El servicio público es de todos

Función Pública

FUNCIÓN PUBLICA

Plan de Seguridad y Privacidad de la Información

2020-2022

VERSIÓN 3

Enero 2021

Versión	Fecha Versión	Observación
1	2020-01-31	Versión excel
2	2020-10-05	Matriz
3	2021-01-30	Actualización 2021

Tabla de contenido

Introducción

El presente documento describe el Plan de Seguridad y Privacidad de Función Pública, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional.

La Política de Gobierno Digital han definido dos (2) componentes: TIC para el Estado y TIC para la Sociedad, y tres (3) habilitadores transversales: Arquitectura, Seguridad y Servicios Ciudadanos Digitales, como se puede observar a continuación:

Ilustración 1 Política de Gobierno Digital - Fuente MINTIC

Donde los componentes permiten mejorar el funcionamiento de las entidades públicas, su relación con otras entidades y el fortalecimiento de su relación con la sociedad. Los habilitadores por su parte, contribuyen al logro de los objetivos definidos en los componentes.

El habilitador de Seguridad y Privacidad, permite a Función Pública garantizar la confidencialidad, disponibilidad e integridad de la información, para lo cual se hace indispensable diseñar el Plan de Seguridad y Privacidad de la Información que a continuación se detalla.

1. Objetivo

1.1. General

Definir la hoja de ruta de la estrategia de ciberseguridad, mediante la aplicación del habilitador de seguridad de la información de la política de gobierno digital, con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información de Función Pública.

1.2. Objetivo específico

- Implementar 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, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- 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".

1.3. Indicador

- **Nombre del Indicador**: Estado de madurez de la Seguridad y Privacidad de la Información de la Entidad.

- **Medición:** Aplicación del instrumento de madurez de MINTIC

  .

2. Marco Normativo

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

Marco Normativo	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública	2020	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
Decreto 103 de 2015,	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2018	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.
Decreto 2573 de 2014	2018	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 1377 de 2013	2018	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 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	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 1273 de 2009,	2016	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 527 de 1999	2015	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.
Constitución Política de Colombia1991 - Artículo 15	2015	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.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Tabla 1. Marco Normativo

3. 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, vigencia 2020. Se evidencia la participación de la alta dirección en la aprobación del Políticas técnicas de seguridad de la información Función Pública, la cual se encuentra publicada en el Sistema Integrado de Planeación y Gestión – SPIG.

Ámbito	Situación Actual
	Es indispensable continuar con la participación activa del Oficial de Seguridad para Función Pública, o de la persona que haga sus veces (contratista o servidor público). Se cuenta con el diagnóstico relacionado con la Seguridad y Privacidad de la Información, el cual liderado por la firma MNEMO con la participación de la Oficina Asesora de Planeación y la Oficina de Tecnologías de la Información y las Comunicaciones.
Plan de Seguridad y privacidad	En la vigencia 2020, se crea y formaliza el plan de seguridad y privacidad de la información para las vigencias 2020-2022. Así mismo, se tiene actualizado dicho plan con las actividades realizadas durante la vigencia 2020 y se actualizaron las actividades a realizar para la vigencia 2021. Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información en Función Pública. Se cuenta con la Declaración de Aplicabilidad de Función Pública en materia de seguridad de la información, conforme a los controles de la norma ISO 27001 2013. Función Pública cuenta con la política del tratamiento de riesgos, se tienen definidos los riesgos de seguridad para cada uno de los procesos de la entidad y se lleva el control de la ejecución de las acciones preventivas asociadas en el Sistema de Gestión Institucional (actividades, tiempos y responsables). La definición de los riesgos y controles fue liderada por la Oficina

Ámbito	Situación Actual
	Asesora de Planeación, con los delegados de cada proceso. Se elaboró, publicó y socializó el procedimiento de gestión cambios, que tiene por objetivo mantener la disponibilidad de los servicios tecnológicos frente a las solicitudes de cambio, estandarizando el registro, planeación, ejecución y monitoreo de los mismo, con el fin de reducir el impacto en la prestación del servicio.
Plan de Implementación	El plan de seguridad y privacidad de la información, se actualiza periódicamente con el fin de hacer seguimiento a las acciones definidas en cada vigencia y determinar las acciones a realizar en las siguientes vigencias. Se mantiene actualizada la declaración de aplicabilidad de la seguridad de la información. La identificación de riesgos e implementación de controles de Seguridad y Privacidad de la Información están alineados al procedimiento denominado “Administración de la Gestión del Riesgo” liderado por la Oficina Asesora de Planeación.
Gestión de Riesgos	Función Púbica ha implementado el manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información, mediante el procedimiento denominado Gestión de Incidentes de Seguridad de la Información. Con el fin de garantizar la transferencia segura de datos de carácter personal requeridos por los entes de control y vigilancia en el marco de sus funciones misionales, se ha implementado el procedimiento “Intercambio Seguro de Datos con Entidades de Vigilancia y Control”.

Tabla 2. Situación Actual Seguridad y Privacidad de la Información

Las principales actividades realizadas durante la vigencia 2020 se describen a continuación:

Eje	Área	Actividades Realizadas
Transformación Digital	Transferencia de información	Se identificaron riesgos de seguridad digital y Diseñar los controles de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros.
	Seguridad para los Servicios ciudadanos digitales (sistemas digitales)	Se actualizó el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales
Riesgos	Actualización de panorama de riesgos de seguridad digital	Se acompañó a los procesos institucionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgo de seguridad digital
	Seguimiento a la implementación de planes de tratamiento de riesgos	Se acompañó a la Oficina asesora de planeación en el seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los procesos
Sensibilización	Reinducción e inducción de funcionarios (apoyo a GGH)	Se apoyaron actividades de inducción y reinducción de los funcionarios de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles del sistema de gestión de seguridad de la información
	Divulgación de la documentación, controles y herramientas de ayuda del sistema de gestión de seguridad de la información	Se diseñaron e implementaron acciones de socialización de la documentación, controles y herramientas del sistema de gestión de seguridad de la información institucional

Eje	Área	Actividades Realizadas
	Continuidad de la plataforma tecnológica y de servicios	Se apoyó técnicamente la implementación de soluciones de detección de intrusos que protejan la infraestructura de servicios institucionales
		Se apoyó técnicamente la implementación de soluciones de protección perimetral de los sistemas de información ante ataques cibernéticos
		Se acompañó el diseño de lineamientos y controles de seguridad que mitiguen los riesgos que puedan impactar la infraestructura de servicios de nube privada institucional
		Se acompañó técnicamente el diagnóstico, diseño e implementación del Plan de Continuidad de Negocio Institucional
Sistema integrado de planeación y gestión	Gestión de la Documentación del Sistema de gestión de seguridad de la información	Se actualizó el documento de contexto de seguridad de la información institucional
		Se diseñaron estrategias y controles que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales
		Se elaboraron y actualizaron los documentos del sistema de gestión de seguridad de la información requeridos por la Norma ISO 27001 y el modelo de seguridad y privacidad de la Información recomendado por el Ministerio de las Tecnologías de la Información y las Comunicaciones
	Medición del desempeño	Se realizó la evaluación de la efectividad de los controles de seguridad de la información

Eje	Área	Actividades Realizadas
		adoptados por la Entidad para el tratamiento de los riesgos de seguridad Digital
	Lineamientos de adopción del Oficial de Seguridad de la Información en Entidades de la Rama Ejecutiva	Apoyar técnicamente la elaboración de una directriz con alcance a todas las entidades del estado para la adopción del rol de oficial de seguridad de la información
Seguridad operativa	Gestión de eventos e incidentes de seguridad	Acompañar a la Oficina de las Tecnologías de información y las comunicaciones en la gestión, evaluación e implementación de acciones de respuesta frente a eventos e incidentes de seguridad de la información
	Seguridad de la Documentación generada en los procesos	Apoyar técnicamente la elaboración de lineamientos y controles para mejorar la seguridad de los datos procesados en los procesos institucionales a través de sistemas de información
	Seguridad de Aplicaciones de procesamiento de información de las plataformas estratégicas	Apoyar el diseño e implementación de lineamientos y controles que mejoren los niveles de seguridad de sistemas de información institucionales como Furag III, Sigep II, Suite SIE
		Apoyar el diseño y adopción de procedimientos de protección de datos personales para los procesos institucionales y sistemas de información misionales que realicen tratamiento de datos personales
	Política de Teletrabajo	Diseñar y apoyar la adopción de controles y lineamientos de seguridad de la información para la estrategia institucional de teletrabajo

Eje	Área	Actividades Realizadas
	Análisis de vulnerabilidades de plataforma tecnológica	Realizar análisis de vulnerabilidades sobre los componentes de infraestructura tecnológica y de servicios de la Entidad
	Ingeniería social	Apoyar el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de los funcionarios, contratistas y colaboradores de la Entidad

Tabla 3 principales actividades realizadas durante la vigencia 2020

4. Plan para la implementación del modelo de privacidad y seguridad 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 análisis del estado actual de la implementación de seguridad y privacidad de la información, se establece el siguiente plan para la implementación del Modelo de Seguridad y Privacidad de la Información:

4.1. Hoja de Ruta 2021

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
Transformación Digital	Transferencia de información		Identificar los riesgos de seguridad digital y Diseñar los controles de seguridad necesarios para garantizar las seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros.	Decreto 2106/2018 Ley 1581/2012 PND Transformación Digital, Art 147	Matriz de riesgos de seguridad de la información para los convenios suscritos por la Entidad cargada en Sistema de Gestión Institucional					X					X			
	Seguridad para los Servicios ciudadanos digitales (sistemas digitales)		Documentar el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales	Decreto 1377 de 2013, Ley 1581 de 2012	Manual Actualizado de protección de datos personales para sistemas de información con información de carácter personal									X				

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
Riesgos	Actualización de panorama de riesgos de seguridad digital		Acompañar los procesos institucionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgo de seguridad digital	Decreto 1078/2015, Política de gobierno Digital	Planes de tratamiento de riesgos de seguridad Digital, cargados en sistema de gestión institucional						X					X		
	Seguimiento a la implementación de planes de tratamiento de riesgos		Acompañar a la Oficina asesora de planeación en el seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los procesos	Decreto 1078/2015, Política de gobierno Digital	Informe de seguimiento a la implementación de planes de tratamiento de riesgos						X						X	
Sensibilización	Botón de políticas de seguridad de la información.		Elaborar contenidos de sensibilización y divulgación de los componentes del sistema de gestión de seguridad de la información institucional y apoyar su publicación en la intranet Institucional	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Plan anual de sensibilización en seguridad de la información			X										
	Sensibilización contratistas		Realizar sesiones de sensibilización sobre seguridad de la información y controles del sistema de gestión de seguridad de la información institucional para el equipo de contratistas de la Entidad	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Informe de resultados de la implementación del plan de sensibilización en seguridad de la información						X						X	
	Reinducción e inducción de funcionarios (apoyo a GGH)		Apoyar las actividades de inducción y reinducción de los funcionarios de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles del sistema de gestión	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Resultado de las charlas en seguridad de la información para directivos, servidores y contratistas						X						X	

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
			de seguridad de la información															
	Gestión de cambio cultural en materia de seguridad de la información (interno y externo con Grupos de valor)		Acompañar del desarrollo e implementación de estrategias de gestión de cambio para funcionarios y contratistas del Departamento Administrativo de la función Pública en materia de apropiación del sistema de gestión de seguridad de la información.	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Diseño de estrategia piloto de gestión de cambio en seguridad de la información interno						X							
					Informe de resultado de implementación de piloto interno de cambio cultura en materia de seguridad digital											X		
	Divulgación de la documentación , controles y herramientas de ayuda del sistema de gestión de seguridad de la información		Diseñar e implementar acciones de socialización de la documentación, controles y herramientas del sistema de gestión de seguridad de la información institucional	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Informe de socialización de documentación del Sistema de gestión de seguridad de la información					X				X			X	
Ciberseguridad-OTIC	Contacto con partes interesadas	Comando Conjunto Cibernético	Participar como delegado del Departamento Administrativo de la Función Pública en las sesiones de trabajo del Comando Conjunto Cibernético del Ministerio de Defensa para la implementación del Plan Nacional de Protección de Infraestructuras Críticas Cibernéticas	Documento CONPES 3854 Política Nacional de Ciberseguridad	Informe de actividades de participación en mesas de trabajo del comando conjunto cibernético				X	X	X	X	X	X	X	X		

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
	Proyectos de infraestructura de seguridad (plan estrategico con OTIC)	Centro de respuesta a incidentes de seguridad	Servir como punto de Contacto técnico con el Centro de respuesta incidentes informáticos del Ministerio de Defensa para realizar la gestión de eventos e incidentes de seguridad de la información que afecten los servicios o la infraestructura de la Entidad	Documento CONPES 3854 Política Nacional de Ciberseguridad	Informe de actividades de gestión de incidentes de seguridad de la información escalados o gestionados ante el centro de respuesta de incidentes de seguridad informática del Ministerio de Defensa				X	X	X	X	X	X	X	X			
		MINTIC	Servir como punto de Contacto técnico con el Ministerio de las tecnologías de información y las comunicaciones en materia de seguridad Digital	Decreto 1078 de 2015, política gobierno digital	Informe de participación en actividades de seguridad digital adelantadas por MINTIC				X				X				X		
		Detección de intrusos -Open source	Apoyar técnicamente la implementación de soluciones de detección de intrusos que protejan la infraestructura de servicios institucionales	Plan nacional de desarrollo Art 147. 5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio	Acompañamiento en la Implementación de un piloto para el sistema de detección de intrusos							X	X	X	X				
		Monitorización de estado de plataforma - (analítica de disponibilidad)	Apoyar técnicamente la implementación de soluciones de monitorización de disponibilidad de componentes tecnológicos, infraestructura de servicios y sistemas de información institucionales	Plan nacional de desarrollo Art 147. 5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio.	Especificaciones técnicas para la adquisición de un sistema monitorización de disponibilidad de infraestructura tecnológica							X							

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
		Web application Firewall	Apoyar técnicamente la implementación de soluciones de protección perimetral de los sistemas de información ante ataques cibernéticos	Plan nacional de desarrollo Art 147. 5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio.	Implementación de las recomendaciones del sistema protección perimetral tipo firewall para aplicaciones Web						X	X	X					
		Seguridad en puesto de trabajo	Apoyar técnicamente la implementación de soluciones de seguridad que protejan las estaciones de trabajo institucionales frente a software malicioso o fuga de información	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Implementación de controles de seguridad para asegurar estaciones de trabajo de usuario final										X				
					Implementación de las recomendaciones a partir de la viabilidad para la unificación de la autenticación.									X					
		Aprovechamiento de funciones de seguridad de Office 365	Apoyar técnicamente el diseño e implementación de controles de seguridad que aprovechen las soluciones colaborativas y de ofimática disponibles en la Entidad	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Análisis para la implementación de controles de seguridad de la información de la suite de Office 365 adquirida por la entidad.				X										

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
	Continuidad de la plataforma tecnológica y de servicios	Seguridad en la Nube privada y pública	Acompañar el diseño de lineamientos y controles de seguridad que mitiguen los riesgos que puedan impactar la infraestructura de servicios de nube privada institucional	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Lineamientos de seguridad para el uso de plataformas de nube contratada por la entidad.						X	X						
		Actualización de plan de continuidad	Acompañar técnicamente el diagnóstico, diseño e implementación del Plan de Continuidad de Negocio Institucional	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Análisis de impacto al negocio para los procesos institucionales, Plan continuidad actualizado, priorizado por vigencia y propuesta de plan de pruebas para el plan de continuidad.								X					
					Informe de pruebas realizadas al plan de continuidad de negocio de conformidad con la priorización establecida para cada vigencia											X		
	Elaboración de Plan Estratégico de Seguridad de la información	Elaborar Hoja de ruta de proyectos de seguridad de la información 2021-2022	Acompañar la elaboración de los componentes del plan estratégico de gestión de seguridad de la información de la Entidad	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Plan estratégico de gestión de la seguridad de la información vigencias 2021-2022					X								

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
Sistema integrado de planeación y gestión	Gestión de la Documentación del Sistema de gestión de seguridad de la información	Actualización del contexto de la seguridad	Realizar la actualización del documento de contexto de seguridad de la información institucional	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Documento actualizado de contexto de la seguridad de la información			X										
		Adopción de políticas de seguridad	Diseñar estrategias y controles que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales	Plan Nacional de desarrollo Art 147. 11. Inclusión y actualización permanente de políticas de seguridad y confianza digital.	Documento de controles de seguridad que soporten las políticas de seguridad de la información institucional			X							x			
					Implementación de controles que soportan las políticas de seguridad institucionales.						X						X	
		TRD de documentos del sistema de gestión de seguridad de la información	Apoyar el diseño de lineamientos y controles que mejoren los niveles de seguridad de los repositorios de información	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Propuesta de estructura de tabla de retención de documentos del sistema de gestión de seguridad de la información					X								
					Implementación de los ajustes al sistema de gestión documental en la TRD del repositorio documental, una vez aprobados por el Archivo General de la Nación											X		
		Actualización de procedimientos de seguridad de la información	Elaborar y actualizar los documentos del sistema de gestión de seguridad de la información requeridos por la Norma ISO 27001 y el modelo de seguridad y privacidad de la Información recomendado por el Ministerio de las Tecnologías de la	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Procedimientos del sistema de gestión de seguridad de la información actualizados						X				X			

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
			Información y las Comunicaciones															
	Medición del desempeño	Evaluación de la efectividad de controles de la seguridad	Realizar la evaluación de la efectividad de los controles de seguridad de la información adoptados por la Entidad para el tratamiento de los riesgos de seguridad Digital	Plan Nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Informe de desempeño de los controles de seguridad de la información						X					X		
		Medición del desempeño de la gestión de la seguridad (indicadores)	Recolectar la información necesaria para realizar al cálculo de los indicadores del sistema de gestión de seguridad de la información y realizar el cálculo de dichos indicadores	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Ficha de indicadores de seguridad de la información diligenciada			X			X			X			X	
	Lineamientos de adopción del Oficial de Seguridad de la Información en Entidades de la Rama Ejecutiva		Apoyar técnicamente la elaboración de una directriz con alcance a todas la entidades del estado para la adopción del rol de oficial de seguridad de la información	Documento CONPES 3854 Política Nacional de Ciberseguridad	Borrador de lineamiento para adopción del rol de oficial de seguridad de la información a nivel de las entidades del estado						X							

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
Seguridad operativa	Gestión de eventos e incidentes de seguridad		Acompañar a la Oficina de las Tecnologías de información y las comunicaciones en la gestión, evaluación e implementación de acciones de respuesta frente a eventos e incidentes de seguridad de la información	Documento CONPES 3854 Política Nacional de Ciberseguridad	Informe de atención a los eventos o incidentes de seguridad de la información			X			X			X			X	
	Seguridad de la Documentación generada en los procesos	Seguridad para el procesamiento de datos desde la captura hasta el almacenamiento y distribución	Apoyar técnicamente la elaboración de lineamientos y controles para mejorar la seguridad de los datos procesados en los procesos institucionales a través de sistemas de información	Plan Nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Lineamientos de seguridad para la etapas de captura, procesamiento y almacenamiento de la información gestionada por los procesos institucionales					X				X				
		Controles de seguridad sobre la información gestionada (carpetas compartidas, plataforma Office 365)	Apoyar el diseño e implementación de lineamientos y controles que mejoren los niveles de seguridad de los repositorios de información configurados en la plataforma Office 365 de la Entidad	Plan Nacional de desarrolllo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Implementación de controles de seguridad de la información de la plataforma Office 365						X			X				
					Informe de resultados de la implementación de controles de seguridad sobre plataforma Office 365										X			

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
	Seguridad de Aplicaciones de procesamiento de información de las plataformas estratégicas	seguridad sobre los sistemas de información FURAG III, SIGEP II, SUIT	Apoyar el diseño e implementación de lineamientos y controles que mejoren los niveles de seguridad de sistemas de información institucionales como Furag III, Sigep II, Suite SIE	Plan nacional de desarrollo Art 147. 6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.	Análisis de seguridad para los sistemas de información misionales y recomendaciones						X					X		
		Manuales de seguridad para protección de datos personales y aplicaciones misionales	Apoyar el diseño y adopción de procedimientos de protección de datos personales para los procesos institucionales y sistemas de información misionales que realicen tratamiento de datos personales	Ley 1581 de 2012 y decreto 1377 de 2013	Procedimientos de seguridad de la información para la protección de información personal gestionada por los sistemas de información institucionales							X			X			
					Implementación de controles de seguridad para bases de datos en el registro nacional de bases de datos						X			X				
		Mejoramiento de roles y privilegios sobre las aplicaciones y servicios informáticos	apoyar las actividades de identificación, mejoramiento e implementación de roles de seguridad para los servicios de información de la entidad	Plan nacional desarrollo Art 147. 6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.	Afinamiento e implementación de controles para el esquema de roles y privilegios de los sistemas de información y bases de datos gestionadas por la Entidad							X						
					Ajuste al procedimiento de administración de usuarios para roles y privilegios en sistemas de información						X			X				
	Cumplimiento de normas legales	Implementación de controles de seguridad	Documentar los controles de seguridad de la información que	Plan nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de	Plan de implementación de controles de seguridad que soportan los requisitos del				X									

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
		para certificar cumplimiento de requisitos legales (Registro Nacional de bases de datos, autorización de tratamiento de datos personales, transparencia y acceso a la información pública	permiten el cumplimiento de los requisitos legales en materia de seguridad de la información obligatorios para la Entidad	estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Registro Nacional de Bases de datos													
	Seguridad del sitio web Institucional	Seguridad sobre sitios web con información disponible al ciudadano	Identificar vulnerabilidades sobre los sitios web institucionales y formular planes de mejoramiento para realizar su tratamiento	Plan nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Realizar la aplicación de Ethical Hacking al portal y micrositios y dar recomendaciones						X					X		
	Política de Teletrabajo	Mejorar estrategias de seguridad para Teletrabajo	Diseñar y apoyar la adopción de controles y lineamientos de seguridad de la información para la estrategia institucional de teletrabajo	Plan nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Lineamientos de seguridad para la estrategia de teletrabajo institucional			X										

Eje	Área	Sub-actividad	Descripción	Marco Legal	Entregable	1 Er. Semestre						2 Do Semestre						2022
						E	F	M	A	M	J	J	A	S	O	N	D	
	Análisis de vulnerabilidades de plataforma tecnológica	Análisis de seguridad técnico de aplicaciones	Realizar análisis de vulnerabilidades sobre los componentes de infraestructura tecnológica y de servicios de la Entidad	Plan nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Informe del análisis de vulnerabilidades sobre la infraestructura tecnológica institucional							X					X	
	Ingeniería social	Análisis de nivel de conciencia en seguridad de la información	Apoyar el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de los funcionarios, contratistas y colaboradores de la Entidad	Plan nacional de desarrollo Art 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Informe de resultados de pruebas de ingeniería social										X			

Tabla 5 Hoja de ruta -Plan de seguridad y privacidad de la información

Plan de Seguridad y Privacidad de la Información

VERSIÓN 3

Proceso de Tecnologías de la Información

Enero de 2021

Departamento Administrativo de la Función Pública

Carrera 6 n.º 12-62, Bogotá, D.C., Colombia

Conmutador: 7395656 Fax: 7395657

Web: www.funcionpublica.gov.co

eva@funcionpublica.gov.co

Línea gratuita de atención al usuario: 018000 917770

Bogotá, D.C., Colombia.