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

DEPARTAMENTO NACIONAL DE PLANEACIÓN

BOGOTÁ, 2020

TABLA DE CONTENIDO

1. OBJETIVO

Definir el componente operacional para gestionar la seguridad de la información con base en los lineamientos del Sistema Integrado de Gestión (SIG) bajo un enfoque tecnológico para resguardar la información digital de software, hardware, servicios tecnológicos, servicios de información (aplicativos, portales, sistemas de información) en su confidencialidad, integridad y disponibilidad, de acuerdo con las disposiciones normativas establecidas por las entidades rectoras en la materia.

2. ALCANCE

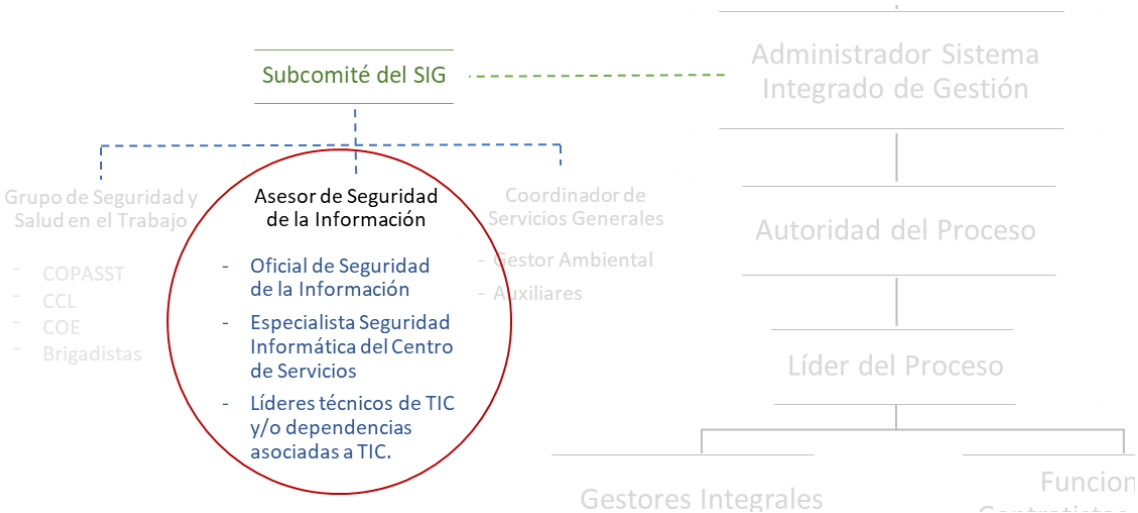
El presente manual operativo aplica para los funcionarios, contratistas, pasantes y terceros del Departamento Nacional de Planeación los cuales se encuentran ubicados en Bogotá y en sus sedes regionales (Regalías), así como para los procesos, productos, infraestructura física y tecnológica de la entidad.

El cumplimiento de lo estipulado en este 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.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

3. OBLIGACIONES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

La estructura operacional para el componente de gestión ambiental se encuentra referenciada en el **Manual del Sistema Integrado de Gestión (MC).**



Fuente: Manual SIG.

3.1. ASESOR SEGURIDAD DE LA INFORMACIÓN DE LA OFICINA DE TECNOLOGÍAS Y SISTEMAS DE 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 Tecnologías 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.
- Identificar e informar los riesgos, amenazas o vulnerabilidades en los activos informáticos.
- Elaborar y/o actualizar las políticas de seguridad de la Información y protección de datos.
- Hacer seguimiento y recomendaciones para mejoramiento del sistema.

3.2. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

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

- Planear y diseñar soluciones de seguridad informática de acuerdo con los requerimientos y necesidades que se presenten en los diferentes proyectos, verificar el cumplimiento de la norma y de los estándares internacionales.
- 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.
- Apoyar a la OTSI en la definición de procesos, procedimientos, lineamientos asociados al componente de Gestión de Seguridad de la Información (GSI).
- Apoyar a la OTSI en la actualización del Manual Operativo de seguridad de la información, 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.
- Apoyar a la OTSI en 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.
- Apoyar la 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.
- Apoyar 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.

3.3. 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 publica).

- Efectuar en sitio la atención y solución de solicitudes de servicios, previamente registradas en la herramienta de gestión de servicios de TIC (ITSM).
- Escalar a un nivel superior, a través de la herramienta de gestión de servicios de TIC (ITSM), con los proveedores relacionados.
- 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.

3.4. LÍDERES TÉCNICOS DE TIC

El rol de líder de los servicios de Información (Sistemas de Información, aplicativos y portales), líder de servicios tecnológicos y el personal de sitio e infraestructura del Centro de servicios tienen las siguientes responsabilidades:

- Apoyar la recolección de evidencia de los incidentes informáticos relacionados con la infraestructura tecnológica.
- Identificación de riesgos de los activos de información de su competencia, de acuerdo con el proceso de Gestión Integral de Riesgos y el Lineamiento Integral para la Gestión de Riesgos

4. ESTRUCTURA DEL COMPONENTE DE GSI

La estructura del componente de Gestión de Seguridad de la Información (GSI) que hace parte del SIG está definida en los Lineamientos para la elaboración y control de documentos del Sistema Integrado de Gestión del DNP.

4.1. 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.

4.1.1. Confidencialidad

La información debe estar debidamente protegida para que sea accedida por el usuario autorizado.

Tabla 1. Requerimientos de Confidencialidad

Calificación	Explicación
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.

Calificación	Explicación
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.

Se considerarán también las clasificaciones de la información según la Ley de Transparencia, las disposiciones generales para la protección de datos personales y Habeas Data.

4.1.1.1. Clasificación de la información según la Ley de Transparencia.

La información[1] del DNP 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

Calificación	Explicación
Información pública	Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal
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 2014
Información pública reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la 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 2014.

4.1.1.2. Clasificación de la información según Datos personales

La información del DNP con datos personales[2] se encuentra almacenada en los sistemas de información y aplicativos, por lo tanto, es importante determinar la clasificación de la misma teniendo en cuenta los artículos

[1] Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen

[2] Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

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.

Calificación	Explicación
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 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
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 superior.

4.1.1.3. **Clasificación de la información según Habeas Data**[3]

La Corte Constitucional determinó los siguientes tipos de información:

Calificación	Explicación
Pública o de dominio público	Se obtiene y se ofrece sin reserva alguna. Ejemplo: Información del Estado Civil de las personas. Circulación: Libre circulación
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 2004
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 2004

[3] http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Calificación	Explicación
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 circular

4.1.1.4. **Relación de las clasificaciones de información**.

La tabla que a continuación se describe, presenta 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	Requerimientos de Confidencialidad • Público Clasificación Datos personales • Dato público • Datos personales laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); • Datos personales académicos (trayectoria educativa, título, número de cédula, certificados, etc.) Clasificación según Habeas Data • Pública o de dominio público
Información pública clasificada: Información exceptuada por daño de derechos a personas naturales o jurídicas	Clasificación según Ley de Transparencia • 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 Requerimientos de Confidencialidad • Uso interno • Uso privado Clasificación según Habeas Data • Semi-privada • Privada • Reservada o secreta Clasificación Datos personales (Datos sensibles) • 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.

Clasificación Ley de Transparencia	Relación otras clasificaciones
	• 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
Información pública reservada: Información exceptuada por daño a los intereses público	Requerimientos de Confidencialidad • Confidencial Clasificación según Ley de Transparencia • 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

4.1.2. Disponibilidad

La información debe estar disponible en cualquier momento.

Tabla 2. Requerimientos de Disponibilidad

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.

4.1.3. Integridad

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

Tabla 3. Requerimientos de Integridad

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.

Calificación	Explicación
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.

4.1.4. Autenticidad

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

4.1.5. Auditabilidad

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

4.1.6. No repudio

Los activos de información 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.

4.2. PREMISAS PARA LA GESTIÓN DE INCIDENTES

- 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 de seguridad de la Información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados que tienen la probabilidad de comprometer las operaciones misionales y amenazar la Integridad, disponibilidad y confidencialidad de la información.
- Virus: es un software que tiene como objetivo infiltrarse en una estación cliente o servidor sin el conocimiento de su dueño y con fin de alterar o dañar el sistema operativo.
- Malware: Utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos.

4.2.1. Clasificación de los incidentes de seguridad.

Los incidentes de seguridad se pueden clasificar en las siguientes categorías:

- 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.
- Incidente múltiple: Ocurrencia de varios incidentes que de forma organizada puedan vulnerar un sistema o dispositivo.

4.2.2. Valoración de los incidentes de seguridad.

Los incidentes de seguridad deben ser valorados según la severidad con que afecten a la organización:

- Leves: 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.
- Moderados: 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.
- Graves: 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, alteración en documentos, alteración en bines y recursos del Estado, Directorio activo, Firewall, servicios financieros, portales WEB.

4.3. PROPIEDAD DE LA INFORMACIÓN

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

5. POLÍTICAS

Son 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.

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 del DNP.

Por lo anterior, se establecen las siguientes políticas generales en seguridad de la información, basados en la norma ISO 27001, las cuales ayudarán a ofrecer servicios seguros, confiables y oportunos en la entidad, como lo dictan las directrices de Gobierno 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 capitulo y el estándar así: [PL02-ES1] corresponde a la política 1 del capítulo 2.

5.1 POLÍTICA DE SEGURIDAD

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

5.2 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 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.

[PL02-ES2]

La OTSI promoverá la sensibilización y divulgación del Manual Operativo de Seguridad de la Información, para lo cual se apoyará en los directores, subdirectores, jefes de oficina, el grupo de planeación y los gestores SIG.

[PL02-ES3]

Todos los usuarios[4] del DNP, deberán conocer y cumplir el Manual Operativo de Seguridad de la Información, el código de integridad y dar uso apropiado a los recursos entregados conforme a lo establecido en el Código Único Disciplinario.

El manual operativo 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.

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@dnp.gov.co.

[PL02-ES5]

La Oficina de Tecnologías 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.

[4] Funcionarios, contratistas, pasantes, proveedores y terceras partes del DNP.

5.3 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 y Desarrollo del Talento Humano y/o al Grupo 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, Grupo de Contratacion, Oficina de Control Interno, Oficina Jurídica, Subdirección Administrativa, Grupo de Planeación y Oficina de Tecnología de 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 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 alistamiento[5], reasignación del equipo a un nuevo usuario.

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 para el control de inventarios en las condiciones y estado en que le fueron entregados.

[PL03-ES5]

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

Cuando se requiera retirar de las instalaciones de la entidad activos informáticos, se deberá solicitar autorización a la SA, 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.

[5] 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.

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.

[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.

[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.

5.4 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 SE-L03 Lineamiento para la identificación y valoración de activos del SGSI.

[PL04-ES1]

La OTSI mantendrá los listados de software incluyendo el Software Específico, Software Free Permitido y No Permitido, los cuales pueden ser consultados en la intranet, en la ruta http://larebeca/gestiondeTIC/Servicios%20TIC/Paginas/Computador-Institucional.aspx

En caso de requerir la instalación del software se debe realizar la solicitud a través del Centro de Servicios de acuerdo con el Proceso Servicios de TIC (Tecnología de la Información y las Comunicaciones) publicado en el Sistema Integrado de Gestión, 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.

Los usuarios a los cuales les sean autorizados permisos de administrador mediante el formato *Compromiso perfiles especiales* (F-OI-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 Manual.

[PL04-ES4]

Todos los requerimientos de aplicativos, equipos informáticos, software deben ser solicitados a través del Centro de Servicios, a la OTSI de acuerdo con el Proceso Servicios de TIC -Tecnologías de la Información y las Comunicaciones- (TI-TI).

[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 atente contra la moral, las buenas costumbres, afecte la imagen y el buen nombre del DNP.

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

[PL04-ES9]

Se encuentra prohibido el uso, e instalación de juegos, almacenar archivos con contenido pornográfico, software ilegal, software malicioso, música, videos, información de carácter personal o no institucional en los equipos del DNP, 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-OI-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 empresarial o SharePoint

empresarial) 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 por la SA.

[PL04-ES19]

Todos los bienes que son adquiridos, transferidos y/o donados al DNP son ingresados a una póliza de seguro por parte de la Subdirección Administrativa.

[PL04-ES20]

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

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

Si 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.

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 para ser entregadas al Asesor de la OTSI para su custodia.

[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 Grupo de Comunicaciones y Relaciones Públicas 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 Grupo de Comunicaciones y Relaciones Públicas (GCRP), la Subdirección de Gestión y Desarrollo del Talento Humano (SGDTH) 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 25 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, Flicker y similares. Con excepción del Grupo de comunicaciones y Relaciones Publicas que tiene asignado un correo institucional para el manejo de redes sociales.

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

El administrador de las redes sociales institucionales debe cerciorarse de que el mensaje se publique desde la cuenta institucional y no desde una cuenta personal, cuando haga uso de dispositivos móviles, como celulares. 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@dnp.gov.co así mismo por favor bórrelo y por ningún motivo haga público su contenido, de hacerlo podrá tener repercusiones legales.

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

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

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

[PL04-ES28]

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

[PL04-ES29]

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-OTSI-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 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 Sectorial, Subdirección General Territorial, y Secretaria General.

[PL04-ES39]

Es responsabilidad de la Oficina de Tecnologías 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 Tecnologías 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 Reservada (Sensible, Confidencial) y/o clasificada a un tercero[6], 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 al criterio de cada dependencia y a las premisas de básicas de seguridad de confidencialidad adoptado por el DNP en este documento.

[PL04-ES44]

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

5.5 CONTROL DE ACCESO

Establece los lineamientos generales para garantizar el acceso seguro a los activos de información del DNP por parte de usuarios autorizados.

[PL05-ES1]

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

[PL05-ES2]

Los usuarios[7] 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.

[6] Entidades externas al DNP.

[7] Funcionarios, contratistas, pasantes y proveedores del DNP.

[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 siete (7) 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.

[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-OI-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 el https://govreccont.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]

No ingerir alimentos ni bebidas en el puesto de trabajo.

[PL05-ES14]

Los activos de Información tecnológicos (estaciones cliente, portátiles, televisores e impresoras) deben ser apagados al finalizar la jornada.

[PL05-ES15]

Los trabajos de impresión que contengan información confidencial deben ser recogidos de forma inmediata por quien los origina.

[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]

El uso de los equipos institucionales debe ser con propósitos laborales.

[PL05-ES20]

Mantener la configuración establecida por la OTSI (Ej.: mecanismos de protección antivirus y la activación de un firewall en el equipo portátil).

[PL05-ES21]

El extravió o hurto de los equipos del DNP deben ser reportados de forma inmediata a la SA.

[PL05-ES22]

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

[PL05-ES23]

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

5.6 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 información[8] 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 SGDTH será el responsable informar a la OTSI quienes son los usuarios autorizados para firmar, para que esta oficina realice la instalación de estos.

La SA 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 restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

[8] 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 desarrolladores de aplicativos informáticos (internos o externos) deben cifrar la información reservada o restringida 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.

5.7 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 SA 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.

[PL07-ES4]

La SA 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 SA 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.

[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 SA 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 SA.

[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 SA 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]

Los equipos que requieran salir de las instalaciones del DNP para reparación o mantenimiento deben estar debidamente autorizados de acuerdo con los procedimientos de la SA, y garantizando que en dichos elementos no se encuentre información de carácter clasificada, reservada, “restringida” o “crítica”.

[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 sobre-escrituras 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 SA, con el fin de realizar la verificación contra los registros de inventarios.

[PL07-ES35]

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

5.8 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.

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 bajado 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 2 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, dispositivos móviles y tablets)

[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 operación[9] de la OTSI deben ser actualizados en los respectivos documentos.

[PL08-ES11]

Cualquier cambio a la plataforma tecnológica del departamento deberá ser documentado y controlado a través del *formato solicitud de cambios* (F-OI-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.

9 Operación: incluye la administración de la plataforma tecnológica y las actividades que realiza a OTSI en el cumplimiento de sus funciones descritas en el artículo 10 del decreto 2189 de 2017.

[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.

[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 ActiveX[10] 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.

[10] Es una tecnología de Microsoft para el desarrollo de páginas dinámicas.

[PL08-ES24]

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

[PL08-ES25]

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

[PL08-ES26]

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

[PL08-ES27]

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 seguro[11] 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.

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

[PL08-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: Firewall[12], Filtro de contenido[13], Antivirus y Antispam.

[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.

[12] Aplicación utilizada para controlar las comunicaciones, permitiéndolas o prohibiéndolas. Tomado de: http://es.wikipedia.org/wiki/

[13] 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/

[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 DNP[14]. Es responsabilidad del usuario reportar al centrodeservicios@dnp.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

[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 registrase en el log.

[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. Sí 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.

[14] Publicidad, sorteos, loterías, suscripciones, etc.

[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 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 SGDTH 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.

5.9 GESTIÓN DE COMUNICACIONES

Enfocadas a generar las políticas de 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-OI-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

[PL09-ES5]

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

5.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Promueve la inclusión de los controles de seguridad en los servicios de información[15], así como su plataforma tecnológica[16].

[PL10-ES1]

La 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.

[PL10-ES2]

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-ES3]

Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

[15] Aplicativos, sistemas de información, portales y subportales web

[16] Infraestructura, software base, comunicaciones, etc.

[PL10-ES4]

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

[PL10-ES5]

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 Tecnologías y Sistemas de Información para su correcto funcionamiento.

[PL10-ES6]

Se presentarán para dar de baja el software que se encuentre ajustado de acuerdo con los lineamientos dados por el Comité Institucional de Gestión y Desempeño, así como el software total mente depreciado o su reconocimiento en cuanto al valor de uso del mismo.

[PL10-ES7]

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

[PL10-ES8]

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

[PL10-ES9]

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-ES10]

La adquisición, adaptación, construcción y/o mantenimiento de un sistema de información, es un proyecto informático y como tal deberá surtir las etapas de planeación, desarrollo, seguimiento y evaluación. Para lo anterior es necesario efectuar la solicitud de concepto técnico a la Oficina de Tecnologías y Sistemas de Información, de acuerdo con los procesos del Sistema Integrado de Gestión y deberá guardar coherencia con lo establecido en Manual de Contratación del Departamento Nacional de Planeación, específicamente en lo que reza el siguiente párrafo: “En los casos de licitación pública, selección abreviada o concurso de méritos, el proyecto de pliego de condiciones es elaborado en el Grupo 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 Grupo de Comunicaciones y Relaciones Públicas del DNP, así como lo relacionado con tecnologías de la información, que deberán contar con el aval de la Oficina de Tecnologías y Sistemas de Información.”

Los planes que se elaboren para proyectos de sistemas de información deberán asegurar el contar con los recursos necesarios para la ejecución de las tareas programadas y la entrega de los productos acordados. En

caso de redireccionar recursos ya planeados hacía otros proyectos, esta decisión deberá ser avalada y aprobada por la Alta Dirección y la Dependencia solicitante del sistema de información.

Adicionalmente, las Dependencias deben contemplar los recursos necesarios para dar sostenibilidad a la operación 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.

[PL10-ES12]

Los aplicativos adquiridos y/o adaptados o construidos 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]

Es responsabilidad de las dependencias dueñas de los sistemas de información, la asignación de recursos humano, y económico para el mantenimiento, actualización, adquisición de licenciamiento, ya que la Oficina de Tecnologías y Sistemas de Información cuenta 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. No obstante lo anterior, la Oficina de Tecnologías y Sistemas de Información deberá dar un aval técnico a la contratación de servicios profesionales de ingenieros de sistemas, electrónicos y afines que apoyen el desarrollo o mantenimiento de sistemas de información o plataformas digitales.

[PL10-ES14]

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

[PL10-ES15]

Los programas fuentes estarán en custodia de la Oficina de Tecnologías y Sistemas de Información mediante un repositorio oficial de código Team Foundation Server

[PL10-ES16]

Para las aplicaciones construidas directamente por el DNP, existe la protección de derechos de autor y propiedad intelectual, por lo tanto, se registrará el software ante la Dirección Nacional de Derecho de Autor a nombre del DNP.

[PL10-ES17]

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-ES18]

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

[PL10-ES19]

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-ES20]

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-ES21]

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

[PL10-ES22]

Se entiende por software de apoyo o base para el desarrollo o funcionamiento de las aplicaciones, a los seleccionados por la Oficina de Tecnologías 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

5.11 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 del departamento.

[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 Manual y Políticas de Seguridad de la Información y tienen las mismas responsabilidades que los usuarios del DNP (cláusula de confidencialidad y políticas de seguridad).

5.12 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 Grupo de Planeación y la Oficina de Tecnologías 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.

[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. Ver “Instructivo Incidente Informático”. El asesor de la Oficina de Tecnologías 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 proceso establecido de Control Disciplinario Interno en el marco del Sistema Integrado de Gestión y deben ser notificadas a la Secretaría General, Oficina de Tecnologías y Sistemas de Información y la Oficina de Control Interno.

[PL12-ES4]

Los incidentes de severidad grave[17] deben ser reportados a la persona encargada de la seguridad de la información quien debe realizar la revisión y análisis de la información encontrada y reportarla al Coordinador del Grupo de Control Disciplinario con copia a la Secretaría General y Oficina de Tecnologías 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 incidentes[18], 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.

[PL12-ES6]

Los usuarios reportan 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 incidente es asignado al Asesor 08 de la Oficina de Tecnologías 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 Tecnologías 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.

[17] Ver numeral 4.2.2 Valoración de los incidentes de seguridad.

[18] Colcert, CsirtGOB, CSIRT PONAL

[PL12-ES9]

Los responsables de seguridad de la información de la Oficina de Tecnologías 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 Grupo 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]

Se podrá realizar las pruebas de Ethical Hacking con proveedores que la Oficina de Tecnologías y Sistemas de Información determine previa autorización del Comité de Institucional Gestión y Desempeño Institucional.

5.13 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) 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 Grupo de Planeación del DNP como administrador del Sistema Integrado de Gestión 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.

[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 ésta. 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.

5.14 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.co Sección Transparencia y Acceso a la Información Pública, Normatividad, Normograma.

[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 y Jefes de Oficina 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.

5.15 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 Lineamiento 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 el portal del DNP www.dnp.gov.co sección “Sistema Integrado de Gestión”, “Macroprocesos de Apoyo”, “Proceso Gestión de la seguridad de la información - componente tecnológico

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.

[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 "Lineamiento para la Política de Tratamiento de la Información de Datos Personales en el DNP", y se deben seguir las directrices descritas en el capítulo "RECOLECCIÓN DE DATOS PERSONALES" del "lineamientos para la identificación y valoración de activos de información en el Sistema de Gestión de Seguridad de la Información" disponible en el portal del DNP www.dnp.gov.co sección "Sistema Integrado de Gestión", "Macroprocesos de Apoyo", "Proceso Gestión de la seguridad de la información - componente tecnológico

[PL15-ES2]

Es el Departamento Nacional de Planeación a través de la dirección técnica, proyecto ó programa. El rol del responsable consiste en 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 "Lineamiento para la Política de Tratamiento de la Información de Datos Personales en el DNP", disponible en el portal del DNP www.dnp.gov.co sección "Sistema Integrado de Gestión", "Macroprocesos de Apoyo", "Proceso Gestión de la seguridad de la información - componente tecnológico

[PL15-ES3]

Los Derechos de los ciudadanos están descritos en capítulo "DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES" del "Lineamiento para la Política de Tratamiento de la Información de Datos Personales en el DNP", disponible en el portal del DNP www.dnp.gov.co sección "Sistema Integrado de Gestión", "Macroprocesos de Apoyo", "Proceso Gestión de la seguridad de la información - componente tecnológico

[PL15-ES4]

El Área Responsable de la atención a los titulares y demás aspectos relacionados con las PQRSD están descritos en el "Lineamiento para la Política de Tratamiento de la Información de Datos Personales en el DNP", disponible en el portal del DNP www.dnp.gov.co sección "Sistema Integrado de Gestión", "Macroprocesos de Apoyo", "Proceso Gestión de la seguridad de la información - componente tecnológico

[PL15-ES5]

El área responsable del tratamiento de los datos personales definirá 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.

[PL15-ES8]

Con el objeto de cerrar la base de datos, bien sea por que el titular de la información lo requirió o por que 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]

El DNP debe incluir las bases de datos creadas en el aplicativo del Registro Nacional de Bases de datos de la Superintendencia de Industria y Comercio.

[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 la misma.

6. CAPACITACIÓN E INDUCCIÓN EN SEGURIDAD DE LA INFORMACIÓN

6.1. 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 con el 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.

Fecha aprobación: 24 de julio de 2020

Elaboró:

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

WALTER SILVA COMBITA
Contratista Grupo de Planeación

Revisó:

CLAUDIA ANGELICA BEN-AMY
Funcionaria Asesor Grado 8 -OTSI

CAMILO CORTÉS MORA
Coordinador Grupo de Planeación – Administrador SIG

Aprobó:

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