-ES29]

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía en el centro de datos o cualquiera que pueda ocasionar una suspensión en el servicio deben ser realizadas y programadas a través del centro de servicios.

[PL07-ES30]

Cuando la OTSI requiera retirar equipos de las instalaciones del DNP para reparación o mantenimiento deben estar debidamente autorizados de acuerdo con el [M-AD-01 Manual Administración de bienes muebles e inmuebles](#) de la Subdirección Administrativa y Relacionamiento con la Ciudadanía y garantizando que en dichos elementos no se encuentre información de carácter [clasificada y reservada](#).

[PL07-ES31]

Para los equipos fuera de las instalaciones se debe suministrar un nivel mínimo de seguridad que al menos cumpla con los requerimientos internos teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior del DNP.

[PL07-ES32]

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe garantizarse la eliminación de toda información residente en los equipos utilizados para el almacenamiento, procesamiento y transporte de la información. Lo anterior utilizando tecnologías para realizar sobrescrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

[PL07-ES33]

Las personas funcionarias, contratistas, pasantes o proveedores que utilicen activos de información tecnológicos personales para el desarrollo de sus actividades laborales o contractuales son responsables de:

- a) Registrar el ingreso y retiro mediante los procedimientos establecidos por la administración del Edificio.
- b) Registrar la solicitud de conexión a la red institucional en el formulario “Red portátil personal” de portal de usuarios de la herramienta CA.
- c) Implementar medidas de seguridad físicas para la protección de los activos de información tecnológicos. El DNP no se hace responsable por el daño que se presenten al conectarse a la red eléctrica u otros eventos.
- d) Implementar medidas de seguridad en el transporte de los equipos de cómputo. El DNP no se hace responsable por la pérdida de estos bienes.
- e) Permitir la instalación del antivirus institucional en el equipo de cómputo con el fin de salvaguardar la red wifi.
- f) Instalar One Drive institucional en el perfil que contiene la información corporativa con el fin de realizar backup periódico de la información institucional almacenada en el equipo de cómputo personal.
- g) Instalar Teams institucional para la gestión remota y respuesta ante incidentes que se presenten con el uso de los activos de información institucionales.
- h) Permitir la recolección de los datos técnicos del equipo de cómputo con el fin de permitir el acceso a la red wifi.
- i) Conectarse a la red wifi DNP-Colaboradores, utilizando su usuario y contraseña institucional.
- j) Configurar mecanismos de protección de contraseña robusta en el equipo de cómputo personal.
- k) Configurar la separación entre la información personal y la información corporativa en el equipo de cómputo personal.



[PL07-ES34]

El retiro e ingreso de todo activo informático propiedad de los visitantes que ingresen al DNP (consultores, pasantes, visitantes) debe ser registrado en la portería del edificio para el respectivo control de ingreso y salida y es obligatoria acatar los procedimientos para el registro de bienes y las medidas de seguridad establecidas.

El personal de vigilancia de la recepción verifica y registra las características de identificación del activo a la entrada y a la salida.

En los casos en que no se hubiera registrado el ingreso a la Entidad, para su retiro se debe solicitar autorización a la Subdirección Administrativa y Relaciónamiento con la Ciudadanía, con el fin de realizar la verificación contra los registros de inventarios.

[PL07-ES35]

Los activos se reciben en la bodega del DNP y el acceso a esta área está autorizado solo al personal identificado y autorizado, sin embargo, por la naturaleza de ciertos bienes, estos se podrán recibir directamente en el lugar donde se utilizarán, situación que se estipulará en el respectivo contrato.

[PL07-ES36]

La Subdirección Administrativa y Relaciónamiento con la Ciudadanía definirá las áreas seguras y los controles de acceso físico (seguridad física y del entorno controles de monitoreo sobre esa área segura, como control de temperatura, humedad, alarma contra incendios, cámaras de vigilancia, entre otros.) para la protección de la información que allí se procese y almacene. La OTSI será la responsable de dichos controles para el centro de datos aplicando las mejores prácticas.

[PL07-ES37]

Todas las personas que ingresen a las instalaciones del DNP deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

13.8. Gestión de operaciones

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la entidad. La OTSI y las dependencias planean, gestionan, respaldan y monitorean la infraestructura tecnológica con el fin de establecer los controles de seguridad pertinentes que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

[PL08-ES1]

Las personas usuarias deben ser conscientes de los riesgos legales que implica la utilización de los medios electrónicos, especialmente en cuanto a la responsabilidad disciplinaria, penal y/o civil en la que pueden incurrir por los inconvenientes, perjuicios y/o reclamaciones de cualquier tipo que llegaren a presentarse como resultado de cualquiera de las siguientes conductas, entre otras:

- Enviar o reenviar información [clasificada, reservada](#) o sensible, sin estar legalmente autorizado para ello.
- Reenviar o copiar sin permiso mensajes "*confidenciales*", clasificados, reservados o protegidos por las normas sobre derechos de autor, o contra expresa prohibición del originador.
- Enviar o reenviar un correo electrónico con cualquier contenido difamatorio, ofensivo, racista u obsceno.
- El uso de internet no debe afectar el oportuno y eficiente cumplimiento de las funciones asignadas, ni la obligación de dedicar la jornada laboral a la realización de tales funciones.



- Evite suscribirse en boletines en línea, con el correo institucional, esto evita la llegada de cadenas de correo, publicidad, etc.

[PL08-ES2]

Todas las personas usuarias del correo electrónico e internet deberán cumplir con las siguientes reglas, sin demeritar ninguna otra expedida por el DNP:

- Todo correo de origen desconocido o de dudosa procedencia, debe ser eliminado, sin abrir, para evitar el contagio de algún virus informático.
- La utilización de estas herramientas (correo electrónico e internet) debe ser racional, eficiente y segura, por lo cual deberá evitarse cualquier actividad que pueda poner en riesgo los equipos y sistemas del DNP o que pueda afectar su correcto y adecuado funcionamiento.
- Está prohibido utilizar estas herramientas, (correo electrónico e internet) como medio para generar o transmitir mensajes que puedan afectar de cualquier manera la imagen, dignidad y buen nombre de terceras personas o del DNP.
- El material que contenga carácter fraudulento, ilegal que vaya en contra de la moral o buena conducta, no podrá ser enviado por correo electrónico o cualquier otra forma de comunicación electrónica (tal como: grupos de noticias, grupos de conversación o chats) o exhibido o almacenado en los equipos del DNP.
- Está prohibido adulterar o intentar adulterar mensajes de correo.
- No está permitido enviar mensajes de correo utilizando la cuenta de correo de otra persona exceptuando la administración de calendarios compartidos cuando el jefe inmediato lo autorice.
- Las listas de distribución son administradas por el responsable del servicio en la OTSI y requieren autorización del jefe inmediato.
- No se puede cambiar o disfrazar, o intentar cambiar o disfrazar el campo de identificación de quien origina el correo.
- Está prohibido enviar información [confidencial, clasificada o reservada](#) del DNP a personas u organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley, y por parte de las personas usuarias internos autorizados internamente para ello.
- No responda mensajes donde le solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Informe al centro de servicios con el fin de bloquear dicho remitente y evitar que esos mensajes lleguen a más personas funcionarias, contratistas y/o pasantes.

[PL08-ES3]

El DNP establecerá controles de acceso a internet para minimizar el riesgo, regular el tráfico y en consecuencia prestar un mejor servicio. El control de acceso a internet será medido con base a la navegación sobre grupo de páginas (por ejemplo, categorías) consideradas como no productivas para el DNP. Es decir, que no sirvan de apoyo para el desempeño de las funciones de las personas usuarias del DNP, que no son de interés general o que son obscenas.

[PL08-ES4]

La OTSI configurará permisos y colocará restricciones de acceso a páginas de Internet según el estándar anterior o por solicitud de un jefe, subdirector, director.



[PL08-ES5]

El DNP tiene el derecho de monitorear todos los aspectos relacionados con sus sistemas de cómputo, incluyendo, pero no limitándose a, grupos de conversación o chats, de noticias, revisión de material descargada de internet, monitoreo de sitios visitados en internet, revisión del correo enviado/recibido por el usuario.

[PL08-ES6]

El DNP puede utilizar tecnología para identificar y bloquear sitios de internet con material considerado inadecuado bajo las regulaciones colombianas. En el evento, que la persona usuaria encuentre este tipo de material en internet, deberá desconectarse del sitio en forma inmediata.

[PL08-ES7]

La persona usuaria deberá borrar todos los correos de cadena masivos (no relacionados con la misión del DNP) y abstenerse de reenviarlos otras personas.

[PL08-ES8]

El acceso a la red inalámbrica del DNP, tendrá 5 tipos de grupos de acceso:

- DNP-FUNCIONARIOS (Exclusiva para usuarios registrados en el Dominio del DNP).
- DNP-INVITADOS (Exclusiva para todos los invitados del DNP con portátiles y tablets).
- DIRECCION GENERAL (Exclusiva conexión director general).
- WIFI GRATIS PARA LA GENTE (Exclusiva visitantes servicio al ciudadano).
- DNP-COLABORADORES (Exclusiva para equipos de cómputo personales de personas funcionarias, contratistas, pasantes)

[PL08-ES9]

Es responsabilidad de la OTSI, mantener debidamente actualizada toda la documentación referente a los procedimientos operativos relacionados con la plataforma tecnológica del DNP. Los líderes técnicos y funcionales son responsables de la actualización de los catálogos y hojas técnicas de servicio de los sistemas de información, portales, aplicativos a su cargo.

[PL08-ES10]

Los cambios que se presenten en las actividades de operación²³ de la OTSI deben ser actualizados en los respectivos documentos.

[PL08-ES11]

Cualquier cambio a la plataforma tecnológica deberá ser gestionado con el procedimiento PT-TI-04-Control de Cambios de Tecnologías de la Información, documentado y controlado a través del [formato solicitud de cambios \(F-TI-18\)](#) y se informará a través de correo electrónico a través del centro de servicios como “*Ventana de Mantenimiento*”. Si no puede realizarse se reprogramará dicha actividad.

[PL08-ES12]

Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas por la OTSI para la adecuada puesta en producción.

²³ Operación: incluye la administración de la plataforma tecnológica y las actividades que realiza a OTSI en el cumplimiento de sus funciones descritas en el Decreto 1893 de 2021.



[PL08-ES13]

Los cambios deben claramente detallar las actividades previas, las actividades durante el cambio, las actividades posteriores al cambio y las actividades en caso de regreso del cambio (Rollback).

[PL08-ES14]

Los administradores de los sistemas o coordinadores de grupo que originan el cambio son los responsables de presentar y coordinar todas las actividades para su ejecución.

[PL08-ES15]

Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral. Se debe contar con la participación de los encargados del servicio.

[PL08-ES16]

El DNP contará permanentemente con las herramientas de protección a nivel de red y de estaciones de trabajo, contra código malicioso que será administrado por la OTSI o el centro de servicios.

[PL08-ES17]

Todos los equipos institucionales que se conecten a la red LAN o a las redes DNP-FUNCIONARIOS y WIFI DVR deben tener instalado el antivirus institucional actualizado.

[PL08-ES18]

Es responsabilidad de cada persona usuaria, revisar que todos los medios extraíbles sean verificados con un antivirus provisto por el DNP, antes de procesarlos en los computadores institucionales o servidores del DNP.

[PL08-ES19]

Es responsabilidad del administrador del antivirus mantener en estado óptimo de funcionamiento (configuración, actualización, licenciamiento) las herramientas y procedimientos que permitan prevenir, detectar y corregir incidentes por código malicioso.

[PL08-ES20]

El antivirus debe ser configurado desde la consola para que diariamente realice escaneo de detección de código malicioso y lo reporte a la consola.

[PL08-ES21]

Los equipos que reporten código malicioso o virus serán aislados de la red LAN hasta tanto sea remediado y se implementen los controles de protección.

[PL08-ES22]

En casos de excepción, sólo se debe permitir la utilización de código ActiveX²⁴ firmados por Entidades de confianza.

[PL08-ES23]

Las copias de respaldo de la información del DNP deben ser realizadas según lo establecido en el procedimiento establecido por la OTSI.

²⁴ Es una tecnología de Microsoft para el desarrollo de páginas dinámicas.



[PL08-ES24]

Deben existir al menos dos copias de la información de los discos de red, una de las cuales deberá permanecer fuera de las instalaciones del DNP.

[PL08-ES25]

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el responsable de la información.

[PL08-ES26]

Los operadores del centro de cómputo periódicamente verificarán la ejecución correcta del backup en el sistema de almacenamiento dispuesto para tal fin.

[PL08-ES27]

El centro de servicios debe mantener un inventario actualizado de las copias de respaldo.

[PL08-ES28]

El centro de servicios es responsable de formatear a bajo nivel los discos duros, aun si éstos van a ser reutilizados. Los discos duros que vayan a ser eliminados por falla, deterioro u obsolescencia deben surtir un proceso de borrado seguro²⁵ y posteriormente serán destruidos por medios mecánicos.

[PL08-ES29]

Es responsabilidad de cada dependencia mantener depurada la información de las carpetas designadas en los discos de red y/o SharePoint, como mejor práctica para la optimización de uso de los recursos que entrega el DNP a las personas usuarias de la dependencia.

[PL08-ES30]

Toda conexión a la red debe contar con un mecanismo de autenticación que valide al usuario.

[PL08-ES31]

Toda estación cliente que se conecte a la red LAN, DNP-FUNCIONARIOS o WIFI DVR, debe estar debidamente autorizada, debe ser incluida en el dominio y cumplir con los mecanismos de control de seguridad como instalación de actualizaciones, herramienta de gestión y antivirus actualizado.

[PL08-ES32]

La conexión de terceras partes a la red LAN del DNP se hará cumpliendo con la debida autorización de la OTSI y con una aceptación por parte de la persona usuaria de cumplir con las características de seguridad y políticas definidas por el DNP.

[PL08-ES33]

La conexión de las personas usuarias que realicen labores de carácter temporal se hará a la red de invitados en la cual solo tendrán acceso al servicio de internet, sin necesidad de incluirlo al dominio.

[PL08-ES34]

La seguridad informática debe tener mecanismos de control que incluyan: [Firewall](#), [Filtro de contenido](#), Antivirus, Antispam y análisis de vulnerabilidades.

²⁵ El borrado seguro se ejecuta cuando al borrar un archivo o formatear un dispositivo de almacenamiento, alguna utilidad de borrado escribe ceros (0) sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente. Tomado de: http://es.wikipedia.org/wiki/Borrado_de_archivos



[PL08-ES35]

Las conexiones con las redes públicas deben estar protegidas por un Firewall y los mecanismos de control, que posea las reglas apropiadas para filtrar el tráfico permitido entre las redes.

[PL08-ES36]

La red interna del DNP debe contar con una segmentación lógica o física que agrupe los elementos de red con al menos los siguientes segmentos: Red LAN que contiene las estaciones cliente, red inalámbrica y la red de servidores.

[PL08-ES37]

El coordinador del grupo de gestión de infraestructura tecnológica es el responsable por garantizar que los medios removibles a cargo del centro de cómputo sean destruidos antes de darlos de baja.

[PL08-ES38]

Los equipos que van a ser objeto de reemplazos por daño de alguno de sus componentes se les debe retirar los medios removibles antes de la salida del DNP.

[PL08-ES39]

Cuando se requiera conectar la red o sistemas de información del DNP con otra Entidad, o sistemas de información, debe ser evaluado por el área funcional en conjunto con la OTSI para su respectiva aprobación.

[PL08-ES40]

El acceso a los buzones de correo electrónico debe estar controlado por contraseña.

[PL08-ES41]

Los correos electrónicos que vengan de personas desconocidas deben ser tratados con precaución.

[PL08-ES42]

Se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas.

[PL08-ES43]

La persona usuaria no debe abrir los archivos anexos a los correos electrónicos. No abrir mensajes que no tienen una relación con las actividades del DNP²⁶. Es responsabilidad de la persona usuaria reportar al centrodeservicios@dnpgov.co los correos sospechosos que reciba cuyo origen es desconocido o poco fiable, con vínculos a formularios donde se piden claves o nombres de usuarios.

[PL08-ES44]

Las personas usuarias no deben enviar información del DNP a través de cuentas de correo no institucional, o herramientas no institucionales. No utilizar la cuenta institucional para trámites personales y/o comerciales.

[PL08-ES45]

Las actividades de los operadores de todos los sistemas de información, computación o comunicaciones del DNP deben registrarse en el log (registro de auditoría del sistema).

²⁶ Publicidad, sorteos, loterías, suscripciones, etc.



[PL08-ES46]

Se deben registrar las fallas de las plataformas de cómputo y comunicaciones mediante el uso de herramientas de monitoreo a través del centro de servicios.

[PL08-ES47]

Todos los servidores, equipos de comunicaciones y estaciones clientes deben estar configurados para sincronizar la hora con el dispositivo que tiene la sincronización con la hora oficial.

[PL08-ES48]

Cuando la SGSGR o la OTSI requieran utilizar hardware²⁷ que haya sido adquirido con un presupuesto distinto al propio, deberán formalizar su necesidad y solicitar la autorización correspondiente mediante memorando dirigido a la dependencia responsable del activo.

12.3.1 Políticas Teletrabajo

[PL08-ES49]

El DNP suministrará al teletrabajador elementos de protección personal en la tarea a realizar, en caso de requerirse.

[PL08-ES50]

El control de la actividad del teletrabajador por parte del DNP se hará mediante medios telefónicos, informáticos o electrónicos. Si por motivos de trabajo fuese necesaria la presencia física de representantes del DNP en el lugar de trabajo de la persona funcionaria y éste fuera su propio domicilio, se hará siempre con previa notificación y consentimiento de éste/a.

[PL08-ES51]

El teletrabajador autoriza a la ARL y al DNP a realizar visitas periódicas a su domicilio que permitan comprobar si el lugar de trabajo es seguro y está libre de riesgos. De igual forma, autoriza las visitas de asistencia para actividades de seguridad y salud en el trabajo. No obstante, el teletrabajador, debe cumplir las condiciones especiales sobre la prevención de riesgos laborales que se encuentran definidas en el componente de Gestión de Seguridad y Salud en el Trabajo (SST).

[PL08-ES52]

El acceso a los diferentes entornos y sistemas informáticos del DNP será efectuado siempre y en todo momento bajo el control y la responsabilidad del teletrabajador y la persona usuaria con conexión remota siguiendo los procedimientos establecidos por el DNP.

[PL08-ES53]

El teletrabajador y la persona usuaria con conexión remota se comprometen a respetar la legislación en materia de protección de datos, derechos de autor, las políticas de privacidad y de seguridad de la información que el DNP ha implementado; a utilizar los datos de carácter personal a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones para con el DNP; a cumplir con las medidas de seguridad que el DNP haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso; a no ceder en ningún caso a terceras personas y ni siquiera a efectos de su conservación.

²⁷ equipos de red, computadores, servidores, etc



[PL08-ES54]

Los derechos de propiedad intelectual e industrial que se generen por las actividades contratadas al Teletrabajador le pertenecen al DNP. El Teletrabajador y la persona usuaria con conexión remota no tendrá las facultades de realizar actividad alguna de uso, reproducción, comercialización, comunicación pública o transformación sobre el resultado de sus funciones, ni tendrá derecho a ejercitar cualquier otro derecho, sin la previa autorización expresa del DNP.

[PL08-ES55]

En la eventualidad de que, por cualquier motivo o circunstancia, fuere necesario hacer uso de la facultad de reversibilidad del teletrabajo, la parte interesada deberá allegar un escrito a la Subdirección de Gestión del Talento Humano con una antelación de cinco (5) días hábiles a través de la cual se justifique la razón por la cual desea dar por terminada la modalidad de teletrabajo.

[PL08-ES56]

Las personas funcionarias que suministren el equipo de cómputo personal para el teletrabajo, deberán cumplir con los lineamientos de la OTSI sobre el licenciamiento mantenimiento y acceso a la información.

[PL08-ES57]

La persona funcionaria teletrabajador debe conocer y aplicar el [M-PG-07 Manual Operativo de Seguridad de la Información](#) y la información relevante del [componente de seguridad de la información](#), deberá presentar anualmente la evaluación de conocimiento de seguridad de la información para el teletrabajo y aprobarla con un puntaje mínimo de 70%.

[PL08-ES58]

Los teletrabajadores que identifiquen cualquier novedad y/o incidente de seguridad en la prestación de algún servicio de TIC deberán reportarlo al Centro de Servicios (centrodeservicios@dnp.gov.co) y/o a la Jefatura de la OTSI, ya que estos son los únicos autorizados para la realización de procedimientos técnicos en los equipos institucionales.

Políticas Scraping

El objetivo de estas políticas es establecer las directrices y procedimientos necesarios para realizar ejercicios de scraping de manera ética, legal y segura, protegiendo la confidencialidad, integridad y disponibilidad de la información, y garantizando el cumplimiento de todas las leyes y regulaciones aplicables a nivel nacional e internacional.

[PL08-ES59]

Las dependencias tienen el deber de realizar scraping de manera ética y legal, por ello deberán asegurar que el ejercicio de scraping responda a una necesidad legítima y velarán por obtener los permisos de los propietarios de los sitios web antes de realizar cualquier actividad de scraping, cumpliendo con todas las leyes y regulaciones aplicables en materia de privacidad, propiedad intelectual, derechos de autor, protección de datos, las políticas institucionales incluidas en el presente manual. Así mismo, deberán gestionar con los propietarios de los sitios web el acceso a APIs oficiales, cuando de ellas se disponga, para la ejecución de algoritmos de scraping, en el ejercicio de sus funciones de desarrollar proyectos y pilotos de analítica de datos, podrá apoyar a las dependencias que tengan la necesidad de desarrollar actividades de scraping si y solo si las dependencias brindan evidencia de que el uso de scraping responde a una necesidad legítima.



La Dirección de Economía Naranja y Desarrollo Digital anualmente capacitarán al personal involucrado en las actividades de scraping sobre el cumplimiento de las políticas y procedimientos. La evidencia de las capacitaciones debe mantenerse documentada para asegurar mejora continua de los ejercicios de scraping.

[PL08-ES60]

Las dependencias son responsables de consultar previamente las políticas web, condiciones y términos de uso de servicio de los sitios web externos objetivos de los ejercicios de scraping para garantizar su cumplimiento. Deben verificar si estos sitios prohíben explícitamente el scraping para prevenir posibles acciones legales contra la Entidad.

Además, las dependencias deben conservar la evidencia de la revisión de las políticas web, condiciones y términos de uso de servicio en cada repositorio de proyecto de scraping previo a realizar la actividad de scraping por primera vez. Para proyectos en los cuales se ejecute la actividad de scraping de forma automática y por más de un mes, la revisión deberá realizarse por lo menos una vez al mes, conservando su correspondiente evidencia, debido a que los responsables de los sitios web externos actualizan de forma periódica sus políticas. La evidencia de las revisiones y las actividades de scraping deben mantenerse documentadas para asegurar la transparencia, auditoria y mejora continua de los ejercicios de scraping.

[PL08-ES61]

Las dependencias son responsables de cumplir con la normatividad vigente para garantizar el cumplimiento de transparencia, derechos de autor, código de integridad, datos personales y seguridad de la información en los ejercicios de scraping a sitios web externos a nivel nacional e internacional, realizando un manejo responsable sobre los datos recolectados, por ello las dependencias deben conservar la evidencia de las actividades de scraping, incluyendo fuentes, propósitos y procedimientos en el repositorio de cada proyecto de scraping cada vez que se ejecuten las actividades.

La evidencia de las actividades de scraping debe mantenerse documentada para asegurar el cumplimiento normativo y la mejora continua de los ejercicios de scraping. Las dependencias pueden incluir la normativa aplicable a web scraping en el normograma institucional.

[PL08-ES62]

Las dependencias son responsables de almacenar la evidencia de los ejercicios de scraping en el Devops server. La Dirección de Economía Naranja y Desarrollo Digital, en el ejercicio de sus funciones de analítica de datos, puede publicar los ejercicios de scraping de carácter público, que no contienen información clasificada y reservada, en el repositorio público autorizado por la OTSI para este fin. Los ejercicios de scraping deben usar la [licencia MIT](#). En caso de que otras dependencias realicen ejercicios de scraping y deseen publicarlos, deberán validar con la OTSI las condiciones de publicación.

[PL08-ES63]

Las dependencias son responsables de almacenar la evidencia de las actividades de scraping, fuentes, propósitos, guías y procedimientos en el repositorio de cada proyecto de scraping cada vez que se ejecuten las actividades, con el fin de conservar la memoria institucional y de tener evidencia de la gestión e insumos ante una posible solicitud de una entidad externa que haya sido objeto de scraping en sus sitios web. El repositorio debe estar configurado en la plataforma tecnológica de la Entidad, de acuerdo con las directrices de la OTSI.

[PL08-ES64]

Las dependencias son responsables de informar a la OTSI sobre las herramientas tecnológicas y software que se utilizan en los proyectos de scraping, cada vez que lo requieran con el fin de verificar que las mismas cuenten



cumplan con el licenciamiento definido, categorizado y aprobado por el DNP, para que sean incluidas en los inventarios administrados por la OTSI. El reporte de las herramientas tecnológicas y software debe realizarse al centrodeservicios@dnp.gov.co para que la solicitud sea registrada en la herramienta ITSM, y se documente la aprobación y/o denegación.

[PL08-ES65]

Las dependencias son responsables de diseñar algoritmos de scraping eficientes para sitios web externos, con el fin de prevenir la sobrecarga de los servidores que alojan estos sitios, cumpliendo con las regulaciones y leyes vigentes del país donde se encuentre el sitio web. Los algoritmos deben incluir límites de velocidad y minimizar las tasas de solicitud, respetando las capacidades y limitaciones de los servidores. Además, deben ejecutar solicitudes maximizando los intervalos de tiempo, y evitando ráfagas o excesos que puedan considerarse ataques de denegación de servicio (DoS).

Las dependencias deben monitorear y ajustar continuamente los patrones de solicitud para adaptarse a los cambios en la capacidad de los servidores objetivo, e implementar mecanismos de control de tráfico y distribución de carga para regular el flujo de solicitudes, de forma que procure un comportamiento responsable durante las actividades de scraping.

Las dependencias son responsables de probar los algoritmos de scraping para los sitios web externos en el ambiente controlado entregado por el DNP con el fin de que el área mida el consumo de recursos de infraestructura, patrones del algoritmo y calidad de los datos recolectados.

La evidencia de las actividades de scraping debe mantenerse documentada para asegurar el cumplimiento normativo y la mejora continua de los ejercicios de scraping.

[PL08-ES66]

Las dependencias son responsables de gestionar acuerdos de confidencialidad entre el DNP y el propietario de sitio web externo (nacional o internacional) cuando sea necesario, incluyendo las responsabilidades de cumplimiento de la normativa de datos personales, derechos de autor y la seguridad de la información con el fin de autorizar la ejecución de scraping. Los acuerdos de confidencialidad deben ser almacenados en el Sistema de gestión Orfeo.

[PL08-ES67]

En caso de que exista una necesidad legítima para la recolección de datos personales a través de scraping y de que se cuente con la autorización de los propietarios para el tratamiento de estos datos, las dependencias serán responsables de asegurar que los algoritmos de scraping recolecten sólo los datos personales necesarios para el propósito específico del análisis, evitando recolectar información sensible o innecesaria. También deberán realizar procesos de anonimización de los datos personales recolectados siempre que sea posible e implementar funciones de sanitización de datos de entrada para prevenir la ejecución de scripts o contenido malicioso que pueda ser obtenido del sitio web objetivo.

[PL08-ES68]

Las dependencias son responsables de garantizar el cumplimiento de la normatividad de datos personales a nivel nacional o internacional, por ello debe implementar mecanismos de anonimización de los datos personales o sensibles recolectados durante el scraping, y adoptar procedimientos de cifrado para la protección de los datos durante su transmisión y almacenamiento, así como medidas de control de acceso para limitar quién puede acceder y manipular los datos recolectados, asegurando que solo personal autorizado pueda interactuar con ellos.



[PL08-ES69]

Las dependencias son responsables de definir períodos de retención, eliminación segura de los datos recolectados, de acuerdo con los requisitos legales aplicables a nivel nacional e internacional, implementando el control de versiones de los algoritmos, la documentación de los proyectos de scraping y almacenar versiones históricas de los datos recolectados para poder realizar análisis comparativos, detectar anomalías o cambios significativos en la información, o responder PQRDS sobre la ejecución de los proyectos de scraping.

[PL08-ES70]

Las dependencias son responsables de ejecutar los algoritmos de scraping con los permisos y privilegios mínimos necesarios para reducir el impacto de cualquier explotación potencial. Los algoritmos deben respetar los archivos de exclusión de robots (protocolos de robots.txt) de los sitios web objetivo.

[PL08-ES71]

Las dependencias son responsables de diseñar algoritmos de scraping que velen por maximizar la calidad de los datos. Estos algoritmos deben incluir funciones para comparar los datos obtenidos de diferentes fuentes y verificar su precisión. Además, deben implementar procesos de limpieza de datos para eliminar duplicados, corregir errores y asegurar la coherencia e integridad de los datos recolectados.

[PL08-ES72]

Las dependencias son responsables de implementar los mecanismos de supervisión continua para detectar y corregir cualquier actividad de scraping que no cumpla con los términos de servicio del sitio web objetivo.

[PL08-ES73]

Las dependencias son responsables de comunicar los incidentes de seguridad de la información o descubrimiento de prácticas inapropiadas al correo de centro de servicios (centrodeservicios@dnpp.gov.co) con el fin gestionar las acciones correctivas para remediar la posible materialización de riesgos.

[PL08-ES74]

Las dependencias son responsables de mantener actualizadas las herramientas de scraping, bibliotecas y sistemas operativos con los últimos parches de seguridad para mitigar vulnerabilidades conocidas y realizar revisiones de seguridad del código de scraping para mitigar los posibles riesgos.

[PL08-ES75]

La persona usuaria externa es responsable por daños directos, indirectos, incidentales, especiales o consecuentes que resulten del uso inadecuado o modificaciones de los algoritmos de scraping publicados por la Dirección de Economía Naranja y Desarrollo Digital o por cualquier otra dependencia del DNP en los repositorios dispuestos para este fin.

Políticas ambientales

[PL08-ES76]

Cuando se requiera dar de baja dispositivos tecnológicos la OTSI realizará la solicitud a la SARC para la gestión integral de los residuos aprovechables, peligrosos, y de manejo especial como son los Residuos de Aparatos Eléctricos, y Electrónicos (RAEE) de acuerdo con lineamientos del M-PG-06 Manual Operativo del Componente de Gestión Ambiental y M-AD-01 Manual Administración de bienes e inmuebles.



13.9. Gestión de comunicaciones

Las dependencias que así lo requieran establecerán los controles para acceso lógico y protección de las redes institucionales, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios tecnológicos y que deberán ser acordados con la alta dirección. La OTSI y las dependencias definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

[PL09-ES1]

Los accesos de VPN para personas usuarias externas (terceros) son exclusivamente para propósitos laborales y su solicitud debe sustentarse con el diligenciamiento del formato [Solicitud servicio conexión remota F-TI-04](#), y envío a través de los canales de contacto del centro de servicios. Los usuarios internos tienen habilitada el acceso por VPN.

[PL09-ES2]

Las conexiones de acceso VPN deben ser registradas en los logs de auditoría.

[PL09-ES3]

Cuando una persona colaboradora requiera el acceso de office 365 y los sistemas internos fuera de Colombia deberá informar al Centro de Servicios su periodo de entrada y salida del país, previa autorización del jefe de la dependencia y/o supervisor.

13.10. Adquisición, implementación y mantenimiento de sistemas

El DNP promueve la inclusión de los controles de seguridad en la [plataforma tecnológica](#), [Servicios de Información](#), [Licencias de Software](#), [Suscripción de Software](#) para prevenir incidentes y piratería de software.

[PL10-ES1]

La compra de una licencia de un programa permitirá al DNP realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.

[PL10-ES2]

Cualquier copia del programa original que no esté en custodia de la Oficina de Tecnología y Sistemas de Información, será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

[PL10-ES3]

La Oficina de Tecnología y Sistemas de Información será la única dependencia autorizada para realizar copias de seguridad del software original.

[PL10-ES4]

Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica del DNP, por cualquier dependencia o proyecto del DNP, deberá ser gestionado por la Oficina de Tecnología y Sistemas de Información para su correcto funcionamiento.



[PL10-ES5]

Se presentarán para dar de baja, el software que se encuentre ajustado a los lineamientos dados por el Comité Institucional de Gestión y Desempeño, así como el software totalmente depreciado o su reconocimiento en cuanto al valor de uso de este.

[PL10-ES6]

El software por instalar debe regirse por las normas Nacionales e Internacionales de Derechos de Autor.

[PL10-ES7]

El software Freeware o libre o Shareware (demostración), no cuenta con soporte técnico por parte del DNP.

[PL10-ES8]

El software Shareware (demostración o versiones trial), sólo podrán utilizarlo en el período estipulado por el fabricante de acuerdo con las normas que lo rigen.

En caso de ser aprobada la instalación de esta clase de software, la responsabilidad de su manejo será asumida por la persona usuaria.

[PL10-ES9]

Las dependencias deben solicitar concepto técnico a la Oficina de Tecnología y Sistemas de Información para el aval técnico a la contratación de servicios profesionales de ingenieros de sistemas, electrónicos, software y afines, y el licenciamiento que apoyen el desarrollo o mantenimiento de sistemas de información o plataformas digitales.

Es responsabilidad de las dependencias, contemplar la asignación de recursos humano y económico para el mantenimiento y actualización de sus sistemas de información; la adquisición de licenciamiento de componentes de software y operación en la nube -cuando aplique-. La Oficina de Tecnología y Sistemas de Información cuenta únicamente con unos recursos específicos ya asignados para el soporte transversal de la plataforma tecnológica, lo cual no incluye nuevos proyectos y/o desarrollos de las dependencias.

[PL10-ES10]

Las dependencias deben solicitar concepto técnico a la Oficina de Tecnología y Sistemas de Información para la adquisición, adaptación, construcción y/o mantenimiento de un sistema de información, de acuerdo con el [SIG](#) y deberá guardar coherencia con lo establecido en [Manual de Contratación M-CT-01](#) y con el [Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información del DNP M-TI-01](#): *“En los casos de licitación pública, selección abreviada (Menor Cuantía o Subasta Inversa) o concurso de méritos, el proyecto de pliego de condiciones es elaborado en la –Subdirección de Contratación con base en los estudios previos y criterios técnicos formulados por la dependencia solicitante. Los estudios previos relacionados con temas de competencia de otra dependencia deberán contar con su aprobación, como es el caso de los contratos editoriales o de agencias de comunicaciones, que deberán contar con la aprobación previa del Oficina Asesora de Comunicaciones del DNP, así como lo relacionado con tecnologías de la información, que deberán contar con el aval de la Oficina de Tecnología y Sistemas de Información.”*

Adicionalmente, las dependencias deben contemplar los recursos necesarios para la operación y sostenibilidad del sistema de información.



[PL10-ES11]

La adquisición, adaptación, construcción y/o mantenimiento de sistemas de información, se regirá en los aspectos pertinentes, por las políticas y lineamientos del Dominio de Sistemas de Información del Marco de Referencia de Arquitectura Empresarial para la Gestión de TIC, establecido dentro de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y de las Comunicaciones - MINTIC.

Los requerimientos funcionales del sistema de información serán definidos, especificados, evaluados y/o avalados por la Dependencia solicitante y por las personas usuarias directamente implicados en su operación.

[PL10-ES12]

Los aplicativos adquiridos y/o adaptados o contruidos a la medida para apoyo a la gestión administrativa, misional y estratégica del DNP, están regidos por los Derechos de Autor y el Contrato que se lleve a cabo entre las partes. Se debe gestionar desde las dependencias ante la Subdirección de Contratación la respectiva cesión de derechos patrimoniales del software.

[PL10-ES13]

Las dependencias deben dar cumplimiento a lo establecido en el [Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información del DNP M-TI-01](#), el diseño de soluciones a la medida debe estar alineado a la arquitectura de referencia de la Entidad, la cual es gestionada por la Oficina de Tecnología y Sistemas de Información, respecto a componentes de infraestructura, componentes de plataforma y componentes transversales de software.

las dependencias deben garantizar la estructuración y la actualización de la documentación relacionada con sus sistemas de información acorde con el [Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información del DNP](#), ningún sistema de información podrá salir a operación si no cuenta con toda la documentación base.

[PL10-ES14]

Los programas fuentes estarán en custodia de la Oficina de Tecnología y Sistemas de Información mediante un repositorio oficial de código Microsoft DevOps Server.

[PL10-ES15]

El DNP puede intercambiar el software construido internamente, con otras Entidades del estado a través de los convenios Interadministrativos o mediante actas de entrega y cooperación, es responsabilidad de las dependencias alojar la información en el repositorio Oficial.

[PL10-ES16]

Dentro del ambiente de producción de aplicativos no se permiten archivos de backup y solo debe permanecer la última versión del aplicativo.

[PL10-ES17]

El Software adquirido o licenciado por los proyectos y/o programas que se encuentran en el DNP, y que adquieran a través de los proyectos y/o programas, debe quedar a nombre del Departamento Nacional de Planeación.



[PL10-ES18]

Los estándares y las versiones de software y/o aplicativos establecidos serán fijados y avalados por la Oficina de Tecnología y Sistemas de Información, quien autoriza su adquisición o construcción, enmarcados dentro de la Plataforma Tecnológica adoptada por el DNP.

[PL10-ES19]

Una vez registrado el sistema en la Dirección Nacional de Derechos de Autor, la persona Líder Funcional y/o Técnico o Supervisor del contrato o la persona contratista o firma externa contratada si aplica, realiza el registro del sistema de información en la Subdirección Administrativa y Relaciónamiento con la Ciudadanía - Almacén del DNP, de acuerdo al [procedimiento para la Administración de Bienes Muebles e Inmuebles \(PT-AD-01\)](#), la documentación resultante de este trámite deberá ser cargada por la persona Líder Funcional y/o Técnica de la dependencia o quien supervise el contrato, en la herramienta de Gestión de Desarrollo de Software en la carpeta de Proyecto, subcarpeta Cierre.

13.11. Políticas relación con proveedores

El DNP busca establecer los lineamientos a fin de preservar la seguridad de la información en las relaciones con los proveedores.

[PL11-ES1]

En las actividades donde la persona contratista interactúe con cualquier activo de información (plataforma e infraestructura tecnológica) del DNP, debe cumplir con las políticas del componente de seguridad de la información de la Entidad.

[PL11-ES2]

La persona contratista no podrá revelar durante la vigencia del contrato y dentro de los dos (2) años siguientes a su expiración, la información confidencial de propiedad del DNP, de la cual el contratista tenga conocimiento con ocasión o para la ejecución de este contrato y que esté relacionada con el objeto contractual o con las funciones y actividades a cargo del DNP sin el previo consentimiento por escrito del DNP, so pena de hacerse acreedor a las sanciones de Ley.

[PL11-ES3]

Los servicios informáticos prestados por un proveedor deben realizarse de forma controlada, segura y organizada, de acuerdo con lo estipulado en el contrato y sus anexos los cuales hacen parte integral del mismo. Para los contratistas de la OTSI que brinden apoyo en la gestión, resolución de ticket y gestión de cambios que conlleven ticket relacionados con el alcance de su rol, deberán ser resueltos, documentados y cerrados en la herramienta ITSM.

[PL11-ES4]

Las personas contratistas y proveedores deben cumplir con las normas de seguridad y controles definidos por el DNP.

[PL11-ES5]

Los proveedores de la Oficina de tecnología y sistemas de información deberán cumplir con los Acuerdos de Nivel de Servicio (ANS) que hayan quedado establecidos en su respectivo contrato.

Los contratistas de la Oficina de Tecnología y Sistemas de Información, en la atención de casos, no estarán sujetos al cumplimiento de los Acuerdos de Nivel de Servicio (ANS), dado que estos no se encuentran



estipulados en sus condiciones contractuales. No obstante, la Oficina de Tecnología y Sistemas de Información realizará seguimiento a la atención que se brinde conforme a los términos establecidos por los fabricantes en los casos amparados por garantía.

Nota: En caso de que la Entidad no cuente con un Centro de Servicios, la OTSI priorizará la gestión sobre la medición de indicadores, toda vez que la gestión de la oficina debe responder a los incidentes, solicitudes y cambios se seguirán reportando y atendiendo por los canales autorizados, según la capacidad operativa de la OTSI.

[PL11-ES6]

Las personas contratistas y proveedoras deben incluir la evaluación de riesgos asociada al cambio, la cual debe ser revisada y aceptada por el interventor o supervisor de contrato.

[PL11-ES7]

Las personas funcionarias, contratistas, pasantes y los terceros que tengan acceso a los activos de información tecnológicos deben a cumplir con el M-PG-07 Manual Operativo de seguridad de la información, las cláusulas incluidas en la [Carta de compromisos de cumplimiento F-TI-05](#) y los lineamientos en seguridad de la información incluidos en el [Manual de Contratación M-CT-01](#), [M-CT-02 Manual de Supervisión e Interventoría](#) y tienen las mismas responsabilidades que Las personas usuarias del DNP (cláusula de confidencialidad y políticas de seguridad).

[PL11-ES8]

Las personas usuarias internas y externas de los portales, aplicativos y sistemas de información son responsables de cumplir con los términos, condiciones, [políticas de privacidad](#), [tratamiento de datos personales](#) y [políticas de derechos de autor y/o autorización de uso divulgados](#) en el portal web del DNP.

[PL11-ES9]

Las personas usuarias externas son los responsables de solicitar la activación y desactivación de usuarios de acuerdo con los protocolos establecidos en cada sistema de información, aplicativo y/o portal.

[PL11-ES10]

Las personas usuarias externas con credenciales entregadas por el DNP deben elegir las contraseñas fuertes²⁸, únicas, personales e intransferibles²⁹. Las personas usuarias externas son responsables de no compartir contraseñas con otras personas, no utilizar la misma contraseña para múltiples cuentas y cambiarlas regularmente (cada 60 días). Abstenerse de almacenar las credenciales de acceso en el gestor de contraseñas del navegador web, en su lugar utilizar un gestor de contraseñas más sofisticado y seguro.

[PL11-ES11]

Las personas usuarias externas deben mantener actualizados sus sistemas operativos, aplicaciones y dispositivos con los últimos parches de seguridad y actualizaciones de software. Esto ayuda a protegerse contra vulnerabilidades conocidas que podrían ser explotadas por los atacantes.

²⁸ Recomendaciones para una personal e intransferible: 1. La "contraseña" debe cambiarse con periodicidad; por lo menos cada dos meses. 2. Cuando se cambie la clave de acceso no se debe utilizar las que se hayan usado previamente. 3. No debe escribir la "contraseña" en papel o en una agenda al alcance de otras personas. 4. No preste su contraseña es personal e intransferible.

²⁹ Recomendaciones para una contraseña fuerte: 1. Debe tener al menos ocho (8) caracteres. 2. No utilizar nombres propios de personas, mascotas, equipos deportivos ni fechas, ni similares. 3. No utilizar caracteres repetidos (por ejemplo: AAAA, xxx, etc.). 4. No utilizar "contraseñas" con caracteres incrementales, por ejemplo: MARIA1, MARIA2. 5. Usar "contraseñas" no pronunciables y sin significado obvio. 6. Ser significativamente diferente de otras contraseñas anteriores. 7. Usar combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales como: !"#%&&()=?!><[*]



[PL11-ES12]

Al acceder a los sistemas del DNP desde ubicaciones externas, como redes Wi-Fi públicas, las personas usuarias externas deben asegurarse de utilizar conexiones seguras, como VPNs (redes privadas virtuales), para proteger la confidencialidad de los datos transmitidos. Configurar con el apoyo del proveedor de internet una clave segura para la red wifi.

[PL11-ES13]

Las personas usuarias externas son responsables de seguir los boletines del [Colcert](#) y [CAI virtual](#) para adquirir capacidades en la identificación de posibles amenazas de seguridad, como correos electrónicos sospechosos, sitios web fraudulentos o comportamientos inusuales en sus dispositivos, y tomar medidas para mitigar esos riesgos, como no hacer clic en enlaces desconocidos.

[PL11-ES14]

Las personas usuarias externas deben cumplir con las políticas de seguridad establecidas por el DNP, que incluyen [Manual Operativo de seguridad de la información](#), el [Manual Datos Personales](#), el [normograma](#), derechos de autor, confidencialidad, propiedad intelectual, [términos y condiciones de uso](#), [las políticas de privacidad](#), [tratamiento de datos personales](#), [derechos de autor y/o autorización de uso](#) que aplican a los sistemas de información, aplicativos y portales del DNP.

[PL11-ES15]

Las personas usuarias externas son responsables de instalar, utilizar y mantener actualizado los softwares de antivirus, antimalware y cortafuegos en los dispositivos que utiliza para acceder a la información del DNP, estas herramientas actualizadas permiten detectar y eliminar posibles amenazas.

[PL11-ES16]

Las personas usuarias externas son responsables no hacer clic en enlaces sospechosos o visitar sitios web no seguros, así como no ingresar información confidencial en sitios web que no sean seguros y tener cuidado al descargar archivos de Internet.

[PL11-ES17]

Las personas usuarias externas son responsables utilizar medidas de seguridad física para proteger los dispositivos que utiliza para acceder a la información del DNP, las medidas contraseñas de inicio de sesión y cifrado de datos.

[PL11-ES18]

Las personas usuarias externas son responsables utilizar medidas de seguridad para configurar el bloqueo de sesión que impide el acceso al equipo después de haber estado inactivo durante un período de tiempo (por ejemplo, 5 minutos). Se recomienda presionar la combinación de teclas Windows + L para bloquear el equipo al levantarse del puesto de trabajo. Así mismo, Las personas usuarias externos son responsables de no dejar sus dispositivos desatendidos en lugares públicos.

[PL11-ES19]

Las personas usuarias externas son responsables configurar los dispositivos móviles para que se bloquee automáticamente después de un período de inactividad.

[PL11-ES20]

Las personas usuarias externas son responsables de proteger físicamente los equipos de cómputo mediante el uso de cerraduras de cable u otros elementos disuasorios contra el robo.



[PL11-ES21]

Si una persona usuaria externa detecta o sospecha de un incidente de seguridad relacionado con los sistemas de información, aplicativos y portales de DNP, debe informar inmediatamente al correo. centrodeservicios@dnpgov.co para que se puedan tomar medidas correctivas y evitar un mayor impacto. Si el incidente no está relacionado con el DNP es responsabilidad de la persona usuaria externa reportarlo al [ColCERT](#).

[PL11-ES22]

Las personas usuarias externas son los responsables de realizar la anonimización de los datos con información personal que pueda estar contenida en los archivos que almacena en los sistemas de información, aplicativos, y portales del DNP.

13.12. Administración de incidentes de seguridad de la información

El DNP busca que los eventos e incidentes de seguridad con los activos de información, sean comunicados y atendidos oportunamente y con los procedimientos definidos para tal fin, de manera que se tomen las acciones correctivas adecuadas y en el momento indicado.

[PL12-ES1]

Las dependencias con el apoyo de la Oficina Asesora de Planeación y la Oficina de Tecnología y Sistemas de Información deberá adelantar análisis de riesgos y controles, o actividades relacionadas que permitan valorar y determinar el estado actual de la seguridad de la información, así como los correctivos a que hubiese lugar. La identificación de riesgos de seguridad de la información se realizará de acuerdo al procedimiento [PT-PG-01 Gestión Integral de Riesgos](#).

[PL12-ES2]

Los incidentes de seguridad se deben reportar al Centro de Servicios y asignarlo a la persona encargada de la seguridad de la información. El asesor de la Oficina de Tecnología y Sistemas de Información encargado del tema de seguridad informática y/o el Oficial de Seguridad de la información, dependiendo de su valoración informará a las instancias para los trámites correspondientes y quedarán documentados en la herramienta del Centro de Servicios hasta su cierre.

[PL12-ES3]

Las investigaciones especiales adelantadas por los entes de control relacionadas con la seguridad de la información deben seguir el procedimiento [PT-ED-06 Procedimiento Instrucción Disciplinaria](#) establecido por la Oficina de Control Interno Disciplinario en el marco del Sistema Integrado de Gestión y deben ser notificadas a la Secretaría General, Oficina de Tecnología y Sistemas de Información.

[PL12-ES4]

Los incidentes de [severidad grave](#) y [muy grave](#) deben ser reportados al Centro de Servicios quien informará al grupo de seguridad de la Oficina de Tecnología y Sistemas de Información para levantar la evidencia, documentar las acciones realizadas y rendir los informes necesarios, en caso de ser requerido la Oficina de Tecnología y Sistemas de Información los presentará a la Secretaría General para efectos de redireccionar el hallazgo a la dependencia correspondiente, a fin de revisar y ejecutar acciones en materia penal, civil, fiscal, contractual y disciplinaria cuando a ello haya lugar.



En caso de requerir apoyo en la investigación de los incidentes de seguridad de la información la OTSI puede solicitar apoyo a los equipos de respuesta de incidentes (Colcert, CsirtGOB, CSIRT PONAL).

[PL12-ES5]

Las personas usuarias de los activos de información del DNP, que observen situaciones sospechosas o que claramente sean incidentes de seguridad de la información tienen la obligación de reportar los incidentes de seguridad al [centro de servicios](#).

[PL12-ES6]

Las personas usuarias deben reportar el incidente a través del Centro de Servicios o través de correo electrónico o por medio telefónico. Independientemente del medio utilizado, debe quedar registrado el evento en la herramienta que utiliza el [centro de servicios](#).

[PL12-ES7]

La Oficina de Control Interno puede cuando lo considere necesario auditar los incidentes de seguridad para hacer evaluación independiente.

[PL12-ES8]

Los incidentes de seguridad que ocasionen materialización de los riesgos de seguridad de la información deben ser reportados en el formato [Reporte de eventos de materialización de riesgos F-PG-02](#) de acuerdo con el procedimiento [PT-PG-01 Gestión Integral de Riesgo](#). El formato debe ser diligenciado en una mesa de trabajo entre la dependencia responsable del activo tecnológico, la Oficina Asesora de Planeación y la Oficina de Tecnología y Sistemas de Información.

[PL12-ES9]

Los incidentes de seguridad que ameriten acciones de tipo legal o penal deben ser investigados por las personas idóneas de los organismos competentes para la recolección de la información que garanticen la admisibilidad y cadena de custodia de las pruebas recolectadas.

[PL12-ES10]

La Oficina de Tecnología y Sistemas de Información puede realizar las pruebas de Ethical Hacking e ingeniería social con proveedores previa autorización del Comité de Institucional Gestión y Desempeño Institucional.

13.13. Administración de la seguridad de la información en la continuidad del negocio

El DNP está enfocado en reaccionar ante las interrupciones de las actividades de la función misional, para proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres; también, es la garantía planeada para asegurar que las operaciones se recuperen dentro del tiempo previsto.

[PL13-ES1]

La Alta Dirección del Departamento Nacional de Planeación adquirió el compromiso de estructurar y mantener un sistema de gestión, que facilite la mejora de eficiencia institucional y el aumento en la satisfacción y percepción de sus partes interesadas. De igual forma, la Alta Dirección del DNP proporciona los recursos necesarios que permiten el cumplimiento de su misión institucional y dirige y controla la gestión sobre los procesos y programas de la Entidad, de manera que los elementos de la plataforma estratégica se logren en beneficio de todas las partes interesadas, por lo tanto es responsabilidad de la Alta dirección la asignación de los recursos (económicos, humanos, logísticos, técnicos) para prevenir interrupciones en las actividades del



DNP que van en detrimento de los procesos críticos de la Institución afectados por situaciones no previstas o desastres.

La Alta Dirección es la responsable de gestionar integralmente los riesgos a los que está expuesta la gestión del DNP, a partir de su plataforma estratégica, procesos críticos y los niveles táctico y operativo, garantizando un nivel de aseguramiento razonable en la Entidad.

[PL13-ES2]

El Oficina Asesora de Planeación como administrador del Sistema Integrado de Gestión (SIG) es responsable de asesorar metodológicamente a las dependencias en las herramientas transversales para la planeación, evaluación y mejora del SIG, incluyendo la planeación de los procesos, productos, matrices de riesgo, indicadores de gestión, acciones preventivas, correctivas y de mejora; la elaboración, actualización y publicación de documentos y el balance de acciones de mejora; facilitar la medición y seguimiento del sistema, a través de encuestas, indicadores y otras herramientas de seguimiento; y divulgar a través de los canales institucionales los aspectos estratégicos y funcionales del mismo.

[PL13-ES3]

La Entidad cuenta con una administración articulada en Gestión de Continuidad del Negocio el cual cuenta con una visión holística que identifica las amenazas potenciales de una organización y los impactos potenciales a las operaciones del negocio permitiendo construir la capacidad para tener una respuesta efectiva para salvaguardar los intereses de los principales interesados, la reputación y las principales fuentes de generación de valor a través de planes y procedimientos para garantizar la continuidad del negocio y los sistemas de información.

[PL13-ES4]

El DNP cuenta con una planificación de la gestión de la continuidad de negocio el cual resalta en su M-PG-14 Manual para la Gestión de Continuidad del Negocio, la identificación y asignación de prioridades a los procesos críticos dentro del DNP de acuerdo con su impacto (BIA), así como su estructuración en el plan de recuperación de desastres.

[PL13-ES5]

La continuidad de negocio es articulada por el gobierno de gestión de continuidad, el cual define los responsables y sus respectivos roles. Ante una activación del plan de continuidad del negocio, estos grupos son responsables de restablecer la operación de los procesos identificados como críticos, dentro de los plazos establecidos.

[PL13-ES6]

El gobierno de la continuidad del negocio está descrito en el [M-PG-14 Manual para la Gestión de Continuidad del Negocio](#) en el numeral Estructura de Gestión de la Continuidad de Negocio, las dependencias que componen este gobierno son las responsables de velar por la implementación de las medidas relativas a la continuidad de negocio. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

[PL13-ES7]

Las dependencias incluidas en la Estructura de Gestión de la Continuidad de Negocio del [M-PG-14 Manual para la Gestión de Continuidad del Negocio](#) se encargarán de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velarán por la implementación y cumplimiento de estas.



[PL13-ES8]

Los directores, subdirectores, jefes de oficina son los responsables de informar a la Oficina Asesora de Planeación y la Oficina de Tecnología y Sistemas de información los datos de contacto de las personas colaboradoras principales y suplentes que para las actividades relacionadas con el gobierno de la continuidad del negocio descrito en [M-PG-14 Manual para la Gestión de Continuidad del Negocio](#).

13.14. Cumplimiento

El DNP velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública

[PL14-ES1]

Las leyes, decretos y resoluciones que aplican al DNP se encuentran registradas en el [normograma](#) que está disponible en la intranet en la sección [Sistema integrado de Gestión](#), y en el portal del DNP www.dnp.gov.co.

[PL14-ES2]

En la República de Colombia actualmente no existe regulación sobre el tema de Criptografía.

[PL14-ES3]

La persona que ejerza la dirección del DNP, la jefatura de las dependencias, coordinador de grupo y/o supervisores de contrato son los responsables de que todos las personas de las dependencias conozcan, acepten y cumplan las políticas de seguridad de la información y velar por el que se cumplan los procedimientos definidos por el DNP.

13.15. Protección de datos

El DNP gestiona los datos personales de conformidad con la normatividad vigente.

[PL15-ES1]

Las políticas de seguridad relacionadas con datos personales están incluidas en el [M-PG-12 Manual Datos Personales](#).

14. CAPACITACIÓN E INDUCCIÓN EN SEGURIDAD DE LA INFORMACIÓN

El DNP realiza charlas periódicas para a las personas colaboradoras del DNP para que conozcan el componente de gestión de seguridad de la información, sus políticas, la importancia en el DNP, los conceptos relacionados del componente de seguridad de la información, identificación de los activos de información, identificación de los tipos de delitos y riesgos cibernéticos en el entorno laboral y personal, los canales de denuncia si son víctima de un delito cibernético, identificación de las responsabilidades de Las personas usuarias del DNP, identificación de la normativa relacionada con seguridad de la información.

Las temáticas de sensibilización de definen anualmente en el [Plan de Seguridad y Privacidad de la Información](#), [Plan estratégico de Seguridad y Privacidad de la información](#) .



Así mismo se realiza divulgación de la información relacionada con el componente de seguridad de la información a través de comunicaciones internas, las campañas pueden ser consultadas en O:\Sistemas\Divulgación.

15. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL CGSI

La Entidad realizará revisiones periódicas al Componente de seguridad de la información. Dichas revisiones estarán enfocadas en los siguientes aspectos: Revisión de indicadores definidos para el Componente de Gestión de Seguridad de la Información, el avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC y el avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin, los resultados del Plan de Seguridad y Privacidad, y los resultados de las auditorías.

El Componente de seguridad de la información ha implementado en el SIG los siguientes indicadores solicitados en la [Resolución 500 de 2021](#), [Resolución 2277 de 2025](#) y el documento [Indicadores de Gestión de Seguridad de la Información](#) del Ministerio de Tecnologías de la Información y las Comunicaciones.

Tabla 7: Indicadores de Gestión de Seguridad de la Información

Código del SIG	Código del Indicador	Nombre del indicador	Definición del indicador	Objetivo del indicador	Periodicidad de medición	Justificación de la periodicidad de medición	Enlace de consulta
GSI-01	SGIN03	Tratamiento de los eventos relacionados con la seguridad y privacidad de la información	El indicador mide el tratamiento de eventos reportados y relacionados con seguridad de la información dentro del periodo en el cual se presentan con el fin de evitar incidentes de seguridad.	Reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una Entidad	Mensual	El indicador se genera con los reportes de casos realizados por las personas usuarias	Interno (Intranet)
GSI-02		Porcentaje de cumplimiento del Plan de Implementación de aspectos de seguridad de la información en la continuidad del negocio en el componente tecnológico.	Mide la eficacia de las herramientas tecnológicas que permitan dar cumplimiento a los tiempos de RTO (Tiempo máximo de retorno) y RPO (Tiempo máximo de pérdida de información) de acuerdo con el levantamiento de información del BIA (Análisis de impacto de negocio) para los procesos críticos que se identifiquen, para	Determinar con la ayuda de las herramientas tecnológicas el punto máximo de recuperación de todos los procesos críticos de los servicios tecnológicos (acceso a los aplicativos, conexión de la VPN, entre otros), el cual se entrega en un informe final para la Oficina de Tecnología y Sistemas de la Información	Semestral	El indicador se genera con el plan de trabajo de continuidad de negocio en el componente tecnológico	Interno (Intranet)



Código del SIG	Código del Indicador	Nombre del indicador	Definición del indicador	Objetivo del indicador	Periodicidad de medición	Justificación de la periodicidad de medición	Enlace de consulta
			disminuir los tiempos descritos en el manual e identificarlos por los dueños de los procesos para asegurar la continuidad operacional de la entidad.	(OTSI) con el fin de realizar adquisiciones del componente tecnológico de acuerdo a la estrategia del negocio, el cual debe asegurar la continuidad operacional de la entidad en caso de presentarse alguna situación adversa.			
GSI-03	SGIN16	Avance en la implementación de controles de seguridad de la información	Mide el nivel de implementación de los controles de seguridad de los sistemas de información que forman parte del catálogo de los sistemas de información, para evaluar que los sistemas de información cumplen con los estándares de seguridad y la normativa interna.	Identificar el nivel de implementación de los controles de seguridad de la información en los sistemas de información que hacen parte del catálogo de los sistemas de información, con el fin de proteger la integridad, confidencialidad y disponibilidad de los activos tecnológicos que apoyan al desempeño institucional.	Cuatrimestral	El monitoreo de riesgos se realiza cuatrimestral de acuerdo con lo establecido en el procedimiento PT-PG-01 Gestión integral de Riesgos	Interno (Intranet)
GSI-04	SGIN04	Plan de sensibilización del componente de seguridad de la información, implementado.	Mide el nivel de participación de los colaboradores en las charlas que hacen parte del plan de sensibilización del componente de seguridad de la Información, con el fin de optimizar las estrategias de sensibilización, asegurando que se logre una participación activa y así reducir los comportamientos	Establecer la eficacia de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.	Cuatrimestral	El indicador se genera con las sensibilizaciones	Interno (Intranet)



Código del SIG	Código del Indicador	Nombre del indicador	Definición del indicador	Objetivo del indicador	Periodicidad de medición	Justificación de la periodicidad de medición	Enlace de consulta
			inapropiados relacionados con la seguridad de la información				

Los demás indicadores son de gestión interna y se documentan en el informe del plan de acción del componente de seguridad de la información.

16. APROBACIÓN Y REVISIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se aprueban de acuerdo con el [M-PG-03 Manual para la elaboración y control de documentos del SIG](#) y el [PO-PG-01 Protocolo crear – actualizar - eliminar documentos SIG](#). Las revisiones de estas políticas se harán en las siguientes condiciones:

- De forma anual.
- Si se dan cambios estructurales en la Entidad (reestructuración de áreas o procesos).
- Incidentes de seguridad de la información que requieran que la política requiera cambios.
- Cambios normativos que afecten el componente de seguridad de la información.

Fecha aprobación: 23 de diciembre de 2025

Elaboró:

ORIGINAL FIRMADO

SANDRA FERNANDA POVEDA AVILA
Contratista Oficial seguridad de la Información- OTSI

Revisó OAP

ORIGINAL FIRMADO

CRISTIAN EDUARDO OVIEDO RODRIGUEZ
Contratista Oficina Asesora de Planeación



Revisó:

ORIGINAL FIRMADO

CLAUDIA ANGELICA BEN-AMY
Funcionaria Asesor Grado 8 -OTSI

Aprobó:

ORIGINAL FIRMADO

ORLANDO BENAVIDES SANTACRUZ
Jefe Oficina de Tecnología y Sistemas de Información (OTSI)