TABLA DE CONTENIDO

RESUMEN EJECUTIVO

Desde el Eje de Seguridad de la Información lidera la Política de Seguridad Digital, la cual se implementa y despliega en la sede de la Dirección General, Regionales y Centros Zonales, mediante el Plan de Seguridad y Privacidad de la información. Para 2023 se definen las siguientes gestiones que agrupan un total de 57 tareas:

Mes	Cantidad
Febrero	6
Marzo	5
Abril	2
Mayo	3
Junio	1
Julio	1

Mes	Cantidad
Agosto	1
Septiembre	10
Octubre	1
Noviembre	1
Diciembre	26
Total	**57**

En el Plan de sostenibilidad del Modelo de Seguridad y Privacidad de la Información comprende y se le hace seguimiento mensualmente a las siguientes gestiones:

1. Gestión de Incidentes de Seguridad de la Información
2. Gestión de Riesgos
3. Gestión de mejora
4. Gestión de Cambio y Cultura de Seguridad y Privacidad de la Información
5. Gestión de Activos de Información
6. Gestión de Gobierno Digital
7. Gestión de Seguimiento a los controles y requisitos de la Norma ISO 27001: 20138.
8. Gestión de Continuidad del Negocio
9. Gestión de Continuidad de la Operación Tecnológica

Finalmente, como herramienta de seguimiento asociado al plan se tiene el indicador PA 140 “Porcentaje de eficacia del Sistema de Gestión de Seguridad de la Información – SGSI” que se evalúa de forma trimestral.

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

Desplegar en la Sede de la Dirección General, Regionales y Centros Zonales el Modelo de Seguridad y Privacidad de la Información, a partir de la definición y ejecución de actividades orientadas al cumplimiento de la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de la Operación Tecnológica, y el Modelo de Operación por Procesos del Instituto Colombiano de Bienestar Familiar – ICBF.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información del Instituto Colombiano de Bienestar Familiar – ICBF 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

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.

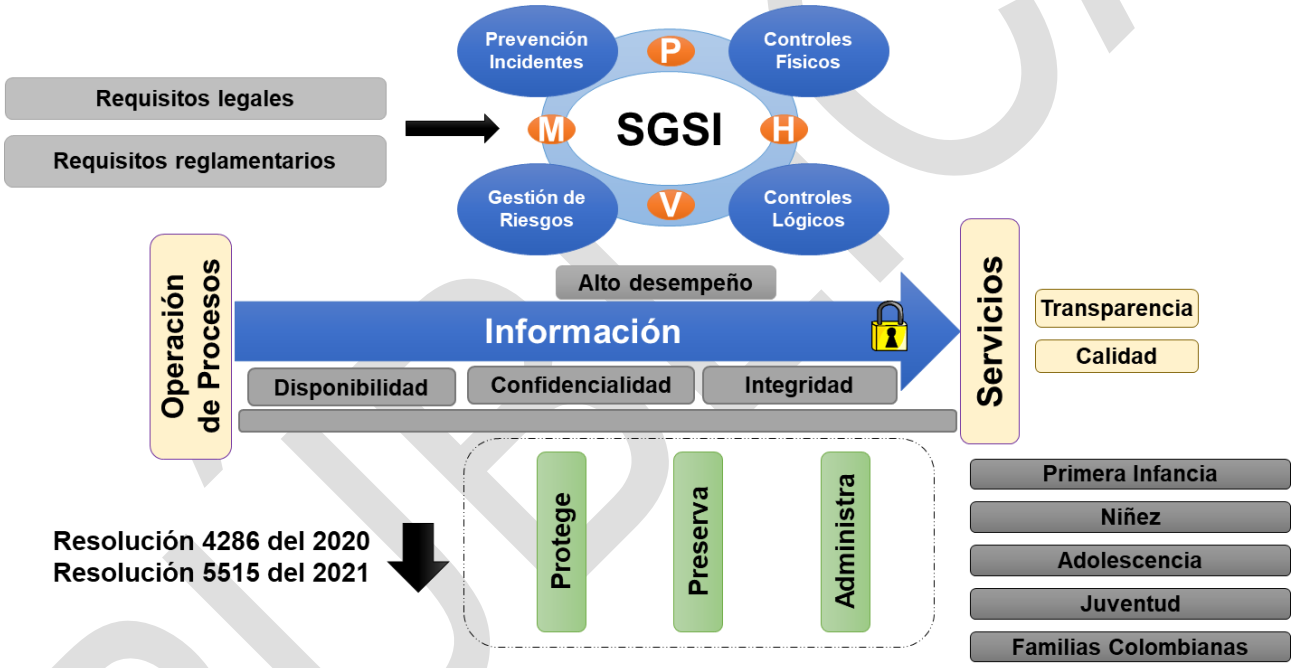
Estos sistemas se implementan, bajo las normas de gestión ISO 9001:2015, ISO 14001:2015, ISO/IEC 27001:2013 e ISO 45001:2018 en la Sede de la Dirección General, las treinta y tres (33) regionales y sus centros zonales.

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, 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.

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 2022, se presentaron y se atendieron un total de 16 incidentes de seguridad de la información los cuales se discriminan de la siguiente manera:

TIPO DE INCIDENTE	CANTIDAD	PORCENTAJE
Indisponibilidad del activo de información	3	18,8%
Borrado de información	3	18,8%
Robo de equipo	2	12,5%
Suplantación de identidad	2	12,5%
Toma de control de equipo usuario final	1	6,3%
Explotación de vulnerabilidad AZURE	1	6,3%
Phishing	1	6,3%
Apropiación	1	6,3%
Malware	1	6,3%
Reporte IP institucional lista negra	1	6,3%
TOTAL	**16**	

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 el siguiente cronograma y se le hace seguimiento mensualmente.

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.	13/02/2023	30/05/2023
		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.	13/02/2023	30/05/2023
		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.	01/02/2023	30/05/2023
	1.2. Gestionar los incidentes de Seguridad de la Información reportados	1.2.1. Gestionar los incidentes de Seguridad de la Información de acuerdo con lo establecido en el procedimiento P5.GTI definido.	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 Tecnología	02/01/2023	31/12/2023
	1.3. Realizar informe de los incidentes de Seguridad de la información	1.3.1. Presentar los informes de los incidentes de seguridad de la información que se materializaron cuando ocurra.	Profesional de la dirección de Información y Tecnología, encargado de la Gestión de Incidentes de Seguridad de la Información.	Informe consolidado de los incidentes presentados por trimestre	02/01/2023	31/12/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	1.4. Seguimiento a los Eventos o vulnerabilidades	1.4.1. 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 de la gestión de Incidentes de Seguridad de la Información, Profesional de la Dirección de Información y Tecnología, encargado de la gestión de riesgos de seguridad de la información.	Correos electrónicos	01/02/2023	29/12/2023
	1.5. Revisar el Procedimiento de gestión de Incidentes y actualizarse en caso de ser necesario.	1.5.1. Actualizar el Procedimiento de gestión de incidentes de seguridad de la Información en caso de ser necesario.	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.	01/06/2023	30/09/2023
2. Gestión de Riesgos	2.1. Sensibilización	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.	01/02/2023	31/03/2023
	2.2. Identificación, análisis, valoración de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del Negocio	2.2.1. Brindar orientación en la Identificación, Análisis, valoración y definición del manejo de los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del negocio tecnológica en la SDG y Regionales	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Actas de identificación de riesgos - Información registrada en SVE	01/02/2023	31/03/2023
		2.2.2. Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento y controles existentes en la SDG y Regionales	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos	01/03/2023	16/04/2023
	2.3. Seguimiento Fase de manejo y monitoreo del riesgo	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	1/03/2023	16/04/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		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.	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	31/03/2023	31/12/2023
	2.4. 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	01/05/2023	23/12/2023
	2.5. Revisión de la Guía Gestión de Riesgos Seguridad de la Información	2.5.1. Actualizar la Guía Gestión de Riesgos Seguridad de la Información en caso de que se requiera.	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	03/07/2023	29/12/2023
	2.6. Monitoreo y Revisión	2.6.1. Monitorear y reportar el resultado del indicador PA 142 “Porcentaje de cumplimiento de las actividades definidas en los planes de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital”	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correo con el Informe del reporte del indicador conforme a su periodicidad de medición	03/04/2023	29/12/2023
3. Gestión de mejora	3.1. Provisión de información a los indicadores de medición del SGSI	3.1.1. Actualizar hoja de vida de los indicadores de medición del SGSI.	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.	29/09/2023	29/12/2023
		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	01/03/2023	29/12/2023
		3.1.3. Reportar los indicadores PA 140 y PA 142	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	01/02/2023	29/12/2023
	3.2. Seguimiento a las Acciones Correctivas y Oportunidades de Mejora	3.2.1. Seguimiento de las Acciones Correctivas y Oportunidades de Mejora	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	01/02/2023	29/12/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	identificadas en el Eje de Seguridad de la Información	3.2.2. Realizar acompañamiento en la definición de oportunidades de mejora y del análisis de causas y plan de acción de las Acciones Correctivas 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	01/02/2023	29/12/2023
4. Gestión de Cambio y Cultura de Seguridad y Privacidad de la Información	4.1. Actualizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	4.1.1. Actualizar el documento Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2023	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 2023	01/02/2023	31/03/2023
	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.	01/02/2023	22/12/2023
	4.3. Medición del plan de cambio y cultura	4.3.1. Diseñar los instrumentos trimestrales 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	01/03/2023	30/10/2023
		4.3.2. Realizar los informes de medición.	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	30/03/2023	20/12/2023
	4.4. Verificación de 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 del Web Master informando la actualización del micrositio y Capturas de Pantalla de la actualización	01/02/2023	29/12/2023
5. Gestión de Activos de Información	5.1. Levantamiento Activos de Información Sede de la Dirección General y Regionales	5.1.1. Revisar la guía de activos de información e instrumento y actualizarse en caso de ser necesario	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.	01/02/2023	02/03/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
		5.1.2. 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	01/02/2023	28/02/2023
		5.1.3. Solicitar a los procesos y a las regionales validar los activos de información identificados en la vigencia anterior a nivel nacional y actualizarlos en caso de ser necesario	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.	Correo electrónico solicitando la validación y actualización de los activos de información en el formato establecido	01/02/2023	28/02/2023
		5.1.4. 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 cuando aplique	01/02/2023	28/02/2023
		5.1.5. 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 cuando aplique	01/03/2023	29/12/2023
	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	01/02/2023	28/02/2023
	5.3. Actualizar el inventario de activos de información	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	02/10/2023	30/11/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	5.4. 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	01/06/2023	30/09/2023
		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	01/06/2023	30/09/2023
		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	01/06/2023	30/09/2023
6. Gestión de Gobierno Digital	6.1. Gestionar el Modelo de Seguridad y Privacidad de la Información y Seguridad Digital en el ICBF	6.1.1. Sensibilizar y Apropiar a los Colaboradores del ICBF en los cambios de la herramienta de MINTIC.	Profesional de la Dirección de Información y Tecnología Responsable Gobierno Digital - Responsable 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	01/02/2023	31/03/2023
		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	01/02/2023	29/12/2023
	6.2. Gestionar la Infraestructura Crítica del ICBF	6.2.1. Participar en las reuniones de las infraestructuras criticas 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 criticas cibernéticas.	01/02/2023	29/12/2023
		6.2.2. Coordinar el reporte de las Infraestructuras Críticas conforme a solicitud de MINTIC o CSIRT Gobierno. cibernéticas del ICBF	Profesional de la Dirección de Información y Tecnología y Responsable Gobierno Digital de SGSI	Correo electrónico remitiendo las Infraestructuras Críticas cibernéticas del ICBF solo si MINTIC o CSIRT Gobierno realizan la solicitud	01/02/2023	29/12/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	6.3. Actualización del FURAG en lo relacionado con la Política de Seguridad Digital	6.3.1. Actualizar el Documento FURAG de la Entidad en 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	01/02/2023	30/09/2022
7. Gestión de Seguimiento a los controles y requisitos de la Norma ISO 27001: 2013	7.1. Planificación Estratégica del plan de seguimiento 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 de la Norma ISO 27001: 2013	Correo electrónico remitiendo la planificación del Plan Operativo del SGSI para el 2023	02/01/2023	28/02/2023
	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 2023	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013	Formato de Listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	01/02/2023	28/02/2023
	7.3. Revisión del Manual Políticas de Seguridad de la Información, Resolución de Seguridad de la Información y documentación transversal al Eje	7.3.1. Actualizar la documentación del Eje de Seguridad de la Información que lo requiera.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013 Equipo SGSI	Documentos que se hayan actualizado	01/02/2023	29/09/2023
	7.4. Revisión de los controles de la norma ISO 27001:2013, 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 Anexo A de la norma ISO 27001:2013	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013 Equipo SGSI	Correo mensual con la Calificación del Plan Operativo de las Regionales y Procesos	01/02/2023	31/12/2023
		7.4.2. Realizar informe del cumplimiento de los controles del Anexo A de la Norma ISO 27001:2013.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013.	Informe con los resultados del cumplimiento a los controles	01/02/2023	29/12/2023
	7.5. Acompañamiento en las auditorías internas y externas de la norma ISO 27001:2013.	7.5.1. Acompañar en las auditorías internas y externas de la norma ISO 27001:2013.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013. Equipo SGSI	Informes de comisiones o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms, o Grabación de la sesión	15/02/2023	31/12/2023
	7.6. Iniciar la migración del Sistema de Gestión de	7.6.1. Realizar diagnóstico para la migración del Sistema de Gestión de	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y	Informe Ejecutivo - Propuesta Declaración de aplicabilidad	01/02/2023	31/08/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	Seguridad de la Información a la norma ISO 27001/2022	Seguridad de la Información del ICBF a la norma ISO 27001 /2022.	requisitos de la Norma ISO 27001: 2013. Equipo SGSI			
		7.6.2. Definir cronograma de transición del Sistema de Gestión de Seguridad de la Información a la norma ISO 27001/2022, y ejecutar las actividades correspondientes a la vigencia 2023.	Profesional de la Dirección de Información y Tecnología responsable de la Gestión de Seguimiento a los dominios y requisitos de la Norma ISO 27001: 2013. Equipo SGSI	Cronograma de trabajo - Evidencias de la ejecución del cronograma de trabajo	1/02/2023	29/12/2023
8. Gestión de Continuidad de la Operación Tecnológica	8.1. Documentación 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	1/02/2023	29/09/2023
		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	29/12/2023
	8.2. Documentación del Plan de Recuperación de Desastres Tecnológicos de la DIT	8.2.1. Coordinar y apoyar la definición y/o actualización de las estrategias del DRP.	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	3/04/2023	29/09/2023
		8.2.2. Aplicar los requisitos de seguridad para cada una de las estrategias presentadas conforme al escenario.	Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Formato de requisitos de seguridad de la información	3/02/2023	22/12/2023
		8.2.3. 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	1/05/2023	30/09/2023
9. Gestión de Continuidad del Negocio	9.1. Documentar el Análisis de Impacto	9.1.1. Coordinar las Actualizaciones de las Actividades Criticas de SDG y Regionales	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Correo con el consolidado de actividades críticas	1/02/2023	30/06/2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
					Fecha inicio	Fecha final
	9.2. Documentar la Gestión de Riesgos de continuidad del negocio	9.2.1. Coordinar los riesgos asociados a continuidad del negocio	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Matriz de riesgos de continuidad del negocio	1/05/2023	30/09/2023
	9.3. Documentar las Estrategias de Continuidad	9.3.1. Coordinar y Actualizar las estrategias de continuidad de SDG y Regionales	Secretaria General Profesional de la Dirección de Información y Tecnología Responsable de Continuidad de la Operación Tecnológica del ICBF	Documento de estrategia de continuidad	1/04/2023	31/07/2023
	9.4. Documentar el Plan de Continuidad del Negocio	9.4.1. Coordinar y apoyar la definición 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	Plan de Continuidad del Negocio	1/02/2023	29/12/2023

4. 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.

5. 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.
- 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.

6. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
N.A.		