

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 1 de 20

TABLA DE CONTENIDO

INTRODUCCIÓN	2
1. OBJETIVO	2
2. ALCANCE	2
3. DESARROLLO.....	2
3.1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN	2
3.2. OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN	3
3.3. ALCANCES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.	3
3.4. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGTI 4	4
3.5. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	4
3.6. ORGANIZACIÓN DEL EJE DE SEGURIDAD DE LA INFORMACIÓN.	4
3.7. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	5
3.8. PLAN DE SOSTENIBILIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	6
3.9. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	19
4. DOCUMENTOS DE REFERENCIA:	19
5. CONTROL DE CAMBIOS:	20

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 2 de 20

INTRODUCCIÓN

El ICBF mediante las resoluciones 11980 de 2019 y 6659 del 2020 por las cuales se adoptan el Modelo de Planeación y Sistema Integrado de Gestión del, asignando roles y responsabilidades en los ejes que lo integran, siendo la Seguridad de la Información uno de ellos. El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3. Principios, define la Seguridad de la Información como: principio de la Política de Gobierno Digital. De igual manera en el artículo 2.2.9.1.2.1 define la estructura de los elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, permitiendo el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

1. OBJETIVO

Proteger los activos de información del Instituto Colombiano de Bienestar Familiar – ICBF a nivel nacional, a partir del despliegue de actividades y controles definidos en el Modelo de Seguridad y Privacidad de la Información, Sistemas de Gestión de Seguridad de la Información y el Modelo de Operación por Procesos.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información del Instituto Colombiano de Bienestar Familiar – ICBF inicia con actividades referentes a la Gestión de Incidentes de Seguridad de la Información y finaliza con actividades asociadas a la Gestión de Continuidad del Negocio, aplica donde se realice recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

3. DESARROLLO

3.1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

El ICBF protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios. La entidad previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información y seguridad digital, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 3 de 20

la primera infancia, la niñez, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas.

3.2. OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del ICBF.
2. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF.
3. Gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación del ICBF.
4. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
5. Fortalecer las capacidades y cultura organizacional de Seguridad de la Información en los colaboradores y contratista del ICBF.

3.3. ALCANCES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

3.3.1. ALCANCE DE IMPLEMENTACIÓN

Diseño, desarrollo, implementación, mantenimiento y mejora continua del Sistema Integrado de Gestión (calidad, ambiental, seguridad de la información y seguridad y salud en el trabajo) conforme con los requisitos legales y otros requisitos, así como con las necesidades y expectativas de las partes interesadas.

Estos sistemas se implementan, bajo las normas de gestión ISO 9001:2015, ISO 14001:2015, ISO/IEC 27001:2013 e ISO 45001:2018 en la Sede de la Dirección General, las treinta y tres (33) regionales y sus centros zonales.

3.3.2. ALCANCE DE CERTIFICACIÓN NTC/IEC ISO 27001:2013

Gestión y control de la seguridad de la información en las actividades asociadas a los procesos involucrados en la prestación del Servicio Público del Instituto Colombiano de Bienestar Familiar para el desarrollo y la protección integral de la primera infancia, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas asociadas a los programas del ICBF, así como propender por las actividades de tecnología de la información y telecomunicaciones (TIC).

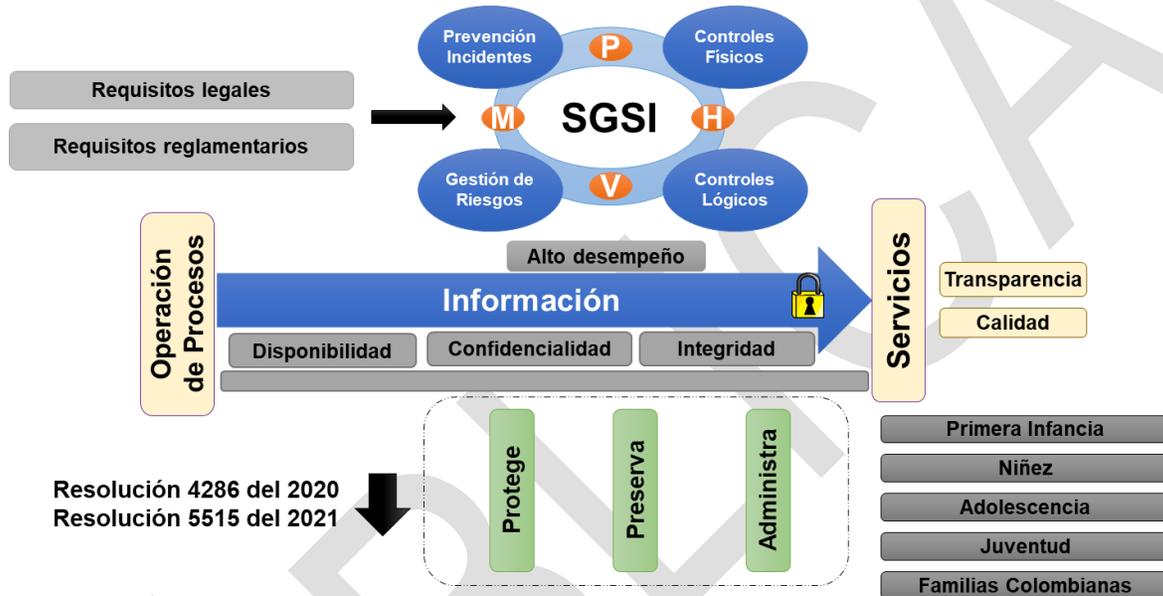
Aplica para la Sede de la Dirección General, la Sede Metrópolis y las Regionales: Amazonas, Antioquia, Arauca, Atlántico, Bogotá, Bolívar, Boyacá, Caldas, Caquetá, Casanare, Cauca, Cesar, Cundinamarca, Córdoba, Huila, Magdalena, Nariño, Norte de Santander, Putumayo, Quindío,

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 4 de 20

Risaralda, San Andres, Santander, Sucre, Tolima, Valle del Cauca, Meta, Guaviare y Centro Zonal Armenia Sur, en lo referente a ISO - IEC 27001:2013.

3.4. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI



Política de operación del Sistema de Gestión de Seguridad de la Información – SGSI

3.5. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Este comité es asumido por el Comité Institucional de Gestión y Desempeño, reglamentado mediante la Resolución No. 8650 del 10 de diciembre de 2021 *“Por la cual se integra y reglamenta el Comité Institucional de Gestión y Desempeño, Subcomité de Arquitectura Empresarial y la Mesa Técnica de Sistemas y Gestión de Información misional en el Instituto Colombiano de Bienestar Familiar”*

3.6. ORGANIZACIÓN DEL EJE DE SEGURIDAD DE LA INFORMACIÓN.

La Resolución 11980 del 30 de diciembre de 2019 establece en el Título I, Capítulo I, artículo 2°, inciso C, Sistema Integrado de Gestión: El Sistema Integrado de Gestión - SIGE del Instituto Colombiano de Bienestar Familiar – ICBF. Es una herramienta gerencial que tiene como propósito promover y facilitar la mejora continua de la gestión, orientada a garantizar el desarrollo del modelo como parte de la planeación estratégica.

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 5 de 20

Esta se despliega a través de sus procesos de manera que se fortalezca la calidad, la gestión ambiental, la seguridad, la salud en el trabajo y la seguridad de la información. Lo anterior, en el marco de la mejora de los resultados a los servicios ofertados a la primera infancia, la niñez, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas.

Adicionalmente, está conformado por los siguientes sistemas de gestión que adelante se denominarán ejes (Calidad, Ambiental, Seguridad y Salud en el Trabajo, Seguridad de la Información) asimismo, establece en el artículo 7° los líderes de los Ejes del Sistema Integrado de Gestión – SIGE, delegando a la Dirección de Información y Tecnología como Líder del Eje de Seguridad de la Información.

3.7. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Uno de los enfoques y objetivos del Plan de Seguridad y Privacidad de la Información es la gestión de incidentes ya que la atención y mitigación de vulnerabilidades conocidas y no conocidas son de vital importancia para identificar mejoras en los controles implementados o definir nuevas actividades que permitan proteger la confidencialidad, disponibilidad e integridad de los activos de información de la Entidad.

En el 2023, se presentaron y se atendieron un total de 34 incidentes de seguridad de la información los cuales se discriminan de la siguiente manera:

MES	CANTIDAD ATENDIDOS
ENERO	5
FEBRERO	1
MARZO	1
ABRIL	8
MAYO	3
JUNIO	6
JULIO	6
AGOSTO	1
SEPTIEMBRE	0
OCTUBRE	0
NOVIEMBRE	3
DICIEMBRE	0
TOTAL	34

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 6 de 20

3.8. PLAN DE SOSTENIBILIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de sostenibilidad del Modelo de Seguridad y Privacidad de la Información comprende las siguientes gestiones:



Para el cumplimiento de las anteriores gestiones, se define el siguiente cronograma en el cual se relacionan las actividades que deben ejecutarse para cada una:

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
1. Gestión de Incidentes de Seguridad de la Información	1.1. Socializar el procedimiento de Gestión de Incidentes de Seguridad de la Información.	1.1.1. Dar a conocer el procedimiento al operador de la mesa de servicio	Profesional de la Dirección de Información y Tecnología, encargado de la Gestión de Incidentes de Seguridad de la Información, en conjunto con el profesional encargado de la Gestión de Cambio y Cultura.	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión.	02/01/2024	30/04/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 7 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		1.1.2. Dar a conocer el procedimiento a los colaboradores de los procesos de la entidad	Profesional de la Dirección de Información y Tecnología, encargado de la Gestión de Incidentes de Seguridad de la Información, en conjunto con el profesional encargado de la Gestión de Cambio y Cultura.	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión.	02/01/2024	31/05/2024
		1.1.3. Dar a conocer el procedimiento a los ingenieros regionales y soportes en sitio.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Incidentes de Seguridad de la Información, en conjunto con el profesional encargado de la Gestión de Cambio y Cultura	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión.	01/02/2024	31/05/2024
	1.2. Gestionar los incidentes de Seguridad de la Información reportados de la Información	1.2.1. Gestionar los incidentes de Seguridad de la Información de acuerdo con lo establecido en el procedimiento P5.GTI.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Incidentes de Seguridad de la Información, Profesional de la Dirección de Información y Tecnología, Profesional de la SubDirección de Recursos Tecnológicos. Profesional de la SubDirección de Sistemas Integrados de Información Profesional de Planeación y Sistemas. (Ingeniero Regional)	Formato Informe de Incidente de Seguridad Digital	02/01/2024	31/12/2024
	1.3. Realizar seguimiento a los eventos o vulnerabilidades	1.3.1. Realizar seguimiento al avance de los planes de mitigación de vulnerabilidades propuestos por la SRT y la SSII	Profesional de la Dirección de Información y Tecnología, encargado del servicio de Seguridad Perimetral. Profesionales de la Dirección de Información y Tecnología integrantes del Equipo de Seguridad de la Información.	Correos electrónicos	01/02/2024	31/12/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 8 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	1.4. Revisar el Procedimiento de gestión de Incidentes.	1.4.1. Revisar el Procedimiento de gestión de incidentes de seguridad de la Información y en caso de ser necesario gestionar su actualización.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Incidentes de Seguridad de la Información.	Procedimiento actualizado de gestión de incidentes de seguridad de la Información o Correo electrónico que evidencie la revisión del procedimiento indicando por qué no es necesario modificarlo.	03/06/2024	30/09/2024
2. Gestión de Riesgos	2.1. Socializar la Guía de Gestión de Riesgos y Peligros en lo relacionado con seguridad de la información	2.1.1. Dar a conocer la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad del Negocio en la SDG y Regionales.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información. Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Cambio y Cultura.	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión.	01/02/2024	29/03/2024
	2.2. Identificar, analizar y valorar los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del Negocio	2.2.1. Gestionar con los procesos y regionales la Identificación, Análisis, valoración y definición del manejo de los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del negocio.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información. Promotores EPICO de la SDG Ingenieros Regionales	Actas de identificación de riesgos - Información registrada en SVE	01/02/2024	29/03/2024
		2.2.2. Realizar la retroalimentación, revisión y verificación de los riesgos identificados por la SDG y Regionales, validando la definición de los planes de tratamiento y controles existentes	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos	01/02/2024	15/04/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 9 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	2.3. Realizar seguimiento Fase de manejo y monitoreo de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del Negocio	2.3.1. Definir el cronograma para el seguimiento de los planes de tratamiento y controles existentes.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos	1/02/2024	15/04/2024
		2.3.2. Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento y controles existentes. Validar si se han materializado.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información. Promotores EPICO de la SDG Ingenieros Regionales	Correo mensual con la Calificación del Plan Operativo para la Gestión de Riesgos - Actas de identificación o revaluación de riesgos, en caso de que haya alguna materialización	01/04/2024	31/12/2024
	2.4. Realizar la evaluación de riesgos residuales	2.4.1. Realizar acompañamiento en la evaluación de riesgos residuales en la SDG y Regionales.	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique	01/05/2024	20/12/2024
	2.5. Revisar la Guía Gestión de Riesgos y Peligros en lo relacionado con Seguridad de la Información	2.5.1. Revisar la Guía Gestión de Riesgos Seguridad de la Información y en caso de que se requiera gestionar su actualización.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Guía Gestión de Riesgos y Peligro Actualizada o Correo en el cual se indique que no es necesario la actualización	01/07/2024	31/12/2024
	2.6. Fortalecer la identificación, análisis, valoración y manejo de los riesgos de seguridad de la información en la Gestión de Proyectos de TI	2.6.1. Realizar mesa de trabajo con los colaboradores responsables de construir los proyectos de TI para definir el proceso de identificación de riesgos de seguridad de la información desde la fase de	Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información. Profesional de la Dirección de Información y Tecnología, encargados de construir los proyectos de TI.	Actas de reunión o Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique	01/02/2024	30/04/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 10 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		planeación de los mismos.				
		2.6.2. Identificar, analizar, valorar y gestionar los riesgos de seguridad de la información en los proyectos de TI.	<p>Profesional de la Dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.</p> <p>Profesional de la Dirección de Información y Tecnología, encargados de construir los proyectos de TI.</p>	Matrices de riesgos definidas para cada proyecto de TI	01/02/2024	31/12/2024
3. Gestión de mejora	3.1. Gestionar los indicadores de medición del SGSI	3.1.1. Actualizar hoja de vida de los indicadores de medición del SGSI de acuerdo con las indicaciones de la Subdirección de Monitoreo y Evaluación.	Profesional de la Dirección de Información y Tecnología encargado de la gestión de Mejora del SGSI	Correo electrónico indicando la propuesta de actualización o ajustes de los indicadores.	1/02/2024	31/12/2024
		3.1.2. Realizar el seguimiento a los indicadores de medición del SGSI.	Profesional de la Dirección de Información y Tecnología encargado de la gestión de Mejora del SGSI Equipo SGSI	Informes del reporte de los indicadores conforme a su periodicidad de medición	01/03/2024	31/12/2024
		3.1.3. Reportar los indicadores PA 140 y PA 142 para su registro en SIMEI.	Profesional de la Dirección de Información y Tecnología encargado de la gestión de Mejora del SGSI	Correo con el Informe del reporte del indicador conforme a su periodicidad de medición	01/02/2024	31/12/2024
	3.2. Gestionar las acciones correctivas u oportunidades de mejora del Eje de Seguridad de la Información	3.2.1. Realizar seguimiento a las oportunidades de mejora y acciones correctivas, incluyendo las actividades definidas en los planes de acción de estas, generando las alertas respectivas cuando sea necesario.	Profesional de la Dirección de Información y Tecnología encargado de la Gestión de Mejora del SGSI	Correos electrónicos y calificación mensual del POSIGE del SGSI	01/02/2024	31/12/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 11 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		3.2.2. Identificar a partir de la verificación del cumplimiento de los controles y requisitos del Sistema de Gestión de Seguridad de la Información acciones correctivas u oportunidades de mejora que fortalezcan las medidas de protección de los activos de información.	Profesionales de la Dirección de Información y Tecnología que conforman el Equipo de Seguridad de la Información	Acciones correctivas u oportunidades de mejora registradas y gestionadas en SVE	01/02/2024	29/11/2024
	3.3. Realizar acompañamiento en las auditorías internas y externas al SGSI, gestionando las oportunidades de mejora y acciones correctivas que se identifiquen.	3.3.1. Realizar acompañamiento en la definición de oportunidades de mejora y del análisis de causas y plan de acción de las Acciones Correctivas del SGSI cuando se requiera.	Profesional de la Dirección de Información y Tecnología encargado de la Gestión de Mejora del SGSI	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique	01/02/2024	31/12/2024
		3.3.2. Realizar seguimiento a las Acciones Correctivas y Oportunidades de Mejora del SGSI.	Profesional de la Dirección de Información y Tecnología encargado de la Gestión de Mejora del SGSI	Correo mensual con la Calificación del Plan Operativo para la Gestión de mejora	01/02/2024	31/12/2024
4. Gestión de Cambio y Cultura de Seguridad y Privacidad de la Información	4.1. Definir mediante el "Plan de Cambio y Cultura de Seguridad y Privacidad de la Información" las estrategias para el uso y apropiación de los colaboradores en temas de seguridad de la información	4.1.1. Actualizar el documento Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2024, definiendo es te las estrategias de uso y apropiación en temas de seguridad de la información.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Plan de Cambio y Cultura de Seguridad y Privacidad actualizado a la versión 2024	01/02/2024	29/03/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 12 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	4.2. Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	4.2.1. Apoyar la implementación de las estrategias del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.	Evidencia del Plan de Cambio y Cultura y la calificación del Plan Operativo del SGSI relacionados con actividades de cultura.	01/02/2024	31/12/2024
	4.3. Realizar medición del nivel de apropiación de los colaboradores en temas de seguridad de la información de acuerdo con el despliegue de actividades del plan de cambio y cultura	4.3.1. Diseñar los instrumentos de medición del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.	Correos remitiendo los instrumentos de medición a los Procesos y Regionales de forma trimestral	01/03/2024	31/12/2024
		4.3.2. Realizar la medición del nivel de apropiación de los colaboradores en temas de seguridad de la información.	Profesional de la Dirección de Información y Tecnología, encargado de la gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.	Informe con los resultados de la medición a nivel nacional	30/03/2024	20/12/2024
	4.4. Gestionar la actualización del micrositio SGSI	4.4.1. Actualizar el Micrositio SGSI, Intranet y Portal WEB, Piezas, videos y noticias referentes al Eje de Seguridad de la Información	Profesional de la Dirección de Información y Tecnología, encargado de la Gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. Equipo de apropiación DIT.	Correos solicitando la actualización del micrositio y los correos de respuesta informando la actualización del micrositio y Capturas de Pantalla de la actualización	01/02/2024	31/12/2024
5. Gestión de Activos de Información	5.1. Gestionar el levantamiento Activos de Información para los procesos de la Sede de la Dirección General y Regionales	5.1.1. Dar a conocer la guía de activos de información y el instrumento para el levantamiento activos, para los procesos y regionales.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	01/02/2024	15/02/2024
		5.1.2. Gestionar con los procesos y regionales la identificación de los activos de	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información con el apoyo del Equipo	Matrices de activos de información consolidadas por proceso.	15/01/2024	29/02/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 13 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		información para la vigencia 2024.	Promotor EPICO e Ingenieros Regionales, líderes de procesos o quienes designen, directores regionales o quienes designen.			
		5.1.3. Revisar el instrumento de activos de cada proceso y solicitar corrección en caso de que se requiera.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información, Equipo promotor EPICO e Ingenieros regionales	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos	15/01/2024	29/02/2024
		5.1.4. Realizar la aprobación de los activos de información.	Líderes o Responsables de los Procesos. Directores Regionales	Memorando de aprobación	15/01/2024	29/02/2024
		5.1.5. Consolidar los activos de información de los procesos y realizar el registro en SVE.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información, Gestión de Riesgos, Equipo promotor EPICO e Ingenieros regionales	Matriz de activos de información consolidada - Información registrada en el módulo de activos de información en SVE	15/01/2024	29/02/2024
		5.1.6. Apoyar en la actualización de los activos de información cuando se presente Materialización de riesgos que cambien la criticidad del activo u otras novedades	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información, Gestión de Riesgos, Equipo promotor EPICO e Ingenieros regionales	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos	01/03/2024	31/12/2024
		5.1.7. Revisar la guía de activos de información e instrumento y en caso de ser necesario gestionar su actualización.	Profesional de la Dirección de Información y Tecnología Responsable de la Gestión de Activos de Información	Guía e instrumento de activos de información actualizada - En caso De no ser necesario actualizarse, informar mediante correo electrónico la justificación.	01/07/2024	29/11/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 14 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	5.2. Consolidar y registrar en el sistema, el inventario de activos de información	5.2.1. Consolidar los activos de información de los procesos y realizar el registro en SVE.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información, Gestión de Riesgos, Equipo promotor EPICO e Ingenieros regionales	Matriz de activos de información consolidada - Información registrada en el módulo de activos de información en SVE	01/02/2024	29/02/2024
	5.3. Actualizar el inventario de activos de información para la vigencia 2025.	5.3.1. Realizar revisión y actualización de los activos de información para definir el inventario final para la próxima vigencia.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información con el apoyo del Equipo Promotor EPICO e Ingenieros Regionales, líderes de procesos o quienes Designen, directores regionales o quienes designen.	Matriz de activos de información consolidada - Información registrada en el módulo de activos de información en SVE	01/10/2024	20/12/2024
	5.4. Apoyar la actualización de los Instrumentos de gestión de Información Pública - ley 1712	5.4.1. Diligenciar el formato de Registro Activos de Información con el insumo del consolidado nacional de las matrices de activos de Información	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información	Matriz de activos de información consolidada	03/06/2024	27/09/2024
		5.4.2. Enviar a control de legalidad el instrumento de Registro Activos de información	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información	Correo electrónico remitiendo el instrumento de Registro Activos de información para el control de la legalidad	03/06/2024	27/09/2024
		5.4.3. Apoyar en la actualización del índice de información clasificada y reservada, así como en la publicación del Registro Activos de Información en el sitio web de la Entidad.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Activos de Información y la Oficina Asesora Jurídica	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique	03/06/2024	29/11/2024
6. Gestión de Gobierno Digital	6.1. Gestionar el Modelo de Seguridad y	6.1.1. Sensibilizar y Apropiar a los Colaboradores del	Profesional de la Dirección de Información y Tecnología	Formato de listado de asistencia o Listado de	01/02/2024	29/03/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 15 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	Privacidad de la Información y Seguridad Digital en el ICBF	ICBF en los cambios de la herramienta de MINTIC.	Responsable Gobierno Digital - Responsable SGSI	Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique		
		6.1.2. Consolidar la autoevaluación de la Entidad en la Implementación del Modelo Seguridad y Privacidad de la Información	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Instrumento de la evaluación del MSPI	01/02/2024	31/12/2024
		6.1.3. Gestionar el cierre de las brechas de seguridad de la información que estén dentro del alcance y gestión de la entidad	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Informe con los resultados de la gestión de brechas de seguridad de la información y evidencias de configuración de políticas en la infraestructura de TI	01/02/2024	31/12/2024
	6.2. Gestionar la Infraestructura Crítica del ICBF	6.2.1. Participar en las reuniones de las infraestructuras críticas cibernéticas conforme a convocatorias que realice el CSIRT Gobierno o MINTIC.	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Invitaciones remitidas por el CSIRT Gobierno o MINTIC, convocando a reuniones de infraestructuras críticas cibernéticas	01/02/2024	31/12/2024
		6.2.1. Establecer con el acompañamiento de MINTIC si el ICBF tiene o no infraestructuras críticas.	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Correos electrónicos, Mesas de trabajo, Aplicación de la metodología de riesgos	01/02/2024	31/12/2024
	6.3. Actualizar el FURAG en lo relacionado con la Política de Seguridad Digital	6.3.1. Actualizar el Documento FURAG de la Entidad en lo relacionado con la Implementación de Seguridad y Privacidad de la Información	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Correo remitiendo la evaluación del FURAG	01/02/2024	30/09/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 16 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
7. Gestión de Seguimiento a los controles y requisitos del SGSI	7.1. Planificar la estratégica de seguimiento del despliegue requisitos y controles del SGSI	7.1.1. Definir las actividades y tareas del plan de seguimiento SGSI para los Procesos de la Sede de la Dirección General y Regionales.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos del SGSI	Correo electrónico remitiendo la planificación del Plan Operativo del SGSI para el 2023	01/01/2024	29/02/2024
	7.2. Dar a conocer el Plan Operativo para el SGSI	7.2.1. Realizar reunión con los procesos y regionales donde se les explique las novedades del plan operativo para el 2024	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos del SGSI	Formato de Listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	01/02/2024	29/02/2024
	7.3. Revisar el Manual Políticas de Seguridad de la Información, Resolución de Seguridad de la Información o documentación transversal al Eje	7.3.1. Revisar la documentación asociadas al Sistema de Gestión de Seguridad de la Información y en caso de ser necesario gestionar su actualización.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos del SGSI Equipo SGSI	Documentos que se hayan actualizado	01/02/2024	30/09/2024
	7.4. Revisar los controles del SGSI, en las regionales y los procesos de la Sede de la Dirección General	7.4.1. Validar mediante el plan operativo de SGSI, el cumplimiento de los controles del SGSI.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los controles y requisitos del SGSI. Equipo SGSI	Correo mensual con la Calificación del Plan Operativo de las Regionales y Procesos	01/02/2024	20/12/2024
		7.4.2. Verificar el cumplimiento de los controles del SGSI y en casos de ser necesario generar las medidas de mejora para controlar las desviaciones que se identifiquen.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos del SGSI.	Informe con los resultados del cumplimiento a los controles	01/02/2024	29/11/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

PL14.GTI

30/01/2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1

Página 17 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
8. Gestión de Continuidad de la Operación Tecnológica	8.1. Actualizar los Planes de Contingencia de los Servicios de Tecnología	8.1.1. Coordinar las actualizaciones de los Planes de Contingencia de los Servicios de la DIT en caso de que se requiera.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Captura de pantalla Planes de contingencia	1/02/2024	29/09/2024
		8.1.2. Coordinar las pruebas de los Planes de Contingencia de los Servicios de tecnología en la SDG.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Documento de resultado de pruebas	3/04/2023	31/12/2024
	8.2. Fortalecer el Plan de Continuidad de la Operación Tecnológico	8.2.1. Coordinar y apoyar la definición y/o actualización de las estrategias del DRP a partir de un análisis BIA y las actividades críticas misionales.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	3/04/2024	29/09/2024
		8.2.2. Fortalecer la infraestructura de TI del Plan de Recuperación de Desastres, gestionando las configuraciones técnicas necesarias para su funcionamiento ante cualquier escenario, teniendo como alcance mínimo las aplicaciones SIM, CUENTAME, PORTAL, MTS y KACTUS.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF Profesionales de la Subdirección de Recursos Tecnológicos responsable de los servicios de bases de datos y aplicaciones, servidores, redes y seguridad perimetral. Profesionales de la Subdirección de Sistemas Integrados de Información que apoyan los sistemas que se incluirán en el DRP.	Documento e instructivos del DRP actualizados Configuraciones en la infraestructura de TI	01/02/2024	31/12/2024
		8.2.3. Aplicar los requisitos de seguridad para cada una de las	Profesional de la Dirección de Información y Tecnología Responsable de	Formato de requisitos de seguridad de la información	1/02/2024	31/12/2024

¡Antes de imprimir este documento... piense en el medio ambiente!



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PL14.GTI

30/01/2024

Versión 1

Página 18 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		estrategias presentadas conforme al escenario.	Continuidad de la Operación Tecnológica del ICBF			
		8.2.4. Coordinar la ejecución de las pruebas "escritorio y funcionales" de las estrategias del DRP.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Actas de Reunión o Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique	1/05/2024	27/09/2024
9. Gestión de Continuidad del Negocio	9.1. Actualizar el Análisis de Impacto	9.1.1. Gestionar la actualización de las Actividades Críticas de los procesos de la SDG y Regionales.	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF. Promotores ÉPICO de la SDG Ingenieros Regionales	Consolidado de actividades críticas	1/02/2024	28/06/2024
	9.2. Identificar nuevos escenarios y estrategias de continuidad del negocio	9.2.1. Establecer a partir de la realización de mesas de trabajo con las dependencias de la SDG y Regionales, nuevos escenarios y estrategias de continuidad del negocio.	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF Ingenieros Regionales	Documentación de los escenarios de continuidad del negocio	1/02/2024	15/09/2024
	9.3. Realizar pruebas del Plan de Continuidad del Negocio	9.3.1. Gestionar la realización de pruebas del plan de continuidad del negocio de la entidad	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Documentación de la prueba de continuidad del Negocio.	1/02/2024	31/12/2024

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 19 de 20

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
			Ingenieros Regionales			

3.9 MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con el indicador de gestión PA 140 cuyo objetivo es medir la eficacia del Plan de Seguridad y Privacidad de la Información a partir del cumplimiento de las actividades ejecutadas en el marco de la implementación del Eje de Seguridad de la Información.

4. DOCUMENTOS DE REFERENCIA:

- Ley 44 de 1993 “por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor).
- 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, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Ley 594 de 2000 “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
- Ley 734 de 2002 “Por la cual se expide el Código Disciplinario Único”.
- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- 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”.
- Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.
- Ley 1955 de 2019 “Por la cual se expide el Plan Nacional de Desarrollo 2018-2023 “Pacto por Colombia, pacto por la Equidad”.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano
- CONPES 3995 Política Nacional de Confianza y Seguridad Digital
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	PL14.GTI	30/01/2024
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 20 de 20

- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)
- Resolución interna 8080 de 2016 se aprueba el Manual del Sistema Integrado de Gestión en el ICBF.
- Resolución interna 4286 del 27 de julio de 2020 Política de Seguridad y privacidad de la información, seguridad digital y continuidad de la operación
- Resolución interna 5515 del 31 de agosto de 2021 por la cual se modifica el artículo 4 de la Resolución 4286 del 27 de julio de 2020.
- Resolución 11980 del 30 de diciembre de 2019- Por la cual se adopta el modelo de Planeación y Sistema Integrado de Gestión del ICBF.
- Resolución 6659 de 15 de diciembre de 2020 Por la cual se modifica el modelo de Planeación y sistema Integrado de Gestión del ICBF
- Resolución No. 8650 de 2021 “Por la cual se integra y reglamenta el Comité Institucional de Gestión y Desempeño, el Subcomité de Arquitectura Empresarial y Mesa Técnica de Sistemas y Gestión de Información misional en el Instituto Colombia de Bienestar Familiar”.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Departamento Administrativo para la Función Pública (DAFP) año 2020.
- Norma ISO/IEC 27001:2013.
- Norma ISO/IEC 27001:2022.

5. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
N/A	N/A	N/A

¡Antes de imprimir este documento... piense en el medio ambiente!