Función Pública

Política Especificas de Seguridad de la Información

Proceso de Tecnologías de la Información

Departamento Administrativo de la Función Pública

Versión 08

Diciembre 2024

Versión	Fecha de versión	Descripción del cambio
7	2024-07-03	Atendiendo los lineamientos de Gobierno, Ley 2345 del 2023 y Directiva Presidencial 06 del 19 de junio del 2024, Función Pública adelanta una estrategia con el fin de realizar el cambio de la imagen institucional.
8	2024-12-16	Ingreso proceso de retest (re-prueba o prueba de regresión) para las prácticas esenciales dentro de las pruebas de software, especialmente en los ciclos de desarrollo ágiles, ya que permite garantizar que los defectos se solucionen correctamente y que el software siga funcionando como se espera después de las correcciones.

Función Pública

Contenido

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 las políticas internas de seguridad de la información plasmada en este Manual de Seguridad de la Información, busca:

- Definir lineamientos, controles, roles perfiles y responsabilidades para la gestión de la información.
- Gestionar al máximo las amenazas a los sistemas de información, control y gestión.
- 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 internas de 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, aseguramiento 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 la Política General de

Seguridad de la Información, los procedimientos y guías vigentes del proceso de Tecnologías de la Información y cultura organizacional, como instrumento para orientar la implementación de la cultura asociada 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.

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.

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 y cuando se considere necesario 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.

Alcance

El presente documento inicia estableciendo los lineamientos de parte de seguridad de la información y aplicables desde seguridad informática en los activos de información propios del DAFP, se establecen los lineamientos de seguridad desde las políticas definidas, para que toda la información gestionada este protegida y segura para que sea disponible y que se le brinde garantía de continuidad operativa, integra y confidencialmente protegidas, por y para todos los servidores públicas, contratistas, proveedores, terceros y demás ciudadanos asociados al DAFP. Esto en ambientes de ciberseguridad, locaciones físicas principales y/o secundarias e incluye el tratamiento de datos personales y aplica en todo el ciclo de vida de la información.

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, de la misma manera que la infraestructura que soporta la información y así mismo las locaciones que resguardan la infraestructura y la información física.

Glosario

Activos de información: Bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información) asociados(as) a seguridad de la información[1].

[1] ISO/IEC 27000:2018

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Amenaza: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización[2].

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo[3].

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[4].

Control: 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

[2] ISO/IEC 27000:2018
[3] ISO 31000:2018
[4] ISO/IEC 27000:2018

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[5].

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de ocurrencia[6].

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Identificación del riesgo: Proceso para encontrar, numerar y caracterizar los elementos del riesgo[7].

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013 y tercera publicación en 2022.

Integridad: Propiedad de la información relativa a su exactitud y completitud[8].

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[9].

Seguridad de la información: Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información en general.

[5] ISO/IEC 27000:2018
[6] ISO 31000:2018
[7] ISO 31000:2018
[8] ISO/IEC 27000:2018
[9] ISO 31000:2018

SGSI: Sistema de Gestión de Seguridad de la Información. Es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Propósito

Describir los lineamientos aplicables de seguridad que se consideran políticas cumplibles para que la información sea protegida de manera efectiva.

Normatividad aplicable

En este sentido el marco de referencia normativo se encuentra detallado en la POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION, publicado en la página principal de la entidad.

Generalidades

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.

Responsabilidad por contravención de la política de seguridad

Los incumplimientos de las políticas de seguridad de la información descritas en este documento se tratan mediante el procedimiento de incidentes de seguridad de la información y se tomaran acciones de acuerdo con la naturaleza del incidente, y los resultados de su tratamiento e investigación permitirá a 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 y así mismo se iniciarán las acciones operativas, tecnológicas y de continuidad requeridas, las cuales contaran con la participación del responsable de control interno y de control disciplinario, para este caso y en caso de requerirlo la cadena de custodia se ejecuta según los lineamientos del Manual de la cadena de custodia, publicado por la Fiscalía General de la Nación.

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 servidores públicos o mediante los criterios definidos en los contratos de prestación de servicios en el caso de contratistas.

Es de tener en cuenta que, 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.

Responsabilidad de la OTIC

La Oficina de Tecnologías de la Información y las Comunicaciones- OTIC es la responsable de cumplir los lineamientos para la incorporación, uso y apropiación de las tecnologías de la información y las comunicaciones que soporten las operaciones propias del DAFP de manera que se brinde la seguridad a la información y la protección de los datos personales, mediante la aplicación de las configuraciones necesarias para este fin.

Así mismo, es responsable del desarrollo de proyectos tecnológicos orientados al cumplimiento de los objetivos institucionales que asocien el aseguramiento necesario para evitar la materialización de riesgos. Así mismo, es la responsable de gestionar de manera integral las tecnologías de la información en la entidad, prestando servicios acordes a las necesidades de la misma, contribuyendo al desarrollo y al logro de las metas misionales, estratégicas y de apoyo evitando incidentes de seguridad que interrumpan el normal desarrollo operativo del DAFP.

Responsabilidad de los servidores públicos, contratistas y/o terceros relacionados al DAFP

El cumplimiento de la política de seguridad de la información de todos los procesos es obligatorio y será compromiso de cada usuario acatar las directrices establecidas para el desarrollo de sus funciones.

Las excepciones a cualquier cumplimiento de la política de operación del proceso de tecnologías de la información y las comunicaciones deben ser aprobadas por el líder de Oficina de Tecnologías de la Información y las Comunicaciones y deben ser formalmente documentadas, registradas, revisadas y aprobadas.

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. ✓ Reportar al director, respecto a oportunidades de

Rol	Responsabilidad
	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***	✓ 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

Rol	Responsabilidad
seguridad de la información	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. ✓ 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

Rol	Responsabilidad
	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 seguridades 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.

Rol	Responsabilidad
Propietarios de los activos de la informacióninstitucional. **Directores, Jefes de Área y Coordinadores degrupo**	✓ 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 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

Rol	Responsabilidad
	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 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.

Rol	Responsabilidad
Grupos de valor y usuarios internos. usuarios de la información y de los sistemas de 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.
Procesamiento de la información	✓ 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

Rol	Responsabilidad
	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.

Lineamientos específicos de seguridad de la información

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:

Responsabilidades

- ✓ 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 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 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.

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 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.

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.

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 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.

Políticas específicas

Política de control de acceso

El DAFP emite un control de acceso a la información, todos los involucrados en el alcance deberán acatar lo siguiente:

Asignar un nombre de usuario para conceder el acceso a los sistemas de información.

Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud a Gestión Humana. Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.

- ✓ Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal (Servidores públicos, contratistas y/ proveedores) que ya no tenga relación con la DAFP, esta revisión la realiza la mesa de ayuda y según los hallazgos

OTIC realiza la depuración según el informe correspondiente. Por tanto, se realizar revisiones periódicas en los diferentes sistemas del DAFP para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.

- ✓ Cada uno de los Servidores públicos, contratistas y/ proveedores del DAFP deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.
- ✓ Cada uno de los Servidores públicos, contratistas y/ proveedores del DAFP, no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

Política de seguridad para proveedores

Acorde al establecimiento de los requisitos de seguridad establecidos asociados a los productos y/o servicios contratados; criterios que dependen de la importancia de los datos y de la información gestionada, transmitida, compartida y/o almacenada en cada servicio contratado. Por lo que, es necesario definir los requisitos en Ciberseguridad alineados con los criterios inicialmente mencionados. Estos requisitos serán coherentes con las políticas de seguridad de la información del DAFP y serán extensibles a los Servidores públicos, contratistas y/ proveedores y estarán consignados en los contratos.

El definir cláusulas contractuales asociadas a seguridad de la información, permiten establecer contratos y acuerdos rigurosos en materia de ciberseguridad, es necesario para documentar las prioridades que deben reflejarse en los contratos con proveedores y/o contratistas.

Política BYOD (Bring Your Own Device = Trae tu propio dispositivo)

Para los servidores públicos pertenecientes al DAFP se asignan equipos de cómputo propios de la entidad con el nivel de aseguramiento.

Para contratistas, pasantes y proveedores, se permite el uso de equipos de cómputo que no son propios de la entidad, sin embargo, estos equipos pasarán por evaluación de seguridad y cumplirán con la Política de dispositivos móviles y teletrabajo, para lo cual los contratistas y/o representantes de los proveedores asumirán los compromisos de un servidor público ante el Sistema de Gestión de Seguridad de la Información.

Política de dispositivos móviles y teletrabajo

Responsabilidades de parte de los funcionarios públicos, contratistas y/o proveedores de acuerdo a lo establecido en las políticas asociadas a la presente, se toma como precedente los aspectos evaluados por el Grupo de Gestión Humana en el cual se incluyen características de habilidades blandas como autonomía, entendiendo que es responsable de realizar las labores asignadas y se acoge a la evaluación periódica estipulada; manejo del tiempo, teniendo en cuenta que se cumple a cabalidad con los objetivos del cargo según lo expuesto en el punto anterior; adaptación al cambio, recursividad y aprendizaje continuo.

Para lo cual, el DAFP se compromete a promover el buen uso de los activos de información asignados a cada servidor público, proveedor o contratista, de la misma manera que promueve la orientación a resultados, que en conjunto permitan el cumplimiento de las expectativas misionales y de atención a ciudadanías que el DAFP responde.

Dado todo lo anterior, el DAFP a través, de OTIC y del Grupo de Gestión Administrativa brinda los recursos técnicos y tecnológicos para que los compromisos anteriormente se cumplan. Para lo cual, se entregarán las herramientas a nivel de bases de datos,

Aplicaciones, ofimáticos y equipos de almacenamiento y procesamiento de datos como servidores, unidades generales de red para almacenamiento de archivos; de la misma manera se garantizan los aspectos de conectividad a estas herramientas, entendiendo que esto depende al servicio de internet que cada servidor público, contratista o proveedor tenga contratado.

En resumen y cumplimiento de los puntos anteriores, se toma como cumplible de manera obligatoria la política de no almacenamiento de información en los equipos de cómputo, ya que genera riesgo de pérdida o fuga de información, por lo cual, se establece que la única herramienta aprobada para el almacenamiento de datos es la conocida como YAKSA. (repositorio.)

Política de clasificación de los 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.
- ✓ El oficial de seguridad de la información y el grupo de mejoramiento institucional deben solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo.

Política de ingreso y retiro de activos tangibles (físicos) e intangibles

- ✓ El ingreso de activos tangibles debe estar debidamente justificado por la Oficina de Tecnologías de la Información y las comunicaciones y ejecutado 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.

Política de claves de acceso

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, los jefes de dependencia y demás 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.

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.

Política 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:

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.

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.

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.

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 y velar por el correcto, oportuno y eficaz ingreso a las aplicaciones, bases de datos, infraestructura administrada y demás activos de información.

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 del DAFP, 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 vinculado al Directorio Activo del DAFP.
- 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.

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 y entregar este informe al Oficial de Seguridad de la información para su revisión y toma de medidas pertinentes.

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.

Política de eliminación y destrucción

Entendiendo la importancia de toda la información tiene para el DAFP y teniendo en cuenta la necesidad de completar el ciclo de vida de la información, el DAFP adopta como política garantizar la de destrucción de la misma.

Se aplican herramientas gratuitas o libres de borrado seguro con el fin de garantizar que los medios que contienen la información ya no la contengan y esta no se puedan recuperar. Durante la destrucción de la información, se debe velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a divulgación y acceso.

Cuando la información repose en infraestructura de terceros proveedores o contratistas, el supervisor del contrato en compañía de OTIC y del Oficial de Seguridad de la Información verifican que la información es borrada de los activos tecnológicos que la almacenan, cuando el contrato vinculante expire. Esto debe ser de conocimiento explícito del proveedor o contratista y debe quedar consignado en el acuerdo contractual.

Es de responsabilidad evaluar si corresponde y es pertinente la destrucción de la información tomando en cuenta los decretos, leyes y otra normativa vigente. En cada proceso de destrucción se debe generar un reporte de actuación que identifique al personal actuante y la metodología empleada para la destrucción de la información, así como las observaciones que éste considere pertinente y se deberá identificar claramente que el proceso se ha efectuado.

Política de pantalla y escritorio limpios

Para evitar la fuga de información y protección de los equipos de cómputo Al levantarse del puesto de trabajo y al finalizar la jornada laboral, el servidor público, contratista o proveedor responsable del equipo debe bloquear la sesión del equipo de cómputo. De la misma forma no es permitido dejar información de manera física o documentos impresos desprotegida éstos deben guardarse en un lugar seguro y bajo llave. Los documentos y/o medios extraíbles con información pública también deben guardarse para evitar la pérdida de esta información.

No es permitido dejar equipos de cómputo abandonados en cualquier lugar de las instalaciones del DAFP.

Política de 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.
- 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.

Política de Copias de seguridad

- Función Pública implementa la Política de Copias 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.

Política de transferencia 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.

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.

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.

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).

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.

- 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.

Política de seguridad física y ambiental (trabajo en 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.
- El Oficial de Seguridad es 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 de OTIC.

- 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.

- Las anteriores se aplican para cualquier Grupo de Valor que gestione su información de manera física y adicional se amplían las medidas de seguridad según la criticidad de su información.

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 Dirección Administrativa y de Gestión Documental 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.

Política de gestión de vulnerabilidades

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.

Política 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.

Política de privacidad y protección de la información personal identificable

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 relación estado ciudadanías.

Política 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 a quien corresponda 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.

Política de Gestión de Actualización de Software, Sistemas Operativos y Firmware

El DAFP define los lineamientos y procedimientos empleados para la aplicación y actualización de parches en los sistemas de información empleados por bases de datos, aplicaciones, activos físicos de información, elementos de red, servidores, tanto la nube como para infraestructura instalada de manera local incluyendo también los sitios alternos de trabajo.

Esta política es aplicable a toda la infraestructura o plataforma del DAFP que maneje Sistemas de Información empleados para el normal desarrollo de sus procesos.

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:

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 y no podrán ser conectados a la red corporativa.
- 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.

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 video vigilancia institucional.
- Función Pública cuenta con cámaras de video vigilancia 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.

Lineamientos para seguridad de la gestión de comunicaciones y operaciones

La Entidad 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:

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.
- Administrar las llaves de encriptación en las herramientas tecnológicas que así lo requieran.

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.

Protección contra software malicioso

- La OTIC dispondrá de herramientas de seguridad antimalware y anti spam 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.
- Los equipos de cómputo de propiedad de los contratistas deben contar con un software de antimalware licenciado y actualizado, el cual será revisado por la Mesa de ayuda.
- 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). E informar a través de ProactivaNET al oficial de seguridad de la información.

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.

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.
- Está 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.

Lineamientos Proceso de Retest

Es una fase dentro del ciclo de pruebas de software que se realiza para verificar que los defectos previamente identificados y corregidos se hayan resuelto correctamente sin afectar otras áreas del sistema. (El proceso de RETEST consiste en volver a verificar las vulnerabilidades o debilidades que fueron detectadas inicialmente).

El retest es la acción de ejecutar nuevamente un conjunto específico de pruebas en el sistema o en una parte del software que ha sido modificada, con el objetivo de verificar que un error identificado previamente haya sido solucionado.

Pasos en el proceso de Retest

- Identificación del defecto o error en una funcionalidad específica del software. Este defecto puede ser reportado por los testers, usuarios o detectado durante las pruebas iniciales.
- Una vez identificado el error, el equipo de desarrollo se encarga de corregirlo. Esto puede implicar cambios en el código, la base de datos o la configuración del sistema.
- Después de que el defecto se ha corregido, el equipo de pruebas debe planificar la ejecución del retest. Esto incluye determinar qué pruebas son necesarias para verificar la solución del defecto y asegurarse de que la corrección no haya afectado otras áreas del sistema.

- El equipo de pruebas ejecuta las pruebas relacionadas con el defecto corregido, que pueden ser las mismas que se realizaron inicialmente cuando se identificó el problema.
- En esta etapa, se valida que el defecto original se haya solucionado de manera efectiva.
- Si la corrección es exitosa y el defecto ya no se reproduce en el sistema, el retest se considera exitoso. Si el defecto persiste, se puede realizar una nueva ronda de corrección y retest.
- Después de realizar el retest, el equipo de pruebas documenta los resultados, indicando si la corrección fue exitosa o no, y si alguna nueva falla ha surgido en el proceso.
- Una vez que el defecto ha sido solucionado y verificado mediante el retest, se cierra el ciclo de defectos, y el sistema se considera en su estado óptimo en relación con esa falla específica.

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, 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.

- Los eventos de seguridad de la información que sean calificados como incidentes de seguridad se administran mediante el procedimiento de gestión de incidentes.
- 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.

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 Oficial 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.

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.

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.

Bibliografía

https://universidadean.edu.co/sites/default/files/manuales/manual-de-seguridad-de-la-informacion.pdf

https://www.copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/tecnologia/manual_de_seguridad.pdf

https://www.minambiente.gov.co/wp-content/uploads/2022/06/Manual-de-seguridad-de-la-informacion-M-E-GET-01.pdf

https://www.contaduria.gov.co/documents/20127/35873/Manual+de+Seguridad+de+la+Información+V.6.pdf/31979ad6-a18a-4015-f96e-865a6d3e45b4

https://www.ccc.org.co/inc/uploads/2020/02/Manual-de-seguridad-de-la-información.pdf

https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf

Función Pública

Políticas Específicas de Seguridad de la Información

Versión 08
Proceso de Tecnologías de la Información
Diciembre de 2024