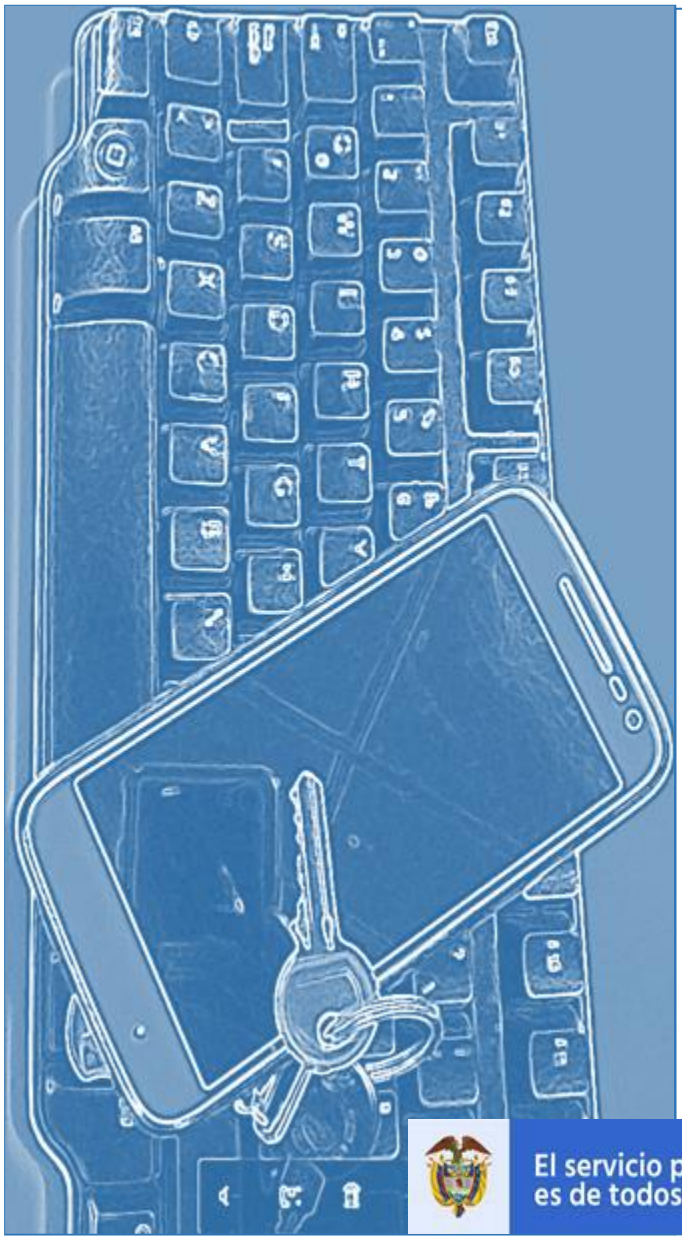

FUNCIÓN PÚBLICA

Plan De Seguridad y Privacidad de la Información

2019

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN LAS COMUNICACIONES

El servicio público es de todos

Función Pública

Julio Cesar Rivera Morato

Jefe Oficina de Tecnologías de la Información y las Comunicaciones

Servicios de TI

Hilda Constanza Sánchez
Coordinadora de Servicios de TI

Equipo de Apoyo:
Andrea Martínez Calvo
Ana Yised Castro
Edwin Vargas
Leonardo Calderón

Servicios de Información

Francisco José Urbina
Coordinador de Servicios de Información

Equipo de Apoyo:
Lucy Villarraga
María Elvira Grueso
Lina Esperanza Escobar
Oiris Olmos
Olga Lucía Beltrán
Gerson Carrillo
Gina Mahecha
José Ángel Torres
Pedro Antonio García
Víctor Jáuregui

Proyectos Estratégicos TI

Eduar Gaviria
Coordinador de Proyectos Estratégicos de TI

Equipo de Apoyo:
Astrid Ruiz
Nelson Gutiérrez
Luis Alejandro Bejarano
Héctor Melo
Sandra Yasmin Flórez
Greistly Vega
Jack Martínez
Jhon Mosquera

TABLA DE CONTENIDO

1. Objetivo

Este documento es el resultado del diagnóstico de Seguridad y Privacidad de la Información en el Departamento Administrativo de la Función Pública, el cual se enmarca dentro de los siguientes objetivos:

- Verificar los alcances establecidos en el Modelo de Privacidad y Seguridad de la Información (MPSI) y la documentación base con la que cuenta la entidad. Revisada esta documentación se realiza el cruce con los lineamientos establecidos en la Política de Gobierno Digital.

- Establecer los lineamientos, optimización e implementación de la política se Seguridad y Privacidad de la Información, que se deben aplicar en el departamento Administrativo de la Función Pública.

- Establecer las actividades encaminadas al cumplimiento en la implementación del Plan de Seguridad y Privacidad de la Información de manera integral para Función Pública.

- Generar capacidades institucionales en cada una de las áreas de Función Pública, que garanticen un adecuado manejo, custodia y control de los componentes de información, asegurando el cumplimiento de los criterios de seguridad y privacidad de la información.

- Desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

- Concientizar a todos los servidores públicos, pasantes y contratistas de la entidad de la importancia de cumplir los lineamientos establecidos en la política de seguridad y privacidad de la información.

En la política se Seguridad aprobada por FUNCIÓN PÚBLICA, se 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.
- 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

El presente documento describe el Plan de Seguridad y Privacidad de Función Pública, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Esta política de seguridad y privacidad de la información aplica a toda la Entidad.

La información que se genera en cada uno de los procesos de la entidad es muy relevante para el logro de las metas y objetivos institucionales, garantizando la integridad, disponibilidad y confidencialidad de los activos de información de la Entidad.

Las políticas de seguridad y privacidad de la información aplican para todos los servidores públicos, contratitas, pasantes y visitantes de Función Pública y deben ser de obligatorio cumplimiento.

3. Marco Normativo

La actualización del plan estratégico se define teniendo en cuenta el siguiente marco normativo:

Marco Normativo	Descripción
Política de seguridad y privacidad de la información de Función Pública – 2018.	La Política de Seguridad de la Información de FUNCIÓN PÚBLICA, con respecto a la protección de los activos de que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información.
Manual política de seguridad y privacidad de la información de función pública – 2018.	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 103 de 2015,	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1494 de 2015	Por el cual se corrigen yerros en la Ley 1712 de 2014
Manual gobierno en línea 3.1 ver 2014 – 06 - 12.	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
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
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley estatutaria 1581 de 2012,	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
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. Disponible en Línea
Decreto 4632 de 2011	Por medio del cual se reglamenta parcialmente la Ley
1474 de 2011	se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1273 de 2009,	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

Constitución Política de Colombia1991 - Artículo 15	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Ley 23 de 1982	sobre Derechos de Autor. Congreso de la República.
Norma técnica colombiana NTC - ISO/IEC 27001	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Tabla 1 – Marco Legal

4. Situación Actual

Función Pública ha realizado actividades tendientes a la adopción del Modelo de Seguridad y Privacidad de la Información, para lo cual se tiene aprobada por la alta dirección la política y manual Seguridad y Privacidad de la Información, obteniendo los siguientes resultados:

Ámbito	Situación Actual
Diagnóstico de seguridad y Privacidad	Se cuenta con un diagnóstico con el estado de la implementación del Modelo de Seguridad y Privacidad de la Información en Función Pública. Se evidencia la participación de la alta dirección en la aprobación de la Política y Manual de Seguridad y Privacidad de la Información, Dicha política se encuentra publicada en el Sistema Integrado de Gestión – SIG. Es indispensable contar con el Oficial de Seguridad para Función Pública a partir de la vigencia 2019. Función Pública ha diligenciado el instrumento de evaluación de la implementación del modelo de seguridad y privacidad de la información, el cual se ha remitido al Ministerio de las TIC. Teniendo en cuenta el resultado del diligenciamiento de éste instrumento, se requiere identificar el nivel de madurez de la Seguridad y Privacidad de la Información en la entidad, identificar las vulnerabilidades técnicas y administrativas y generar planes de mejoramiento para subsanar dichas vulnerabilidades.

Plan de Seguridad y privacidad	Se creará y formalizará un plan de entrenamiento en seguridad de la información, junto con un formato de métricas y medición. Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información en Función Pública, actividad que debe ser liderada por la Oficina Asesora de Planeación y Oficina de Tecnologías de la Información y las Comunicaciones. Se cuenta con la Declaración de Aplicabilidad de Función Pública en materia de seguridad de la información del Proceso de Tecnología de la Información y las Comunicaciones, conforme a los controles de la norma ISO 27001 2013. Se debe extender la declaración de aplicabilidad a toda la entidad. Se deben establecer políticas del tratamiento de riesgos y revisión en un periodo adecuado, reformando el modelo de manejo de incidentes de seguridad para ser elaborado con las especificaciones adecuadas. Se considera necesaria la conformación y puesta en funcionamiento del grupo de Cambios al menos cada mes para revisar y validar los cambios que surjan en la implementación de los proyectos, el cual estará liderado por el área de seguridad.
Plan de Implementación	El Modelo de Privacidad y Seguridad de la Información debe implementarse en toda la entidad, tomando como base las políticas descritas en el Manual de Seguridad y Privacidad de la Información de la entidad. El plan de seguridad y privacidad se elaborará bajo una alineación con el propósito misional para garantizar su efectividad, este documento es de carácter urgente para el área de seguridad de la información. Actualizar la declaración de aplicabilidad seguridad de la información a toda la entidad y establecer una hoja de ruta para su implementación a corto, mediano y largo plazo. La identificación de riesgos e implementación de controles de Seguridad y Privacidad de la Información debe estar alineados al procedimiento denominado “Administración de la Gestión del Riesgo” liderado por la Oficina Asesora de Planeación.

Gestión de Riesgos	Se requiere implementar un desarrollo de manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información y establecer los modelos de métrica y medición de dichos controles. Es importante implementar el proceso de mejoramiento continuo, para lo cual preparará un plan de auditorías de seguridad e implementará un formato de métricas y medición.

Tabla 2 - Situación Actual Seguridad y Privacidad de la Información

5. Plan para la Implementación del Modelo de Seguridad y Privacidad de la Información

Teniendo en cuenta la política y manual de seguridad y privacidad de la información aprobado por FUNCIÓN PÚBLICA y el resultado del diligenciamiento del instrumento de evaluación de la implementación del modelo de seguridad y privacidad de la información en la entidad, se establece el siguiente plan para la implementación del Modelo de Seguridad y Privacidad de la Información el cual el cual responde a la gobernabilidad de la siguiente manera: MinTIC lidera la política de Gobierno Digital, El Director de Función Pública es el responsable de la política de Gobierno Digital en la Entidad, el Comité institucional de Gestión y Desempeño orienta la implementación y la Oficina Asesora de Planeación, Oficina de Tecnologías de la Información y las Comunicaciones implementan en articulación con las otras instancias de la Entidad.

A continuación, las actividades requeridas para la ejecución del plan:

Determinar las acciones a implementar según lo estipulado en la política y manual de seguridad y privacidad de la información a probado por la entidad y el resultado del diligenciamiento de la herramienta de diagnóstico proporcionada por MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.
Actualizar la declaración de aplicabilidad de la política de Seguridad y Privacidad de la Información para Función Pública y ejecutar el cronograma de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información
Identificar vulnerabilidades técnicas y administrativas en torno al modelo de seguridad y privacidad de la información.

Liderar Identificación, clasificación y valoración de activos de información, validarlo y aprobarlo.
Identificar y valorar el tratamiento de riesgo de seguridad de la información.
Fomentar la seguridad de la información y la continuidad en la organización.
Realizar actividades de seguimiento y evaluación de la implementación de la seguridad y privacidad de la información, con el fin de establecer los planes de mejora continua.
Implementar el plan de tratamiento de riesgos.
Establecer los indicadores de gestión que permitan medir el nivel de cumplimiento de la política de seguridad y privacidad de la información en la entidad.
Revisar y hacer seguimiento a la implementación de la política de seguridad y privacidad de la información en la entidad.
Establecer los planes de mejora continua.
Actualizar la política y Manual de Seguridad y Privacidad de la Información de Función Pública.

Tabla 3. Plan para la Implementación del Modelo de Seguridad y Privacidad de la Información

A continuación, se relacionan las políticas de seguridad y privacidad de la información aprobadas por el Comité de Gestión y Desempeño Institucional de Función Pública, que deben ser implementadas en su totalidad para la vigencia 2019:

Política de estructura organizacional de seguridad de la información	Roles y responsabilidades en materia de seguridad de la información
Políticas de gestión de activos de información	Política responsabilidad en la gestión de los activos de información
	Política responsabilidad de la gestión de la infraestructura tecnológica
	Política responsabilidad visitantes
	Política de uso aceptable de los activos
	Usos no autorizados
	Política de retiro (baja) de activos tangibles (físicos)
	Política de retiro (baja) de activos intangibles (software)
Políticas de gestión de seguridad de recursos humanos	Política de control de acceso servidores públicos, contratistas y pasantes
	Política de control de acceso del personal de vigilancia
	Política de circulación interna de servidores públicos, contratistas, pasantes y visitantes
	Política de seguridad para el teletrabajo
Política de seguridad física y ambiental	Política de áreas seguras
	Centro de cómputo y centros de cableado
	Almacén, archivo y correspondencia
	Sala de capacitación
	Política de seguridad de equipos
	Política de Seguridad de las Cámaras de Video

Políticas de gestión de comunicaciones y operaciones	Política de asignación de responsabilidades operativas
	Política de protección contra software malicioso
	Política de respaldo de Backup
	Política de gestión de seguridad en la red
	Política de gestión de medios removibles
	Política de Intercambio de Información
	Política de monitoreo
	Política de borrado seguro
	Política de gestión de cambios
Políticas de control de acceso	Política para el control de acceso
	Política de gestión de acceso al usuario
	Política de responsabilidades del usuario
	Política de control de acceso a la red
	Política de control de acceso al sistema operativo
	Política de control de acceso a aplicaciones e información
	Política y acciones para construir contraseñas seguras
Políticas de adquisición, desarrollo y mantenimiento de sistemas de información	Política para el establecimiento de los requisitos seguridad de los sistemas de información
	Política de desarrollo seguro, pruebas y soporte
	Política de gestión de la continuidad del negocio
	Política de controles criptográficos
	Política de gestión de vulnerabilidad técnica
Políticas de gestión de incidentes de seguridad de la información	Política general del sistema de gestión de seguridad de la información
	Política para el reporte y tratamiento de incidentes de seguridad

Tabla 4. Políticas de Seguridad y Privacidad de la Información aprobadas para Función Pública.