
 <div>El futuro digital es de todos</div> <div>Gobierno de Colombia MinTIC</div>	ARQUITECTURA INSTITUCIONAL	Código	SPI- TIC- CD- 001	
	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	CARTA DESCRIPTIVA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión	1	

Líder de Proceso:	Oficial de Seguridad y Privacidad de la Información • Asesor
--------------------------	---

Objetivo:	Garantizar permanentemente la Seguridad y Privacidad de la información, seguridad digital y continuidad de la operación de los servicios, por medio de la definición de políticas, programas, lineamientos, estrategias, actividades conforme a la normativa aplicable y lo establecido en el plan de acción, con el fin de generar confianza y seguridad digital a los grupos de interés del Ministerio.
------------------	---

Alcance:	El proceso inicia con la definición de los lineamientos para la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios del Ministerio/Fondo único TIC, continua con el acompañamiento a las áreas y entidades adscritas al sector y finaliza con la implementación, evaluación y seguimiento de estos.
-----------------	--

Documentos internos y externos:	• MIG-TIC-DI-005 Listado de Documentos Externos e Internos MINTIC
--	---

Recursos:	Humanos: funcionarios y contratistas de seguridad y privacidad de la información. Financieros: presupuesto asignado por la Entidad. Físicos: puestos de trabajo, instalaciones físicas dispuestas por la Entidad. Tecnológicos: Infraestructura Tecnológica, Sistema de Información del Modelo Integrado de Gestión - SiMIG.
------------------	---

Requisitos Legales:	• Documentos internos y externos
----------------------------	--

Requisitos de las normas técnicas aplicables al proceso:	Requisitos NTC ISO 9001:2015 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 7.5.1 Generalidades 7.5.2 Creación y actualización 8.1 Planificación y control operacional 8.2 Requisitos para los productos y servicios 9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 10. Mejora
---	--

Políticas de operación:	1. El Oficial de Seguridad y Privacidad de la Información actualizará periódicamente la documentación referente al proceso 2. El líder del proceso apoyará en la implementación de los controles de seguridad y privacidad de la información al interior de las dependencias 3. El líderes del proceso ejecutará las estrategias de cambio y cultura para la apropiación de los temas en seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en el interior de las dependencias.
--------------------------------	---

Proveedores	Entradas	No. PHVA	Descripción de la actividad	Responsable	PPC	Salidas	Clientes
	1. Normatividad legal vigente y lineamientos en materia de Seguridad y Privacidad de la Información y seguridad digital						

1. Gobierno Nacional	2. Plan Estratégico Institucional Plan Estratégico Sectorial Marco Estratégico Plan de acción anual Avance en las metas del Plan Estratégico Sectorial, Plan Estratégico Institucional y Plan de Acción Anual	2. Lineamientos y directrices para la gestión institucional, políticas de gestión institucional, Revisión por la Dirección, DOFA, Contexto Interno y Externo, etc.)	Planear la Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio	CGSI1. Validar la divulgación y apropiación de la política y lineamientos	1. Plan de Seguridad y Privacidad de la información	
2. Direccionamiento Estratégico	3. Necesidades de los procesos y proyectos frente a lineamientos, procedimientos y directrices para el cumplimiento de seguridad y privacidad y privacidad de la información, seguridad digital y continuidad de la operación.	3. Necesidades de los procesos y proyectos frente a lineamientos, procedimientos y directrices para el cumplimiento de seguridad y privacidad y privacidad de la información, seguridad digital y continuidad de la operación.	A partir del contexto estratégico, los lineamientos del Gobierno Nacional, las directrices para la gestión institucional, la normatividad aplicable y las necesidades de los procesos frente a la implementación de seguridad y privacidad de la información, se realiza un análisis para la planeación estructurada y detallada de las actividades necesarias que den cumplimiento a dichos requisitos, enmarcados en un plan de seguridad y privacidad de la Información asociado al Plan de Acción de la Entidad. Se definen los compromisos para su implementación, a través de políticas institucionales de seguridad y privacidad de la información, documentos que especifican actividades y criterios de aplicación de los controles técnicos y administrativos, los cuales se aprueban en Comité MIG, con el fin de propender por la confidencialidad, integridad, disponibilidad y privacidad de la información de la Entidad, así como, la continuidad de la prestación del servicio público de TIC en el país	CGSI2. Revisión y aprobación por el COMITÉ MIG de los Planes, Políticas y Manuales de Seguridad y privacidad de la información	1. Plan Operativo	
3 Todos los procesos	4. Comité Institucional de Coordinación de Control interno	4. Lineamientos frente a la Administración de Riesgos de Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación		CGSI3. Verificar la ejecución de los controles definidos a través del diligenciamiento de la herramienta diseñada.	1 y 3 Política de Seguridad y Privacidad de la información	
5. Grupos de interés (CSIRT, CCOCI, MINTIC, Policía Nacional - DIJIN, CCP - Centro Cibemético Policial, COLCERT, SIC - Superintendencia de Industria y comercio)	6. Organización Internacional de Estandarización (ISO)	5. Nuevas tecnologías, tendencias en seguridad de la información y ciberseguridad, grupos, foros, sitios, boletines de seguridad de la información y ciberseguridad	Ministro Oficial de Seguridad y Privacidad de la Información Comité MIG • Asesor	CGSI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información.	1 y 3 Manual de Políticas de seguridad y Privacidad de la información	1. Todos los procesos
7 Instituto Nacional de Estándares y Tecnología - NIST	8. Entidades Adscritas al Ministerio	6 Estándares nacionales e internacionales en seguridad y privacidad de la información, Seguridad Digital y Continuidad de		CGSI5. Solicitar a las dependencias competentes en la oportunidad debida los recursos y el personal necesario para poder ejercer las actividades del plan Seguridad y privacidad de la información.	1 y 3 Política de Tratamiento de datos personales	2. Entidades Adscritas
					1. Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información	3. Grupos de Interés
					1 y 3 MIG-TIC-MA-010 - Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales	
					1. Plan de Continuidad de la operación de los servicios del Ministerio/Fondo Único TIC	
					2. Lineamientos para las Entidades adscritas al Ministerio	

	<p>la operación.</p> <p>7. Lineamientos para la identificación de las Infraestructuras Críticas Cibemáticas del país del Sector TIC</p> <p>8. Contexto interno y externo de las entidades adscritas al Ministerio referente a seguridad y privacidad de la información, seguridad digital y continuidad de la Operación</p>							
<p>1. Proceso de Seguridad y Privacidad de la información</p> <p>2. Grupos de interés (Colaboradores, Usuarios, Proveedores externos)</p>	<p>1. Plan de Seguridad y Privacidad de la información</p> <p>1. Plan Operativo para la implementación de actividades que permitan dar cumplimiento a la normatividad de seguridad y privacidad de la información</p> <p>1. Política de Seguridad y Privacidad de la información</p> <p>1. Manual de Políticas de seguridad y Privacidad de la información</p> <p>1. Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales</p> <p>1. Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información</p> <p>1. Lineamientos, procedimientos y directrices para el cumplimiento de seguridad y privacidad de la información</p> <p>2. Nuevas tecnologías,</p>	2	H	<p>Implementar los lineamientos establecidos</p> <p>De acuerdo con la planeación realizada, se lleva a cabo la identificación de los activos de información y su clasificación, para determinar los riesgos de seguridad y privacidad de la información, seguridad digital y de interrupción de la operación, y de esta manera gestionar efectivamente los incidentes y vulnerabilidades de seguridad y privacidad de la información, de acuerdo a lo enmarcado en la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios del Ministerio</p> <p>Con base en lo anterior, se desarrollan actividades de uso y apropiación con el fin de generar una cultura basada en la confianza y seguridad digital y de la información, propendiendo por la confidencialidad, integridad, disponibilidad, privacidad y no repudio de la información, así como la continuidad de la operación.</p>	<p>Oficial de Seguridad y Privacidad de la Información</p> <p>Todas las Dependencias</p> <p>• Asesor</p>	<p>CGSI1. Validar la divulgación y apropiación de la política y lineamientos</p> <p>CGSI2. Revisión y aprobación por el COMITÉ MIG de los Planes, Políticas y Manuales de Seguridad y privacidad de la información</p> <p>CGSI3. Verificar la ejecución de los controles definidos a través del diligenciamiento de la herramienta diseñada.</p> <p>CGSI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información.</p> <p>CGSI5. Solicitar a las dependencias competentes en la oportunidad debida los recursos y el personal necesario para poder ejercer las actividades del plan Seguridad</p>	<p>Evidencias de las actividades implementadas:</p> <p>1 y 3. Matriz de activos y clasificación de información y de ciberseguridad revisados</p> <p>1. Riesgos de seguridad y privacidad de la información identificados, valorados y tratados</p> <p>1, 2 y 3. Informe de incidentes de seguridad revisados</p> <p>1 y 3. Vulnerabilidades técnicas gestionadas y Planes de remediaciones</p> <p>1 y 2 Propuestas para estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios</p> <p>1, 2, 3 Matriz de Requisitos legales correspondiente a seguridad y</p>	<p>1. Todos los procesos</p> <p>2. Grupo de interés</p> <p>3. Entes de Control</p>

	tendencias en seguridad de la información y ciberseguridad, grupos, foros, sitios, boletines de seguridad de la información y ciberseguridad				y privacidad de la información.	privacidad de la información revisada	
1. Todos los procesos Grupos de interés (Aliados, Operadores externos) 2. Organización Internacional de Estandarización (ISO) 3.Gobierno Nacional 4. Proceso de Seguridad y Privacidad de la información 5. Gestión del Talento Humano 6. Gestión de Atención a Grupos de Interés	1 y 4. Resultados del Plan de Continuidad de la Operación 2. Estándares nacionales e internacionales en seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación. 3. Lineamientos impartidos por la estrategia de Gobierno Digital 5 Plan de Salud y Seguridad en el Trabajo 6. Informe de avance estrategias RSI (política Ambiental)	3	H	Implementar el Plan de Continuidad de la Operación de los Servicios Implementación de la continuidad de la operación, realizando un análisis de impacto a la operación (BIA), determinando los procesos críticos de la Entidad basados en una gestión de riesgos de interrupción de los servicios, con el fin de generar unos escenarios de recuperación ante desastres de cualquier tipo o interrupciones parciales o totales de la operación, a través de la implementación de un plan de recuperación de desastres (DPR) y el plan de continuidad de la operación de los servicios del Ministerio (BCP), asegurando la disponibilidad de las instalaciones del procesamiento de la información y los servicios. Con base en lo anterior, se desarrollan actividades de uso y apropiación con el fin de generar una cultura con el fin de propender por la continuidad y no interrupción de la prestación del servicio público de TIC para el país.	Ministro Oficial de Seguridad y Privacidad de la Información Todas las dependencias • Asesor	CGSI1. Validar la divulgación y apropiación de la política y lineamientos CGSI2. Revisión y aprobación por el COMITÉ MIG de los Planes, Políticas y Manuales de Seguridad y privacidad de la información CGSI3. Verificar la ejecución de los controles definidos a través del diligenciamiento de la herramienta diseñada. CGSI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información. CGSI5. Solicitar a las dependencias competentes en la oportunidad debida los recursos y el personal necesario para poder ejercer las actividades del plan Seguridad y privacidad de la información. 1. Análisis de impacto - BIA 1 y 2. Planes de continuidad de la operación y de recuperación ante desastres 1. Matrices de Riesgos de interrupcion de Continuidad a la operación de los servicios actualizadas a la vigencia 1. Resultados de las pruebas del BCP plan de continuidad del negocio y DRP plan de recuperación de desastres 1 y 2. Propuestas para estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios	1. Todos los procesos 2. Grupos de interés
1. Gobierno	1 y 3 Normativa aplicable y guías emitidas			Implementar los lineamientos para la protección y tratamiento de datos personales A partir de los lineamientos, normativa y buenas prácticas en cuanto a la Protección de Datos Personales, se implementa la política de tratamiento de Datos Personales y el Manual de lineamientos de Seguridad		CGSI1. Validar la divulgación y apropiación de la política y lineamientos CGSI2. Revisión y aprobación por el COMITÉ MIG de los Planes, Políticas y Manuales de Seguridad y privacidad de la información CGSI3. Verificar la ejecución de los controles definidos a través del diligenciamiento 1. Implementación de Procedimientos, guías, controles etc. relacionados con protección de datos personales	

Nacional	para la protección de datos personales			para la protección y tratamiento de Datos Personales, se obtienen a través de diferentes mecanismos, las bases de datos que contienen datos de personas naturales en la Entidad, se realiza el análisis de la información reportada y se reporta al Registro Nacional de Bases de Datos a través del aplicativo dispuesto por la Superintendencia de Industria y Comercio lo anterior con el propósito de cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.	Oficial de Seguridad y Privacidad de la Información Todas las Dependencias • Asesor	de la herramienta diseñada. CGSI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información. CGSI5. Solicitar a las dependencias competentes en la oportunidad debida los recursos y el personal necesario para poder ejercer las actividades del plan Seguridad y privacidad de la información. CSPI6. Verificar que el compromiso de confidencialidad para los contratistas del proceso.	1 y 3. Inventario de bases de datos personales 1, 2, 3 . Reportes Registro Nacional de Bases de Datos personales 1. Propuestas para estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios	1. Todos los procesos 2. Superintendencia de Industria y Comercio 3. Entes de Control
4. Proceso de Seguridad y Privacidad de la información	2y 4. Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales	4	H	Con base en lo anterior, se desarrollan actividades de uso y apropiación con el fin de generar una cultura con el fin de propender por protección de los datos personales en la Entidad.				
1. Proceso Seguridad y Privacidad de la información 2. Evaluación y Apoyo al Control de la Gestión 3. Proceso Direccionamiento Estratégico 4. Entes externos de control 5. Entes certificadores 6. Departamento Administrativo de la Función Pública	1. Procedimientos, Indicadores de eficacia y efectividad, Riesgos de Seguridad y Privacidad de la información 2. Plan de Auditorías Internas 4 y 5. Plan de Auditorías Externas 6. Resultado del cuestionario del FURAG	5	V	Realizar seguimiento y medición de la implementación de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación Hacer seguimiento y evaluación de las actividades del proceso. De igual manera realizar la medición de los indicadores y el seguimiento a la implementación de controles de los riesgos de seguridad y privacidad, seguridad digital y continuidad de la operación, identificados y el cumplimiento de los procedimientos asociados, siendo el insumo para la revisión por la dirección, que permita la toma de decisiones sobre la Seguridad y privacidad de la información en la Entidad.	Ministro Oficial de Seguridad y Privacidad de la Información Evaluación y Apoyo al Control de la Gestión Fortalecimiento Organizacional	CGSI3. Verificar la ejecución de los controles definidos a través del diligenciamiento de la herramienta diseñada. CGSI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información. CGSI5. Solicitar a las dependencias competentes en la oportunidad debida los recursos y el personal necesario para poder ejercer las actividades del plan Seguridad y privacidad de la información.	1. Resultados de la medición de: - Indicadores de eficacia y efectividad - Implementación de controles para los riesgos identificados - Cumplimiento de los planes derivados del proceso	1. Todos los procesos 2. Entes de Control
				Identificar el conocimiento requerido para el fortalecimiento de su operación e implementar las estrategias de gestión del conocimiento que apliquen Identificar el conocimiento requerido para el fortalecimiento de su				

Gestión del Conocimiento	Lineamientos de gestión del conocimiento	6	V	<p>operación: Cada uno de los procesos realizarán la actividad relacionada con la identificación de conocimientos requeridos teniendo en cuenta el marco estratégico institucional (misión, visión objetivos, funciones, carta descriptiva del proceso, lecciones aprendidas, plan estratégico y plan acción de su área o dependencia). El conocimiento requerido no existente puede ser generado a través de las estrategias de gestión del conocimiento y sus mecanismos de transferencia o del plan institucional de capacitación.</p> <p>Implementar las estrategias necesarias para el mejoramiento de su gestión a partir de la gestión del conocimiento: De acuerdo a los lineamientos impartidos desde el proceso de GESCO (Gestión del conocimiento), se deben aplicar las herramientas suministradas para el desarrollo de la estrategia a implementar</p>	Oficial de Seguridad y Privacidad de la Información	Revisar la implementación de las estrategias de gestión del conocimiento.	<p>Documento soporte de la estrategia implementada teniendo en cuenta la herramienta disponible.</p> <p>Información para el Inventario de activos de conocimiento del proceso</p> <p>Información para el listado de conocimiento estratégico existente y faltante del proceso</p>	<p>1. Gestión del conocimiento</p> <p>2. Gestión del talento humano</p>
<p>Departamento Administrativo de la Función Pública</p> <p>Fortalecimiento Organizacional</p> <p>Entes internos y externos de control y normativos</p> <p>Proceso Gestión de Atención a Grupos de Interés</p>	<p>Lineamientos para la gestión organizacional de las entidades públicas</p> <p>Criterios de autoevaluación para su aplicación en los procesos de la Entidad</p> <p>Resultados del seguimiento, gestión y desempeño de los procesos y del MIG</p> <p>Resultados del seguimiento, gestión y desempeño de Fortalecimiento Organizacional (indicadores, riesgos, acciones de mejora)</p> <p>Documentación para la operación al interior del Ministerio en términos de procesos</p> <p>Lineamientos, estrategias y políticas internas del MIG</p> <p>Resultados de las mediciones de gestión y desempeño</p>	7	A	<p>Realizar seguimiento, autoevaluación y formulación de acciones con base en los resultados de la gestión del proceso, ejecución de los requisitos y controles establecidos en el Sistema Integrado de Gestión</p> <p>Con base en la información registrada de la gestión del proceso (indicadores, monitoreo de riesgos, Plan Operativo del Sistema Integrado de Gestión, acciones de mejora, respuesta a PQRS, conocimientos requeridos para la eficiencia de la entidad, entre otros) se define la necesidad de formular acciones de mejora para actualizar sus documentos, identificar requisitos aplicables al proceso para su actualización constante y reorientar el desempeño del proceso cuando se presentan incumplimientos o se proponen transformaciones de las prácticas institucionales, las cuales se evidenciarán mediante el seguimiento a controles de manera periódica según los lineamientos para el fortalecimiento organizacional. Esta actividad hace parte de la</p>	<p>Líder del Proceso Oficial de Seguridad y Privacidad de la Información</p> <p>Líderes del Sistema Integrado de Gestión</p> <p>Gestor del Proceso</p> <p>• Coordinador</p>	<p>Verificar el cumplimiento del Plan Operativo del Sistema Integrado de Gestión.</p> <p>Revisar y hacer seguimiento de respuestas a las solicitudes registradas en el sistema de gestión documental de la entidad, por parte del facilitador documental del grupo.</p> <p>Verificar que se realice la consolidación y</p>	<p>Cumplimiento del Plan Operativo del Sistema Integrado de Gestión, verificando los requisitos de cada sistema.</p> <p>Necesidades de fortalecimiento del Proceso (recursos, actualización documental, buenas prácticas).</p> <p>*Acciones de mejora del proceso formuladas, requeridas</p> <p>*Acciones de gestión que requieran incorporarse o actualizarse en el plan FOGEDI</p> <p>*Resultados de</p>	<p>Todos los procesos</p> <p>Fortalecimiento organizacional</p>

Líder del Sistema Integrado de Gestión	institucional			autoevaluación del proceso.	registro de la información de Seguimiento a la gestión del proceso.	la autoevaluación, gestión y desempeño del proceso y del MIG (riesgos, indicadores, diseño de procesos y productos o servicios, control de salida no conforme, seguridad de la información, protección de datos personales, entre otros)
Comité MIG	Lineamientos y estrategias para el fortalecimiento de la apropiación del MIG			Notas: Respecto de la autoevaluación del proceso, se deben tener en cuenta lo anterior, así como el contexto organizacional y del proceso, su gestión y desempeño, las buenas y mejores prácticas derivadas de la aplicación de las actividades del mismo, para contar con un panorama general que permita orientar la toma de decisiones en caminadas al fortalecimiento institucional.	Verificar y analizar la información de gestión del proceso	
Proceso de Fortalecimiento Organizacional	Actas de Comité MIG					
Gestión del conocimiento	Informe de resultados de auditorías internas y externas					
	Resultados encuesta de satisfacción PQRS					
	Plan Operativo del Sistema Integrado de Gestión			Las acciones de mejora derivadas del seguimiento y autoevaluación del proceso deben cumplir con los criterios definidos en el proceso de Fortalecimiento Organizacional.		
	Conocimientos requeridos para la eficiencia de la entidad					

Indicadores:	<ul style="list-style-type: none"> • Porcentaje de incidentes de Seguridad y Privacidad de la Información • Porcentaje de eficacia del Modelo de Seguridad y Privacidad de la Información • Porcentaje de efectividad del Plan Operativo del Modelo de Seguridad y Privacidad de la Información.
---------------------	---

Riesgos::	<ul style="list-style-type: none"> • Mapa de Riesgos Seguridad y Privacidad de la Información
------------------	--

VERSIÓN	FECHA	DESCRIPCIÓN
1	04/Dic/2020	Creación del documento.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Giovanni Andres Espitia Roa Cargo: Contratista Fecha: 04/Dic/2020	Nombre: Laura Yádira Abril Frade Cargo: Funcionario Fecha: 04/Dic/2020 Nombre: Giovanni Andres Espitia Roa Cargo: Contratista Fecha: 04/Dic/2020 Nombre: Carolina Castañeda de Avila Cargo: Funcionario Fecha: 04/Dic/2020	Nombre: Andres Diaz Molina Cargo: Funcionario Fecha: 06/Dic/2020 Nombre: Diego Luis Ojeda León Cargo: Funcionario Fecha: 07/Dic/2020

COPIA CONTROLADA