Líder de Proceso:	Oficial de Seguridad y Privacidad de la Información
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-023 Matriz Identificación de Requisitos Legales y de Otra Índole
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:	• MIG-TIC-DI-023 Matriz Identificación de Requisitos Legales y de Otra Índole
Requisitos de las normas tecnicas aplicables al proceso:	• MIG-TIC-DI-025 Matriz relación ISO_PROCESOS

1. 1. SISTEMA INTEGRADO DE GESTIÓN (SIG)
1.1 Identificación y socialización de los requisitos legales y otros requisitos aplicables del Sistema Integrado de Gestión de acuerdo con el procedimiento establecido.
1.2 Reporte y cumplimiento del Plan Operativo del Sistema Integrado de Gestión.
1.3 Todos los integrantes del proceso, independiente de su tipo de vinculación, participarán en la identificación, valoración y seguimiento de peligros ocupacionales, riesgos de corrupción, gestión, ambiental, Seguridad y privacidad de la información, Seguridad Digital,
continuidad de la operación y determinación de controles de acuerdo con la metodología de riesgos.
1.4 Identificación de necesidades, competencias, formación y expectativas para el fortalecimiento del Sistema Integrado de Gestión.
1.5 El Líder y gestor de proceso serán los responsables de implementar los lineamientos, procedimientos, manuales y normativa aplicable al Sistema Integrado de Gestión de acuerdo con los roles y responsabilidades enmarcados en la resolución del MIG.
1.6 Los lideres y equipos de trabajo participarán en las actividades de cambio, cultura y prevención del Sistema Integrado de Gestión.

1.7. Sistema de Gestión de Seguridad y Privacidad de la Información (SG-SyPI)
1.7.1 Identificación, actualización y aprobación de los activos de información del proceso de acuerdo con el Plan de Seguridad y Privacidad de la Información.
1.7.2 Reporte de incidentes de seguridad y privacidad de la información cuando se presenten, de acuerdo con el procedimiento de Incidentes de Seguridad y Privacidad de la Información.
1.7.3 Aprobación, implementación de los planes y participación en las estrategias de Continuidad de la operación de acuerdo con el Plan de Continuidad de la Operación de la Entidad.
1.7.4. 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.

1.8 Sistema de Gestión de Calidad (SG-GC)
1.8.1 El líder del proceso debe formular, implementar y realizar seguimiento a las actividades de promoción del uso y apropiación de su proceso y del MIG y del fortalecimiento de la cultura organizacional, como mínimo deberá implementar la estrategia de GCP
1.8.2 El proceso apropiará el MIG mediante la socialización de los lineamientos, procedimientos, indicadores, acciones de mejora,

Politicas de operación:	riesgos y controles a su equipo de trabajo en GCP. 1.8.3 El líder del proceso es el responsable de informar, divulgar y apropiar los documentos del proceso. 1.8.4 El líder y/o gestor de procesos debe revisar periódicamente la normatividad aplicable y actualizar los documentos del proceso en caso de ser necesario. 1.9 Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) 1.9.1 El líder del proceso participará en las investigaciones de incidentes de Seguridad y Salud en el Trabajo. 1.9.2 Todos los integrantes del proceso, participarán en la elección del COPASST, Comité de Convivencia Laboral, ejecución de exámenes médicos ocupacionales, establecimiento de la Política y Objetivos SST. 1.10 Sistema de Gestión Ambiental (SG-Ambiental) 1.10.1 Los lideres y equipos de trabajo desarrollaran buenas prácticas enfocadas en los programas establecidos en el Plan Institucional de Gestión Ambiental - PIGA. 1.10.2 Los lideres y equipos de trabajo deberán asistir a las charlas de sensibilización ambiental desarrolladas por el Grupo Interno de Trabajo de Fortalecimiento de las Relaciones con los Grupos de Interés - GITFRGI. 1.10.3 Los lideres y equipos incluirán criterios de sostenibilidad ambiental en los procesos de contratación cuando apliquen. 1.11 Responsabilidad Social (MRSI) 1.11.1 Los líderes del proceso deberán acatar los lineamientos definidos por el Modelo de Responsabilidad Social Institucional-RSI, aplicables al proceso, en los componentes: Económico, Ambiental, Social y de Servicio al Ciudadano, para el desarrollo de las buenas prácticas de sostenibilidad para la Entidad. 1.11.2 El líder del proceso y/o gestor del proceso o equipo de trabajo, desarrollarán y reportarán los indicadores GRI- (Global Reporting Iniciative) aplicables al proceso, teniendo en cuenta las estrategias de recolección de la información solicitado por el GITFRGI. 1.12 Gestión del Conocimiento (SG-Conocimiento) 1.12.1 Los lideres del proceso deberán seguir los lineamientos presentados por Gestión del Conocimiento referentes a la identificación del conocimiento requerido para el funcionamiento de su operación. 1.12.2 Los lideres y equipos de trabajo deberán implementar bajo los lineamientos de Gestión del Conocimiento, las estrategias necesarias para el mejoramiento de su gestión, utilizando las herramientas existentes para tal fin.

Proveedores	Entradas	No.	PHVA	Descripción de la actividad	Responsable	PPC	Salidas	Clientes
1. Gobierno Nacional	1. Normatividad legal vigente y lineamientos en materia de Seguridad y Privacidad de la Información y seguridad digital. 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.) 3. Necesidades de los procesos y proyectos frente a			Planear la Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios del Ministerio A partir del contexto estratégico, los lineamientos del Gobierno Nacional, las directrices para la gestión institucional, la			1. Plan de Seguridad y Privacidad de la información. 2. Plan Operativo de Seguridad y Privacidad de la información. 3. Política de Seguridad y Privacidad de la información.	

2. Direccionamiento Estratégico 3 Todos los procesos 4.Comité Institucional de Coordinación de Control interno 5. Grupos de interés Externos 6. Organización Internacional de Estandarización (ISO) 7 Instituto Nacional de Estándares y Tecnología - NIST 8. Entidades Adscritas al Ministerio	lineamientos, procedimientos y directrices para el cumplimiento de seguridad y privacidad y privacidad de la información, seguridad digital y continuidad de la operación. 4. Lineamientos frente a la Administración de Riesgos de Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación. 5. Nuevas tecnologías, tendencias en seguridad de la información y ciberseguridad, grupos, foros, sitios, boletines de seguridad de la información y ciberseguridad. 6 Estándares nacionales e internacionales en seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación. 7. Lineamientos para la identificación de las Infraestructuras Críticas Cibernéticas del país del Sector TIC 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.		1	**P**	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.	Oficial de Seguridad y Privacidad de la Información Comité MIG	CSPI5. 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.		4. Manual de Políticas de seguridad y Privacidad de la información. 5. Política de Tratamiento de datos personales. 6. Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información. 7. Plan de Continuidad de la operación de los servicios del Ministerio/Fondo Único TIC. 8. Lineamientos Seguridad y Privacidad de la información para las Entidades adscritas al Ministerio. 9. Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales.	1-7 y 9. Todos los procesos 8. Entidades Adscritas 3, 4, 5 y 9 Grupos de Interés
	1. Plan de Seguridad y Privacidad de la información 1. Plan Operativo para la implementación de actividades									

1. Proceso de Seguridad y Privacidad de la información. 2. Grupos de interés externos	que permitan dar cumplimiento a la normatividad de seguridad y privacidad de la información 1. Política de Seguridad y Privacidad de la información 1. Plan de Seguridad y Privacidad de la información. 1. Plan Operativo para la implementación de actividades que permitan dar cumplimiento a la normatividad de seguridad y privacidad de la información. 1. Política de Seguridad y Privacidad de la información. 1. Manual de Políticas de seguridad y Privacidad de la información. 1. Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales. 1. Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información. 1. Lineamientos, procedimientos y directrices para el cumplimiento de seguridad y privacidad de la información. 2 y 3. Nuevas tecnologías, tendencias en seguridad de la información y ciberseguridad, grupos, foros, sitios, boletines de seguridad de la información y ciberseguridad.		2	**H**	Asesorar la implementación de los lineamientos establecidos 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 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.	Oficial de Seguridad y Privacidad de la Información	CSPI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información.		1. Activos y clasificación de información y de ciberseguridad revisados. 2. Matriz de Riesgos de seguridad y privacidad de la información identificados, valorados y tratados. 3. Informe de incidentes de seguridad revisados. 4. Vulnerabilidades técnicas gestionadas y Planes de remediaciones. 5. Estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios. 6. Matriz de Requisitos legales correspondiente a seguridad y privacidad de la información revisada revisada.	1-6. Todos los procesos 3, 5 y 6. Grupo de interés 1, 3-6. Entes de Control
	1 y 4. Resultados del Plan de				Acompañar la Implementación del Plan de Continuidad de la Operación de los					

1. Todos los procesos 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	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). 6. Estrategias de fortalecimiento en la gestión del servicio con los grupos de interés y de buenas practicas de RSI.		3	**H**	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.	Oficial de Seguridad y Privacidad de la Información	CSPI3. Verificar el diligenciamiento de la herramienta diseñada. CSPI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información.		1. Análisis de impacto - BIA. 2. Planes de continuidad de la operación y de recuperación ante desastres. 3. Matrices de Riesgos de interrupción de Continuidad a la operación de los servicios actualizadas a la vigencia. 4. Resultados de las pruebas del BCP plan de continuidad del negocio y DRP plan de recuperación de desastres. 5. Estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.	1-5. Todos los procesos 2 y 5. Grupos de interés
1. Gobierno Nacional 2. Superintendencia de Industria y Comercio. 3. Proceso de Seguridad y Privacidad de la información.	1 y 2 Normativa aplicable y guías emitidas para la protección de datos personales. 3. Política de Tratamiento de datos personales. 3. Manual de lineamientos de Seguridad para la protección y tratamiento de Datos Personales.		4	**H**	Asesorar la Implementación de 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 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. Con base en lo anterior, se desarrollan actividades de uso y apropiación con el	Oficial de Seguridad y Privacidad de la Información	CSPI3. Verificar el diligenciamiento de la herramienta diseñada. CSPI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información. CSPI6. Verificar que el compromiso de confidencialidad para los contratistas del proceso. CSPI10. Verificar el cumplimiento de Declaración de conflicto de intereses y en motivar su compromiso.		1. Inventario de bases de datos personales. 2. Reportes Registro Nacional de Bases de Datos personales 3. Estrategias de uso y apropiación acerca de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios	1. Entes de Control 2. Superintendencia de Industria y Comercio 3. Todos los procesos

					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. Entes internos y externos de control y normativos. 4. Departamento Administrativo de la Función Publica.	1. Procedimientos, Indicadores de eficacia y efectividad, Riesgos de Seguridad y Privacidad de la información. 2. Plan de Auditorías Internas. 3. Plan de Auditorías Externas e Informe de resultados de auditorias externas. 4. 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.	Oficial de Seguridad y Privacidad de la Información	CSPI1. Validar la divulgación y apropiación de la política y lineamientos CSPI3. Verificar el diligenciamiento de la herramienta diseñada. CSPI4. Revisar el avance de cada una de las actividades formuladas en el plan de seguridad y privacidad de la información.		1. Indicadores de eficacia y efectividad. 2. Controles para los riesgos identificados de los procesos. 3. Cumplimiento de los planes derivados del proceso.	1. Comité MIG 2. Todos los procesos.
Gestión del Conocimiento	Conocimiento requeridos para el desarrollo del proceso.		6	V	Identificar el conocimiento requerido para el fortalecimiento de su operación e implementar las estrategias necesarias para el mejoramiento de su gestión a partir de la gestión del conocimiento Identificar el conocimiento requerido para el fortalecimiento de su 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. 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	Oficial de Seguridad y Privacidad de la Información	CSPI2. Revisar la implementación de las estrategias de gestión del conocimiento. CSPI8. Verificar y analizar la información de la gestión del proceso.		1. Documento soporte de la estrategia implementada teniendo en cuenta la herramienta disponible. 2. Información para el Inventario de activos de conocimiento del proceso 3. Información para el listado de conocimientos requeridos para la eficiencia de la entidad.	1,2 y 3. Gestión del Conocimiento 3. Gestión del Talento Humano

					conocimiento), se deben aplicar las herramientas suministradas para el desarrollo de la actividad a implementar					
1. Departamento Administrativo de la Función Pública 2. Fortalecimiento Organizacional 3. Entes de control y Entes Certificadores 4. Proceso Gestión de Atención a Grupos de Interés 5. Líder del Sistema Integrado de Gestión 6. Comité MIG 7. Gestión del Conocimiento	1. Lineamientos para la gestión organizacional de las entidades públicas. 1. Criterios de autoevaluación para su aplicación en los procesos de la Entidad. 2. Resultados del seguimiento, gestión y desempeño de los procesos y del MIG. 2. Documentación para la operación al interior del Ministerio en términos de procesos 2. Lineamientos, estrategias y políticas internas del MIG 2. Resultados de las mediciones de gestión y desempeño institucional 2. Lineamientos y estrategias para el fortalecimiento de la apropiación del MIG 3. Informe de resultados de auditorias internas y externas 4. Resultados del nivel de satisfacción de los Grupos de Interés. 4. Informe de gestión de PQRSD 5. Plan Operativo del Sistema Integrado de Gestión 6. Actas de Comité MIG		7	**A**	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 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 PQRSD, conocimiento explícito 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 autoevaluación del proceso. 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 practicas 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. Las acciones de mejora derivadas del seguimiento y autoevaluación del proceso deben cumplir	Líder del Proceso de Seguridad y Privacidad de la Información. Líderes del Sistema Integrado de Gestión Gestor del Proceso	CSPI7. Verificar la consolidación y registro de la información de Seguimiento a la gestión del proceso CSPI8. Verificar y analizar la información de la gestión del proceso CSPI9. Revisar y hacer seguimiento de respuestas a las solicitudes registradas en el aplicativo de Gestión Documental por parte del facilitador documental del grupo. CSPI10. Verificar el cumplimiento de Declaración de conflicto de intereses y en motivar su compromiso.		1. Necesidades de fortalecimiento del Proceso (recursos, actualización documental, buenas prácticas). 2. Acciones de mejora del proceso formuladas, requeridas 3. Acciones de gestión que requieran incorporarse o actualizarse en el plan FOGEDI 4. Resultados de 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)	Todos los procesos

	7. Estrategias de apropiación de la Gestión del Conocimiento 7. Conocimiento explicito para la eficiencia de la entidad.			con los criterios definidos en el proceso de Fortalecimiento Organizacional.				

Indicadores:	• 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::	• Mapa de Riesgos Seguridad y Privacidad de la Información

Clasificación de la Información :Pública

VERSIÓN	FECHA	DESCRIPCIÓN
1	04/Dic/2020	Creación del documento.
2	14/Dic/2021	Se actualizó: Políticas de operación, Entradas, Proveedores, Actividades, Riesgos, Salidas y Clientes

ELABORÓ	REVISÓ	APROBÓ
Nombre: Rosa Lucia Ortega Muleth **Cargo:** Profesional Especializado **Fecha:** 14/Dic/2021	**Nombre:** Ahimer Andres Pardo Moreno **Cargo:** Contratista **Fecha:** 14/Dic/2021 **Nombre:** Andres Diaz Molina **Cargo:** Oficial de Seguridad de la Información **Fecha:** 14/Dic/2021 **Nombre:** Carolina Castañeda de Avila **Cargo:** Coordinador **Fecha:** 14/Dic/2021	**Nombre:** Juddy Alexandra Amado Sierra **Cargo:** Jefe de Oficina **Fecha:** 15/Dic/2021