Función Pública

Política General de Seguridad de la Información

Proceso de Tecnologías de la Información

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA

Versión 01

Octubre 2024

Función Pública

Contenido

Introducción

Es para la Función Pública muy importante la protección de la información de la Entidad, puesto que su misión de gestionar los planes de políticas de desarrollo administrativo, aplicación de políticas de cumplimiento organizacional y estatal a nivel nacional. Por lo que, la Función Pública vela por la custodia segura de la información.

Adicional a esto, es necesario que la información presentada a los ciudadanos que consultan la información sean asegurados acordes a los desafíos que se presentan para la gestión correcta del aseguramiento de la información. Por lo que en este documento se encuentra la Política General de Seguridad de la Información aplicada en la DAFP.

Glosario

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas se establecen para asegurar que las características de seguridad de los sistemas usados con regularidad estén configuradas y administradas uniformemente, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos definen las políticas, estándares, mejores prácticas y guías que se implementarán en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Se usan para delinear los pasos que debe seguir una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Los procedimientos se desarrollan, implementan y supervisan por el dueño del proceso o del sistema, seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías lo más cerca posible, y se ajustarán a los requerimientos procedimentales técnicos establecidos dentro del a dependencia donde se aplican.

DAFP: Departamento Administrativo de la Función Pública.

Propósito

La comunidad interesada debe conocer la gestión que el Departamento Administrativo de la Función Pública realiza sobre la información segura, aplicando los estándares que permiten evaluar el cumplimiento de los más altos niveles de seguridad de la información, como lo son ISO 27001:2022, ISO 27032:2019, ISO 27701: 2019, ISO 37701:2019 y las leyes colombianas que exigen a la OAFP brindar seguridad a la información que se resguarda en referencia a los documentos del Modelo de Seguridad y Privacidad de datos personales que se describen en el marco normativo.

Objetivo

El Departamento Administrativa de Función Pública- DAFP, comprende la importancia de garantizar la confidencialidad, integridad y la disponibilidad de la información de la cual el DAFP es responsable, y esto lo logra con el diseño de una Política General de Seguridad de la información, con el establecimiento de políticas internas, la implementación de controles a la infraestructura, a los activos de información que componen la seguridad perimetral y demás activos.

Lo anterior se convierte en el objetivo principal del Sistema de Gestión de Seguridad de la Información, y, por tanto, este documento se alinea con los objetivos organizacionales que apoyan el cumplimiento de la misión del DAFP.

Objetivos secundarios

- Implementar el sistema de gestión de seguridad y privacidad de la información
- Minimizar el riesgo de los procesos y procedimientos de la entidad.
    - En la gestión de datos personales e información propia de la gestión misional del DAFP
    - En la gestión del riesgo de seguridad de la información, ciberseguridad y datos personales.
- Cumplir con los principios de seguridad de la información en toda la DAFP.
- Cumplir con los objetivos secundarios descritos y apoyar el cumplimiento de los objetivos organizacionales del DAFP.
- Mantener la confianza de los ciudadanos, servidores públicos, terceras partes interesadas, en las tecnologías de información incluidos el hardware y el software, y la gestión realizada sobre estos a nivel de seguridad de la información.

- Proteger los activos de información y los datos, incluyendo la de los servidores públicos y de la ciudadanía.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información e incluir en los documentos pertenecientes a otros procesos, los criterios de seguridad de la información necesarios.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, terceras partes comprometidas, titulares de los datos, encargados de los datos, en la información, en los procesos.
- Garantizar la continuidad del negocio, la gestión del cambio, gestión de accesos, gestión del riesgo y gestión de incidentes.

Audiencia

La ciudadanía colombiana puede consultar este documento a través de la página oficial del Departamento Administrativo de la Función Pública, al igual que los servidores públicos del DAFP, contratistas y personas interesadas.

Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas, pasantes, colaboradores y la ciudadanía en general, para asegurar que todos los aspectos importantes preservan la seguridad de la información en el Departamento Administrativo de la Función Pública están adecuadamente gestionados, definidos según normas internacionales ISO/IEC 27001.

El sistema de gestión de seguridad de la información (SGSI), que incluye los componentes de ciberseguridad, continuidad del negocio y protección de datos personales, cubre a toda la DAFP, y sus procesos, sin descuidar proceso alguno.

Marco Legal

El Departamento Administrativo de la Función Pública cumple con lo dispuesto en el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

Incluye lo dispuesto en los numerales 4 y 5 del artículo 34 y numerales 16 y 43 del artículo 48 de la ley 734 de 2002.

Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

Ley 527 de 1999 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos - Se entiende por control interno el sistema integrado por el esquema de organización y el conjunto de planes, métodos principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por cada entidad, con el fin de procurar que todas las actividades operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas y objetivos previstos-

Ley 594 de 2000 Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones - El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser,

entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax". -

Ley 599 DE 2000 Por la cual se expide el Código Penal. - Responsabilidad "Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos" Administración y acceso. "Es una obligación del Estado la administración de los archivos públicos y un derecho de los ciudadanos el acceso a los mismos, salvo las excepciones que establezca la ley; -

Ley 599 DE 2000 Por la cual se expide el Código Penal. -En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa." -

Ley 734 de 2002 Por la cual se expide el Código Disciplinario Único. - Art 34. Deberes. Son deberes de todo servidor público "4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
5. Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos. " -

La Ley 850 de 2003 Por medio de la cual se reglamentan las veedurías ciudadanas. - Principio de Transparencia "A fin de garantizar el ejercicio de los derechos, deberes,

instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia”

Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. - Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

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

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

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

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

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

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado. Directiva 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos. Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos.

Artículos 25 y 26. Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.

Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

CONPES 3995 de 2020. Política Nacional de confianza y Seguridad digital.

1. Política de Seguridad de la Información

El Departamento Administrativo de la Función Pública, entiende y cumple con las obligaciones propias de sus funciones y, dentro del entendido de la importancia de la gestión de la seguridad de la información, se compromete con la ciudadanía, los servidores públicos del DAFP a cumplir con los principios de seguridad de la información (la confidencialidad, integridad, disponibilidad), mediante la gestión de riesgos de seguridad que permita prevenir incidentes de seguridad, de igual manera realizar la implementación de controles a nivel técnico, tecnológico y procedimentales; y cumpliendo los requisitos

legales y reglamentarios, incluyendo la aplicación de la protección de datos personales y garantiza así también la continuidad de los servicios misionales del DAFP.

Teniendo todo lo anterior en cuenta, y con el fin de asegurar la dirección estratégica del DAFP, se establece un objetivo general de seguridad de la información que cuenta con toda la compatibilidad con los objetivos de seguridad de la información. Dado que se adquiere un compromiso de parte del responsable de la seguridad de la información de Implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, basado en lineamientos establecidos y publicados, que estén acorde a las necesidades del cumplimiento misional institucional del DAFP, que cubre también la protección de la seguridad de la información gestionada en el ciberespacio, el aseguramiento y buena gestión de los datos personales y la continuidad de los servicios que el DAFP presta a la ciudadanía y los requerimientos regulatorios asociados a estos.

De igual manera, minimizar la superficie de vulnerabilidad que permita la materialización del riesgo de la seguridad de la información, y así, garantizar el cumplimiento de los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información, protección de datos personales, ciberseguridad y continuidad del negocio.

Todo lo anterior acompañado de un programa completo, independiente y eficaz, de auditorías que permitan la mejora continua del sistema de gestión de seguridad de la información, ciberseguridad, protección de datos personales y continuidad de la prestación de servicios para los cuales el DAFP fue creado.

2. Compromisos y responsabilidades

2.1. Roles y Responsabilidades

Todo servidor público funcionario, contratista, pasante, y colaborador entre otros que estén involucrados con información del Departamento Administrativo de la Función Pública.

Alta Gerencia

- Aprobar e impartir las directrices de cumplimiento la política y objetivos de seguridad digital.
- Asignar los recursos necesarios para el sistema de gestión de seguridad digital.
- Dirigir a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad digital.
- Aprobar y promover el cumplimiento de los controles de seguridad digital definidos para el tratamiento de los riesgos identificados.
- Revisar los resultados de la evaluación de desempeño, riesgos e incidentes del sistema de gestión de seguridad digital, gestión de datos personales y continuidad del negocio incluyendo recurso humano, técnico y tecnológico.
- Apoyar al Oficial de Seguridad de la información, en la toma de decisiones, la aplicación de los controles necesarios, cumplimiento del Sistema de Gestión de Seguridad de la Información por parte de toda la entidad.

Oficial de Seguridad de datos personales

- Actualizar al Sistema de Gestión de la Seguridad de la Información en Función Pública de acuerdo con la normativa vigente.
- Actualizar el diagnóstico de seguridad y privacidad de la información, el plan de seguridad y privacidad de la información y el plan de tratamiento y mitigación de riesgos de información, según lineamientos establecidos en el habilitador Seguridad y Privacidad de la Información y normatividad vigente.

- Gestionar el cierre de las brechas de seguridad, realizar seguimiento a los controles de seguridad y acciones de mitigación de vulnerabilidades conforme a los lineamientos institucionales.
- Realizar remediación, pivoteo, control y auditoria de seguridad sobre la infraestructura tecnológica, sistemas y servicios de información institucional con la periodicidad que le sea requerida.
- Revisar, actualizar y ejecutar pruebas de los planes de contingencia, continuidad y recuperación asociados a los servicios de TI, para la recuperación de los mismos.
- Identificar y evaluar los riesgos de seguridad, así como implementar y configurar los componentes de seguridad asociados a la infraestructura y servicios de TI de Función Pública.
- Planear, ejecutar y hacer seguimiento en los contratos que involucren temas de seguridad de la información de acuerdo con la normativa vigente.
- Monitorizar los planes de contingencia, control de cambios, planes de continuidad de servicios y planes de recuperación de TI, que se establezcan en el Sistema de Seguridad de la Información del Departamento.
- Establecer y cumplir con el plan de acciones correctivas y de mejora continua que propendan con la correcta aplicación de los principios de seguridad de la información, ciberseguridad, protección de datos personales, riesgos de seguridad de la información y continuidad del negocio.

Especialista en Seguridad de la Información

- Implementar las políticas y procedimientos de seguridad de la información.
- Monitorear y analizar incidentes de seguridad.
- Realizar auditorías internas y evaluaciones de cumplimiento.
- Capacitar y concienciar a los empleados sobre seguridad de la información.
- Gestionar herramientas y tecnologías de seguridad.

- Apoyar al Oficial de seguridad en todo lo relacionado con seguridad

Propietarios de Información

- Determinar los requisitos de seguridad de la información para sus activos.
- Asegurar la correcta clasificación y protección de los datos.
- Aprobar el acceso a la información.
- Evaluar y aceptar riesgos residuales para los activos de información.

Control Interno

- Realizar auditorías periódicas del SGSI para evaluar su eficacia.
- Identificar no conformidades y áreas de mejora.
- Proveer recomendaciones para la mejora continua del SGSI.

Departamento Administrativo de la Función Publica

- Analizar las acciones disciplinarias a tomar en caso de presentarse incumplimiento por parte de los servidores públicos pertenecientes al DAFP en materia de seguridad digital, gestión del riesgo, gestión de incidentes, protección de datos personales y continuidad del negocio.
- Analizar las necesidades y expectativas del área en materia de seguridad digital.
- Coordinar las actividades de gestión de riesgos de seguridad digital al interior de su dependencia.
- Adoptar los controles de seguridad de la información definidos para el tratamiento de los riesgos de seguridad digital identificados.
- Aplicar y cumplir los planes de mejora continua y de acciones de mejora derivadas de las auditorías al sistema de gestión de seguridad digital, continuidad del negocio y datos personales."

3. Cumplimiento

La aplicación de esta política es de carácter mandatorio para la DAFP, para todas las partes interesadas que participen en las operaciones de la Entidad. Por tanto, la Dirección respalda el Sistema de Gestión de Seguridad de la Información, y promueve, comunica y monitoriza el cumplimiento de las políticas.

A lo anterior y teniendo en cuenta que desde la dirección se apoya todo lo dispuesto en el sistema, se indica que los servidores públicos, contratistas y terceros que interactúen con la gestión de la información de cualquier manera incluyendo a la ciudadanía. Están obligados a reportar cualquier situación que consideren insegura o que atenten contra los principios de seguridad de la información, a los correos a los canales de atención al ciudadano https://www.funcionpublica.gov.co/formule-su-peticion.

Función Pública

Política General de Seguridad de la Información

Versión 01
Proceso de Tecnologías de la Información
Octubre de 2024