El servicio público es de todos

Función Pública

FUNCIÓN PÚBLICA

Políticas Técnicas de Seguridad de la Información

Proceso de Tecnologías de la Información

VERSIÓN 05
OCTUBRE 2021

Versión	Fecha de versión (aaaa-mm-dd)	Descripción del cambio
1	2018-03-23	Creación de la “Política general de seguridad de la información Función Pública”. Se requiere para cumplir los lineamientos de Seguridad y Privacidad de la Información establecida por Gobierno Digital.
2	2018-12-07	Se requiere actualizar la Política de Operación del Proceso de Tecnologías de la Información, debido a la nueva imagen institucional
3	2019-03-08	De acuerdo a la nueva imagen de gobierno se realiza actualización de la documentación en cuanto a logo e imagen institucional.
4	2020-09-30	Ajuste del documento de acuerdo con requerimientos del Modelo de seguridad y privacidad de la información de MINTIC
5	2021-10-26	Incorporación de la política técnica de seguridad de correos masivos

Contenido

Tabla de tablas

1 Introducción

Uno de los insumos principales para la gestión, el control y la toma de decisiones de Función Pública es la información que la entidad genera, almacena y administra, por tanto, es primordial establecer políticas claras y contundentes para la recolección, almacenamiento, administración y entrega de la información.

De igual modo, la tecnología es el recurso clave para el buen manejo de dicha información, la cual se desarrolla, crece y evoluciona de manera rápida y constante, requiriendo establecer lineamientos de seguridad que minimicen las alteración, fuga o indisponibilidad de la información durante las etapas de fabricación, diseño e implementación de las herramientas, incluso durante el uso de las mismas. Por esta razón la política de seguridad de la información busca i) definir lineamientos, controles, roles perfiles y responsabilidades para la gestión de la información, y ii) gestionar al máximo las amenazas a los sistemas de información, control y gestión y iii) limitar la capacidad de los atacantes para violentar y dar un mal uso a la información.

Por lo anterior, la entidad consolida en el presente documento las políticas en seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios.

Dado que la entidad cuenta con un Sistema Integrado de Planeación y Gestión, este documento hace parte integral del mismo, complementando los procedimientos y guías vigentes del proceso de Tecnologías de la información, como instrumento para orientar la implementación de la política de seguridad de la información y sensibilizar a los servidores públicos, pasantes y contratistas acerca de la importancia del buen manejo de la información.

2 Objetivos de la seguridad de la información

La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades.

2.1 Objetivos específicos:

- Mejorar continuamente las capacidades y habilidades necesarias en todos los servidores públicos para identificar, reportar y gestionar los riesgos de seguridad digital mediante acciones de sensibilización y capacitación

- Implementar, mantener y mejorar anualmente el conjunto de controles de seguridad de la información recomendados por el modelo de seguridad y privacidad de la información mediante la aplicación del plan de seguridad y privacidad de la información institucional, para mantener en niveles aceptables los riesgos residuales de seguridad digital.

- Fortalecer continuamente la función institucional mediante la implementación, difusión y mejoramiento continuo del modelo de seguridad y privacidad de la información para mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

3 Alcance

Las políticas de Seguridad de la Información son aplicables a todos los servidores públicos, pasantes, y contratistas de Función Pública que procesan y/o manejan información de la entidad.

4 Generalidades

4.1 Administración de las políticas de seguridad de la información

Las políticas de seguridad de la información se revisan y actualizan anualmente con el fin de garantizar su vigencia y pertinencia para el cumplimiento de los objetivos institucionales. De la misma forma se revisan cuando se presenten situaciones como: cambios organizacionales, culturales o del entorno interno o externo, cambios operativos o normativos que afecten a la entidad, cuando ocurren incidentes de seguridad de la información que obliguen al fortalecimiento de controles o lineamientos, o de acuerdo con los resultados de la gestión de riesgos institucionales.

De igual manera, se implementan mediante lineamientos, procedimientos o controles que especifican los detalles técnicos de su operación.

5 Marco normativo

A continuación, se referencian las normas y leyes colombianas que aplican en el ámbito de seguridad de la información, si cualquier disposición de estas condiciones pierde validez o fuerza obligatoria, por cualquier razón, todas las demás disposiciones conservan su fuerza obligatoria y carácter vinculante.

- **Constitución Política de Colombia** Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar". De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

- **Constitución Política de Colombia** Articulo 23. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

- Ley 23 de 1982, Sobre derechos de autor

- Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

- Ley 603 de 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995, Articulo 2. Artículo 2º. Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos.

- Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

- Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

- Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.

- Ley 1032 de 2006, Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.

- Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

- Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

- Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC.

- Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- Ley 1336 de 2009 (Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.) por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

- Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Artículo 24. Informaciones y documentos reservados.

- LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

- Ley 1672 de 2013, Lineamientos para la Adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos

- Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 128 de 2018, Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

- Ley 1955 del 25 de mayo de 2019. "Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022. "Pacto por Colombia, Pacto por la Equidad". Incluyó el artículo 147 de Transformación Digital Pública y 148 de Gobierno Digital como política de gestión y desempeño institucional

- Ley 1955 de 2019, Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad", Articulo 147 y Artículo 148

- Decreto 1474 de 2002, por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).

- Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley

- 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

- Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones

- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo

- Decreto 1081 de 2015 **(**Decreto Reglamentario Único del Sector Presidencia de la Republica), Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, Título 1, Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional

- Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública

- Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014

- Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

- Decreto No. 2106 del 22 de noviembre de 2019. “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.”

- Documento CONPES 3854, Política Nacional de Seguridad Digital

- Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES)

- Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado.

- Circular Externa Conjunta No. 04 del 5 de septiembre de 2019. Tratamiento de datos personales en sistemas de información interoperables.

- Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6 Responsabilidad por contravención de la política de seguridad

El incumplimiento de las políticas de seguridad de la información descritas en este documento se trata mediante el procedimiento de incidentes de seguridad de la información, de acuerdo con la naturaleza del incidente y los resultados de su tratamiento e investigación y los responsables de los procesos institucionales evalúan la necesidad de adelantar procesos disciplinarios o legales.

Cuando los incidentes de seguridad de la información correspondan a delitos informáticos calificados como tales por la normatividad vigente, el comité de emergencia formulará la recomendación al Comité Institucional de Gestión y Desempeño para iniciar las acciones legales ante la respectiva autoridad competente. Cuando el incidente de seguridad de la información no esté calificado como un delito informático, las acciones disciplinarias o legales se adelantan de acuerdo con la competencia del código único disciplinario en el caso de funcionarios públicos o mediante los criterios definidos en los contratos de prestación de servicios en el caso de contratistas.

Los servidores públicos del Departamento Administrativo de Función Pública que ocasionen algún incidente de seguridad de la información por realizar acciones que contravengan o incumplan alguna de las disposiciones descritas en el presente documento, serán reportados por correo electrónico al Jefe inmediato, al Jefe de la Oficina Asesora de Planeación, al Coordinador del Grupo de Gestión Humana y Jefe de la Oficina de Control Interno, para la revisión del caso y la adopción de las medidas respectivas de acuerdo con las políticas aplicables en la entidad.

Respecto a los contratistas y pasantes, estos serán reportados al supervisor del contrato y al director(a), subdirector(a) y jefe de área, para la revisión del caso y tomar las medidas respectivas.

7 Glosario

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

Activo de información: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos, intangibles (imagen y reputación).

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

Amenaza informática: situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado

Antivirus: programas cuyo objetivo es detectar y eliminar software malicioso.

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

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas), direcciones, información de contacto, números identificativos, apodos o cargo por otros datos para evitar la identificación de personas y preservar la confidencialidad de la información.

Archivos PST: son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico

Autenticación: mecanismo técnico que permite garantizar que una persona o entidad es la correcta.

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

Back up: se refiere a una copia de respaldo de información**.**

Buzón: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.

Canal de comunicación: medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.

Centro de cómputo: espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado.

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

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.

Confiabilidad: persona o cosa en la que se puede confiar.

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

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

Claves, contraseña o password: forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Correo electrónico. es correo electrónico es un mensaje de datos. Art 2. Ley 527 de 1992. "ARTÍCULO 2º. Definiciones. Para los efectos de la presente ley se entenderá por: a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;" Ley 527 de 1999

Correo electrónico. un correo electrónico (en inglés: electronic mail, normalmente abreviado e-mail o email) es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica. https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

Correo no deseado (SPAM). mensajes masivos no solicitados, es decir, mensajes enviados a varios destinatarios que no los solicitaron ver: Que es spam (Internet Society)

Criterios para adquisición de tecnología: condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología, como:

- Compatibilidad: el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad.
- Calidad: se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo en el mercado.
- Garantía: se deben tener en cuenta los plazos de vigencia de la garantía ofrecidos y los requeridos para el proceso de implementación, adaptación, pruebas, y puesta en funcionamiento.
- Acuerdos de servicio: se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes.
- Mantenimiento, actualizaciones y soporte: se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice.
- Transacciones: se deben identificar cuáles transacciones realiza el sistema, de qué manera las realiza y dónde se almacenan.
- Reportes o salidas: se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.

Custodio de activo de información: individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.

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

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

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

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

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

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

DAFP: Departamento Administrativo de la Función Pública

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético que pueden ser grabados, borrados y regrabados como una cinta de audio.

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

Dirección IP: (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

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

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

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

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

Grupos de Valor: para Función Pública corresponden a las entidades del estado, servidores públicos y ciudadanos.

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

Infraestructura tecnológica: elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.

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

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

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

Internet: corresponde a una interconexión de diferentes redes de computadoras, permitiendo la creación de una red única de alcance mundial.

Intranet: red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

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

OTIC: Oficina de Tecnologías de Información y las Comunicaciones

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

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

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

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Responsable de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.

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

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

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

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

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

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

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

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

Spamming**:** el uso de los servicios de correo electrónico para difundir mensajes no solicitados de manera indiscriminada a una gran cantidad de destinatarios. Decreto 1078 de 2015, Reglamento único del sector TIC, Artículo 2.2.10.1.2. Definiciones.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

8 Roles y responsabilidades en materia de seguridad de la información

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la entidad, cualquiera sea su calidad jurídica, el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe.

Todos los servidores públicos, contratistas, proveedores y cuando sea aplicable los grupos de valor, deben utilizar los activos de información institucionales para el desarrollo de las actividades misionales, nunca para su beneficio personal o en detrimento de los objetivos institucionales.

De igual forma, todos los servidores públicos, contratistas y proveedores deben preservar la confidencialidad de la información que por razones de su cargo o responsabilidades designada esté bajo su custodia.

Tabla 1 Roles y responsabilidades en seguridad digital

Rol	Responsabilidad
Director de Función Pública	• Aprobar las políticas de seguridad de la información. • Evaluar el proceso de gestión de Seguridad de la Información • Sancionar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño. • Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información.
Comité Institucional de Gestión y Desempeño	• Revisar y proponer al director, para su aprobación, la Política de Seguridad de la Información. • Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información. • Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas. • Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones.

Rol	Responsabilidad
	• Reportar al director, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.
La Secretaría General	• Coordinar la atención de la mesa de servicio de primer nivel. • Coordinar la realización del mantenimiento correctivo y preventivo de los computadores de escritorio, portátiles, impresoras y demás periféricos de la entidad. • Seguir los lineamientos que la Oficina de Tecnologías de la Información y las Comunicaciones establezca para tal fin. • Coordinar el mantenimiento preventivo y correctivo a la infraestructura eléctrica de la entidad. • Velar por la incorporación de las cláusulas en materia de seguridad de la información, en los contratos, acuerdos u otra documentación que la entidad firme con contratistas y proveedores, a través del grupo de gestión contractual
* Oficial o encargado de la seguridad de la información institucional. *Servidor público delegado o nombrado por el director como su oficial en materia de seguridad de la información*	• Organizar las actividades del Comité Institucional de Gestión y Desempeño en materia de seguridad de la información. • Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la entidad y el control de su implementación; y velar por su correcta aplicación. • Supervisar el monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos de seguridad digital. • Gestionar la coordinación con otras áreas de la entidad para apoyar los objetivos de seguridad. • Hacer el enlace con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información. • Apoyar a los diferentes procesos institucionales en la adopción del sistema de gestión de seguridad de la información. • Servir de enlace con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información

Rol	Responsabilidad
	• Mantener contacto con las autoridades en materia de ciberseguridad para conocer de primera mano indicios o alertas en materia de seguridad de la información y recibir el apoyo de grupos de respuesta ante incidentes de seguridad de la información. • Mantener contacto con grupos de interés especial en materia de seguridad de la información para asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa. Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades
Encargado técnico de seguridad de la información institucional *Servidor público delegado por el director como su asesor en materia técnica de seguridad de la información*	• Gestionar operativamente las soluciones a los incidentes de seguridad de la información que afecten los activos de la información institucionales. • Monitorear el avance de cada una de las etapas de la implementación de la Política de Seguridad de la Información, en sus diversos aspectos. • Establecer puntos de enlace con los encargados técnicos de seguridad de otros servicios públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de la seguridad pertinentes.
	• Cumplir con los procedimientos relativos a los dominios de control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información y gestión de los canales de comunicación y operaciones. • Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Entidad. • Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
Propietarios de los activos de la información institucional.	• Clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad de los mismos, documentar y mantener actualizada la clasificación Definir qué usuarios deberán tener permisos de

Rol	Responsabilidad
Directores, Jefes de Área y Coordinadores de grupo	acceso a la información de acuerdo con sus funciones y competencia. • Entregar orientaciones básicas que se establezcan por parte de la alta dirección y su equipo de trabajo en materia de seguridad de la información. • Ejercer liderazgo compromiso en la aplicación de la política de Seguridad de la Información.
Coordinador del Grupo de Gestión Humana	• Cumplir con los procedimientos relativos al tema de Seguridad de la Información del Talento Humano. • Cumplir con los procedimientos relativos al tema de Seguridad de la Información del Talento Humano. • Notificar a todo el Talento Humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. • Ejecutar tareas de capacitación continuas en materia de seguridad de la información. • Definir y coordinar un Plan de Capacitación y Sensibilización en temas de seguridad de la información, el cual se estructura con base en requerimientos del encargado de seguridad.
Director Jurídico	• Velar por el cumplimiento legal de la Política de Seguridad de la Información en la entidad. • Definir, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes en materia de seguridad de la información, y el establecer enfoque de la entidad para satisfacer esos requerimientos, para cada sistema de información y la entidad. • Asesorar en materia legal, asociada a seguridad de la información, a la entidad y establecer las pautas legales que permitan cumplir con los requerimientos legales en esta materia.
Oficina de control interno	• Cumplir con los procedimientos relativos al cumplimiento de la Política de Seguridad de la Información. • Practicar auditorias periódicas, o cuando lo considere pertinente, sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta

Rol	Responsabilidad
	Política y por las normas, procedimientos y prácticas que de ella surjan. • Informar al encargado de seguridad, el resultado de las auditorías realizadas. • Proponer soluciones a las debilidades encontradas en las auditorias e informarlas al Comité Institucional de Gestión y Desempeño.
Grupos de valor y usuarios internos. usuarios de la información y de los sistemas de procesamiento de la información	• Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente y todas las normas y procedimientos establecidos por la Entidad en esta materia. • Dar buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones o actividades, la relación de estos debe estar registrada en el Sistema de Inventarios de la entidad. • Hacer entrega en buen estado de los equipos de cómputo y periféricos que le sean asignados, cuando se presente retiro de la entidad, cambio de funciones o culminación del contrato según sea el caso. • Custodiar la información alojada en el equipo de cómputo y periféricos asignados. • Cumplir las políticas de respaldo, custodia y recuperación de la información definidas por la Oficina de Tecnologías de la Información y las Comunicaciones. • Permitir cuando el Departamento Administrativo de la Función Pública lo requiera, la revisión del equipo de cómputo a nivel físico, software instalado e información alojada.
Visitantes y grupos de valor	• Todos los visitantes de Función Pública que tengan acceso autorizado a los activos de información deben cumplir las políticas de seguridad de la información institucionales. • Los visitantes de Función Pública pueden acceder a la red local de invitados, la cual restringe el acceso solo a internet. Esta red, no permite el acceso a servidores a la red interna de la entidad. • El acceso a los activos de información es restringido a los visitantes, todo acceso debe ser autorizado por el responsable del mismo.

9 Lineamientos de gestión de activos de información en Función Pública

Las políticas de seguridad de información requieren definir lineamientos para la identificación de los activos de información institucionales y la responsabilidad respecto la protección de la información y medidas de control para prevenir la materialización de riesgos de seguridad digital.

Por lo anterior, en Función Pública se define:

- Los activos de información de Función Pública están conformados por la información, sistemas de información, aplicaciones, servicios de información, bases de datos, archivos físicos, personas, infraestructura tecnológica, manuales, procesos y procedimientos.

9.1 La responsabilidad frente a los activos de información:

- Todos los servidores públicos, contratistas y pasantes de Función Pública, deben propender por la seguridad y la calidad de la información en los criterios de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, confiabilidad y cumplimiento
- Todos los servidores públicos, contratistas y pasantes de Función Pública deben aplicar los controles de seguridad de la información definidos por la entidad para garantizar la preservación de la confidencialidad, integridad, disponibilidad de los activos de información institucionales.
- Está prohibido realizar cambios a los activos de información de Función Pública, sin contar con la autorización formal del responsable del activo.
- Está prohibido utilizar los activos de información de la entidad para fines diferentes al cumplimiento de las funciones asignadas.
- El oficial o encargado de Seguridad de la Información, son los responsables de realizar las consultas para la identificación de comportamientos tecnológicos, análisis estadísticos de uso e investigaciones técnicas digitales en el momento en que así lo determine o lo soliciten las áreas de control o la Dirección de Función Pública.
- La información generada, procesada, almacenada y entregada (medio físico y digital) es de propiedad de la Función Pública, los sistemas de información, servicios tecnológicos, infraestructura tecnológica y activos tangibles e intangibles.
- Función Pública actuará como responsable del tratamiento de los datos personales y hará uso de los mismos únicamente para las finalidades para las que se encuentra facultado, según lo establece en su política institucional de tratamiento de datos personales" aprobado por la entidad y publicada en la página web http://www.funcionpublica.gov.co/
- Todos los activos de información deben estar inventariados y deben estar asignados a un responsable

- El responsable debe inventariar y actualizar de manera periódica dichos activos, custodiar la información y tener definidas y actualizadas las restricciones de acceso.
- Los propietarios de los activos de información son responsables de su uso y protección mientras estén en su custodia ya sea física o electrónica. Así mismo, son responsables de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados.
- Los activos de información digitales y físicos deben seguir los lineamientos para la organización documentos asociados al proceso de Gestión Documental de Función Pública, que tiene como fin orientación a los servidores públicos, pasantes y contratistas de la entidad, en todos los aspectos relacionados con la organización, manejo, control y servicios de los documentos que producen cada una de las dependencias en el cumplimiento de sus funciones.
- Los responsables de los activos de información deben seguir el Plan Institucional de Archivos de Función Pública– PINAR, el cual es un instrumento de planeación para la labor archivística, que determina elementos importantes para la Planeación Estratégica y Anual del Proceso de Gestión Documental y da cumplimiento a las directrices del Archivo General de la Nación y a la normatividad vigente frente a la administración de los documentos.
- Los propietarios de los activos de información son responsables de su uso y protección mientras estén en su custodia ya sea física o electrónica, de tal forma que se evite su modificación, perdida y divulgación no autorizada, acorde a su valor, confidencialidad e importancia.
- No está permitido que áreas diferentes a la Oficina de Tecnologías de la Información y las Comunicaciones tengan a cargo equipos servidores o conecten a la red de la Entidad equipos de cómputo y servidores sin previa autorización de la Oficina de Tecnologías de la Información y las Comunicaciones.

9.2 La responsabilidad sobre la infraestructura tecnológica:

La Oficina de Tecnologías de la Información y las Comunicaciones de Función Pública es responsable de:

- Administrar los equipos de hardware y comunicaciones alojados en el centro de datos.
- Gestionar los servicios de información y de tecnología alineados con los objetivos sectoriales e institucionales para el cumplimiento de su misión.
- Custodiar la información almacenada en los sistemas de información, aplicaciones y bases de datos.
- Disponer de las medidas de seguridad para proteger la información digital de Función Pública.
- Informar al Comité Institucional de Gestión y Desempeño de los eventos de seguridad que se presenten y la solución planteada.

- Dar los lineamientos para la administración de los equipos de cómputo, dispositivos de almacenamiento externo, sistemas de información, aplicativos e infraestructura tecnológica.
- Responder por la disponibilidad de los servicios tecnológicos e informar al comité de emergencias cualquier novedad que pueda afectar la normal prestación de los mismos.
- Realizar el monitoreo y control automático del software instalado en los equipos de cómputo de la entidad. Si se encuentra instalado software no autorizado, se notificará al jefe inmediato o supervisor para que se informe el motivo de la irregularidad y se tomen las medidas del caso.

9.3 La responsabilidad de los servidores públicos, contratistas y pasantes:

- Dar buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones o actividades, la relación de los mismos debe estar registrada en el Sistema de Inventarios de la entidad.
- Hacer entrega en buen estado de los equipos de cómputo y periféricos que le sean asignados, cuando se presente retiro de la entidad, cambio de funciones o culminación del contrato según sea el caso.
- Custodiar la información alojada en el equipo de cómputo y periféricos asignados.
- Cumplir las políticas de respaldo, custodia y recuperación de la información definidas por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Conectarse a la red con el usuario asignado y la respectiva clave de acceso.
- Utilizar solamente software licenciado y autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones. En caso de requerir la instalación de software adicional, el director o jefe del área debe realizar la solicitud por medio de la Sistema de mesa de servicio, con la debida justificación para revisión y a probación.
- Permitir, cuando Función Pública lo requiera, la revisión del equipo de cómputo a nivel físico, software instalado e información alojada.

9.4 Sobre el uso aceptable de los activos

Todas las actividades de administración y operación que se realicen en los activos de información deben ser orientadas a garantizar el correcto cumplimiento de la misión de entidad, por lo tanto:

- Los servidores públicos y contratistas de Función Pública deben mantener y actualizar continuamente el inventario de los activos de la información a su cargo.
- Todos los servidores públicos, pasantes y contratistas deben reportar a la mesa de servicio cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información de la entidad.
- Cualquier modificación a los activos de información de Función Pública y que implique una afectación del servicio, debe cumplir con lo dispuesto en el procedimiento de

gestión de cambios, a fin de tener una trazabilidad de los cambios realizados en los activos.

- Los servidores públicos, pasantes y contratistas de Función Pública no podrán instalar ningún programa o software desarrollado en la Entidad, en los equipos, estaciones de trabajo u otro dispositivo de almacenamiento externo sin la autorización de la entidad.
- Los servidores públicos, pasantes y contratistas de la entidad no podrán almacenar información reservada en ningún dispositivo de almacenamiento personal.
- A la información sensible de Función Pública se tendrá acceso controlado y solo puede ser utilizada con autorización de la entidad.
- Ningún servidor público, pasante y contratista deberá compartir la cuenta de usuario y contraseñas.

9.5 Sobre la calificación de activos de información.

En cumplimiento de las obligaciones 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, Función Pública, adoptó el esquema de calificación de la información definido por la ley, por lo cual:

- La calificación e inventario de la información se realiza a través del procedimiento de calificación de información.
- El registro de activos de información, el esquema de publicación de información y el índice de información clasificada y reservada son gestionados por el proceso de gestión documental.
- Los instrumentos de gestión pública de información se publican en la sección de transparencia del sitio web institucional.
- La identificación de riesgos de seguridad digital contempla la identificación de los activos de información calificados como reservados o clasificados.
- La información calificada como datos abiertos es evaluada por el proceso de gestión documental para autorizar su publicación en el portal datos.gov.co
- La calificación de la información se debe tener en cuenta al momento de autorizar el acceso a los diferentes activos de información institucionales.
- El índice de información clasificada y reservada debe ser verificado al momento de autorizar acceso o transferencia de información con todas las partes interesadas y grupos de valor.
- Los líderes de procesos deben solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo

9.6 Sobre el ingreso y retiro de activos tangibles (físicos) e intangibles

- El ingreso de activos tangibles debe estar debidamente justificado y verificado por el grupo de Gestión Administrativa. Para llevar a cabo lo anterior, se siguen los

procedimientos del subproceso de gestión administrativa y las políticas contables institucionales.

- El retiro de activos tangibles debe estar debidamente justificado y verificado por el grupo de Gestión Administrativa. Para llevar a cabo lo anterior, se deberá levantar un acta donde se indique el concepto técnico y se anexen los soportes en caso de ser necesario.
- El ingreso de los activos intangibles (software) al inventario, es solicitado por el supervisor del contrato o el responsable del intangible de la Oficina de Tecnologías de la Información y las Comunicaciones, utilizando para ello la Herramienta de Mesa de Servicio ProactivaNet. Para ello, se debe adjuntar la factura (si aplica) y especificar los detalles del activo para su ingreso al almacén y aplicación contable.
- El retiro o dada de baja de los activos intangibles (software) del inventario, es solicitado con la justificación técnica del responsable del intangible de la Oficina de Tecnologías de la Información y las Comunicaciones, utilizando para ello la Herramienta de Mesa de Servicio ProactivaNet. La solicitud es verificada y avalada por la Secretaría General (Grupo de Gestión Administrativa y Grupo de gestión Financiera) y una vez aprobada, se genera la respectiva acta, se actualizan los registros físicos y contables, se notifica al solicitante y se actualiza el inventario.

10 Lineamientos para la gestión de seguridad de recursos humanos

Las políticas de seguridad de información pretenden asegurar que los funcionarios, contratistas y pasantes comprendan sus responsabilidades y sean idóneos en los roles asignados respecto a la seguridad de la información, por lo tanto, la entidad, define:

10.1 Sobre la vinculación y desvinculación de servidores públicos

- Que se gestiona la seguridad de los recursos humanos a través del proceso de Gestión del Talento Humano.
- Que los procesos de selección de los servidores públicos vinculados a la entidad cumplen con los requisitos del Subproceso Gestión Ciclo de Vida de Talento Humano, el cual incluye la verificación de antecedentes disciplinarios, fiscales y de policía, además de la verificación de experiencias académicas y laborales.
- Que la selección y vinculación de servidores públicos sigue el procedimiento Vinculación y Permanencia de personal.
- Que, durante la permanencia como servidores públicos de la entidad, éstos deben participar en las actividades definidas por el subproceso Gestión Ciclo de Vida de Talento Humano para su capacitación y sensibilización en materia de seguridad de la información.
- Que al momento de la finalización de su relación laboral el servidor público debe cumplir con el procedimiento de desvinculación del proceso de gestión de talento humano.

- Que en cumplimiento de los requisitos del código único disciplinarios los servidores públicos aceptan la obligación legal de mantener la reserva de la información bajo su responsabilidad.
- Que todo el personal vinculado a la Entidad debe aceptar formalmente el cumplimiento de las políticas de seguridad de la información institucionales, las políticas de operación institucionales y los procedimientos del sistema integrado de gestión institucional.

10.2 Sobre la vinculación y desvinculación de los pasantes

- Los pasantes se vinculan a la Entidad mediante al acta administrativa de vinculación formativa, donde el supervisor delegado es el encargado de asignar tareas y realizar seguimiento al cumplimiento de las actividades asignadas.
- El Grupo de Gestión Humana es el encargado de solicitar por medio de la Herramienta de Mesa de Servicio ProactivaNet la creación, actualización y eliminación de cuentas de usuario y asignación de equipos de cómputo para el cumplimiento de las actividades que le sean asignadas.
- Los pasantes deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información institucionales, las políticas de operación institucionales y los procedimientos del sistema integrado de gestión institucional.

10.3 Gestión de contratistas frente a la seguridad de la información

- Para los contratos de prestación de servicios, el Grupo de Gestión Contractual es el encargado de solicitar por la Herramienta de Mesa de Servicio ProactivaNet el usuario institucional, para lo cual debe proporcionar los datos del contratista y del contrato.
- Si el contrato establece que la Entidad debe proporcionar el equipo de cómputo, el supervisor del contrato debe realizar la solicitud para que el Grupo de Gestión Administrativa verifique su disponibilidad y proceda a su entrega. El equipo de cómputo proporcionado al contratista debe quedar a cargo del supervisor del contrato.
- Para los contratos con personas jurídicas, en el caso de requerirse, el supervisor debe realizar la solicitud de la cuenta de usuario proporcionando los datos del contrato y de las personas que tendrán a cargo dichas cuentas de usuario.
- El supervisor del contrato y contratistas, deben dar cumplimento al Manual de Contratación del Proceso de Recursos – Subproceso Gestión Contractual.
- Al momento de terminar el plazo de ejecución del contrato, el supervisor del mismo debe solicitar la eliminación de la cuenta(s) de usuario asociada(s) al contrato. Si se asignó equipo de cómputo al contratista, el supervisor debe realizar la devolución del bien al almacén.

- Los contratistas deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información institucionales, las políticas de operación institucionales y los procedimientos del sistema integrado de gestión institucional.

10.4 Control de acceso servidores públicos, contratistas, pasantes y visitantes

- Los servidores públicos, contratistas, pasantes y visitantes deben portar el carné que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de la Función Pública.
- Si el servidor público, contratista, pasante y visitante porta un carné institucional que no le corresponde, será considerado como suplantación de identidad y deberá notificarse al Grupo de Gestión Humana.
- Los servidores públicos de la entidad deben registrar el ingreso y la salida de la jornada laboral en el dispositivo biométrico ubicado en el primer piso de las instalaciones de Función Pública.
- El Grupo de Gestión Humana cada dos meses debe entregar periódicamente el listado de los pasantes, indicando: nombres, apellidos, número de identificación y área en la que realiza sus labores. Esta lista puede ser utilizada por la empresa de vigilancia para verificación al ingreso a las instalaciones de Función Pública.
- El Grupo de Gestión Contractual debe entregar cada dos meses el listado de los contratistas activos indicando: nombres, apellidos, número de identificación y área en la que realiza sus actividades. Esta lista puede ser utilizada por la empresa de vigilancia para verificación al ingreso a las instalaciones de Función Pública.
- Función Pública actuará como responsable del tratamiento de sus datos personales y hará uso de los mismos únicamente para las finalidades para las cuales se encuentra facultado, según lo establece La Política de tratamiento de datos personales aprobada por la entidad y publicado en la página web www.funcionpublica.gov.co.
- Los contratistas que realicen actividades en las instalaciones de Función Pública de forma regular en razón la prestación de servicios contratados por terceros, deben utilizar prendas distintivas que faciliten su identificación. Tal es el caso de las empresas de vigilancia, aseo y adecuación de infraestructura física.

10.5 Control de acceso del personal de vigilancia

- El personal de vigilancia debe observar que los funcionarios públicos, pasantes, contratistas y visitantes no se encuentren en estado de ebriedad, bajo el efecto de sustancias alucinógenas, armado o en cualquier estado dudoso que pueda afectar la seguridad de la Entidad e informar cualquier novedad al Grupo de Gestión Humana.
- El personal de vigilancia debe estar debidamente uniformado.

- El personal de vigilancia debe solicitar a todos los visitantes un documento de identificación personal vigente, de preferencia con foto, con el fin de verificar los datos y solicitar confirmación telefónica con la persona o área que visita. Una vez realizada la verificación el documento de identificación será devuelto al visitante de forma inmediata.
- Una vez registrado el visitante en el sistema de control de registro, recibirá una ficha de acceso con el número del piso al que se le ha autorizado previamente el ingreso por parte de un servidor, pasante o contratista. Deberá portar la ficha en un lugar visible durante el tiempo en que permanezca dentro de la entidad. Una vez culmine la vista a las instalaciones de la Entidad, el servidor público, pasante o contratistas debe registrar la salida en el sistema de control de registro con el fin de autorizar la salida del edificio del visitante, y devolver ficha para que se registre en el sistema la hora de salida.
- En caso de no disponer de un documento de identificación, se deberá llamar al servidor público, contratista o pasante que vista, con el fin de que se presente en la recepción a recibirlo y se dejará la anotación en el libro de registro de visitas.
- Si el visitante entrega un documento que no le corresponde, será considerado como suplantación de identidad y deberá notificarse al servidor público, contratista o pasante que visita y al Grupo de Gestión Humana.
- Si alguna persona llega a una dependencia sin que previamente haya sido autorizado su ingreso y registrado el mismo en la recepción del edificio, de manera inmediata se debe informar dicha situación al personal de seguridad en la extensión 100, para oficializar su visita.
- En caso de que, como producto de la atención brindada a un usuario, sea necesario reorientar al visitante a otra área de la entidad, el servidor público, pasante o contratista que está siendo visitado deberá informar al personal de seguridad en la extensión 100 sobre el desplazamiento de la persona y acompañar a esta al nuevo lugar de destino
- El personal de vigilancia deberá hacer arqueos periódicos a los carnés de visitantes para asegurar su existencia según inventario.
- Cuando en desarrollo de eventos institucionales se deba autorizar el ingreso masivo de personal al edificio, es indispensable que el servidor público o contratista que haya organizado la actividad remita al correo electrónico recepcion@funcionpublica.gov.co, en formato Excel y con mínimo 4 horas de anticipación al inicio del evento, el listado del personal que asistirá al mismo, reportando: nombres y apellidos, número del documento de identificación y entidad de origen. Con esta información, el personal de recepción autorizará el acceso directo del visitante para que se registre en debida forma, en la mesa destinada para tal fin. A este personal no se le entregará ficha y, si alguno de los usuarios requiere desplazarse a otro piso, el servidor o contratista visitado deberá informar a la portería.
- Es responsabilidad de los servidores públicos que laboran en la entidad, informar al personal de seguridad en la extensión 100, cuando encuentre en las dependencias o en los pasillos de acceso, personas desconocidas en actitud sospechosa o que no porten la ficha o el carné institucional.

- El personal de vigilancia debe registrar la entrada o salida los equipos de cómputo, portátiles y demás equipos electrónicos en el libro de registro de elementos ubicado en la recepción.
- Función Pública no se responsabiliza por los equipos de cómputo, portátiles, equipos electrónicos y otros objetos personales que ingresen a la entidad. Por lo tanto, la custodia y cuidado de estos elementos es de total responsabilidad de su propietario, por lo cual es responsabilidad de la empresa de vigilancia informar esto al propietario del bien que se ingresa a las instalaciones de la Entidad
- El personal de vigilancia debe asegurar que ningún visitante salga de las instalaciones de la entidad con activos de información de la entidad, sin el debido formulario de autorización que otorga el Grupo de Gestión Administrativa.

10.6 Circulación interna de servidores públicos, contratistas, pasantes y visitantes

- Todo ser servidor público, contratista, pasante y visitante deberá portar su carné de identificación de manera visible.
- El Grupo de Gestión Humana, es el responsable de solicitar, actualizar y retirar los carnés de los servidores públicos y pasantes. Los supervisores de contratos son los responsables de solicitar y devolver los carnés al Grupo de Gestión Humana de los contratistas a su cargo.
- El primer carné que se entregue no tendrá costo para servidor público, contratista, pasante o visitante. En caso de pérdida del carné, el responsable debe reportar la pérdida del documento en la página de la Policía Nacional - opción Constancia por perdida de documentos y notificar al Grupo de Gestión Humana a la mayor brevedad posible. El servidor público, contratista o pasante deberá cubrir el costo de la reposición de su carné por motivo de perdida.
- Al momento de presentarse un contratista para prestar un servicio externo en las instalaciones de Función Pública, el servidor público, contratista o pasante que autoriza el ingreso debe realizar el acompañamiento constante hasta que finalice el o los servicios prestados.
- Todo ingreso de servidores públicos, contratistas y pasantes en horario no hábil, debe ser autorizado previamente por el Coordinador del Grupo de Gestión Administrativa o quien haga sus veces.

10.7 Seguridad para el teletrabajo

- El Departamento Administrativo de la Función Pública ha adoptado una política de teletrabajo que es conforme con los requerimientos de la Ley 1221 de 2008. La política institucional de teletrabajo se describe en el manual de operaciones y calidad institucional.

- El Grupo de Gestión Humana es el responsable de realizar y/o coordinar la visita domiciliaria, pruebas de meritocracia y ofimática de los servidores públicos que se postulan a teletrabajo.
- El Grupo de Apoyo a la Gestión Meritocracia es responsable de realizar las pruebas de meritocracia del postulante a teletrabajo.
- El Grupo de Gestión Humana es el responsable de realizar la prueba de ofimática del postulante a teletrabajo. La evaluación de las pruebas de ofimática es responsabilidad la Oficina de Tecnologías de la Información y las Comunicaciones.
- El Grupo de Gestión Humana es el responsable de realizar visita domiciliaria, para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar, sean las adecuadas en cuanto a iluminación, ruido, ventilación, puesto de trabajo, ergonomía y ubicación de los elementos del lugar donde realizaría el teletrabajo.
- El Grupo de Gestión Humana en compañía del Grupo de Gestión Administrativa son los responsables de realizar visita domicilia para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar sean las adecuadas en cuanto a equipo de cómputo, internet, red eléctrica, teléfono (fijo o móvil), software y antivirus instalado y debidamente licenciado.
- El Grupo de Gestión Humana es el responsable de solicitar a la Oficina de Tecnologías de la Información y las Comunicaciones la activación de la red virtual privada – VPN, que permite al teletrabajador conectarse de manera segura a la red de datos de Función Pública.
- Es responsabilidad del teletrabajador, acatar las políticas de seguridad de la información establecidas por Función Pública.
- Es responsabilidad del teletrabajador cumplir con los controles técnicos que defina la Oficina de las Tecnologías de Información y las comunicaciones para garantizar la seguridad en las actividades de teletrabajo incluido:

    - Utilizar únicamente los equipos autorizados por la Entidad para tener acceso a los sistemas de información e infraestructura tecnológica institucional
    - Asegurar su acceso Internet local con contraseña fuerte siguiendo los lineamientos de seguridad institucionales
    - Conectarse a la red local institucional únicamente mediante conexión de red privada virtual autorizada para tal fin.
    - Limitar el uso de familiares, amigos o desconocidos a los equipos de cómputo utilizados para las actividades
    - Reportar a la mesa de servicio, cualquier comportamiento sospechoso o inusual que se detecte cuando se realicen actividades de teletrabajo
    - Conocer y estar alerta a los tipos de amenazas informáticas socializadas por la Entidad para evitar ser víctima de estafas o software malicioso
    - En caso de utilizar equipos de propiedad personal para las actividades de teletrabajo, cumplir con los lineamientos de seguridad que determine la Oficina de las tecnologías de información y las comunicaciones para este tipo de dispositivos.

11 Lineamientos de seguridad física y ambiental

Dos elementos relevantes en esta política son los asociados a la seguridad física y ambiental de la entidad, que buscan prevenir el acceso físico no autorizado, el daño e interferencia a la información, instalación de procesamiento y almacenamiento de la información institucional, entre ellos:

11.1 Áreas seguras

Se consideran áreas seguras los sitios donde se gestiona la información sensible de la entidad cuyo acceso debe ser controlado. Para ello se implementan mecanismos de seguridad física y control de acceso. En Función Pública se catalogan como áreas de acceso restringido el centro de cómputo, los centros de cableado, el almacén, el área financiera, el área de archivo documental, el área de correspondencia. Los lineamientos para estas áreas son:

Centros de cómputo y cableado

- Solo personal autorizado puede acceder a las áreas consideradas como seguras, siendo responsabilidad del coordinador del área segura designar el encargado(s) de gestionar los accesos.
- La Secretaria General es la responsable de establecer y divulgar los lineamientos de seguridad física y seguridad de los servidores públicos, pasantes, contratistas y visitantes que laboren o visiten la entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones y el Grupo de Gestión Humana son los responsables de dar cumplimiento a las normas del sistema de gestión de seguridad y salud en el trabajo para el centro de datos.
- El acceso al centro de cómputo de la Entidad está a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, la cual es la responsable de enrolar, asignar tarjetas de acceso y dar los permisos de acceso según el caso, con el fin de garantizar la seguridad de los activos.
- La solicitud de enrolamiento para ingreso al centro de cómputo debe realizarse a través de Sistema de Mesa de Servicio ProactivaNet.
- El acceso y mantenimiento de los centros de cableado es responsabilidad del Grupo de Gestión Administrativa.
- La Oficina de Tecnologías de la Información y las Comunicaciones debe proveer en cada vigencia los elementos físicos necesarios que garanticen la correcta operación de la plataforma tecnológica ubicada en el centro de cómputo.
- La Oficina de Tecnologías de la Información y las Comunicaciones debe disponer en todo momento para el centro de cómputo de un sistema de control de acceso, sistema de control de temperatura y humedad, un sistema de detección y extinción de incendios, un sistema de alimentación eléctrica ininterrumpida (UPS) y un sistema de vigilancia y monitoreo.

- La Oficina de Tecnologías de la Información y las Comunicaciones y el Grupo de Gestión Administrativa son los responsables de gestionar el procedimiento ante incidentes asociados a la detección de incendio y cumplimiento de normas de seguridad industrial del centro de cómputo. Así mismo, son responsables de las actividades de evacuación del centro de cómputo y área de control de operaciones.
- La Oficina de Tecnologías de la Información y las Comunicaciones y el Grupo de Gestión Humana son los responsables de dar cumplimiento a las normas del sistema de gestión de seguridad y salud en el trabajo para el centro de cómputo.
- En el centro de cómputo y área de destinada al de control de operaciones, está prohibido realizar actividades que generen polvo, suciedad o partículas ya que pueden causar un mal funcionamiento de los equipos y generar falsas alarmas de incendio, dando como resultado el daño parcial o total de la infraestructura tecnológica y activos de información de la entidad.
- No está permitido el ingreso al centro de cómputo y centros de cableado de líquidos, alimentos y material inflamable. Las áreas deben permanecer ordenadas, limpias y sin elementos que no correspondan con la operación del área.
- Es responsabilidad de las personas autorizadas para el ingreso y mantenimiento del centro de cómputo y los centros de cableado mantener organizado los cables de voz, de datos y conexiones eléctricas (peinado).
- La limpieza y aseo del centro de datos y de los centros de cableado está a cargo del Grupo de Gestión Administrativa y debe efectuarse en presencia de un servidor público o contratista autorizado por parte de la Oficina de Tecnologías de la Información y las Comunicaciones o Grupo de Gestión Administrativa según sea el caso.
- El personal de limpieza debe ser capacitado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Así mismo, está prohibido el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
- La grabación de vídeo en las instalaciones del centro de cómputo con destino a terceras partes debe estar autorizada por el Comité Institucional de Gestión y Desempeño Institucional.
- Todo cambio dentro del centro de cómputo se debe tramitar a través del procedimiento de gestión de cambios establecido por la Oficina de Tecnologías de Información y las comunicaciones. La autorización de ejecución de cambios en el centro de cómputo es responsabilidad de la Oficina de Tecnologías de Información y las comunicaciones.
- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cuando se finalice la actividad.
- Mientras no se encuentren personas dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- El centro de cómputo contará con: señalización adecuada de todos y cada uno de los diferentes equipos y elementos, luces de emergencia y de evacuación, pisos elaborados con materiales no combustibles, sistema de refrigeración por aire acondicionado de precisión, unidad de potencia ininterrumpida UPS, que proporcione respaldo al centro de datos en caso de falla en el fluido eléctrico, alarmas de

detección de humo y sistemas automáticos de extinción de fuego, sistema contra incendios debidamente probado, con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales, cableado de la red protegido de interferencias mediante canaletas u otros mecanismos que impidan acceso o interferencia no autorizada, cables de potencia separados de los cables de comunicaciones, siguiendo las normas técnicas, puertas seguras y siempre cerradas.

- El centro de datos contará con chapa de seguridad que restrinja el acceso de personal no autorizado a los equipos.
- Las llaves de los centros de cableado están a cargo de la empresa de vigilancia, la cual debe garantizar el registro de ingreso y salida del personal que acceda a estas áreas.

Almacén, archivo y correspondencia

- El acceso al almacén estará autorizado por el Coordinador del Grupo de Gestión Administrativa, el cual coordinará el debido acompañamiento para garantizar la seguridad de los activos.
- El Coordinador del Grupo de Gestión Administrativa, garantizará las condiciones de seguridad física y ambiental de las áreas de almacenamiento de activos. Así mismo, contará con equipos de almacenaje adecuados que permitan la fácil ubicación, correcta custodia y minimicen los riesgos de accidente y daño.
- El acceso al área de archivo estará autorizado por el Coordinador del Grupo de Gestión Documental, el cual coordinará el debido acompañamiento para garantizar la seguridad de los activos.
- El Coordinador del Grupo de Gestión Documental, debe garantizar las condiciones de seguridad física y ambiental del área de archivo, tales como ventilación, iluminación, temperatura y humedad. Contará al igual con equipos de almacenaje adecuados para los diferentes tipos de formatos que maneja Función Pública (papel, microfilm, cintas, rollos, fotografías, disquetes, CD, DVD, memorias extraíbles).
- El acceso al área de correspondencia está restringido, solo se permite el acceso al personal designado por el Grupo de Gestión Documental. Toda la documentación que deba ser radicada se debe entregar en la ventanilla destinada para tal fin, ubicada en el cuarto piso para su respectivo trámite. Para el caso de los visitantes, el acceso para la radicación de documentos debe ser previamente autorizado por la empresa de vigilancia.

11.1.1 Sala de capacitación

- El acceso a la sala de capacitación está a cargo del Grupo de Gestión Administrativa. Las solicitudes se realizan a través de la Herramienta de Mesa de Servicio indicando la fecha, hora inicio, hora fin, tema, número de asistentes, elementos hardware y software requeridos y responsable. Una vez autorizado el uso de la sala de capacitación se debe notificar a la empresa de vigilancia para que realice la apertura y entrega de la sala en la fecha establecida.

- La empresa de vigilancia es la responsable de custodiar la llave de acceso a la sala de capacitación, hacer entrega de la sala (documentando las condiciones y elementos) y recibir la sala en las condiciones iniciales.
- Los equipos de cómputo asignados a la sala de capacitación se encuentran conectados a la red de datos y tienen asociada una única cuenta de usuario. Estos equipos de cómputo cuentan con permisos de acceso a Internet y a los recursos de la máquina, con restricción para la administración del mismo.
- Los equipos de cómputo asignados a la sala de capacitación deben permanecer con guaya y la clave debe ser administrada por el Grupo de Gestión Administrativa.

12 Lineamientos para la seguridad de equipos

Función Pública adopta los mecanismos que permiten evitar la pérdida, robo o daño de la plataforma tecnológica de la entidad a través de las siguientes directrices:

12.1 Equipos de cómputo

- La Oficina de Tecnologías de la Información y las Comunicaciones debe gestionar los mantenimientos preventivos y correctivos de la infraestructura del centro de cómputo y equipos de red.
- El Grupo de Gestión Administrativa realizará mantenimientos preventivos y correctivos a los equipos de cómputo de los usuarios, centros de cableado, periféricos, de comunicaciones y de seguridad de la entidad, de forma periódica según la programación establecida para cada vigencia.
- El Grupo de Gestión Administrativa seguirá el procedimiento de provisión de equipos de cómputo establecido por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Los equipos de cómputo y periféricos de Función Pública deben conectarse a la red eléctrica regulada. En caso de no tener red eléctrica en el área, se debe disponer de un regulador externo.
- Los equipos de cómputo de Función Pública contarán con una herramienta de protección contra software malicioso instalado y permanentemente actualizado (tanto en su versión de software como su base de amenazas), la cual permitirá:

    - Activación toda vez que se inicie sesión en el dispositivo y debe permanecer siempre activo
    - Escanear en busca de amenazas en cualquier medio removible (pendrive, discos duros, etc.) cuando sea conectado a alguna estación de trabajo.
    - Detectar código malicioso y notificada automáticamente.

- Los servidores públicos, pasantes y contratistas deben conectar los equipos de cómputo asignados por la entidad a la red de datos, con el fin de mantener actualizar

el software y actualizar el inventario de todos los equipos informáticos, licencias y configuración de los mismos. En caso de trabajar sin conexión a la red por largos periodos de tiempo, se entregará dicha relación al Grupo de Gestión Administrativa y a la Oficina de Control Interno para determinar las causas y tomar lo correctivos a que haya lugar.

- Para retirar equipos de cómputo asignados a servidores públicos, contratistas o pasantes de Función Pública de las instalaciones de la entidad se registrarán los datos en la planilla de ingreso y retiro de elementos provista por la empresa de seguridad. Una vez los equipos de cómputo se encuentren fuera de la entidad, su seguridad es responsabilidad de la persona no de la entidad.
- Función Pública dispondrá de una póliza que ampara los equipos de su propiedad en caso de daño o pérdida.
- Cuando un equipo de cómputo es solicitado en calidad de préstamo se debe realizar la solicitud a través de la Sistema de mesa de servicio indicando el motivo, fecha inicio y fecha fin. La solicitud debe ser autorizada por el Grupo de Gestión Administrativa acorde a la disponibilidad que se tenga.
- Los equipos portátiles de Función Pública deben entregarse con guaya de seguridad cuando sea viable la instalación de ésta y es responsabilidad de la persona que recibe el equipo, mantenerlo asegurado con la guaya provista.
- La empresa de seguridad es la encargada de ejercer vigilancia y control sobre los equipos eléctricos y electrofónicos de la entidad, que permanezcan en ella, o que ingresan o salgan de la misma.
- El ingreso y salida de elementos que conforman la infraestructura tecnológica de Función Pública (servidores, rack, impresoras, access point, discos externos, partes de computador, switches, aire acondicionado, televisores, micrófonos y teléfonos, entre otros) serán autorizados por el Grupo de Gestión Administrativa y registrados en la planilla de entrada y salida de elementos provista por la empresa de seguridad.
- Las personas externas a Función Pública que ingresen equipos de cómputo personales, deben registrarlos en la planilla de ingreso y retiro de elementos provista por la empresa de seguridad. La seguridad de los elementos ingresados es responsabilidad del propietario del equipo.
- La empresa de vigilancia informará al visitante que la entidad no se hace responsable por la pérdida o daño de los elementos personales que se ingresen a las instalaciones de la Entidad.
- Función Pública dispone en la zona de registro de visitantes de un mensaje informativo que indica al visitante que la Entidad no asume responsabilidad por la pérdida, hurto o daño de equipos propiedad de particulares.

12.2 Cámaras de video

Función Pública en cabeza de la Secretaría General autoriza la instalación de las cámaras de video en las instalaciones de la entidad para la captura y grabación de imágenes y video, como mecanismo de seguridad. El uso de cámaras fotográficas y celulares solo está autorizado para fines institucionales y cumple con los requisitos de la ley de protección de datos personales 1581 de 2012 y sus decretos reglamentarios.

- Función Pública dispone en la zona de registro de visitantes de un mensaje informativo que alerta a los funcionaros, contratistas, pasantes y visitantes de la existencia, naturaleza y propósitos del sistema de videovigilancia institucional.
- Función Pública cuenta con webcams ubicadas en las oficinas y pasillos de la entidad, que permiten grabar las actividades realizadas por los servidores públicos, contratistas, pasantes y visitantes, exceptuando el área de baños.
- La Secretaría General es la responsable de asignar el servidor público y autorizar al personal de seguridad para realizar monitoreo a las cámaras de video instaladas en la entidad, previo acuerdo de confidencialidad.
- En caso de un incidente de seguridad o por solicitud expresa de un director, jefe o coordinador de Función Pública, la Secretaría General y la empresa de vigilancia son los encargados de realizar la investigación sobre las imágenes y videos de la entidad.
- La Secretaría General en conjunto con la Oficina de Tecnologías de la Información y las Comunicaciones, son los responsables establecer los mecanismos de custodia de las imágenes y videos, así como de establecer los tiempos de retención de dicha información.

13 Lineamientos para seguridad de la gestión de comunicaciones y operaciones

La Entidad buscar busca asegurar la protección de la información en las redes y las instalaciones de procesamiento de información a través de una definición clara de responsabilidades y lineamientos, así:

13.1 Asignación de responsabilidades operativas

La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de:

- La administración de la infraestructura tecnológica de Función Pública.
- En conjunto con el Grupo de Gestión Administrativa, realizar mantenimiento preventivo y correctivo de los equipos alojados en el centro de cómputo: servidores, aire acondicionado, sistema de control de incendios y sistema de alimentación ininterrumpida -UPS.

- Administración del centro de cómputo, licenciamiento de software y provisión de la infraestructura tecnológica alojada en el centro de datos para el adecuado funcionamiento de los servicios de información.
- Disponer de los procedimientos relacionados con la administración y operación tanto de la de la plataforma tecnológica como de los servicios de información.
- Mantener custodiadas las claves de acceso a cada uno de los servicios de tecnología.
- Garantizar la seguridad de los recursos tecnológicos y de bases de datos.
- Proveer y mantener actualizada herramienta de protección contra software malicioso.
- Coordinar la instalación y configuración de la herramienta de protección contra software malicioso en los equipos del centro de datos.

El grupo de Gestión Administrativa es responsable de:

- Atender la mesa de servicio de TI de primer nivel.
- realizar el mantenimiento correctivo y preventivo de los centros de cableado, red eléctrica, computadores de escritorio, equipos portátiles, impresoras, televisores.
- Instalar, configurar y dar soporte a la herramienta de protección contra software malicioso en los equipos de cómputo de la entidad.

13.2 Protección contra software malicioso

- La OTIC dispondrá de herramientas de seguridad antimalware y antispam debidamente licenciadas, que minimizan el riesgo de contagio de software malicioso.
- La OTIC actualiza permanente el software antimalware, en caso de requerir deshabilitar dicho software se solicitará autorización al Comité Institucional de Gestión y Desempeño.
- Los servidores públicos, contratistas y pasantes no deben cambiar o eliminar la configuración del software antimalware configurada en los equipos de cómputo de propiedad de Función Pública. Solamente pueden realizar tareas de escaneo de virus en diferentes medios de almacenamiento.
- Los equipos de cómputo de propiedad de los contratistas deben contar con un software de antimalware licenciado y actualizado.
- Cuando el software de antimalware notifique que el equipo de cómputo o archivo se encuentra infectado, es responsabilidad de los servidores públicos, contratistas y pasantes ejecutar el escaneo y limpieza del software malicioso (malware).
- En caso de detectar o sospechar que el equipo de cómputo se encuentra infectado por software malicioso, es responsabilidad de los servidores públicos, contratistas y pasantes informar a través de la Sistema de Mesa de Servicio esta situación, para que se tomen las medidas pertinentes.

13.3 Respaldo de información y copias de seguridad

- Función Pública adoptó la Política de Respaldo, Custodia y Recuperación de la información, publicada en el Sistema Integrado de Gestión Institucional, la cual es de estricto cumplimiento y aplica a todos los sistemas de información y dispositivos de almacenamiento de datos que contengan información misional de la Entidad
- Estos lineamientos deben ser aplicados por todos los responsables de administrar, gestionar e interactuar con la infraestructura tecnológica y/o que tengan cualquier relación con información de la entidad incluidos terceros, los cuales debe adoptar la Política de Respaldo, Custodia y Recuperación de la información establecida por la Oficina de Tecnologías de la Información y las Comunicaciones.

13.4 Gestión de seguridad en la red

- Función Pública dispondrá en cada vigencia los recursos necesarios la correcta operación de la infraestructura tecnológica de red.
- La OTIC es la encargada de administrar la infraestructura de red y proporcionar la configuración necesaria para el cumplimiento de las funciones y/ actividades de cada área.
- La OTIC establece los mecanismos para proveer la disponibilidad y aseguramiento de la infraestructura de red de la entidad.
- La OTIC contará con mecanismos de seguridad que otorguen la protección necesaria ante amenazas y permita control del tráfico de entrada y de salida para la red LAN de la entidad.
- La OTIC mantendrá segmentada la red por centros de cableado y acceso WIFI.
- La OTIC define y comunica los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica.
- La OTIC garantiza la comunicación segura entre las redes internas y externas de Función Pública.

13.5 Gestión de medios removibles

- El uso de periféricos y medios de almacenamiento externo (memorias USB, CD, cámaras, discos de almacenamiento externo, tarjetas de memoria y tablets) están permitidos para los servidores públicos y pasantes, como apoyo al desarrollo de las funciones asignadas por Función Pública.
- Estás prohibido: i) el uso de periféricos y medios de almacenamiento externo para los visitantes; ii) almacenar y descargar software sin autorización del jefe inmediato, almacenar y iii) compartir información de carácter reservado en periféricos y medios de almacenamiento externo sin la autorización de Función Pública.
- Está prohibido almacenar y descargar en los dispositivos de almacenamiento externo: software licenciado de Función Pública, software no licenciado, juegos, audios,

videos, imágenes, información que atente con las normas legales e información confidencial o reservada sin previa autorización del jefe inmediato o supervisor.

- Es responsabilidad de Función Pública a través de la Oficina de Tecnologías de la Información y las Comunicaciones, concientizar a los servidores públicos, contratistas y pasantes de los riesgos del uso de periféricos y medios de almacenamiento externo, para propender por el uso adecuado de los mismos.
- Es responsabilidad de los servidores públicos, contratistas y pasantes hacer el uso adecuado de los periféricos y medios de almacenamiento, así mismo, de garantizar la seguridad de los activos de información de la entidad, dando cumplimiento a los criterios de confidencialidad, integridad y confiabilidad, de tal forma que se minimicen los riesgos.

14 Lineamientos para la transferencia e intercambio de información

A continuación, se definen las pautas y las reglas generales para la protección de la información durante su intercambio entre los funcionarios, contratistas o grupos de valor de la Entidad o entre la Entidad y partes externas, preservando las características de disponibilidad, integridad y confidencialidad.

14.1 Uso de internet

- Función Pública, en cabeza de la OTIC dispone de un canal de Internet que apoya el cumplimiento de las funciones de los servidores públicos y pasantes.
- El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas asignadas al funcionario, contratista o parte interesada. Ver ley 734 de 2002, por la cual se expide el Código Disciplinario Único. “Artículo 34, Deberes. Numeral 4: Deberes”
- El acceso al servicio de Internet podrá ser asignado a las personas que tengan algún tipo de relación con la Entidad, ya sea como funcionario, contratista o miembro de un grupo de valor. La autorización de uso del servicio de acceso a internet para los visitantes de las instalaciones de la Entidad debe ser solicitada por los responsables de procesos o dependencias que visita la persona.
- Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña para el DAFP y para los cuales este formal y expresamente autorizado.
- El acceso a servicios de redes sociales, video en línea, audio o servicios no directamente afectos a la función misional solo están autorizados a las dependencias cuya función misional requiere del servicio. La Entidad se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la OTIC
- Todo usuario del servicio de Internet es responsable de informar a su superior o la mesa de ayuda de la OTIC, el acceso vía Internet a contenidos o acceso a servicios que no le estén autorizados o no le correspondan para la ejecución de las funciones

asignadas. El responsable de la dependencia o proceso debe coordinar con la OTIC, el ajuste de los privilegios de acceso al servicio de navegación por Internet.

- Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que él envíe desde las redes de datos del DAFP o se descargue desde Internet usando su cuenta de acceso.
- La Entidad puede supervisar el uso y acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales. En los procesos verificación del uso apropiado del servicio de acceso a Internet se respetan los derechos a la intimidad y privacidad.
- Cuando un funcionario, contratista o miembro de grupo de valor al que le haya sido autorizado el uso de una cuenta de servicio de Internet o de acceso a la red local finalice su relación con la Entidad, debe seguir los procedimientos definidos por la OTIC para entregar su cuenta de usuario y accesos a servicios informáticos provistos.
- Es responsabilidad de los servidores públicos, contratistas y pasantes, salvaguardar la información de entidad, cumpliendo con los criterios de integridad, disponibilidad y confidencialidad. Así mismo, deben velar porque la información de la entidad sea protegida de divulgación no autorizada.

Para los servidores públicos, pasantes, contratistas y visitantes está prohibido:

- Intercambiar información de Función Pública con terceros sin previa autorización del jefe de área, supervisor o responsable de la información.
- Instalar software no licenciado.
- Descargar software no autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones.
- El ingreso a servicios interactivos, redes sociales y servicios de mensajería instantánea para fines personales.
- Descargar e intercambiar archivos de audio, juegos, video, imágenes y software de libre distribución.
- El ingreso a páginas relacionadas con violencia, pornografía, drogas, alcohol, web proxys, hacking o cualquier sitio web que puedan implicar compromiso de seguridad de la información.
- Visitar y/o realizar transacciones a través de páginas web de entidades bancarias o comerciales.

14.2 Convenios de interoperabilidad y transferencia de información

- La transferencia e intercambio de información para propósitos de interoperabilidad con grupos de valor se realiza conforme con la normatividad vigente
- Las condiciones técnicas para el intercambio de información deben ser definidas y aprobadas por la Oficina de las Tecnologías de Información y las comunicaciones

- Las condiciones administrativas para el intercambio de información deben ser definidas y aprobadas por el líder del proceso responsable del intercambio de información con el grupo de valor el cual se compartirá la información.
- Para el intercambio seguro de información se aplican los lineamientos de seguridad para interoperabilidad definidos por el Ministerio de las Tecnologías de Información y las Comunicaciones.

14.3 Uso del correo electrónico

La Función Pública en cabeza de la Oficina de Tecnologías de la Información y las Comunicaciones, dispone de un servicio de correo electrónico que apoya las actividades de los servidores públicos, contratistas y pasantes de la entidad.

- Los servidores públicos, contratistas y pasantes son responsables de todas las actividades realizadas con la cuenta de correo asignada por la entidad. Toda la información transmitida a través de la cuenta de correo es responsabilidad del propietario de dicha cuenta.
- El Grupo de Gestión Humana es el responsable de solicitar la creación, modificación y eliminación de las cuentas de correo para los servidores públicos y pasantes de la entidad.
- El Grupo de Gestión Contractual es el responsable de solicitar la creación, modificación y eliminación de las cuentas de correo para contratistas.

Está prohibido:

- Suministrar los datos de acceso o clave de la cuenta de correo asignada por la entidad.
- Utilizar la cuenta de correo asignada por la entidad, para actividades personales.
- Participar en la transmisión correos spam (cadenas).

14.4 Correos masivos

El servicio de correo institucional provisto por la oficina de las tecnologías de información y comunicaciones está configurado para prevenir el envío de correos masivos sin autorización.

El departamento administrativo de la función pública cuenta con un servicio de correo masivo que debe ser utilizado por las dependencias o los sistemas de información cuando el servicio de correo institucional no tiene la capacitad técnica para el envío de comunicaciones masivas.

Se debe considerar correo masivo cualquier envió de comunicaciones de correo electrónico que supera los límites técnicos contratados por la Entidad para sus servicios de correo electrónico institucional.

Cuando una dependencia o un sistema de información requieran enviar correos masivos a grupos de valor externos o internos, el responsable de la dependencia o el administrador del sistema de información deben

registrar una solicitud en el sistema de mesa de ayuda proactiva net para determinar si las comunicaciones se pueden enviar a través del correo institucional o mediante el servicio de correos masivos.

Los servicios de correo masivo que una dependencia o un sistema de información pueden usar se clasifican en:

- Correos masivos de contenido informativo o comunicativo.
    - Aquellos que difunden un contenido netamente informativo o comunicativo como los remitidos por la Oficina Asesora de Comunicaciones (Boletín Externo Sirvo a mi País, Revista Carta Administrativa, boletines o comunicados de prensa dirigidos a medios de comunicación y los mensajes informativos dirigidos a los servidores públicos).
- Correos masivos para recolección de datos personales o actualización de información personal
    - Aquellos orientados a informar al miembro del grupo de valor de la necesidad de actualizar sus datos personales en un sistema de información institucional o ante un punto de contacto en una dependencia. Correos masivos destinados a distribuir a miembros de los grupos de valor información técnica sobre los sistemas de información, como pueden ser: información sobre su cuenta de usuario, mecanismos para restablecimiento de correo, alta y baja de cuentas de usuario en sistemas de información.
- Cualquier envío de correo masivo debe estar aprobados por la Dirección o Subdirección del Departamento Administrativo de la Función Pública y ser revisados previamente por la Oficina Asesora de Comunicaciones y la Oficina de las Tecnologías de la Información.
- Todo correo masivo debe cumplir con los lineamientos de uso de imagen institucional definidos por la oficina asesora de comunicaciones, seguridad digital definidos por la oficina de tecnologías de información y comunicaciones y requisitos de sistema integrado de planeación y gestión.
- Todo correo masivo destinado al manejo de temas institucionales debe utilizar los formatos previamente aprobados y publicados en el Sistema Integrado de Gestión, los cuales tendrán los lineamientos de imagen y usabilidad definidos por la Oficina Asesora de Comunicaciones.
- Cuando se requiera solicitar información excepcional a los miembros de los grupos de valor, se deberá sustentar la motivación ante la Dirección o Subdirección de la entidad y deberá estar acompañada de una estrategia que abarque los aspectos comunicativos y tecnológicos, definidos con la Oficina Asesora de Comunicaciones y la Oficina de Tecnologías de información y comunicaciones. En el caso de comunicaciones masivas asociadas a uso de información estadística los lineamientos para su distribución son definidos por la Oficina Asesora de Planeación.
- Para evitar el riesgo de ser incluido en la lista negra o acusado de enviar correos no deseados, es crucial que tome las siguientes medidas:

- Está prohibida uso o recolección de correo electrónicos para el envío de comunicaciones masivas sin contar con la autorización del titular del dato en los términos descritos por la ley 1581 de 2012, salvo las excepciones previstas por la misma ley y sus decretos reglamentarios
- El envío de correos masivos a miembros de grupos de valor, solo se debe realizar si el destinatario está en la base de datos de correos masivos gestionada por la Oficina Asesora de comunicaciones, la cual debe contener la lista de todos los correos institucionales publicados por las diferentes entidades públicas y las direcciones de correo electrónico personal de miembros de grupos de valor que han autorizado su adición a la base de datos de correo masivos de la Entidad.
- Cuando el destinatario no cuente con un correo institucional, la dependencia interesada en enviarle correo masivo, debe tramitar previamente su autorización para inscripción voluntariamente a la base de datos de correo masivo. Si se obtiene la autorización se deben formalizar la actualización de la base de datos de correos masivos mediante un tiquete de mesa de ayuda ProactivaNet dirigido a la oficina asesora de comunicaciones.
- Todas las direcciones de correo electrónico para correos masivos deben ser validadas antes de utilizarlas y se deben descartar toda dirección errónea o duplicada.
- Todo mensaje enviado a través servicios de correo masivo deberá contar con un link para que los usuarios puedan desuscribirse (opt-out) de forma automática y con un solo clic cuando la dirección de correo electrónico no es institucional.
- Se deben cancelar automáticamente las suscripciones de los usuarios cuyas direcciones se rechacen más de 3 veces por error en la entrega.
- Todos los mensajes destinados a correo masivo deben tener un pie de página que identifique plenamente al departamento administrativo de la función pública como el remitente y el responsable por el contenido del mensaje. A su vez, el e-mail de respuesta deberá ser un email válido para que los receptores puedan responder el correo y esas respuestas puedan ser atendidas por la dependencia responsable de la comunicación
- La redacción de los correos electrónicos destinados a distribución masiva debe cumplir con los siguientes requisitos técnicos:
    - Usar el formato el estándar de Internet (RFC 5322).
    - Al redactar mensajes en formato HTML, se deben usar estándares HTML.
    - No se deben utilizar códigos HTML ni CSS para ocultar contenido en los mensajes de correo masivo
    - En los encabezados de remitente (De): de los mensajes masivos solo debe figurar una dirección de correo electrónico
    - Los enlaces que figuran en el cuerpo de los mensajes deben sean visibles y fáciles de entender, de modo que los usuarios sepan dónde les dirigirán cuando hagan clic.
- Los correos masivos deben seguir los lineamientos de la política de operación de la Oficina asesora de comunicaciones.

- Se debe preferir enviar los correos masivos desde la misma dirección IP. Si no es posible enviar los correos masivos desde una dirección IP única, se deberían utilizar direcciones diferentes para distintos tipos de mensajes, clasificando los mensajes por categorías de acuerdo con su contenido. (Ejemplo mensajes de los sistemas de información, mensajes de invitación a eventos, mensajes para recolección de información)
- Se debe configurar una dirección de correo para que los grupos de valor denuncien usos inadecuados del correo electrónico como suplantación, correos no deseados, confirmación de veracidad de comunicaciones recibidas.
- La oficina de las tecnologías de información y las comunicaciones debe verificar semanalmente que las direcciones IP y dominios de internet asignados a la Entidad no figuren reportadas en listas de correo no deseado y en caso de reporte negativo realizar los trámites para resolver el incidente ante los proveedores de servicios de Internet (ISP)
- Está prohibido realizar pruebas de ingeniería social o suplantación de identidad (phishing) usando las direcciones IP o los dominios web institucionales debido a las mismas pueden ser bloqueadas por intento de delito informático.
- Para minimizar el riesgo de que las direcciones IP y las direcciones de correo institucionales sean reportadas por SPAM la oficina de las tecnologías de información y las comunicaciones debe incluir dentro de los requisitos técnicos para la contratación de servicios de correo electrónico los siguientes controles técnicos:
  - Publicar el registro SFP del dominio de correo institucional Set up SPF to help prevent spoofing
  - Activar la firma DKIM en los mensajes. Use DKIM to validate outbound email sent from your custom domain
  - Publicar el registro DMARC del dominio institucional Use DMARC to validate email
  - Posibilidad de cancelar la suscripción a listas, cumpliendo con el RFC 2369. “The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields”

14.5 Acuerdos de confidencialidad

- La Función Pública establece acuerdos de confidencialidad e intercambio de información con terceros que manipulen, requieran o provean información física y/o digital de carácter reservado.
- Ver Intercambio Seguro de Datos con Entidades de Vigilancia y Control
- La Dirección Jurídica y el Grupo de Gestión Contractual, definen los acuerdos de confidencialidad y/o intercambio de información entre Función Pública y grupos de valor.

- El acuerdo de confidencialidad incluye compromisos adquiridos por Función Pública y terceros, penalidades de incumplimiento y destrucción de la información suministrada a los terceros una vez se haya culminado el contrato o convenio.
- El Grupo de Gestión Documental es el responsable de proporcionar los lineamientos para el intercambio de información física con terceros.
- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de proporcionar los lineamientos para el intercambio de información digital con terceros de manera segura con el fin de proteger la información de manipulación, modificación y divulgación no autorizada.
- El grupo de Grupo de Gestión Contractual es el responsable de realizar el acompañamiento a las diferentes áreas de la entidad para que se garantice la inclusión de los acuerdos de confidencialidad en los contratos o convenios que lo requieran.

14.6 Borrado seguro

- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de gestionar el procedimiento de borrado seguro.
- El Grupo de Gestión Administrativa en cabeza de la mesa de servicio de primer nivel, es el responsable de realizar el borrado seguro acorde al procedimiento establecido por la Oficina de Tecnologías de la Información y las Comunicaciones. En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, éste hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente.
- Al finalizar la vida útil o determinar que ya no son necesarios para las labores institucionales, los medios de almacenamiento de equipos de cómputo, medios de almacenamiento extraíbles como discos externos, discos ópticos u otros medios que puedan contener información institucional, deben ser sometidos a borrado seguro que impida su recuperación de información.
- En caso de imposibilidad tecnológica de aplicar borrado seguro, los medios deben ser sometidos a destrucción siguiendo las políticas de manejo de residuos electrónicos institucionales

14.7 Gestión de cambios

- Los cambios en la infraestructura tecnológica y servicios de información en Función Pública se deben realizar de acuerdo con el procedimiento establecido por la Oficina de Tecnologías de la Información y las Comunicaciones. Ver: Gestión de Cambios

- Es responsabilidad de las áreas que publican o actualizan contenidos en los sitios web de la entidad, designar los gestores de contenido (Web Locales) responsables del manejo, mantenimiento, consulta, ingreso, modificación, eliminación y/o divulgación, de la información almacenada en los sitios web que les corresponda.

15 Lineamientos para el control de acceso a la información

Función Pública regula el tratamiento de datos personales y acceso a la información de acuerdo con su Política de tratamiento de datos personales que se encuentra publicada en la página web de la entidad www.funcionpublica.gov.co solamente a los legítimamente autorizados. Dentro de estos lineamientos cabe resaltar:

Responsabilidad

- Los líderes de los procesos institucionales, los jefes de dependencia y demás servidores públicos servidores públicos, así como los pasantes y contratistas de la entidad, son los responsables de cumplir y hacer cumplir los lineamientos establecidos en el proceso de gestión documental en todo lo relacionado con la administración de los documentos y registros, tanto físicos como electrónicos de la entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de implementar controles de acceso a los servicios de información e infraestructura tecnológica. Es responsabilidad de los dueños de los servicios de información restringir el acceso a los servidores públicos, pasantes y contratistas de acuerdo con las funciones y/o actividades a realizar.
- Los responsables de los activos de información son los encargados su protección y uso mientras estén en su custodia ya sea física o electrónica. Así mismo, es responsable de establecer las restricciones de uso, alteración y divulgación.

15.1 Organización de documentos electrónicos

- El Grupo de Gestión Documental define los lineamientos para la organización de documentos electrónicos, los cuales son de obligatorio cumplimiento y se encuentra publicado en el Sistema Integrado de Gestión – SGI. Ver Lineamientos organización documentos electrónicos
- Para la administración de los permisos sobre el servidor de archivos compartidos donde se alojan las carpetas asociadas a las Tablas de Retención Documental – TRD, es responsabilidad del servidor público asignado por cada director o jefe de área.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de capacitar a los servidores públicos a cargo de la administración de las carpetas asociadas a la TRD en el servidor de archivos compartidos.

15.2 Gestión de acceso al usuario

- El Grupo de Gestión Humana es el responsable de solicitar la creación, modificación y eliminación de las cuentas usuarios relacionadas con servidores públicos y pasantes, a través de la herramienta mesa de servicio.
- El Grupo de Gestión Contractual es la responsable de solicitar la creación, modificación y eliminación de las cuentas usuarios relacionadas con los contratistas, a través de la herramienta mesa de servicio.
- Los líderes funcionales de los sistemas de información, aplicaciones y portales son los responsables de la administración de los usuarios.
- Los líderes técnicos de los sistemas de información, aplicaciones y portales son los responsables de establecer los lineamientos de seguridad que se deben aplicar y velar por su cumplimiento.
- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de establecer y divulgar los lineamientos de seguridad a nivel de infraestructura tecnológica.

15.3 Control de acceso a la red

- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de implementar los protocolos de seguridad e la infraestructura de red local, que permitan acceder a los recursos de manera segura.
- Con el propósito de proteger los equipos de cómputo, equipos de comunicaciones y demás dispositivos tecnológicos de Función Pública, no se permite la conexión a la infraestructura de red local de la entidad a los equipos de cómputo y de comunicaciones propiedad de terceros sin previa autorización del director, jefe, coordinador o supervisor de contrato, mediante la solicitud realizada por medio del Sistema de Mesa de Servicio.
- Los servidores públicos, contratistas y pasantes pueden acceder a la infraestructura red local de la entidad a través de conexión LAN y WIFI, utilizando el equipo de escritorio o portátil asignado por la entidad, el usuario asignado y clave.
- Se pueden conectar a los recursos de conexión remota – VPN los servidores públicos y contratistas previamente autorizados por el director, jefe, coordinador o supervisor de contrato, solicitud que debe realizarse a través de la Sistema de mesa de servicio a la Oficina de Tecnologías de la Información y las Comunicaciones.
- Cuando se requiera la habilitación de una VPN para usuarios externos a la entidad, dicha solicitud debe realizarse por medio del Sistema de Mesa de Servicio, anexando el acuerdo de confidencialidad y la aprobación de la entidad externa del usuario que requiere el acceso a VPN con la debida justificación, fecha inicio y fin.

15.4 Control de acceso al sistema operativo

- La Oficina de Tecnologías de la Información y las Comunicaciones se asegura que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos de la infraestructura tecnológica y bases de datos sean modificados y asegurados al ingresar a la infraestructura de la entidad y periódicamente.
- El Grupo de Gestión Administrativa se asegura que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos y software instalado en los computadores de escritorio, equipos portátiles, impresoras y demás dispositivos adquiridos por la entidad sean modificados antes de entrar en uso. Dichos elementos deben entregarse sin permisos de acceso al sistema operativo.
- La Oficina de Tecnologías de la Información y las Comunicaciones se asegura que desde los sistemas de información, aplicaciones y portales no se acceda directamente a los sistemas operativos.
- La Oficina de Tecnologías de la Información y las Comunicaciones a través de la Sistema de mesa de servicio debe realizar monitoreo periódico del software instalado en los equipos de cómputo conectados a la red de Función Pública.

15.5 Control de acceso a aplicaciones e información

- Las áreas propietarias de los sistemas de información, aplicaciones y portales de Función Pública con el apoyo de la Oficina de Tecnologías de la Información y las Comunicaciones son responsables de mantener actualizados los privilegios de acceso a los sistemas de información de sus usuarios.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de garantizar la seguridad de la plataforma tecnológica donde se encuentran alojados los sistemas de información, aplicaciones y portales de Función Pública.
- Los directores y jefes designan al servidor público que es responsable del manejo funcional del cada sistema de información, aplicación y portal de Función Pública.
- El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones es el encargado de designar el servidor público y/o contratitas responsables de atender los requerimientos realizados por un área funcional para un determinado sistema de información, aplicación o portal de Función Pública.
- Los líderes funcionales y técnicos deben seguir los lineamientos establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones publicados en el Sistema Integrado de Gestión SIG – documento “Responsabilidades del líder funcional y líder técnico”.

15.6 Gestión de contraseñas

- Las contraseñas o claves de acceso a los activos de información son personales e intransferibles.

- Toda acción realizada con el usuario y contraseñas asignadas es responsabilidad del funcionario, contratista, pasante o tercero al que se le ha asignado.
- Las contraseñas deben cambiarse mínimo una vez al mes y seguir los lineamientos institucionales para una contraseña segura.
- Las contraseñas no deben ser divulgadas o compartidas entre usuarios. Cualquier daño o alteración de la información es responsabilidad del usuario que la realizó.
- No se debe prestar el usuario asignado ni la contraseña, ya que, en caso de haber alguna violación de seguridad, la responsabilidad recae sobre la persona a cargo de dicho usuario.
- Las contraseñas sede deben construir de acuerdo con las guías e instrucciones que emita la Oficina de Tecnologías de Información y Comunicaciones

Lineamientos para una contraseña segura

- Utilizar al menos 12 caracteres para crear la clave.
- Debe incluir números, mayúsculas, minúsculas y símbolos
- Se debe utilizar caracteres que alternen aleatoriamente mayúsculas y minúsculas.
- Elegir una contraseña que pueda recordarse fácilmente y que pueda digitarse rápidamente (preferiblemente sin que sea necesario mirar el teclado).
- Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios de información.
- No se debe utilizar información personal en la contraseña (nombre del usuario, nombre de familiares, apellidos, apodos, fecha de nacimiento, número de documento, número de teléfono, nombre de mascotas, actores preferidos).
- Evitar utilizar secuencias básicas de teclado. Por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” o “98765”.
- No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar las claves de acceso en documentos de texto o en el celular sin el debido aseguramiento por cifrado.
- No enviar la contraseña por correo electrónico o mensajes de texto.

16 Lineamientos para la adquisición, desarrollo y mantenimiento de sistemas de información

A través de lineamientos generales para el desarrollo seguro, mantenimiento y adquisición de software al interior del Departamento Administrativo de la Función Pública se definen los controles de seguridad en el desarrollo de código fuente, así:

16.1 Establecimiento de los requisitos seguridad de los sistemas de información

- La OTIC es la responsable de dar cumplimiento a los estándares de seguridad establecidos con los líderes funcionales de los sistemas de información y aplicaciones.
- Para los sistemas de información, aplicaciones y portales que manejen datos confidenciales o reservados, los líderes funcionales y técnicos de los servicios deben velar por el cumplimiento de los controles de seguridad que garanticen la preservación de la confidencialidad e integridad de la información.
- La OTIC establece los lineamientos de seguridad de la infraestructura tecnología, que garantice el cumplimiento de los controles y la salvaguarda de la información de manera segura.
- Los líderes técnicos de los sistemas de información, aplicaciones y portales de la entidad deben asegurar que desde los sistemas de información, aplicaciones y portales no se permita la modificación de parámetros a nivel de sistema operativo y software base. Así mismo, se debe garantizar que no se visualicen en pantalla ni se almacene en base de datos las contraseñas con cadenas de conexión e información en texto plano.
- Está prohibida la manipulación de información directamente desde la base de datos. Si en algún momento se requiere realizar ajustes directamente en la base de datos, deberá dejarse el registro en la Sistema de mesa de servicio con la aprobación del propietario del activo de información o jefe del área.
- Los líderes técnicos de los sistemas de información, aplicaciones y portales de la entidad deben asegurar que la información establecida como reservada, cuente con mecanismos seguridad necesarios que eviten su alteración o borrado por personal no autorizado.
- Los desarrolladores Internos y Externos deben asegurarse de que los controles criptográficos, de los sistemas de información desarrollados para Función Pública, cumplan con los lineamientos o directrices establecidos por la OTIC.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de mantener licenciado el software institucional necesario para el desarrollo y puesta en producción de los sistemas de información, aplicaciones y portales.
- La OTIC debe asegurase que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un adecuado licenciamiento y se debe especificar las condiciones de uso del software y los derechos de propiedad patrimoniales. Una vez recibido por la entidad se debe dejar registro en almacén para que ingrese al inventario de activos.

16.2 Desarrollo seguro, pruebas y soporte

Función Pública vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad y buenas prácticas para desarrollo seguro y pruebas de aceptación de los Sistemas de Información, Aplicaciones y Portales desarrollados. Así mismo, se asegura que el software desarrollado o adquirido cuente con el nivel de soporte requerido por la Entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de:

- Establecer la metodología para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- Seguir los lineamientos establecidos en el "Procedimiento para el Desarrollo y Mantenimiento de Software".
- Disponer de una herramienta para el control de versiones que permita a los desarrolladores llevar el control de versiones del software desarrollado.
- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- Asegurar la infraestructura tecnología necesaria para la puesta en producción de los sistemas de información, aplicaciones y portales, ya sean nuevos o ajuste a los existentes.
- Ofrecer soporte especializado a los sistemas de información, aplicaciones y portales a través de la Sistema de mesa de servicio.
- Realizar monitoreo periódico del soporte especializado a los sistemas de información, aplicaciones y portales.

Los líderes técnicos y desarrolladores de los sistemas de información, aplicaciones y portales de la entidad son responsables de:

- Velar por que los desarrolladores internos y externos implementen los lineamientos de seguridad, de tal forma que se controle el acceso no autorizado a éstos.
- Considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Mantener actualizada la documentación (desarrollo interno o externo) de acuerdo a la lista de chequeo de la documentación de los sistemas de información, donde se establece los documentos mínimos exigidos dependiendo de su clasificación.
- Garantizar que el desarrollo se realice con herramientas y software debidamente licenciado por Función Pública.
- Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como captcha o el ingreso de parámetros adicionales de verificación.

- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos en idioma español.
- Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- Definir el servicio y los acuerdos de niveles de servicio para la atención de incidencias y peticiones a nivel técnico.
- Proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de Función Pública; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Garantizar que los sistemas de información, aplicaciones y portales sean compatibles con los protocolos IPv4 e IPv6.
- Si el contratista requiere la utilización de software libre, software gratuito o software licenciado que no esté contemplado desde el inicio de las especificaciones, debe solicitar a la Oficina de Tecnologías de la Información y las Comunicaciones la autorización para utilizarlo. De no ser así, incurre en falta grave y puede ser rechazado el producto o servicio ofrecido, dando a lugar incumplimiento en las obligaciones del contrato.

Los líderes funcionales y propietarios de los sistemas de información, aplicaciones y portales de la entidad son responsables de:

- Definir los requerimientos funcionales de los sistemas de información.

- Una vez aprobados los requerimientos funcionales, cualquier ajuste se debe realizar por control de cambios para el análisis respectivo, para su aprobación o rechazo. En caso de ser rechazado el ajuste se debe anexar la debida justificación.
- Realizar las pruebas de funcionales para el recibo a satisfacción para paso a producción. El recibo a satisfacción debe quedar documentado.
- Aprobar las migraciones a producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.
- Realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.
- Definir el servicio y los acuerdos de niveles de servicio para la atención de incidencias y peticiones a nivel funcional.

17 Lineamientos para la gestión de la continuidad del negocio

El departamento administrativo de la función pública (DAFP) adopta los siguientes lineamientos para que la gestión de la seguridad de la información este alineada e incluida dentro de los planes de continuidad de negocio y la estrategia de recuperación ante desastres:

- La Oficina Asesora de Planeación coordinará el establecimiento y revisión anual del Plan de Continuidad del Negocio institucional, mediante la identificación de los eventos que constituyen una emergencia o desastre, elaborando con el oficial o el encargado de Seguridad y los responsables de los activos de información de la entidad, los planes de contingencia que permitirán mitigar los efectos adversos de un evento y disminuyendo los riesgos de afectación de las operaciones. Ver: Plan de recuperación de desastres tecnológicos
- El Comité Institucional de Gestión y Desempeño es el responsable de promover la definición del Plan de continuidad del Negocio, así como vigilar por su divulgación, cumplimiento mejora continua. Documento técnico - Plan de Continuidad
- Los directores y jefes de cada dependencia junto con los responsables de los activos de información, deben garantizar la aprobación, pruebas y revisión periódica de los planes de contingencia de los servicios a cargo.
- A través de su proceso de gestión de tecnologías de información Función Pública, mantienen, prueba y mejora su plan de continuidad de negocio.

El comité institucional de gestión y desempeño:

- Identificar y evaluar las situaciones que serán consideradas como emergencia o desastre para Función Pública y autorizar la activación de planes de manejo de emergencias o continuidad de negocio.
- Fijar los lineamientos de respuesta ante incidentes de seguridad y desastres.

- Liderar la activación del plan de continuidad del negocio y la recuperación ante cualquier tipo de desastre.
- Evaluar y hacer seguimiento a los resultados de las pruebas periódicas del plan de recuperación ante desastres o continuidad de negocio.

La Oficina de Tecnologías de Información y las comunicaciones:

- Elabora el plan de recuperación ante desastres, para el centro de cómputo de la entidad y un plan de contingencia para cada uno de los servicios, sistemas operativos y recurso informático existente. Ver
- Participa en las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos al Comité Institucional de Gestión y Desempeño.
- Formula las mejoras a los planes de contingencia y recuperación ante desastres de acuerdo con los resultados de las pruebas efectuadas
- Lidera la aplicación del plan de recuperación ante desastres y apoya dentro de su competencia a las dependencias en la ejecución de sus planes de contingencia

Las dependencias de la Entidad:

- Participan de la elaboración del plan de contingencia, para los servicios y productos a su cargo.
- Participan en las pruebas de contingencia de servicios planificadas y efectuadas, notificando los resultados obtenidos al Comité Institucional de Gestión y Desempeño.
- Formulan las mejoras a los planes de contingencia de acuerdo con los resultados de las pruebas efectuadas
- Lideran la aplicación del plan de contingencia a su cargo y apoyan, dentro de su competencia, a las dependencias en la ejecución de sus planes de contingencia

El responsable o delegado de seguridad de la información:

- Apoya la realización de los análisis de impacto a negocio análisis de riesgos de continuidad.
- Propone estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio
- Contempla los controles de seguridad de la información que se deben adoptar en caso de ser necesario activar el plan de continuidad o recuperación ante desastres

18 Lineamientos de controles criptográficos

Con estas acciones la entidad busca asegurar el uso apropiado y eficaz de la criptografía para preservar la confidencialidad e integridad de la información institucional, así:

- Función Pública en cabeza de la OTIC vela por que toda información digital, etiquetada como reservada y clasificada sea cifrada cuando se transmita, almacene y recibida, garantizando la preservación de la confidencialidad e integridad de la misma.
- La OTIC define, implementa y comunica los estándares para la aplicación de controles criptográficos.
- La OTIC vela por que los desarrolladores internos y externos que diseñan desarrollan y/o implementan sistemas de información, aplicaciones y/o portales donde se maneje información digital reservada o confidencial, cuente con mecanismos de cifrado de datos. Para los sistemas de información, aplicaciones y/o portales ya desarrollados que no cuentan con mecanismos de cifrado de datos, se debe hacer el análisis del impacto y el plan para su implementación. Si no es posible su implementación, se debe llevar el riesgo al Comité de Gestión y Desempeño para su respectivo análisis.

19 Lineamientos para la gestión de vulnerabilidad técnica

El objetivo de estas directrices es prevenir la ocurrencia de eventos e incidentes de seguridad de la información generadas por el aprovechamiento de vulnerabilidades técnicas por parte de atacantes, las cuales se definen a continuación:

- El responsable de seguridad realiza un análisis de vulnerabilidades periódica de los servicios y análisis de riesgos de los activos de información. Como resultado del análisis, se establece un plan de tratamiento de riesgo acorde con los recursos técnicos y financieros con los que se cuente, a fin de cerrar las brechas de seguridad encontradas.
- El responsable de Seguridad es el encargado de dar lineamientos y recomendaciones para la mitigación de las vulnerabilidades.
- El responsable de Seguridad y el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, establecen la prioridad en la ejecución de los controles dentro de la declaración de aplicabilidad y los responsables de su ejecución.
- El Comité de Gestión y Desempeño establece el procedimiento y los protocolos para la gestión de incidentes de seguridad, el cual debe seguirse cuando se considere que un incidente es causado por una falla de seguridad.

20 Lineamientos de gestión de incidentes de seguridad de la información

Con el fin de gestionar adecuadamente los eventos e incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información, Función Pública, adopta, implementa, mantiene y mejora un procedimiento de gestión de incidentes de seguridad de la información, (ver Gestión de Incidentes de Seguridad de la Información) el cual se complementa con los siguientes lineamientos:

- Todos los servidores públicos, contratistas o pasantes deben reportar sin demoras injustificadas a los responsables de sus dependencias, o a los responsables de los procesos o la Oficina de Tecnologías de Información y Comunicaciones cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información.
- El reporte de los eventos o incidentes de seguridad de la información se realiza de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información en la mesa de ayuda de la Oficina de Tecnologías de Información y Comunicaciones.
- La evaluación de los diferentes eventos e incidentes de seguridad de la información es realizada por la mesa de ayuda de la OTIC. Los eventos de seguridad de la información que sean calificados como incidentes se seguridad de la información se administran mediante el procedimiento de gestión de incidentes de seguridad de la información.
- La Entidad evaluará como incidentes de seguridad de la información eventos asociados a: incumplimiento de las políticas de seguridad de la información los que correspondan a delitos informáticos calificados como tales por la normatividad vigente y los eventos que materialicen riesgos de seguridad digital.
- El procedimiento de gestión de incidentes de seguridad de la información define las acciones específicas para el reporte de eventos, incidentes o debilidades en seguridad de la información, evaluación y respuesta ante incidentes de seguridad de la información, aprendizaje y recolección de evidencias asociadas a los incidentes de seguridad de la información.

20.1 Acerca de la gestión de seguridad de la información

- La Política de Seguridad de la Información se desarrolla y actualizada en cada vigencia de acuerdo con los riesgos, los requerimientos institucionales y la normatividad colombiana, atendiendo las nuevas necesidades, la situación de la entidad y las mejores prácticas de la industria.
- El Comité de Gestión y Desempeño Institucional y el encargado de Seguridad de la Información Institucional: i) Identifican las situaciones que serán consideradas como emergencia o desastre para Función Pública, ii) definen las actuaciones ante la presencia de incidentes de seguridad y desastres, iii) coordinan los temas relacionados con la continuidad del negocio y la recuperación ante cualquier tipo de desastre, iv) aseguran la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y documentando el resultado de dichas pruebas.
- El responsable de Seguridad de la información del departamento administrativo de la función pública realiza los análisis de impacto a la entidad y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio, con las consideraciones de seguridad de la información a que sean pertinentes tener en cuenta.

- Garantiza que los planes de contingencia incluyan las consideraciones de seguridad de la información necesaria y requerida, para el cumplimiento de los objetivos trazados.
- La OTIC y el Profesional de Seguridad de la Información elaboran un plan de recuperación ante desastres para el centro de datos de la entidad y un plan de contingencia para cada uno de los servicios, sistemas operativos y recurso informático existente.
- La OTIC y el Profesional de Seguridad de la información coordinan las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos al Comité Institucional de Gestión y Desempeño.

20.2 Reporte y tratamiento de incidentes de seguridad

- Función Pública promoverá entre los servidores públicos y contratistas el reporte de incidentes relacionados con la seguridad de la información y los medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.
- La Entidad asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
- De acuerdo con los criterios definidos en el procedimiento de gestión de incidentes, la Entidad puede declarar la activación de los planes para el tratamiento de situaciones de crisis (continuidad de negocio, recuperación ante desastres). Las acciones de tratamiento de las situaciones de crisis se gestionan mediante el Documento Técnico de del Plan de Continuidad de negocio.
- El director, subdirector o Secretario General son los únicos autorizados para reportar incidentes de seguridad ante las autoridades o delegar este reporte en otro funcionario; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas sobre incidentes de seguridad de la información.
- Los propietarios de los activos de información deben informar a la Oficina Asesora de Planeación, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Teniendo en cuenta que el encargado de la seguridad de la información hace parte de la Oficina Asesora de Planeación, es responsabilidad del jefe de la Oficina Asesora de Planeación:

- Establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Evaluar todos los incidentes de seguridad de acuerdo con las circunstancias particulares y escalar a la Oficina de Tecnologías de la Información y las

Comunicaciones y al Comité Institucional de Gestión y Desempeño, aquellos que considere pertinente.

- Designar un servidor público o contratista calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.
- Crear bases de conocimiento para los incidentes de seguridad presentados con las respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros. Lo anterior con el apoyo con la Oficina de Tecnologías de la Información y las Comunicaciones, la Dirección de Gestión de Conocimiento y la Secretaría General.
- Una vez materializado, convocar al Comité de Crisis para evaluar el incidente, tomar las medidas a que haya lugar y generar un plan de mejoramiento para evitar nuevamente su ocurrencia.

21 Lineamientos para el cumplimiento de requisitos legales y contractuales

Con la identificación de estos lineamientos se pretende evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad de la información, por lo tanto:

- Para la elaboración de las políticas del Sistema de Gestión de Seguridad de la Información de Función Pública, se tomarán como base los requisitos legales en materia de seguridad de la información, la política de gobierno digital controles y requisitos identificados en el Modelo de Seguridad y Privacidad de la información de MINTIC y estándar ISO/IEC 27001.
- Las políticas incluidas se constituyen como parte fundamental del Sistema de Gestión de Seguridad de Función Pública y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.
- La seguridad de la información es una prioridad para Función Pública y, por lo tanto, es responsabilidad de todos los servidores públicos, contratistas y pasantes cumplir con lo establecido en la Política de Seguridad de la Información, de tal forma que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.
- Las actualizaciones sobre la política del Sistema de Gestión de Seguridad de la Información se publicarán en el Sistema Integrado de Planeación y Gestión - SIPG (Intranet).
- La entidad verifica permanentemente sus obligaciones legales en materia de seguridad de la información y documenta dichas revisiones mediante la matriz de obligaciones legales
- Los derechos de propiedad e intelectual se respetan y garantizan a través de procedimientos documentados en los procesos de Tecnologías de Información, gestión de recursos, Comunicación, y Evaluación Independiente

- De conformidad con sus obligaciones en materia de protección de datos personales, la entidad ha adoptado la Política de Tratamiento de la Información de Datos Personales desde su proceso de servicio al ciudadano.

Esta política hace parte fundamental del Sistema Integrado de Planeación y Gestión de la Entidad -SIPG- y es comunicada de manera permanente a todos los servidores públicos y partes interesadas en su versión vigente a través del portal web y la intranet.

Políticas Técnicas de Seguridad de la Información

VERSIÓN 05
Proceso de Tecnologías de la Información
OCTUBRE DE 2021

Departamento Administrativo de la Función Pública
Carrera 6 n.º 12-62, Bogotá, D.C., Colombia
Conmutador: 7395656 Fax: 7395657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Línea gratuita de atención al usuario: 018000 917770
Bogotá, D.C., Colombia.