FUNCIÓN PÚBLICA

Política general de seguridad de la información Función Pública

Proceso Tecnologías de la Información y las Comunicaciones

Diciembre de 2018

Tabla de contenido

1. Introducción y declaración

La Política de Seguridad de la Información es la declaración general de FUNCIÓN PÚBLICA, con respecto a la protección de los activos de información (los grupos de valor, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la publicación de las políticas, procedimientos e instructivos, así como la asignación de roles y responsabilidades, para la aplicación de la seguridad de la información, en el marco del Modelo Integrado de Planeación y Gestión

FUNCIÓN PÚBLICA, establece la compatibilidad de la política y objetivos de seguridad de la información, alineados con el cumplimiento de su misión, visión y objetivos estratégicos, apegados al marco del código de integridad (los valores institucionales), con los siguientes objetivos específicos:

- ✓ Proteger los activos de información de Función Pública, con base en los criterios de confidencialidad, integridad y disponibilidad.
- ✓ Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- ✓ Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno Digital, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- ✓ Socializar esta política para conocimiento de los grupos de valora través de los distintos canales de comunicación.
- ✓ Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte del Comité Institucional de Gestión y Desempeño y auditorías internas planificadas a intervalos regulares. De igual manera, socializar estos resultados a la Alta Dirección.
- ✓ Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.

2. Alcance y aplicabilidad

Esta política de seguridad de la información aplica a toda la Entidad y centra su alcance, en primera instancia, en dos procesos transversales que impactan directamente el cumplimiento de los objetivos estratégicos. Estos procesos son:

"Gestión Documental" proceso a través del cual se ejecutan actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final con el objeto de facilitar su utilización y conservación.

"Gestión Tecnológica" proceso a través del cual se lidera la gestión de las Tecnologías de la Información y las Comunicaciones, articulada con la estrategia del negocio, generando valor, en el marco de las políticas, normas y los lineamientos establecidos por la autoridad competente.

Cabe destacar que la información que se genera en ambos procesos es muy relevante para el logro del objetivo institucional al que están asociados y la misión institucional, garantizando la integridad, disponibilidad y confidencialidad de los activos de mayor criticidad de la Entidad

A los demás procesos de la Entidad les serán aplicados los lineamientos de esta política de acuerdo con el plan de implementación de seguridad de la información.

3. Nivel de cumplimiento

Todos los actores cubiertos dentro del alcance y aplicabilidad deben dar cumplimiento al 100% de la política.

A continuación se establecen los aspectos de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de FUNCIÓN PÚBLICA:

- ✓ FUNCIÓN PÚBLICA resolvió definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos y normatividad que le aplica a su naturaleza.

- ✓ Las responsabilidades frente a la seguridad de la información serán compartidas, y aceptadas por cada uno de los grupos de valor.

- ✓ FUNCIÓN PÚBLICA protegerá la información generada, procesada o resguardada por los diferentes procesos de la entidad y los activos de información que hacen parte de los mismos.

- ✓ FUNCIÓN PÚBLICA protegerá la información creada, procesada, transmitida o resguardada por los diferentes procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- ✓ FUNCIÓN PÚBLICA protegerá su información de las amenazas originadas por parte del talento humano de la entidad.

- ✓ FUNCIÓN PÚBLICA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- ✓ FUNCIÓN PÚBLICA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- ✓ FUNCIÓN PÚBLICA implementará controles de acceso a la información, sistemas y recursos de red.
- ✓ FUNCIÓN PÚBLICA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información institucionales.
- ✓ FUNCIÓN PÚBLICA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ FUNCIÓN PÚBLICA garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- ✓ FUNCIÓN PÚBLICA cumplirá con las obligaciones legales, regulatorias y contractuales relacionadas con la seguridad de la información.

El incumplimiento de la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, en cuanto a Seguridad de la Información se refiere.

4. Roles y responsabilidades en materia de seguridad de la información.

La política de seguridad de la información es de aplicación obligatoria para todo el talento humano de la entidad.

Director(a) de FUNCIÓN PÚBLICA

Director(a) de la FUNCIÓN PÚBLICA tendrá las siguientes responsabilidades:

- ✓ Aprobar las políticas de seguridad de la información.
- ✓ Validar 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 su ejecución.

Comité Institucional de Gestión y Desempeño

El Comité tendrá las siguientes funciones y responsabilidades en temas de Seguridad de la Información:

- ✓ Revisar y proponer al Director(a), 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 a la Alta Dirección, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.

Encargado de Seguridad de la Información Institucional.

Es un servidor público nombrado por el Director(a) de Función Pública como su asesor en materia de seguridad de la información. El Encargado de Seguridad de la Información tendrá las siguientes funciones y responsabilidades:

- ✓ Organizar las actividades del Comité Institucional de Gestión y Desempeño en materia de seguridad de la información.
- ✓ Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la entidad y el control de su implementación; y velar por su correcta aplicación.
- ✓ Supervisar el Monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos.
- ✓ 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.

Encargado Técnico de Seguridad de la Información Institucional.

Es un servidor nombrado por la Director(a) de FUNCIÓN PÚBLICA como su asesor en materia técnica de seguridad de la información. El Encargado Técnico de Seguridad de la Información tendrá las siguientes funciones y responsabilidades:

- ✓ 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, reportando periódicamente al Encargado de Seguridad de la Información.
- ✓ Establecer puntos de enlace con los encargados técnicos de seguridad de otros Servicios públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de la seguridad pertinentes.

Responsable de la Oficina de Tecnologías de la Información las Comunicaciones.

Esta función recae en el Jefe de la Oficina de Tecnologías de la Información y Comunicaciones quien deberá:

- ✓ Cumplir con los procedimientos relativos a los dominios de control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información y gestión de los canales de comunicación y operaciones.
- ✓ Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Entidad.
- ✓ Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

Propietarios de los Activos de la Información Institucional.

Esta función recae en los Directores, Jefes de Área y Coordinadores de grupo o aquellos que la Dirección asigne, quienes deberán:

- ✓ Clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad de los mismos, documentar y mantener actualizada la clasificación efectuada.
- ✓ Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a 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.

Responsables del Grupo de Gestión Humana y Jefe de la Oficina Asesora de las Comunicaciones.

Esta función recae en el Coordinador(a) del Grupo de Gestión Humana y el Jefe de la Oficina Asesora de las Comunicaciones, quienes deberán:

- ✓ 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.

Responsable de la Dirección Jurídica.

Cumplir con los procedimientos relativos al cumplimiento de la Política de Seguridad de la Información.

- ✓ 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.
- ✓ 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.
- ✓ 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 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 de forma periódica, 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.

Usuarios de la Información y de los Sistemas de Procesamiento de la Información.

Esta función recae en todos los grupos de valor, los que deberán:

- ✓ Ser responsables de 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.