



**El futuro
es de todos**

DNP
Departamento
Nacional de Planeación

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

**DEPARTAMENTO NACIONAL DE PLANEACIÓN
BOGOTÁ, 2022**




TABLA DE CONTENIDO

1. OBJETIVO	4
1.1.OBJETIVO GENERAL DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN	4
1.2.OBJETIVOS ESPECIFICOS DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN	4
1.3.ALINEACIÓN DE OBJETIVOS INSTITUCIONALES CON LOS OBJETIVOS DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN	4
2. ALCANCE/APLICABILIDAD	5
3. MARCO DE REFERENCIA DEL COMPONENTE TECNOLÓGICO DE SEGURIDAD DE LA INFORMACIÓN	6
3.1.MARCO DE REFERENCIA INTERNO	6
3.2.MARCO DE REFERENCIA EXTERNO	7
3.2.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.....	7
4. DEFINICIONES	8
5. OBLIGACIONES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN	8
5.1 ASESOR SEGURIDAD DE LA INFORMACIÓN.....	9
5.2 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.....	9
5.3 ESPECIALISTA CONTINUIDAD DE NEGOCIO DEL COMPONENTE TECNOLÓGICO	10
5.4 ESPECIALISTA SEGURIDAD INFORMÁTICA DEL CENTRO DE SERVICIOS	10
5.5 LÍDERES TÉCNICOS DE TIC	10
6. ESTRUCTURA DEL COMPONENTE DE GSI	11
6.1.PREMISAS BÁSICAS DE SEGURIDAD DE LA INFORMACIÓN	11
6.1.1 CONFIDENCIALIDAD	11
6.1.2 DISPONIBILIDAD	13
6.1.3 INTEGRIDAD.....	13
6.1.4 AUTENTICIDAD	13
6.1.5 AUDITABILIDAD.....	13
6.1.6 NO REPUDIO	13
6.2.PROPIEDAD DE LA INFORMACIÓN	13
7. POLÍTICAS	14
7.1.POLÍTICA DE SEGURIDAD	14
7.2.SEGURIDAD ORGANIZACIONAL	14
7.3.SEGURIDAD DEL RECURSO HUMANO.....	16
7.4.GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN	18
7.5.CONTROL DE ACCESO	26
7.6.CRIPTOGRAFÍA.....	31
7.7.SEGURIDAD FÍSICA Y AMBIENTAL	33
7.8.GESTIÓN DE OPERACIONES	38
7.9.GESTIÓN DE COMUNICACIONES	46
7.10. ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS	47
7.11. RELACIÓN CON PROVEEDORES.....	51
7.12. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	52
7.13. ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO	54
7.14. CUMPLIMIENTO	56
7.15. PROTECCIÓN DE DATOS	57
8. CAPACITACIÓN E INDUCCIÓN EN SEGURIDAD DE LA INFORMACIÓN	60
8.1.CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.....	60
9. CLASIFICACION DE LAS POLITICAS DE SEGURIDAD	60
10. DEFINICIONES	60
10.1. SIGLAS Y ABREVIACIONES	60



10.2.	CONCEPTOS DE LOS PILARES DE SEGURIDAD	62
10.3.	CONCEPTOS RELACIONADOS DE EL M-PG-07 MANUAL OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN	62
10.4.	CONCEPTOS RELACIONADOS CON LOS ACTIVOS DE INFORMACIÓN	66
10.5.	CONCEPTOS RELACIONADOS CON LA CATEGORÍA INFORMACIÓN	68
10.6.	CONCEPTOS RELACIONADOS CON LA CATEGORÍA SOFTWARE	68
10.7.	CONCEPTOS RELACIONADOS CON LA CATEGORÍA SERVICIOS DE TI	68
10.8.	CONCEPTOS RELACIONADOS CON LA LEY DE TRANSPARENCIA.....	69
10.9.	CONCEPTOS RELACIONADOS CON EL USO DE LA INFORMACIÓN.	70
10.10.	CONCEPTOS RELACIONADOS CON DATOS PERSONALES.....	70
10.11.	CONCEPTOS RELACIONADOS CON LOS INCIDENTES DE SEGURIDAD	74
10.12.	CONCEPTOS RELACIONADOS CON LOS RIESGOS DE SEGURIDAD DIGITAL	75
10.13.	CONCEPTOS RELACIONADOS CON AMENAZAS, VULNERABILIDADES Y GRUPOS CAUSALES.....	75
10.14.	CONCEPTOS RELACIONADOS CON LOS EFECTOS DE LA MATERIALIZACIÓN DE LOS RIESGOS.....	76
10.15.	CONCEPTOS RELACIONADOS CON LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	78

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 4 de 81 VERSIÓN: 7</p>
--	--	---

1. OBJETIVO

1.1. OBJETIVO GENERAL DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

Gestionar la confidencialidad, integridad y disponibilidad de la información digital de software, hardware, servicios de TI, 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).

El componente de seguridad de la información (GSI) está alineado con la Política del Sistema Integrado de Gestión¹. Así mismo, el objetivo del GSI 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 datos abiertos y personales, protegiendo su integridad, disponibilidad y confidencialidad.”*

1.2. OBJETIVOS ESPECIFICOS DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

- 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 los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.
- 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.
- 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.
- 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.

1.3. ALINEACIÓN DE OBJETIVOS INSTITUCIONALES CON LOS OBJETIVOS DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

1.3.1. OBJETIVOS ESTRATÉGICOS DEL DNP²

- **OE1:** Coordinar el diseño de planes, políticas y programas que atiendan efectivamente las necesidades sectoriales y territoriales.
- **OE2:** Diseñar e implementar estrategias que mejoren la calidad de la inversión pública
- **OE3:** Fortalecer las capacidades técnicas de los sectores y territorios que promuevan la productividad, la competitividad, la sostenibilidad y la equidad.

¹ <https://intranet.dnp.gov.co/SGC/Paginas/SGC.aspx>

² <https://www.dnp.gov.co/la-entidad/objetivos>



- **OE4:** Mejorar el desempeño institucional que garantice el cumplimiento de los objetivos y metas definidos por la entidad

1.3.2. OBJETIVOS ESPECÍFICOS DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

- **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 los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.
- **OECS 2:** 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.

Tabla 1: Alineación de Objetivos Institucionales 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

2. ALCANCE/APLICABILIDAD

El presente manual operativo aplica para los funcionarios, contratistas, pasantes y terceros del Departamento Nacional de Planeación los cuales se encuentran ubicados en Bogotá y en sus sedes regionales (Regalías), así como para los procesos del Sistema Integrado de Gestión³, 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 todos los usuarios 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.

³ <https://www.dnp.gov.co/DNP/gestion/Paginas/Modelo-de-operacion-por-Procesos.aspx>

 El futuro es de todos DNP Departamento Nacional de Planeación	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 6 de 81 VERSIÓN: 7

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 intranet⁴ y en la sede electrónica⁵ del DNP y aceptadas por cada uno de los colaboradores⁶, proveedores⁷, o terceros⁸.

3. MARCO DE REFERENCIA DEL COMPONENTE TECNOLÓGICO DE SEGURIDAD DE LA INFORMACIÓN

El Componente de Gestión de Seguridad de la Información incluye la identificación, análisis y gestión de riesgos de los activos digitales de la Entidad, así como la identificación de los controles que permita mitigar las vulnerabilidades y amenazas en el entorno tecnológico.

Acorde con la premisa que la información digital es uno de los activos más relevantes, es necesario establecer el marco de referencia interno y externo articulado con el contexto del DNP identificado en el Manual del SIG y en relación con la seguridad de la información, para identificar cuáles son los aspectos para mejorar los controles existentes.

3.1. MARCO DE REFERENCIA INTERNO

El DNP cuenta con una estructura organizacional de acuerdo con el Decreto 1893 de 2021 la cual está reflejada en el organigrama disponible consultado en la sede electrónica⁹ de la Entidad.

El factor humano como parte de los activos de información digitales se encuentran representados en servidores públicos, contratistas, pasantes y proveedores los cuales gestionan, procesan, almacenan, distribuyen, intercambian y/o consultan información que puede ser pública, clasificada y/o reservada.

El DNP propende por la aplicación controles en los activos de información digitales de conformidad con la normativa vigente, datos personales, transparencia y acceso a la información pública, es por ello por lo que se realizan sensibilizaciones periódicas sobre seguridad de la información a todos los colaboradores del DNP.

El DNP cuenta con una infraestructura tecnológica moderna, con los centros de datos principal y alterno dotados mecanismos de seguridad que permiten la protección de los activos de información tecnológicos. Así mismo para el desarrollo y sostenibilidad de los sistemas de información cuenta con las herramientas de software y hardware requeridas como sistemas de información geográfica, componentes de analítica de datos e inteligencia de negocios y Big Data, cada licenciamiento es actualizado periódicamente.

Por otra parte, la sede del DNP está ubicada en el centro de la ciudad de Bogotá desde la cual se desarrollan las funciones y actividades contractuales de los servidores públicos, contratistas y pasantes, los edificios cuentan con controles de acceso y registro de ingreso para visitantes en la recepción, los cuales son supervisados por la Subdirección Administrativa y Relación con la Ciudadanía de la Entidad. En cada uno de los pisos existen áreas seguras, sistemas de detección, extinción de incendios. Así mismo, existen áreas de evacuación y señalización que son supervisadas por la Subdirección de Gestión del Talento Humano.

⁴ <https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx>


⁵ <https://www.dnp.gov.co/DNP/gestion/Modelo-operacion-procesos/procesos-estrategicos/Paginas/planeacion-y-gestion-institucional-orientada-a-resultados.aspx>

⁶ 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.

⁷ La aceptación se realiza en las cláusulas contractuales

⁸ La aceptación se realiza en las cláusulas contractuales

⁹ <https://www.dnp.gov.co/la-entidad/organigrama>

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 7 de 81 VERSIÓN: 7

3.2. MARCO DE REFERENCIA EXTERNO

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 SGSI se encuentran identificadas y documentadas en el Normograma y otros documentos de Origen Externo.

De acuerdo con lo establecido en el artículo 209 de la Constitución Política, el título 9 del Decreto 1078 de 2015 del Ministerio de Tecnologías de la Información y las Comunicaciones y el artículo 10 del Decreto 1893 de 2021 del Departamento Nacional de Planeación trabaja permanentemente en el mantenimiento y mejora continua del componente de seguridad de la información siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Política de Gobierno Digital, con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información digital mediante la definición de políticas se actualizan de acuerdo con la dinámica del entorno.

El Componente de Gestión de Seguridad de la Información (CGSI) incluye la implementación de la Política de Gobierno Digital, Política de Seguridad Digital y Conpes 3995 Política de Seguridad y Confianza Digital. Las actividades del CGSI incluyen la participación en las mesas de trabajo de infraestructura crítica, sector Gobierno, y relación con otras entidades como MINTIC, Comando Conjunto Cibernético, Equipo de Respuesta a Incidentes del Sector Gobierno CSIRTGOB, Equipo de Respuesta a Incidentes de la Policía Nacional CSIRTPONAL y Grupo de Respuesta a Emergencias Cibernéticas colCERT.

Como entidad del Gobierno Nacional el diagnóstico del cumplimiento de la política 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 Pública¹⁰.

3.2.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Desde la implementación del Componente de Seguridad de la Información la Entidad ha adoptado los principios de seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI)¹¹ del 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 intranet¹² y en la sede electrónica¹³ del DNP y aceptadas por cada uno de los colaboradores¹⁴, proveedores¹⁵, o terceros¹⁶.
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.

¹⁰ <https://www.funcionpublica.gov.co/web/mipg/resultados-medicion>

¹¹ Guía 2 - Política General MSPI v1. Elaboración de la política general de seguridad y privacidad de la información. Pag 10. https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

¹² <https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx>

¹³ <https://www.dnp.gov.co/DNP/gestion/Modelo-operacion-procesos/procesos-estrategicos/Paginas/planeacion-y-gestion-institucional-orientada-a-resultados.aspx>

¹⁴ 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.

¹⁵ La aceptación se realiza en las cláusulas contractuales

¹⁶ La aceptación se realiza en las cláusulas contractuales



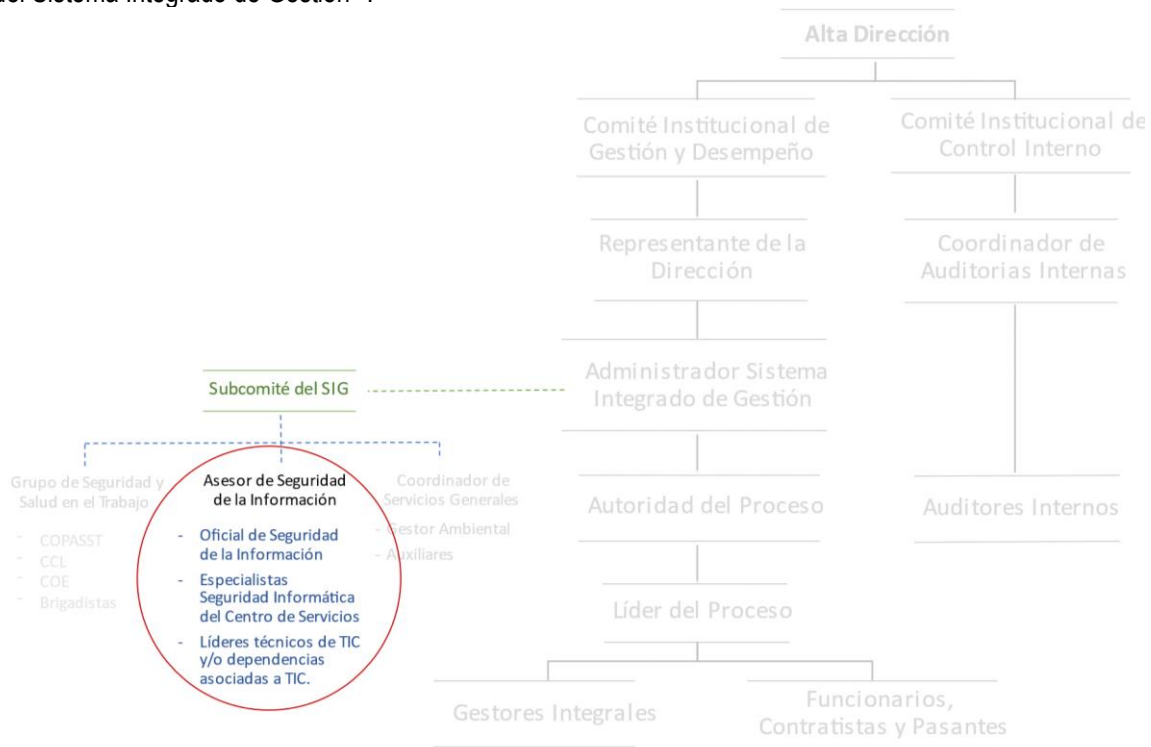
4. El DNP implementa los controles de acceso para la información digital, sistemas y recursos de red.
5. El DNP vela porque la seguridad informática sea parte integral del ciclo de vida de los sistemas de información institucionales.
6. El DNP realiza una adecuada gestión de los eventos de seguridad informática.
7. El DNP vela por el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas relacionadas con la seguridad informática.

4. DEFINICIONES

Las definiciones están en el Anexo 1

5. OBLIGACIONES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN


La estructura operacional del equipo de seguridad de la Información se encuentra referenciada en el Manual del Sistema Integrado de Gestión¹⁷.



Fuente: Manual SIG.

¹⁷ <https://intranet.dnp.gov.co/SGC/manual-de-calidad-y-operaciones/Paginas/Manual%20del%20Sistema%20Integrado%20de%20Gesti%C3%B3n.aspx>

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

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 9 de 81 VERSIÓN: 7</p>
--	--	---

5.1 ASESOR SEGURIDAD DE LA INFORMACIÓN

El rol de Asesor de Seguridad de la Información es la figura que coordina, promueve y participa en las actividades que tengan que ver con la Seguridad Informática e Información, y estará a cargo de un Asesor de la Oficina de Tecnología y Sistemas de Información (OTSI).


Sus responsabilidades son:

- Coordinar las actividades relacionadas con el componente de Gestión de Seguridad de la Información (GSI), que incluyen actualización y sensibilización de las Políticas de Seguridad de la Información.
- Realizar junto con la OTSI 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 (GSI).

5.2 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El rol de Oficial de Seguridad de la información tiene las siguientes responsabilidades:

- Liderar las personas que hacen parte del equipo de seguridad de la información de la Oficina de Tecnología y Sistemas de Información (OTSI) y el Centro de Servicios (CDS).
- Emitir conceptos técnicos, con el objeto de aconsejar y orientar la toma de decisiones en relación con la seguridad de los proyectos informáticos y demás requerimientos.
- Acompañar a la OTSI en la definición de procesos, procedimientos, manuales asociados al componente de Gestión de Seguridad de la Información (GSI).
- Realizar junto con la OTSI la actualización de las políticas del M-PG-07 Manual Operativo de seguridad de la información.
- Orientar a las dependencias en la identificación de los activos de información e identificación de los riesgos en materia de tecnologías de informática y comunicaciones con el fin de velar por la disponibilidad, seguridad, integridad y respaldo de la información que el DNP utiliza y procesa para su funcionamiento y toma de decisiones.
- Acompañar a la OTSI en la ejecución de las actividades relacionadas con la implementación de la estrategia de ciberseguridad definida por el Ministerio de Defensa, la política de seguridad digital definida por la Presidencia de la República y la normativa de protección de datos personales de la Superintendencia de Industria y Comercio.
- Actuar como enlace sectorial de seguridad digital ante el Coordinador Nacional de Seguridad Digital de la Presidencia de la República, y los equipos de respuesta a incidentes del Gobierno Nacional.
- Asesorar en el diagnóstico y aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el componente de Gestión de Seguridad de la Información (GSI) de la Entidad, alineado con la norma NTC ISO 27001:2013 y la Estrategia de Gobierno Digital en el componente de Seguridad y privacidad de la información.
- Realizar las actividades de divulgación y promoción de la importancia del componente de Gestión de Seguridad de la Información (GSI) y los temas relacionados en la normativa aplicable.
- Elaborar la generación de insumos que permitan la documentación de la gestión de requerimientos e incidentes relacionados con seguridad de la información y seguridad digital

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 10 de 81 VERSIÓN: 7

5.3 ESPECIALISTA CONTINUIDAD DE NEGOCIO DEL COMPONENTE TECNOLÓGICO

El rol de Especialista de Continuidad de negocio del componente tecnológico tiene las siguientes responsabilidades:

- Evaluar, construir y documentar las políticas y controles de seguridad de la información de la norma ISO 27001:2013 como base para la certificación que la Entidad desea hacer en vigencias futuras.
- Realizar el diagnóstico de cumplimiento de los requisitos del Anexo 3 “Seguridad Digital Web” de la Resolución 1519 de 2020 Resolución 1519 de 2020 para las publicaciones del DNP.
- Evaluar, construir y documentar las políticas y controles de seguridad de la información, y acompañar en la ejecución de las actividades relacionadas con el diagnóstico e implementación de la continuidad del negocio en el componente tecnológico según la norma ISO 22301:2019
- Evaluar, construir y documentar las políticas y controles de seguridad de la información, y acompañar en la ejecución de las actividades relacionadas con el diagnóstico e implementación del Plan de recuperación de Desastres (DRP) según la norma ISO 22301:2019 y las guías de MINTIC.
- Proponer las actividades del Plan de trabajo de continuidad de Negocio.
- Colaborar en las actividades relacionadas en el Plan de Trabajo de Seguridad y Privacidad.
- Realizar las actividades de divulgación y promoción de la importancia del componente de Gestión de Seguridad de la Información (GSI) y los temas relacionados en la normativa aplicable.
- Elaborar la generación de insumos que permitan la documentación de la gestión de requerimientos e incidentes relacionados con seguridad de la información y seguridad digital
- Elaborar insumos que contribuyan al mejoramiento de la Gestión de la Oficina mediante nuevas soluciones de tecnologías de la información y las comunicaciones.
- Articularse con la Oficina Asesora de Planeación para la estructuración del Plan de Continuidad de Negocio en el componente tecnológico.

5.4 ESPECIALISTA SEGURIDAD INFORMÁTICA DEL CENTRO DE SERVICIOS

El rol de Especialista Seguridad Informática del Centro de Servicios tiene las siguientes responsabilidades:

- Efectuar la administración, configuración, supervisión y control de la seguridad de la infraestructura de la red de datos, abarcando incluso la nube (privada y/o pública).
- Prestar en sitio o remoto la atención y solución de solicitudes de servicios, previamente registradas en la herramienta de gestión de servicios de TIC (ITSM).
- Escalar a los proveedores relacionados con los equipos y/o software, los requerimientos e incidentes en coordinación con el supervisor del contrato y registrar su seguimiento a través de la herramienta de gestión de servicios de TIC (ITSM).
- Mantener al día la documentación de los procesos y procedimientos asociados con la prestación de los servicios a cargo.
- Efectuar la administración, configuración, supervisión y control de las herramientas de seguridad de la entidad como Firewall, IDS, IPS, entre otros.
- Realización de Pruebas de Vulnerabilidades y apoyar en la solución de estas.
- Gestionar de las alertas e informes del Centro de Operaciones de Seguridad (SOC).

5.5 LÍDERES TÉCNICOS DE TIC

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 OTSI, proveedores con contratos vigentes que apoyen la gestión de la plataforma tecnológica (en caso de ser requerido) tienen las siguientes responsabilidades:

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



- Gestionar la recolección de evidencia de los incidentes informáticos relacionados con la infraestructura tecnológica.
- Realizar la identificación de riesgos de los activos de información de su competencia, de acuerdo con el PT-PG-01 Procedimiento de Gestión Integral de Riesgos¹⁸.
- Realizar la identificación de los activos de información e identificación de los riesgos en materia de tecnologías de informática y comunicaciones con el fin de velar por la disponibilidad, seguridad, integridad y respaldo de la información que el DNP utiliza y procesa para su funcionamiento y toma de decisiones.

6. ESTRUCTURA DEL COMPONENTE DE GSI

6.1. 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 la información, protegiéndola desde la plataforma tecnológica, infraestructura física y recurso humano que la soporta.

6.1.1 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.

Clasificación Ley de Transparencia	Relación otras clasificaciones
Información pública	<p>Usos de la información en la Entidad</p> <ul style="list-style-type: none"> • Público <p>Clasificación Datos personales</p> <ul style="list-style-type: none"> • Dato público • Datos personales laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); • Datos personales académicos (trayectoria educativa, título, número de cédula, certificados, etc.) <p>Clasificación según Habeas Data</p> <ul style="list-style-type: none"> • Pública o de dominio público
Información pública clasificada: Información exceptuada por daño de derechos a personas naturales o jurídicas	<p>Clasificación según Ley de Transparencia</p> <ul style="list-style-type: none"> • Los secretos comerciales, industriales y profesionales • El derecho de toda persona a la intimidad • El derecho de toda persona a la vida, la salud o la seguridad <p>Usos de la información en la Entidad</p> <ul style="list-style-type: none"> • Uso interno • Uso privado <p>Clasificación según Habeas Data</p>

¹⁸ <https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx>



Clasificación Ley de Transparencia	Relación otras clasificaciones
	<ul style="list-style-type: none"> • Semi-privada • Privada • Reservada o secreta <p>Clasificación Datos personales (Datos sensibles)</p> <ul style="list-style-type: none"> • Ideológicos: creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas. • Sobre la vida y hábitos sexuales, origen (étnico y racial.) • Características físicas: color de piel, iris y cabellos, señales particulares, etc. • Características como tipo de sangre, ADN, huella digital, etc. • Salud: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc. • Patrimoniales: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc. • Identificación: nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad. • Datos personales de menores
<p>Información pública reservada: Información exceptuada por daño a los intereses público</p>	<p>Usos de la información en la Entidad</p> <ul style="list-style-type: none"> • Confidencial <p>Clasificación según Ley de Transparencia</p> <ul style="list-style-type: none"> • La defensa y seguridad nacional • La seguridad pública • Las relaciones internacionales • La prevención, investigación y persecución de los delitos y las faltas disciplinarias • El debido proceso y la igualdad de las partes en los procesos judiciales • La administración efectiva de la justicia • Los derechos de la infancia y la adolescencia • La estabilidad macroeconómica y financiera del país • La salud pública

La información digital¹⁹ 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.

La información digital con datos personales se encuentra almacenada en los sistemas de información y aplicativos, por lo tanto, es importante determinar la clasificación de esta teniendo en cuenta 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.

¹⁹ Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen
Este documento es fiel copia del original que reposa en la Oficina Asesora de Planeación. Su impresión se considera copia no controlada



6.1.2 DISPONIBILIDAD

La información debe estar disponible en cualquier momento.

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

6.1.3 INTEGRIDAD

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

Calificación	Explicación
Baja	Se requiere un bajo grado de exactitud y completitud de la información.
Mediana	Se requiere un mediano grado de exactitud y completitud de la información.
Alta	Se requiere un alto grado de exactitud y completitud de la información.
Muy Alta	Se requiere un muy alto grado de exactitud y completitud de la información.

6.1.4 AUTENTICIDAD

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

6.1.5 AUDITABILIDAD


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

6.1.6 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.

6.2. PROPIEDAD DE LA INFORMACIÓN

La información pertenece al DNP, a menos que en una relación contractual se establezca lo contrario.

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 14 de 81 VERSIÓN: 7

7. POLÍTICAS

Las políticas incluidas en el M-PG-07 Manual Operativo de seguridad de la información contienen las directrices que deben cumplir los usuarios 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 y estén sometidos a los controles correspondientes para su adecuada protección; a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como Internet y el correo electrónico; a brindar a los usuarios pautas para la utilización apropiada ; y a contribuir a minimizar los riesgos de una eventual pérdida de los activos de información digital del DNP.

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.

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

7.1. POLÍTICA DE SEGURIDAD

El presente documento contiene las políticas con respecto a la seguridad de la información del DNP.

7.2. SEGURIDAD ORGANIZACIONAL

Gestiona la seguridad de la información dentro del DNP. (Roles, compromisos, 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 (GSI) del SIG. El 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 los directores, subdirectores, jefes de oficina, el Oficina Asesora de Planeación y los gestores SIG.



[PL02-ES3]

Todos los usuarios²⁰ del DNP, deberán conocer y cumplir el M-PG-07 Manual Operativo de seguridad de la información, el código de integridad²¹ y dar uso apropiado a los recursos entregados conforme a lo establecido en el Código Único Disciplinario²².

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

Los funcionarios 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 los funcionarios, contratistas, pasantes deberán presentar la evaluación de conocimiento de Seguridad de la Información, hasta que el resultado sea aprobado.

[PL02-ES4]

Todos los usuarios que identifiquen cualquier anomalía, debilidad, mal funcionamiento y/o incidente de seguridad en la prestación de algún servicio de TIC deberán reportarlo al Centro de Servicios y/o a la Jefatura de la OTSI, llamando a la extensión 11234, 11200, y/o al correo electrónico centrodeservicios@dnpgov.co.

[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.

²⁰ Funcionarios, contratistas, pasantes, proveedores y terceras partes del DNP.

²¹ <https://www.dnp.gov.co/DNP/recursos-humanos/Paginas/C%C3%B3digo-de-Integridad.aspx>

²² Ley 734 de 2002



7.3. SEGURIDAD DEL RECURSO HUMANO

Políticas que buscan asegurar que los usuarios, entiendan sus responsabilidades en relación con las políticas de seguridad del DNP y actúen de manera consistente con las mismas.

[PL03-ES1]


Cuando un usuario termine su relación laboral o finalice su relación contractual, y/o sea trasladado de dependencia, el jefe de la dependencia y/o supervisor, 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 los usuarios al centro de servicios y/o la OTSI.

[PL03-ES2]

Cuando un usuario se encuentre ad- portas de terminar su relación laboral o contractual con la entidad, el jefe de área responsable y/o supervisor del contrato, deberá 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 a retirar los accesos lógicos de ingreso a los activos de información a los que el usuario tenía acceso.

Para permitir un tiempo de entrega del cargo e información, empalme o presentación de informes del estado de las actividades realizadas por 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 el 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 los funcionarios deben establecerse en estado inactiva, máximo a los diez (10) días calendario de finalizar la relación laboral.
- Las cuentas de acceso para los 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 los 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 del usuario se dará dentro de los quince (15) días calendario siguientes a la finalización de la relación contractual.
- Las cuentas de acceso para los 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 los contratistas que pertenezcan a la Subdirección Financiera, Subdirección de Contratación, Oficina de Control Interno, Oficina Jurídica, Subdirección Administrativa y Relacionamento 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 aquellos colaboradores que se encuentren en trámite del proceso de contratación tendiente a la suscripción del

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 17 de 81 VERSIÓN: 7

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 un usuario sea trasladado de dependencia, el jefe de área responsable y/o supervisor, deberán informar a los líderes funcionales y técnicos, administradores 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 el usuario tenía acceso y realizar la respectiva reasignación.
- Todo jefe de área y/o supervisor del contrato, deberá 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.

[PL03-ES3]

Cuando un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia, el jefe de área responsable y/o supervisor deberán verificar la entrega de la información, su organización en los discos de red para garantizar su preservación y conservación, para posterior alistamiento²³, reasignación del equipo a un nuevo usuario. Para la verificación de la información se debe tener en cuenta el M-AD-03 Manual para la Gestión de Documentos y Administración de Archivo²⁴.

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 un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia el jefe de área responsable y/o supervisor deberán verificar que los activos asignados a los funcionarios, contratistas, pasantes o proveedores sean devueltos a la Subdirección Administrativa y Relación 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 inmuebles²⁵.

[PL03-ES5]


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

Cuando un usuario requiera retirar de las instalaciones de la entidad activos informáticos, se deberá solicitar autorización a la Subdirección Administrativa y Relación con la Ciudadanía, con el fin de registrar, controlar y hacer seguimiento a los mismos. El usuario que retire el activo será el responsable de la custodia, salvaguarda de la información que allí este almacenada.

²³ Alistamiento: Procedimiento de formateo de las estaciones cliente, instalación de software base, eliminando la información del usuario que se retira o traslada de la dependencia.

²⁴ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>

²⁵ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 18 de 81 VERSIÓN: 7

Los funcionarios, 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 inmuebles²⁶.

[PL03-ES6]

Para acceder a la información del correo electrónico institucional y/o la estación de trabajo, se debe contar con la autorización expresa del usuario titular de la cuenta. 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 del usuario el acceso será entregado al jefe inmediato y/o supervisor previa solicitud de este la gestión de la solicitud se adjuntará al ticket asignado.

[PL03-ES7]

Cuando un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia el jefe de área responsable y/o supervisor deberán verificar que el usuario entregue copia de los mensajes electrónicos institucionales almacenados en su buzón de correo, para que estos puedan ser consultados posteriormente.

7.4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Establecen los lineamientos que se relacionan con el mantenimiento y protección apropiados de todos los activos de información son identificados con base en el Procedimiento para la identificación de activos²⁷.

[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 intranet²⁸.

En caso de requerir la instalación del software se debe realizar la solicitud a través del Centro de Servicios de acuerdo con el Procedimiento PT-TI-01 Atención a Requerimientos de Servicios TIC²⁹, 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, el usuario deberá gestionar la solicitud con la OTSI, enviando la siguiente información: nombre software, área usuaria, funcionario 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 los usuarios.

²⁶ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>

²⁷ <https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx>

²⁸ <http://intranet.dnp.gov.co/gestiondeTIC/Servicios%20TIC/Paginas/Computador-Institucional.aspx>

²⁹ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-de-tic.aspx>

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 19 de 81 VERSIÓN: 7

Los usuarios 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 aquellos usuarios 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]

Los usuarios deben de solicitar a través del Centro de Servicios los requerimientos de aplicativos, equipos informáticos, software de acuerdo con el Procedimiento PT-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 los usuarios, 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. Los usuarios 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.

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



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, y en los discos de red. La OTSI realizará el monitoreo e informará a las dependencias para su respectiva eliminación.

[PL04-ES10]

Los usuarios no deberán realizar las siguientes labores sin previa autorización de la OTSI:

- (1) instalar software en cualquier equipo del DNP,
- (2) bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del DNP;
- (3) modificar, revisar, transformar o adaptar cualquier software;
- (4) descompilar o realizar ingeniería de reverso en cualquier software.

[PL04-ES11]

El Usuario 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]

El usuario es responsable de todas las transacciones o acciones efectuadas con su usuario.

[PL04-ES13]

Cada usuario 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 solicitud de cambios* (F-TI-18) y será realizado de acuerdo con los procedimientos definidos por el DNP para su ejecución.



[PL04-ES16]

Es responsabilidad de los usuarios 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 se podrán almacenar borradores de los documentos institucionales.

Es responsabilidad de la OTSI el respaldo de forma frecuente de la información para ser recuperada en caso de incidentes de seguridad con los equipos de procesamiento y almacenamiento.

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

El respaldo de la información contenida en las estaciones cliente es responsabilidad de los usuarios.

[PL04-ES17]

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

Antes de autorizar cualquier acceso a la estación cliente (para servicios de mantenimiento, actualizaciones o cambios de equipos), el usuario 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 del usuario 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 inmuebles³⁰ de la Subdirección Administrativa y Relación 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 Relación con la Ciudadanía.

[PL04-ES20]

Los equipos que ingresan temporalmente al DNP que son de propiedad de terceros, deben ser registrados por los usuarios 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.

³⁰ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 22 de 81 VERSIÓN: 7</p>
--	--	--

Si el usuario 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 seguridaddigital@dn.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 vengan 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 el usuario este activo en la entidad, exceptuando los correos que el usuario haya eliminado directamente en el servidor.

[PL04-ES25]

Los usuarios 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

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 23 de 81 VERSIÓN: 7

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. 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 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 usuarios 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, los usuarios deben utilizar su correo personal no institucional, con la finalidad de reducir el riesgo de atribuciones erróneas al DNP sobre opiniones.

Los usuarios 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.

[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@dnpc.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@dnpc.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]

Los usuarios 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 los usuarios están dados por los siguientes Grupos:

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]

Se prohíbe extraer, divulgar y/o publicar información física, digital, y/o almacenada en los discos de red, 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 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]

Ningún usuario 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 de la OTSI.

[PL04-ES36]

Es responsabilidad del usuario 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 usuarios para que todos los usuarios del DNP y los jefes de las distintas dependencias puedan 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.

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 26 de 81 VERSIÓN: 7</p>
--	--	--

[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 los usuarios la importancia de su protección y reducir 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 tercero³¹, 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.

7.5. CONTROL DE ACCESO

El DNP implementará control de acceso a la información digital, sistemas y recursos de red. Las políticas mencionadas a continuación establecen los lineamientos generales para garantizar el acceso seguro a los activos de información digitales del DNP por parte de usuarios autorizados.

³¹ Entidades externas al DNP.



[PL05-ES1]

La identificación de los usuarios ante cada sistema de información será única y confidencial.

[PL05-ES2]

Los usuarios³² 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]

Todos los usuarios 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 a través del centro de servicios de 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.

³² Funcionarios, contratistas, pasantes y proveedores del DNP.



[PL05-ES7]

Las cuentas de usuario se asignarán con privilegios de usuario normal, es decir sin privilegios de administración. Los usuarios 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 el jefe inmediato 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, el usuario la utilizará solo en el primer inicio de sesión obligándolo a realizar el cambio para acceder al servicio.

Para facilitar al usuario el cambio de las contraseñas, el DNP cuenta con el sistema de recuperación de contraseñas que está disponible en <https://govrecont.dnp.gov.co/>, adicionalmente el usuario puede llamar 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 inactivas.

[PL05-ES11]

Los usuarios 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.

- Los archivadores y escritorios deben permanecer cerrados con llave.
- No dejar documentos confidenciales a la vista de otras personas.
- Los documentos confidenciales deben ser destruidos antes de ser arrojados a la basura.
- Al finalizar las labores diarias o si el usuario se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.
- Evitar papeles autoadhesivos que contengan información confidencial, especialmente contraseñas.
- Mantener organizado y en orden el puesto de trabajo.

[PL05-ES13]

Los usuarios son responsables de no ingerir alimentos ni bebidas en el puesto de trabajo.



[PL05-ES14]

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

[PL05-ES15]

Los usuarios deben recoger los trabajos de impresión que contengan información confidencial de forma inmediata.

[PL05-ES16]

Mostrar una advertencia indicando la responsabilidad que asume el usuario 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 tipo SSL, para garantizar la seguridad de la información entre las entidades participantes.

[PL05-ES19]

Los usuarios deben usar los equipos institucionales con propósitos laborales.

[PL05-ES20]

Los usuarios 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]

Los usuarios deben reportar el extravió 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 inmuebles³³.

[PL05-ES22]

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

³³ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>

[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 el usuario propietario.

[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 los usuarios 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.



7.6. CRIPTOGRAFÍA

Establece las generalidades del cifrado de la información.

[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 servicios de información³⁴ las dependencias responsables deben solicitar a la OTSI la configuración de los certificados de sitio web seguro, 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, 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 los usuarios autorizados para firmar, para que esta oficina realice la instalación de estos.

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

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

En caso de pérdida de token de firma digital u olvido de la contraseña el usuario 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.

³⁴ Aplicativos, portales, sistemas de información



[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 las claves de cifrado y para la aplicación de controles criptográficos

[PL06-ES8]

Los líderes técnicos de TIC (internos o externos) deben cifrar la información reservada 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.



7.7. SEGURIDAD FÍSICA Y AMBIENTAL

Busca prevenir el acceso físico no autorizado a las instalaciones del DNP, para prevenir daños o interferencias a los activos de 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 Relacionamento 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 Logística³⁵.

[PL07-ES4]

La Subdirección Administrativa y Relacionamento 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.

[PL07-ES5]

La limpieza y aseo del centro de datos y afines está a cargo de la Subdirección Administrativa y Relacionamento con la Ciudadanía y debe efectuarse en presencia de un funcionario del DNP, 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.

³⁵ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>



[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 Relacionamento 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 un funcionario 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 Relacionamento 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 Relacionamento 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 inmuebles³⁶ de la Subdirección Administrativa y Relaciónamiento 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]

El retiro e ingreso de todo activo informático de propiedad de los usuarios del DNP, utilizados para fines personales se realiza mediante los procedimientos establecidos por la administración del Edificio. El DNP no se hace responsable por la pérdida de estos bienes o el daño que se presenten al conectarse a la red eléctrica del departamento o por otros eventos.

[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.

³⁶ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-administrativa.aspx>



[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.



7.8. GESTIÓN DE OPERACIONES

Establece los lineamientos y busca asegurar la correcta y segura operación de la gestión de información.

[PL08-ES1]

Los usuarios 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 sensible, sin estar legalmente autorizado para ello.
- Reenviar o copiar sin permiso mensajes "confidenciales" 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]

Todos los usuarios 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 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 los funcionarios autorizados internamente para ello.

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

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	<p>MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)</p>	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 39 de 81 VERSIÓN: 7</p>
---	---	--

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 funcionarios.

[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 los usuarios 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 el usuario encuentre este tipo de material en internet, deberá desconectarse del sitio en forma inmediata.

[PL08-ES7]

El correo en cadena es un mensaje enviado a un número de destinatarios para que estos a su vez se lo reenvíen a otros. El envío de correo masivo se refiere aquel enviado un gran número de receptores sin un propósito relacionado con la misión del DNP. El usuario 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)
- WIFI DVR (Exclusiva para funcionarios Regalías a nivel nacional con portátiles y tablets)
- DIRECCION GENERAL (Exclusiva conexión director general).
- WIFI GRATIS PARA LA GENTE (Exclusiva visitantes servicio al ciudadano).

[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.

[PL08-ES10]

Los cambios que se presenten en las actividades de operación³⁷ de la OTSI deben ser actualizados en los respectivos documentos.

[PL08-ES11]

Cualquier cambio a la plataforma tecnológica deberá ser 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.

[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 la red WIFI de funcionarios del DNP deben tener instalado el antivirus institucional actualizado.

³⁷ 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-ES18]

Es responsabilidad de cada usuario, revisar que todos los medios extraíbles sean verificados con un antivirus provisto por el DNP, antes de procesarlos en los computadores personales 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 ActiveX³⁸ 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.

[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.

³⁸ Es una tecnología de Microsoft para el desarrollo de páginas dinámicas.

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

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <p>Página 42 de 81 VERSIÓN: 7</p>
--	--	--

[PL08-ES27]

La OTSI 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 seguro³⁹ 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, como mejor práctica para la optimización de uso de los recursos que entrega el DNP a sus usuarios.

[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 o WIFI de funcionarios del DNP, 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 del usuario de cumplir con las características de seguridad y políticas definidas por el DNP.

[PL08-ES33]

La conexión de usuarios 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 perimetral debe tener mecanismos de control que incluyan: Firewall⁴⁰, Filtro de contenido⁴¹, Antivirus y Antispam.

³⁹ 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

⁴⁰ Aplicación utilizada para controlar las comunicaciones, permitiéndolas o prohibiéndolas. Tomado de: <http://es.wikipedia.org/wiki/>

⁴¹ Programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. Tomado de: <http://es.wikipedia.org/wiki/>

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

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07 Página 43 de 81 VERSIÓN: 7
--	--	--

[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 plataforma 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]

El usuario no debe abrir los archivos anexos a los correos electrónicos. No abrir mensajes que no tienen una relación con las actividades del DNP⁴². Es responsabilidad del usuario reportar al centrodeservicios@dnpc.gov.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

⁴² Publicidad, sorteos, loterías, suscripciones, etc.



[PL08-ES44]

Los usuarios 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).

[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]

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

[PL08-ES49]

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 del funcionario y éste fuera su propio domicilio, se hará siempre con previa notificación y consentimiento de éste/a.

[PL08-ES50]

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-ES51]

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 del usuario con conexión remota siguiendo los procedimientos establecidos por el DNP.



[PL08-ES52]

El teletrabajador y el usuario con conexión remota se comprometen a respetar la legislación en materia de protección de datos, 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.

[PL08-ES53]

Los derechos de propiedad intelectual e industrial que se generen por las actividades contratadas al Teletrabajador le pertenecen al DNP. El Teletrabajador y el usuario con conexión remota no tendrán 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-ES54]

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 quince (15) días hábiles a través de la cual se justifique la razón por la cual desea dar por terminada la modalidad de teletrabajo.

7.9. GESTIÓN DE COMUNICACIONES

El DNP controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos. Las siguientes políticas están enfocadas en el intercambio de información y gestión de la seguridad en las redes.

[PL09-ES1]

Los accesos de conexión remota son exclusivamente para propósitos laborales y su solicitud debe sustentarse con el diligenciamiento del formato *solicitud servicio conexión remota* (F-TI-04).

[PL09-ES2]

El acceso remoto de usuarios a la red LAN del DNP se permitirá por medio del servicio de conexión remota y VPN

[PL09-ES3]


La activación de conexión remota de usuarios internos o externos debe ser debidamente solicitada, justificada y aprobada a través de un procedimiento formal y documentado.

[PL09-ES4]

Si las dependencias requieren conexiones remotas o VPN deben ser solicitadas a la OTSI, a través de los canales de contacto del centro de servicios.

[PL09-ES5]

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

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 47 de 81 VERSIÓN: 7

7.10. ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS

Promueve la inclusión de los controles de seguridad en la plataforma tecnológica⁴³, Servicios de Información⁴⁴, Licencias de Software⁴⁵, Suscripción de Software⁴⁶ 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-ES5]

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.

⁴³ Infraestructura, software base, comunicaciones, etc.

⁴⁴ Representan los portales (páginas web) y sistemas de información desarrollados a la medida para el Departamento Nacional de Planeación (DNP).

⁴⁵ 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.

⁴⁶ 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.

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



[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 el usuario.

[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 dueñas de los sistemas de información, la asignación de recursos humanos y económicos para el mantenimiento, actualización, adquisición de licenciamiento, ya que 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 SIG⁴⁷ y deberá guardar coherencia con lo establecido en Manual de Contratación⁴⁸ del DNP: *“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 el 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 los usuarios directamente implicados en su operación.

⁴⁷ Sistema Integrado de Gestión <https://intranet.dnp.gov.co/SGC/manual-de-calidad-y-operaciones/Paginas/modelo-de-operacion-por-procesos.aspx>

⁴⁸ Página 18. M-CT-01 Manual de Contratación <https://www.dnp.gov.co/la-entidad/contrataci%C3%B3n>



[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.

[PL10-ES13]

Las funcionalidades de los aplicativos serán definidas por las dependencias usuarias. La Oficina de Tecnología y Sistemas de Información brindará el apoyo técnico de acuerdo con las políticas y lineamientos técnicos adoptados por la Oficina de Tecnología y Sistemas de Información.

[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.

[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 administradores de los diferentes activos de Información deben en forma activa implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información, de acuerdo con las políticas de seguridad de la información del DNP.


[PL10-ES19]

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-ES20]

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	<p>MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)</p>	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 50 de 81 VERSIÓN: 7</p>
---	---	--

Se entiende por software de apoyo o base para el desarrollo o funcionamiento de las aplicaciones, a los seleccionados por la Oficina de Tecnología y Sistemas de Información de acuerdo con su Plataforma Tecnológica, entre estos son: sistema operativo, comunicaciones, Web, herramientas de modelamiento y desarrollo, motores de bases de datos, software de uso común y software específico.

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 51 de 81 VERSIÓN: 7

7.11. RELACIÓN CON PROVEEDORES

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 el contratista interactúe con cualquier activo de información (plataforma e infraestructura tecnológica) del DNP, debe cumplir con las políticas del componente de GSI de la Entidad.

[PL11-ES2]

El 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 contratistas y proveedores deben realizarse de una forma controlada, segura y organizada definida a través de Acuerdos de Niveles de Servicio (ANS).

[PL11-ES4]

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

[PL11-ES5]

Los contratistas y proveedores están obligados a cumplir los Acuerdos de Nivel de Servicio (ANS).

[PL11-ES6]

Los contratistas y proveedores 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]

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 y tienen las mismas responsabilidades que los usuarios del DNP (cláusula de confidencialidad y políticas de seguridad).

7.12. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

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 del 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 el procedimiento PT-PG-01 Gestión integral de riesgos⁴⁹.

[PL12-ES2]

Los incidentes de seguridad se deben reportar al Centro de Servicios y asignarlo a la persona encarga de la seguridad de la información. El asesor de la Oficina de Tecnología y Sistemas de Información encargado del tema de seguridad informática, 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-TH-07 Indagación preliminar e investigación disciplinaria⁵⁰ 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 y la Oficina de Control Interno.

[PL12-ES4]

Los incidentes de severidad grave y muy grave⁵¹ deben ser reportados al Centro de Servicios y serán escalados al Grupo de Seguridad quienes deben realizar la revisión y análisis de la información encontrada y reportarla a la Oficina de Control Interno Disciplinario con copia a la Secretaría General y Oficina de Tecnología y Sistemas de Información.

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 incidentes⁵², previa autorización de la Secretaria General.

[PL12-ES5]

Los usuarios 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.

⁴⁹ <https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx>

⁵⁰ <https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-y-desarrollo-del-talento-humano.aspx>

⁵¹ Glosario conceptos relacionados con incidentes de seguridad

⁵² Colcert, CsirtGob, CSIRT PONAL



[PL12-ES6]

Los usuarios 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]

El Centro de servicios escalará los incidentes de seguridad 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, los cuales deben ser presentados a través de la Oficina de Tecnología y Sistemas de Información a la Secretaría General con copia al Jefe de la Oficina Asesora Jurídica y al Jefe Inmediato o Supervisor del contrato, según sea el caso, 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.

[PL12-ES8]

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

[PL12-ES9]


Los responsables de seguridad de la información de la Oficina de Tecnología y Sistemas de Información deben analizar el comportamiento de los incidentes de seguridad ocurridos con el fin de mitigar los riesgos e informar a los líderes de los procesos involucrados en los incidentes y al Oficina Asesora de Planeación.

[PL12-ES10]

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-ES11]

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

	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 54 de 81 VERSIÓN: 7

7.13. ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

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 y los niveles táctico y operativo, garantizando un nivel de aseguramiento razonable en la entidad.

[PL13-ES2]

El Oficina Asesora de Planeación del DNP 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]

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales del DNP podrán ser restaurados dentro de escalas de tiempo razonables.

[PL13-ES4]

El DNP deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos: Identificación y asignación de prioridades a los procesos críticos dentro del DNP de acuerdo con su impacto. Documentación de la estrategia de continuidad del negocio. Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente. Plan de pruebas de la estrategia de continuidad del negocio, mejoramiento del plan de continuidad de negocio a partir de su revisión y pruebas.



[PL13-ES5]

La continuidad del negocio será gestionada por la Secretaria General.

[PL13-ES6]

La Secretaria General es la responsable, ante el DNP, de velar por la implantación 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]

La Secretaria General se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de estas.

7.14. CUMPLIMIENTO

Busca prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

[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, Normativa, y en el portal del DNP www.dnp.gov.co⁵³.

[PL14-ES2]

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

[PL14-ES3]

El director del DNP, los Subdirectores, la Secretaria General, Jefes de Dependencia, Jefes de Oficina y Coordinadores de Grupo son los responsables de que todos sus colaboradores conozcan, acepten y cumplan las políticas de seguridad de la información y velar por el que se cumplan los procedimientos definidos por el DNP.

⁵³ <https://www.dnp.gov.co/normativas/normograma>

7.15. PROTECCIÓN DE DATOS

La protección de los datos personales está consagrada en la Constitución Política, como el derecho fundamental que tienen todas las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

Tal y como se puede evidenciar desde su concepción constitucional, este derecho surgió vinculado con otras garantías como la honra, la intimidad, la reputación, el libre desarrollo de la personalidad y el buen nombre. No obstante, en el desarrollo jurisprudencial del mismo, se consolidó como un derecho autónomo catalogado como Hábeas Data y en algunas oportunidades, como derecho a la autodeterminación informativa o informática.

Actualmente el derecho de Hábeas Data debe estudiarse desde dos contextos: primero y como se expuso anteriormente, como derecho autónomo y adicionalmente como garantía de otros derechos y libertades que dependen de una administración de datos deficiente, “Por vía de ejemplo, el habeas data opera como garantía del derecho al buen nombre, cuando se emplea para rectificar el tratamiento de información falsa. Opera como garantía del derecho a la seguridad social, cuando se emplea para incluir, en la base de datos, información personal necesaria para la prestación de los servicios de salud y de las prestaciones propias de la seguridad social. Opera como garantía del derecho de locomoción, cuando se solicita para actualizar información relacionada con la vigencia de órdenes de captura, cuando éstas por ejemplo han sido revocadas por la autoridad competente. Y finalmente, puede operar como garantía del derecho al trabajo, cuando se ejerce para suprimir información que funge como una barrera para la consecución de un empleo”.

Es importante tener claro que el ámbito de protección de este derecho no abarca cualquier tipo de información que se relacione con una persona, pues depende de un entorno vinculado con la administración de bases de datos personales. Es así como, en procura de amparar el derecho de Hábeas Data, se incorporaron al ordenamiento jurídico normas que establecen reglas para aquellas personas (naturales y jurídicas) de carácter público y privado que recolectan información personal en bases de datos.

Por lo anterior, y dado que el Departamento Nacional de Planeación (DNP) requiere para el ejercicio de sus funciones recolectar datos personales de los ciudadanos e incorporarlos en bases de datos, así como, la información que de otras entidades relacionada con datos personales.; elaboró la presente política de datos el presente documento que contiene los lineamientos a seguir para la creación, tratamiento y cierre de las bases de datos, el cual incluye buenas prácticas y estándares universales en la materia.

Así mismo elaboró el M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP, de conformidad con el artículo 2.2.2.25.3.1 Política de Tratamiento de la Información del Decreto 1074 de 2015, el cual se encuentra disponible en la sede electrónica del DNP⁵⁴.

Con la implementación de esta política por parte de las personas vinculadas a la entidad, se busca asegurar que los datos personales no sean informados y utilizados por terceros sin contar con la previa, expresa y libre autorización del titular de la información. En el caso de la información que se levanta en los contratos de consultoría es usada por los consultores (que son terceros) pero cuando se solicita la autorización a los entrevistados se dice que es para esa evaluación. De esa manera, se ha dispuesto de manera sencilla lo largo del instrumento la descripción del paso a paso para ser aplicado por cualquier colaborador del DNP, independientemente de su formación académica y que cumpla el rol de encargado o responsable de las bases de datos.

⁵⁴ <https://www.dnp.gov.co/DNP/gestion/Modelo-operacion-procesos/procesos-estrategicos/Paginas/planeacion-y-gestion-institucional-orientada-a-resultados.aspx>

[PL15-ES1]

Cuando una dependencia del DNP requiera recolectar datos personales para crear una base de datos, debe identificar claramente el ¿Por qué? necesita esa información la finalidad estar relacionada con las funciones atribuidas al DNP las cuales están descritas en capítulo “información que recopila el DNP” del M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP⁵⁵.

[PL15-ES2]

El responsable del tratamiento de los datos es el Departamento Nacional de Planeación a través de las dependencias. El responsable de tratamiento de datos personales es el responsable de tomar las decisiones sobre las bases de datos y/o el tratamiento de los datos. Define la finalidad y la forma en que se recolectan, almacenan y administran los datos. Asimismo, está obligado a solicitar y conservar la autorización en la que conste el consentimiento expreso del titular de la información

El tratamiento de la información que realiza el DNP está descrito en capítulo “tratamiento de la información” del M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP.

[PL15-ES3]

Los Derechos de los ciudadanos están descritos en capítulo derechos de los titulares de los datos personales” del M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP.

[PL15-ES4]

La Subdirección Administrativa y Relacionamiento con la Ciudadanía es el área responsable de la atención a los titulares y demás aspectos relacionados con las PQRSD están descritos en el M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP.

[PL15-ES5]

Las dependencias definirán los colaboradores que accederán a las bases de datos; así como, las contraseñas y procedimientos que sean necesarios.

[PL15-ES6]

Durante el tratamiento de los datos personales los titulares de la información pueden solicitar la supresión de estos. Una vez radicada esta solicitud, se debe indicar al titular los tiempos de respuesta que existen para dar trámite a esta.

[PL15-ES7]

Teniendo en cuenta que para la recolección de la información se debe establecer su finalidad, es claro que cuando ésta deja de existir no es procedente seguir con el tratamiento de los datos personales; no obstante, si el término que se había establecido inicialmente no es suficiente y se requiere prorrogarlo, es necesario contar nuevamente con la autorización del titular de la información.

⁵⁵ <https://www.dnp.gov.co/DNP/gestion/Modelo-operacion-procesos/procesos-estrategicos/Paginas/planeacion-y-gestion-institucional-orientada-a-resultados.aspx>



[PL15-ES8]

Con el objeto de cerrar la base de datos, bien sea porque el titular de la información lo requirió o porque se agotó su finalidad, se deben llevar a cabo la anonimización de la información. Este es un procedimiento mediante el cual se “expresa un dato relativo a entidades o personas, eliminando la referencia a su identidad” (RAE). Para realizarlo de manera adecuada, se deben tener en cuenta los siguientes aspectos:

El proceso de anonimizar información no sólo implica la eliminación de las variables de identificación directa de la unidad de observación (por ejemplo, la cédula o el NIT de una empresa), sino que se deben realizar procedimientos adicionales para garantizar la confidencialidad de los datos.

Se debe valorar el “riesgo de revelación individual”, es decir, la probabilidad que tiene una observación de ser descubierta a partir de características que contiene la información. Por ejemplo, basado en información detallada de las empresas de un sector económico, se pueden identificar las variables que incrementan el riesgo de identificar las firmas más grandes. Algunos casos de este tipo de variables pueden ser el número de empleados o el valor de los activos.

Esta valoración se puede realizar de manera rigurosa mediante la programación de algoritmos en programas estadísticos que arrojan la probabilidad exacta del riesgo de revelación individual, o analizando una por una las variables e identificando aquellas que aumentan este riesgo.

Una vez se ha establecido el “riesgo de revelación individual”, se define un umbral de riesgo tolerable. Luego, se evalúan los distintos métodos de anonimización reconocidos en la literatura, tales como: i) microagregación, ii) ruido, iii) data swaping, iv) supresión, v) supresión local, entre otros, con el objetivo de aplicarlos a las observaciones cuyo riesgo sobrepasa el umbral. Es importante aclarar que entre más se reduce el riesgo de revelación, menos útil es la información.

[PL15-ES9]

La OTSI debe incluir las bases de datos creadas en el aplicativo del Registro Nacional de Bases de datos de acuerdo con el procedimiento definido por la Superintendencia de Industria y Comercio⁵⁶.

[PL15-ES10]

Es responsabilidad de los usuarios organizadores de las reuniones en Teams, configurar la privacidad de estas, en caso de que la reunión requiera ser grabada el moderador deberá informar a los asistentes de esta acción. Al unirse a la reunión los usuarios aceptan los términos y condiciones de esta. Los videos serán almacenados de forma automática en el One Drive del organizador.

⁵⁶ <https://www.sic.gov.co/registro-nacional-de-bases-de-datos>



8. CAPACITACIÓN E INDUCCIÓN EN SEGURIDAD DE LA INFORMACIÓN

8.1. CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El DNP realiza charlas periódicas sobre para que los usuarios del DNP conozcan el Sistema de Gestión de Seguridad de la Información (SGSI), sus políticas, la importancia en el DNP, los CONCEPTOS RELACIONADOS del SGSI, identificación de los activos de información, identificación de los tipos de delitos y riesgos cibernéticos en el entorno laboral y personal, conocer los canales de denuncia si son víctima de un delito cibernético, identificación de las responsabilidades de los usuarios del DNP, identificación de la normativa relacionada con el SGSI y conocimiento de la oferta educativa del Gobierno Nacional en temas relacionados con seguridad de la información.

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

9. CLASIFICACION DE LAS POLITICAS DE SEGURIDAD

El Anexo 1 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 27001:2013⁵⁷.

10. DEFINICIONES

10.1. SIGLAS Y ABREVIACIONES

- **CERT** (Computer Emergency Response Team): Equipo de Respuesta a Emergencias cibernéticas. Se refiere a una institución definida y concreta con capacidad centralizada para la coordinación de gestión de incidentes.
- **CSIRT** (Computer Security Incident & Response Team): Equipos de Respuestas ante Incidentes de Seguridad⁵⁸. Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.
- **CCOC**: Comando Conjunto Cibernético del Comando General de las Fuerzas. Militares de Colombia Se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en

⁵⁷ <https://intranet.dnp.gov.co/SGC/manual-de-calidad-y-operaciones/Paginas/SGSI.aspx>

⁵⁸ Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). <https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT>

el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional, contribuyendo a generar un ambiente de paz, seguridad y defensa nacional⁵⁹.

- **CCP:** Centro Cibernético Policial de la Policía Nacional de Colombia. Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones⁶⁰.
- **ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia):** Su finalidad es asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Así mismo, es el punto único de contacto y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciber amenazas, incluyendo la coordinación a nivel nacional e internacional de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.
- **CSIRT de Gobierno:** brinda acompañamiento y apoyo a las entidades del estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital⁶¹.
- **ICC:** Infraestructuras Críticas Cibernética. Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales⁶².
- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones⁶³.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital⁶⁴.
- **TI:** Tecnologías de Información. Es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas⁶⁵.

59 CCOCI. <https://www.ccoci.mil.co/nosotros/ccoci/24>

60 ¿Quiénes somos? <https://cc-csirt.policia.gov.co/quienes-somos>

61 <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/>

62 Infraestructura Crítica Cibernética. Página 2. <https://acis.org.co/archivos/Conferencias/2016/GuialCC.pdf>

63 <https://mintic.gov.co/portal/inicio/>

64 <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

65 https://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_la_informaci%C3%B3n

- **TIC:** Tecnologías de la Información y las Comunicaciones son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes⁶⁶.
- **TO:** Tecnologías de Operación. Está dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas⁶⁷.
- **Servicio esencial:** Es el servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades

10.2. CONCEPTOS DE LOS PILARES DE SEGURIDAD

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados⁶⁸. La información debe estar debidamente protegida para que sea accedida por el usuario autorizado.
- **Disponibilidad:** La información debe estar disponible en cualquier momento. Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Integridad:** Propiedad de exactitud y completitud⁶⁹. La información debe estar adecuadamente protegida para asegurar que no sea alterada.

10.3. CONCEPTOS RELACIONADOS DE EL M-PG-07 MANUAL OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

- **Alcance:** El alcance del SGSI define los límites y ampliación y puede estar determinado en función a los activos de información de la empresa, la ubicación física, la estructura organizacional, procesos o actividades principales, en definitiva, de los elementos críticos a proteger. Esto quiere decir que no importa si está en la nube o en equipos locales o si se accede a través de una red local o mediante acceso remoto la información que necesitamos proteger⁷⁰.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización⁷¹.

66 Art. 6 Ley 1341 de 2009. <http://www.suin-juriscal.gov.co/viewDocument.asp?id=1677762>

67 Diferencias entre IT y OT y su convergencia. <https://oasys-sw.com/diferencias-entre-it-y-ot/>

68 Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020. Función Pública

69 Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020. Función Pública

70 Determinación del alcance del SGSI. <https://www.pmg-ssi.com/2020/08/determinacion-del-alcance-del-sgsi/>

71 Amenaza. <https://www.iso27000.es/glosario.html>

- **Aplicativo:** Programa informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo⁷².
- **Atacantes:** personas naturales o jurídicas que intentan acceder, interceptar o dañar un sistema informático afectando la integridad, confidencialidad y disponibilidad de los datos y los sistemas⁷³
- **Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio⁷⁴.
- **Autenticación:** Proceso que garantiza y confirma la identidad de un usuario⁷⁵.
- **Autenticidad:** Es la seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad⁷⁶.
- **Capacidades:** Son recursos con los que se cuenta o que se requieren para lograr la gestión de las amenazas a las cuales se encuentran expuestas los activos⁷⁷.
- **Ciberdelincuencia (Delito cibernético):** Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio⁷⁸.
- **Ciberdefensa:** Es el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales⁷⁹.
- **Ciberdelincuencia:** Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático⁸⁰.
- **Ciberdelito/Delito cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito⁸¹.

72 Blog Informática. <http://informaticallc.blogspot.com/2011/05/sistema-aplicativo.html>

73 Modelo de Gobernanza para mejorar la seguridad digital

74 Modelo de gestión del riesgo digital https://mintic.gov.co/portal/715/articulos-61854_documento.docx

75 3.5 Autenticación. <https://normaiso27001.es/referencias-normativas-iso-27000/#terminos>

76 3.6 Autenticidad <https://normaiso27001.es/referencias-normativas-iso-27000/#terminos>

77 Modelo de Gobernanza para mejorar la seguridad digital

78 CONPES 3854 de 2016, pág. 87

79 Infraestructura Crítica Cibernética. Página 2. <https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf>

80 Modelo de gestión del riesgo digital https://mintic.gov.co/portal/715/articulos-61854_documento.docx

81 Modelo de gestión del riesgo digital https://mintic.gov.co/portal/715/articulos-61854_documento.docx

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

- **Ciberespacio:** Entorno virtual complejo resultante de la interacción de personas, software, hardware y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.
- **Ciberseguridad:** Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio⁸².
- **Ciberterrorismo:** Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas⁸³.
- **Computo forense:** También llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal⁸⁴.
- **Controles:** Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control⁸⁵.
- **Declaración de aplicabilidad:** Conocida también como SoA (por sus siglas en inglés) establece los riesgos de información y los controles de seguridad que son relevantes y aplicables al SGSI de su organización, como resultado de la determinación de sus evaluaciones periódicas del riesgo o según lo exijan las leyes, reglamentos o buenas prácticas. La función esencial del documento SoA es evidenciar que los controles recomendados en el Anexo A de ISO/IEC 27001 se aplican cuando están dentro del alcance y son apropiados para su organización o, por el contrario, no se justifica el esfuerzo de su aplicación por diferentes decisiones de gestión estratégicas o de coste/efectividad que deben ser formalmente registradas y justificadas para convencer a los auditores de que no los ha descuidado, ignorado o excluido arbitrariamente o de forma inadvertida⁸⁶.
- **Firma digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación⁸⁷.

82 Infraestructura Crítica Cibernética. Página 2. <https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf>

83 CONPES 3854 de 2016, pág. 88

84 Computo forense: https://es.wikipedia.org/wiki/C%C3%B3mputo_forense

85 Controles. <https://www.iso27000.es/glosario.html>

86 Declaración de aplicabilidad (6.1.3). <https://www.iso27000.es/sgsi.html>

87 Literal c. Art. 2. Ley 527 de 199. <http://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013>

- **Mensaje de datos:** La información generada, enviada, recibida, almacenada comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax⁸⁸.
- **Múltiples partes interesadas:** El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades⁸⁹.
- **Operadores de infraestructura crítica:** entidades que prestan servicios esenciales los cuales son considerados como estratégicos del país. Ej.: servicios energéticos, financieros, entre otros⁹⁰.
- **Piratería de Software:** Incluye la copia, la distribución y el uso no autorizado de software protegido por el derecho de autor. Esto puede llevarse a cabo al copiar, descargar, compartir, vender, usar, instalar múltiples copias en equipos personales o laborales sin las licencias correspondientes. Lo que se desconoce es que cuando se compra software se está comprando una licencia para su uso y no el software en sí. Esa licencia es la autorización que le permitirá instalar el software una determinada cantidad de veces, por lo que es importante que se lea. Si instala más copias del software de lo que la licencia le permite, usted está incurriendo en actos de piratería, los cuales constituyen un delito.
- **Política:** Establece y confirma el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del SGSI, entre otros posibles aspectos relevantes⁹¹.
- **Portal:** Espacio de una red informática que ofrece, de forma sencilla e integrada, acceso a recursos y servicios⁹².
- **Relaciones:** son las interacciones entre los componentes tecnológicos⁹³.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas⁹⁴.
- **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

88 Literal a. Art. 2. Ley 527 de 199. <http://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013>

89 CONPES 3854 de 2016, pág. 29


90 Modelo de Gobernanza para mejorar la seguridad digital

91 Política del SGSI (5.2). <https://www.iso27000.es/sgsi.html>

92 Diccionario Real Academia Española. <http://dle.rae.es/?id=TjqJUpv>

93 Modelo de Gobernanza para mejorar la seguridad digital

94 Seguridad de la información. <https://www.iso27000.es/glosario.html>

	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 66 de 81 VERSIÓN: 7

la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano⁹⁵.

- **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 país⁹⁶.
- **Seguridad Informática:** o también llamada ciberseguridad, 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 terceros⁹⁷.
- **Sistema de Información.** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos⁹⁸.
- **Usuarios:** funcionarios, contratistas, pasantes y proveedores del DNP.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas⁹⁹.
- **Vulnerabilidad de seguridad digital:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.

10.4. CONCEPTOS RELACIONADOS CON LOS ACTIVOS DE INFORMACIÓN

- **Activos de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización¹⁰⁰.
- **Información:** Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. Sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal¹⁰¹. Así mismo la información son los datos

95 Decreto 1078 de 2015 <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>

96 CONPES 3854 de 2016, pág. 29

97 ¿Qué es la seguridad informática y cuáles son sus tipos? <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

98 Literal f. Art. 2. Ley 527 de 199. <http://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013>

99 Vulnerabilidad. <https://www.iso27000.es/glosario.html>

100 Activo. <https://www.iso27000.es/glosario.html>

101 Información. <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

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

almacenados o procesados física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros¹⁰².

- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas¹⁰³. En el DNP incluye software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas. El inventario del software es actualizado por la Subdirección Administrativa y Relacionamiento con la Ciudadanía en el Sistema de información Seven.
- **Recurso Humano:** son aquellas personas que, por su conocimiento, experiencia y criticidad para los procesos de Sistema Integrado de Gestión, son consideradas activos de información. En el DNP corresponden a los servidores públicos, contratistas, pasantes y terceros. Servidores públicos de carrera administrativa, provisional, y libre nombramiento y remoción. Contratistas de DNP, Fonade, SGR, BID y otras fuentes de financiación. La Subdirección de Gestión del Talento Humano y el Subdirección de Contratación son los responsables de solicitar la creación, modificación o cancelación de las cuentas electrónicas al Centro de Servicios y la Oficina de Tecnología y Sistemas de Información (OTSI). El inventario del recurso humano del DNP está en el Directorio Activo de la Entidad.
- **Hardware:** son los equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos. El inventario del hardware es actualizado por la Subdirección Administrativa y Relacionamiento con la Ciudadanía en el Sistema de información SEVEN y es monitoreado por la Oficina de Tecnología y Sistemas de Información en la herramienta ITSM.
- **Servicio de TI:** Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los servicios de TI deben tener asociados unos acuerdos de nivel de servicio¹⁰⁴.
- **Servicios de información:** Consiste en la entrega de información de valor para los usuarios de una entidad a través de un proveedor de servicio interno o externo. Un servicio de información se describe a través de un contrato funcional (qué recibe como entrada y qué produce como salida) y un conjunto de acuerdos de servicio que debe cumplir¹⁰⁵.
- **Servicios tecnológicos:** Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.¹⁰⁶.

102 Página 12. Guía para la Gestión y Clasificación de Activos de Información. https://www.mintic.gov.co/gestioniti/615/articles-5482_G5_Gestion_Clasificacion.pdf


103 Definiciones de Oxford Languages

104 Servicio de TI. <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

105 <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

106 <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

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

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 68 de 81 VERSIÓN: 7

10.5. CONCEPTOS RELACIONADOS CON LA CATEGORÍA INFORMACIÓN

- **Registro de activos de información:** Es el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal¹⁰⁷.
- **Índice de información clasificada y reservada:** Es el inventario de la información pública generada, obtenida, adquirida o controlada por el sujeto obligado, en calidad de tal, que ha sido calificada como clasificada o reservada¹⁰⁸.

10.6. CONCEPTOS RELACIONADOS CON LA CATEGORÍA SOFTWARE

- **Software Específico:** El Departamento Nacional de Planeación ha adquirido una serie de herramientas de uso específico que permiten a los funcionarios, contratistas y pasantes cuando así lo requieran, contar con los elementos informáticos adicionales necesarios para el desarrollo de sus funciones
- **Software Free Permitido:** Para el desarrollo de algunas funciones, es indispensable contar con herramientas informáticas que no están incluidas dentro de la línea base de las estaciones cliente, no obstante existen dentro del mercado una serie alternativas de software de uso específico con licencia abierta para su instalación, uso y distribución; pero que cubren el requerimiento del usuario de manera satisfactoria, estas herramientas son evaluadas por el equipo encargado de la seguridad de la información de la Oficina de Tecnología y Sistemas de Información y autorizadas o no según sea el caso.

10.7. CONCEPTOS RELACIONADOS CON LA CATEGORÍA SERVICIOS DE TI

- **Catálogo de infraestructura crítica cibernética:** contiene el inventario de la infraestructura estratégica cibernética, la infraestructura cibernética (IC) son las infraestructuras soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO). el instrumento no será publicado sino será de consulta interna¹⁰⁹.
- **Infraestructura Crítica Cibernética (ICC):** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su suspensión, afectación o destrucción tendría un grave impacto sobre los servicios esenciales del Estado¹¹⁰.

107 Artículo 37. Decreto 103 de 2015. <http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726>

108 Art 39. Decreto 103 de 2015. <http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726>

109 Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. Comando Conjunto Cibernético (CCOC).2015

110 Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. Comando Conjunto Cibernético (CCOC).2015

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

- **Infraestructura Cibernética (IC):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO)¹¹¹.
- **Infraestructura Crítica (IC):** Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales¹¹².
- **Infraestructura estratégica:** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales.
- **Catálogo de sistemas de información:** Es un inventario detallado y documentado que contiene las fichas técnicas de los sistemas de información de una institución. Este es uno de los artefactos que se utiliza para describir la arquitectura de sistemas de información¹¹³.
- **Catálogo de servicios de TI:** Es un inventario detallado y documentado de los servicios de TI que la institución tiene implementados y que se encuentran activos, incluyendo los que están disponibles para ser desplegados. El catálogo de servicios de TI es el subconjunto del portafolio de servicios publicado para los usuarios¹¹⁴.

10.8. CONCEPTOS RELACIONADOS CON LA LEY DE TRANSPARENCIA

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal¹¹⁵.
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014¹¹⁶.
- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014¹¹⁷.

111 Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. Comando Conjunto Cibernético (CCOC).2015

112 Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. Comando Conjunto Cibernético (CCOC).2015

113 Catálogo de sistemas de información. <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

114 Catálogo de servicios de TI <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html>

115 Literal b. Art 6 Ley 1712 de 2014. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

116 Literal c. Art 6 Ley 1712 de 2014. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

117 Literal d. Art 6 Ley 1712 de 2014. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

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

10.9. CONCEPTOS RELACIONADOS CON EL USO DE LA INFORMACIÓN.

- **Público:** Cualquier información no clasificada se considera como privada. La información pública, será aquella cuya divulgación no afecte a la Entidad en términos de pérdida de imagen y/o económica.
- **Uso interno:** Información que, sin ser privada ni confidencial, debe mantenerse dentro de la Entidad y no debe estar disponible externamente, excepto para terceros involucrados en el tema. En el caso de terceros, deberán comprometerse a no divulgar dicha información firmando un acuerdo de confidencialidad.
- **Uso privado o restringido:** Información sensible, interna a áreas o proyectos a los que deben tener acceso controlado otros grupos, pero no toda la Entidad debido a que se puede poner en riesgo la seguridad e intereses de la Entidad, de sus clientes o asociados y empleados.
- **Confidencial o de reserva:** Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.

10.10. CONCEPTOS RELACIONADOS CON DATOS PERSONALES

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales¹¹⁸.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento¹¹⁹.
- **Cesión o transferencia nacional de la base de datos.** la información relacionada con la cesión o transferencia nacional de datos incluye la identificación del cesionario, quien se considerará responsable del tratamiento de la base de datos cedida a partir del momento en que se perfeccione la cesión. no es obligatorio para el cedente registrar la cesión de la base de datos. sin embargo, el cesionario, como responsable del tratamiento, debe cumplir con el registro de la base de datos que le ha sido cedida¹²⁰.
- **Dato:** Es una representación simbólica de una característica particular de un elemento o situación, que pertenece a un modelo de una realidad. Tiene un tipo (por ejemplo, numérico, cadena de caracteres o lógico) que determina el conjunto de valores que el dato puede tomar. En el contexto informático, los datos se almacenan, procesan y comunican usando medios electrónicos. Constituyen los elementos primarios de los sistemas de información¹²¹.

118 Literal a. Art 3. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

119 Literal b. Art 3. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

120 https://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf

121 Glosario Arquitectura TI MINTIC

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

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables¹²².
- **Dato personal privado:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular¹²³.
- **Dato personal semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países¹²⁴.
- **Dato personal sensible:** Aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos¹²⁵.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos personales de menores:** Se proscribe el tratamiento de datos personales de menores de edad salvo aquellos datos que sean de naturaleza pública. La Corte Constitucional precisó que tal prohibición debe interpretarse en el sentido de que los datos personales de los menores de 18 años pueden ser tratados, siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior¹²⁶.
- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

122 Literal c. Art 3. <http://www.suin-juriscal.gov.co/viewDocument.asp?ruta=Leyes/1684507>


123 Artículo 3 Ley 1266 de 2008

124 Artículo 3 Ley 1266 de 2008

125 Artículo 5 Ley 1581 de 2012

126 <https://www.intranetpasto.gov.co/index.php/descargas/category/203-capacitacion-ley-de-proteccion-de-datos-personales?download=4726:presentacion-ley-1581-entidades-publicas-2017>

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

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 72 de 81 VERSIÓN: 7

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento¹²⁷

- **Incidentes de seguridad.** Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, que deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

- **Información Privada Información personal de ámbito privado:** Ejemplo: Libros de comercio, documentos privados, historias clínicas, información tomada de la inspección del domicilio. Circulación: Por orden de autoridad judicial en cumplimiento de sus funciones – En materia penal Ley 906 de 2004¹²⁸.

- **Información Privada:** Información personal de ámbito privado. Ejemplo: Libros de comercio, documentos privados, historias clínicas, información tomada de la inspección del domicilio. Circulación: Por orden de autoridad judicial en cumplimiento de sus funciones – En materia penal Ley 906 de 2004¹²⁹.

- **Información Pública o de dominio público:** Se obtiene y se ofrece sin reserva alguna. Ejemplo: Información del Estado Civil de las personas. Circulación: Libre circulación¹³⁰

- **Información Reservada o secreta:** Relacionada con la intimidad, dignidad y libertad. Ejemplo: Datos sensibles, ideología, orientación sexual, hábitos de la persona, pertenencia a organizaciones sociales o políticas. Circulación: No puede recolectarse, No puede circular¹³¹.

- **Información Semi-privada:** Información personal o impersonal que tiene un grado mínimo de limitación. Ejemplo: Relación de usuarios con las entidades de Seguridad Social – datos del comportamiento financiero. Circulación: A solicitud de autoridad administrativa – Potestativo. Por orden de autoridad judicial - En materia penal Ley 906 de 2004¹³².

- **Información Semi-privada:** Información personal o impersonal que tiene un grado mínimo de limitación. Ejemplo: Relación de usuarios con las entidades de Seguridad Social – datos del comportamiento financiero. Circulación: A solicitud de autoridad administrativa – Potestativo. Por orden de autoridad judicial - En materia penal Ley 906 de 2004¹³³.

127 Literal d. Art 3. <http://www.suin-juricol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

128 <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

129 Sentencia T-729/02


130 Sentencia T-729/02

131 <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

132 Sentencia T-729/02

133 <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

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

 <p>El futuro es de todos</p> <p>DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	<p>CÓDIGO: M-PG-07</p> <hr/> <p>Página 73 de 81 VERSIÓN: 7</p>
---	--	--

- **Medidas de seguridad de la información.** Corresponde a los controles implementados por el responsable del Tratamiento para garantizar la seguridad de las bases de datos que está registrando, teniendo en cuenta las preguntas dispuestas para el efecto en el RNBD. Tales preguntas no constituyen de ninguna manera instrucciones acerca de las medidas de seguridad que deben implementar los responsables del tratamiento de datos personales¹³⁴.

- **Registro Nacional de Bases de Datos (RNBD):** Es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos¹³⁵.

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos¹³⁶.

- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento¹³⁷.

- **Transferencia de datos:** tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país¹³⁸. la información relacionada con la transferencia internacional de datos personales comprende la identificación del destinatario como responsable del tratamiento, el país en el que este se encuentra ubicado y si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio o por una causal de excepción en los términos señalados en el artículo 26 de la Ley 1581 de 2012.¹³⁹

- **Transmisión de datos personales:** implica la comunicación de estos dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el encargado por cuenta del responsable¹⁴⁰. La información relacionada con la Transmisión internacional de datos comprende la identificación del destinatario como Encargado del Tratamiento, el país en el que este se encuentra ubicado, si se tiene un contrato de transmisión de datos en los términos señalados en el artículo 2.2.2.25.5.2 de la Sección 5 del Capítulo 25 del Decreto Único 1074 de 2015 o si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio¹⁴¹.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión¹⁴².

134 https://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf

135 Registro Nacional de Bases de Datos. <https://www.sic.gov.co/registro-nacional-de-bases-de-datos>

136 Literal e. Art 3. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

137 Literal f. Art 3. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

138 <https://www.sic.gov.co/preguntas-frecuentes-pdp>

139 https://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf

140 <https://www.sic.gov.co/preguntas-frecuentes-pdp>

141 https://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf

142 Literal g. Art 3. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>

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


10.11. CONCEPTOS RELACIONADOS CON LOS INCIDENTES DE SEGURIDAD

- **Evento:** Según Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad¹⁴³.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información¹⁴⁴.
- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos¹⁴⁵.
- **Incidente de seguridad digital:** cualquier evento adverso intencionado o no intencionado, que puede cambiar o afectar el curso esperado de una actividad en el entorno digital.
- **Incidente:** Cualquier evento que no es parte de la operación normal de un servicio, que puede causar una interrupción o una disminución en la calidad del mismo servicio.
- **Incidente múltiple:** Ocurrencia de varios incidentes que de forma organizada puedan vulnerar un sistema o dispositivo.
- **Incidentes con impacto bajo:** Incidentes que afectan activos de información que son considerados de criticidad menor o que su falla o interrupción afecta a un máximo de 10 usuarios, algunos ejemplos son: estaciones de trabajo, impresoras, puntos de red.
- **Incidentes con impacto medio:** Incidentes que afectan activos de información que son considerados de criticidad media o que su falla o interrupción afecta un rango de usuarios entre 10 y 100 usuarios, algunos ejemplos son: switches de piso, intranet, navegación de Internet, aplicaciones batch, registro de ingreso de computadores, sistemas administrativos.
- **Incidentes con impacto alto:** Incidentes que afectan activos de información que son considerados de criticidad alta o que su falla o interrupción afecta un rango de usuarios mayor a 100 usuarios, algunos ejemplos son: Bases de datos misionales, correo electrónico, Switch de core, comunicaciones externas,

143 [ISO/IEC TR 18044:2004]

144 Incidente de seguridad de la información. <https://www.iso27000.es/glosario.html>

145 CONPES 3854, pág. 87

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07
		Página 75 de 81 VERSIÓN: 7

alteración en documentos, alteración en bienes y recursos del Estado, Directorio activo, Firewall, servicios financieros, portales WEB.

- **Incidentes con urgencia alta (Grave):** El incidente debe atenderse de forma inmediata y menor a 2 horas.
- **Incidentes con urgencia media (Muy grave):** El incidente debe atenderse de en un tiempo menor a 6 horas.
- **Incidentes con urgencia baja (Menos grave y Menor):** El incidente debe atenderse en un tiempo menor a 48 horas.

10.12. CONCEPTOS RELACIONADOS CON LOS RIESGOS DE SEGURIDAD DIGITAL

- **Efectos:** Materialización de un incidente no deseado, daño a un sistema o la organización.
- **Gestión de riesgos de seguridad digital:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego¹⁴⁶.
- **Impacto:** El coste de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros (pérdida de reputación, implicaciones legales, etc.)¹⁴⁷.

10.13. CONCEPTOS RELACIONADOS CON AMENAZAS, VULNERABILIDADES Y GRUPOS CAUSALES

- **Capacidades:** Son recursos con los que se cuenta o que se requieren para lograr la gestión de las amenazas a las cuales se encuentran expuestas los activos.
- **Relaciones:** son las interacciones entre los componentes.
- **Operadores de infraestructura crítica:** entidades que prestan servicios esenciales los cuales son considerados como estratégicos del país. Ejemplo: servicios energéticos, financieros, entre otros.

¹⁴⁶ CONPES 3854, pág. 24.

¹⁴⁷ Impacto. <https://www.iso27000.es/glosario.html>

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

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad¹⁴⁸.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto¹⁴⁹.
- **Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo¹⁵⁰.
- **Denegación de servicio:** Es un ataque a la red que causa que un servicio o recurso sea inaccesible a los usuarios.
- **Código malicioso:** Programas no deseados que se infiltran o dañan la Plataforma Tecnológica sin el conocimiento de su dueño.
- **Acceso no autorizado:** Personal que tiene acceso a información y programas para las cuales no está autorizado.
- **Uso inapropiado:** Utilización de servicios o dispositivos de computación para fines diferentes a los laborales afectando la productividad. Alteración de documentos e información.

10.14. CONCEPTOS RELACIONADOS CON LOS EFECTOS DE LA MATERIALIZACIÓN DE LOS RIESGOS

- **Alteración de la aplicación:** Modificación de una aplicación.
- **Alteración de la información:** Modificación de la información.
- **Detrimiento del patrimonio de la Entidad:** Pérdida o deterioro del conjunto de bienes, derechos y obligaciones, pertenecientes a una empresa -como persona jurídica- que impiden cumplir sus objetivos.
- **Divulgación de información confidencial:** Difundir información privada sin previo consentimiento.


¹⁴⁸ Riesgo. <https://www.iso27000.es/glosario.html>

¹⁴⁹ NTC ISO 31000:2011

¹⁵⁰ NTC ISO 31000:2011



- **Fraude y malversación de fondos:** El núcleo del tipo penal de estafa consiste en el engaño. Se denomina fraude de ley o fraude a la ley al método de incumplimiento indirecto del Derecho (objetivo) en el sentido de que supone la obtención de un resultado contrario al conjunto del orden jurídico determinado alcanzado a través de la puntual observancia de lo dispuesto en la norma jurídica.
- **Incumplimiento de tipo legal o contractual:** No cumplimiento de deberes previamente concertados legalmente.
- **Indisponibilidad colateral de otros servicios:** No disponibilidad de servicios secundarios adscritos a un servicio principal.
- **Interrupción del servicio o del negocio:** No disponibilidad de un servicio o sistema en un momento determinado sin previo aviso.
- **Peculado:** Es un delito consistente en la apropiación indebida del dinero perteneciente al erario por parte de las personas que se encargan de su control y custodia.
- **Pérdida de competitividad o volumen del negocio:** Disminución de la capacidad por parte una persona o entidad para producir bienes y/o servicios en forma eficiente (con costes declinantes y calidad creciente), haciendo que sus productos no sean atractivos. Incapacidad para lograr niveles elevados de productividad que permitan aumentar la rentabilidad y generar ingresos crecientes.
- **Pérdida de confidencialidad de los datos del cliente:** Acceso no autorizado a la información exclusiva de un Cliente.
- **Pérdida de imagen / credibilidad:** Incapacidad de generar confianza y grado de conocimiento por parte de una persona o entidad.
- **Pérdida de productividad de los empleados:** Disminución de la capacidad por parte una persona o entidad para producir bienes y/o servicios en forma eficiente, haciendo que sus productos no sean atractivos. Incapacidad para lograr niveles elevados de productividad que permitan aumentar la rentabilidad y generar ingresos crecientes.
- **Pérdida económica:** Perdida de dinero.
- **Perjudicar las relaciones de la entidad con otros organismos:** Detrimiento de las relaciones de la entidad con otros organismos.


 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07 Página 78 de 81 VERSIÓN: 7
--	--	--

10.15. CONCEPTOS RELACIONADOS CON LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

- **Controles:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. El control es también utilizado como sinónimo de salvaguarda.
- **Antivirus:** Software que previene el contagio de virus informático en los servidores y estaciones de trabajo que dañen o modifiquen la información.
- **Campañas de sensibilización:** Concientizar a los usuarios sobre algo mediante la implementación de mensajes por diferentes métodos.
- **Control de acceso:** Permitir que solo personal autorizado acceda a la información.
- **Control de versiones:** Una versión, revisión o edición de un producto, es el estado en el que se encuentra dicho producto en un momento dado de su desarrollo o modificación. Se llama control de versiones a la gestión de los diversos cambios que se realizan sobre los elementos de algún producto o una configuración de este.
- **Controles contra códigos maliciosos:** se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
- **Copias de respaldo:** Una copia de seguridad o backup en informática es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.
- **Detección de intrusos:** Identificación de un acceso desautorizado a un sistema, a una red o a un usuario, la identificación se puede hacer usando patrones o comparando contra comportamiento normales del sistema, la red o de los usuarios, adicionalmente protege a los sistemas computacionales de ataques y abusos.
- **Documentación:** Conjunto de escritos mediante los cuales se prueba o acredita algo.
- **Ejecución Pruebas:** Realización de guiones de pruebas para verificar el cumplimiento de las funciones de un sistema.



- **Existencias de políticas:** Implementación de procedimientos orientados ideológicamente hacia la toma de decisiones para la consecución de los objetivos propuestos.
- **Gestión de cambios:** se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- **Gestión de capacidad:** para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
- **Uso de contraseñas encriptados:** Frases cifradas utilizadas en los sistemas de información/aplicativos para ser accedidos, previa decodificación y validación de estos.
- **Logs de Auditorias:** Procedimiento por el cual se deja rastro de quien, como, cuando, donde fue modificada la información.
- **Mantenimiento a sistemas de información/aplicativos:** Proceso mediante el cual se asegura el funcionamiento de los sistemas de información/aplicativos a través del tiempo.
- **Metodología para ciclo de vida de los aplicativos:** Fases por las cuales pasan los aplicativos, desde su concepción hasta su obsolescencia.
- **Módulos de seguridad:** Sistema para asegurar el acceso a la información.
- **Monitoreo de servicios:** Seguimiento y control a un servicio prestado para garantizar su debido funcionamiento.
- **Planes de contingencia:** orientado a permitir la continuación de las principales funciones tecnológicas en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de continuidad del negocio (Business Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Procedimientos de operación documentados:** los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.

 <p>El futuro es de todos DNP Departamento Nacional de Planeación</p>	MANUAL OPERATIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (GSI)	CÓDIGO: M-PG-07 Página 80 de 81 VERSIÓN: 7
--	--	--

- **Protección contra códigos maliciosos:** asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- **Protocolos de seguridad:** Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información.
- **Redes privadas virtuales (VPN):** una tecnología de red que permite extender la red local sobre una red pública relativamente hablando
- **Restricción de acceso al centro de cómputo:** Solo personal autorizado puede acceder al Centro de Cómputo.
- **Respaldo de información:** se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
- **Separación de los ambientes de desarrollo, pruebas y operación:** se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
- **Tecnologías de encriptación:** Sistemas para enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la criptología.
- **Tokens:** Un token de seguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Fecha aprobación: 28 de febrero de 2022

Elaboró:

ORIGINAL FIRMADO

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



Revisó:

ORIGINAL FIRMADO

JUAN CARLOS ALARCON SUESCUN
Contratista Oficina Asesora de Planeación

ORIGINAL FIRMADO

CLAUDIA ANGELICA BEN-AMY
Funcionaria Asesor Grado 8 -OTSI

ORIGINAL FIRMADO

YANETH LILIAN ENRIQUEZ SOTO
Coordinador (E) Oficina Asesora de Planeación – Administrador SIG

ORIGINAL FIRMADO

Aprobó:

ROBERTO DIAZGRANADOS DIAZ
Jefe Oficina de Tecnología y Sistemas de Información (OTSI)