Contenido

1. INTRODUCCIÓN

El presente manual hace parte integral de la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del ICBF.

El ICBF mediante resolución 11980 del 30 de diciembre de 2019, por la cual se adopta el Modelo de Planeación y el Sistema Integrado de Gestión, asigna roles y responsabilidades en los ejes que lo integran, siendo la Seguridad de la Información uno de ellos. El Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, ahora Gobierno Digital bajo Decreto 1008 de 2018, en el cual se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus Habilitadores Transversales el de la Seguridad y Privacidad de la Información, permitiendo el desarrollo de los componentes de TIC para el Estado y TIC para la Sociedad y el logro de los propósitos de la Política de Gobierno Digital, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada. La resolución 4594 del 15 de junio de 2017, que modifica la resolución 7600 del 29 de julio de 2016, por la cual se adopta la modalidad de Teletrabajo Suplementario a nivel nacional en el Instituto Colombiano de Bienestar Familiar.

Además de las anteriores normativas, se tienen en cuenta las siguientes leyes y decretos:

- ✓ Constitución Política de Colombia. Artículo 15.
- ✓ 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”.
- ✓ CONPES 3854 de 2016. Política Nacional de Seguridad Digital en la República de Colombia
- ✓ CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital en la República de Colombia
- ✓ Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- ✓ Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- ✓ Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- ✓ Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- ✓ 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”.

- ✓ Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- ✓ Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- ✓ 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)
- ✓ Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

2. TÉRMINOS Y DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones:

- **Actividades de seguimiento:** Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.
- **Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
- **Activo crítico:** Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos misionales de ICBF.
- **Administración de Riesgos**: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Impacto al Negocio:** Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Áreas Seguras:** Son aquellas en donde se encuentren sistemas de procesamiento y almacenamiento informático o de datos. En el ICBF se identifican las siguientes áreas seguras:
    - Cuarto de cableado.
    - Centro de datos.
    - Archivos generales y de gestión.

  - Lugares que contengan información Reservada (oficinas con expedientes de adopción, oficinas de los Defensores de Familia).
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Centro de cableado:** el centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).
- **Ciberactivo crítico:** Ciberactivo que es crítico para la operación de un activo crítico.
- **Ciberactivo:** Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del ICBF, destinado a apoyar el cumplimiento de las normas, procesos y procedimientos de seguridad de la información.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **CCOCI:** Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.
- **COLCERT:** Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.
- **Codificación segura:** se refiere a las prácticas y técnicas de desarrollo para escribir software que sea resistente a vulnerabilidades y ciberataques, protegiendo la integridad, confidencialidad y disponibilidad de la información. Estas prácticas incluyen la validación de entradas, la gestión segura de autenticación y sesiones, el control de acceso, la criptografía, y el manejo adecuado de errores y registros.

- **CSIRT:** Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
- **Desastre Tecnológico:** Se define como una situación, derivada de un accidente en el que se involucran sustancias químicas peligrosas o equipos peligrosos; que causa daños al ambiente, a la salud, al componente socioeconómico y a la infraestructura, siendo estos daños de tal magnitud que exceden la capacidad de respuesta del componente del afectado.
- **DRP:** Sigla en inglés (Disaster Recovery Plan), Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.
- **Datacenter:** Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Dispositivos móviles:** Equipo de cómputo pequeño, cuyo concepto principal es la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **DMZ:** Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet de VPN.
- **Eliminación de información:** La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
- **Enmascaramiento de datos:** El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
- **Equipos activos de red:** son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos del ICBF.
- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
- **Filtrado web:** El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.

- **G58:** Es la persona que desempeña el rol con funciones u obligaciones para notificar las novedades de activación y desactivación de las cuentas de usuario ante la mesa de servicio.
- **Gestión de la configuración:** Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
- **Incidente de Seguridad:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Información Pública Clasificada:** "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado…"
- **Información Pública Reservada:** "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos..."
- **Infraestructura Crítica (IC):** Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.
- **Infraestructura Crítica Cibernética (ICC):** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa.
- **Inteligencia de Amenazas:** es la recopilación, análisis y difusión de información sobre amenazas de ciberseguridad, incluyendo vulnerabilidades, tácticas, técnicas y procedimientos (TTP) de los autores de amenazas, y también indicadores de compromiso (IOC).
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
- **Medio removible:** Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.
- **Mesa de servicio:** Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes

reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de servicio que la Dirección de Información y Tecnología se informa de las necesidades que tienen los funcionarios en cuanto a los recursos informáticos a nivel nacional.

- **Monitoreo de seguridad física:** Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Paneles de conexión (patch panel):** Elemento encargado para la organización de conexiones en la red.
- **Plan de Continuidad de Negocio:** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Prevención de fuga de datos:** Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
- **Propietario del riesgo:** Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **Responsable de Seguridad de la información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Seguridad de la Información para el uso de servicios en la nube:** se refiere a las prácticas y medidas que se implementan para proteger los datos y la información cuando se utilizan servicios en la nube. Esto incluye la gestión de riesgos, la selección de proveedores, la garantía de seguridad, y la gestión de incidentes.
- **Sistemas batch:** sistema por lotes, ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario. Generalmente, este tipo de ejecución se utiliza en tareas repetitivas sobre grandes conjuntos de información, ya que sería tedioso y propenso a errores realizarlo manualmente. Un ejemplo sería la generación de extractos bancarios, el cálculo de intereses corrientes o moratorios de cuentas de crédito, la

generación automática de archivos de interfaz con otros sistemas, etc. Los programas que ejecutan por lotes suelen especificar su funcionamiento mediante scripts o guiones (procedimientos) en los que se indica qué se quiere ejecutar y, posiblemente, qué tipo de recursos necesita reservar.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del ICBF.
- **Tecnologías de la Información:** Las tecnologías de la información y las Comunicaciones (TIC o TICs), Nuevas Tecnologías de la Información y de la Comunicación (NTIC), agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.
- **Test de penetración:** es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- **VPN:** red virtual privada por sus siglas en ingles Virtual Private Network.

3. PARTES INTERESADAS

Las partes interesadas corresponden a las personas naturales o jurídicas con la cual el ICBF interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas por la Seguridad de la Información del Instituto y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del Sistema de Gestión de Seguridad de la Información - SGSI.

Estas partes interesadas se basan en el A1.P21.DE Anexo Identificación y Actualización de Necesidades y Expectativas que se encuentra publicado en el portal web del ICBF en el espacio del Proceso de Direccionamiento Estratégico.

Sin embargo, a continuación, se especifican las necesidades, expectativas y el nivel de aplicación de las partes interesadas para el **ESTADO Y ALIADOS ESTRATÉGICOS**:

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
ESTADO						
MINTIC - Ministerio de las Tecnologías de la Información y Comunicaciones	Brindar información sobre la ejecución de los planes, servicios, ejes temáticos, marco estratégico de TI y Gobierno Digital.	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del SGSI.	Lineamientos Normativa.	Cumplimiento normativo de Gobierno Digital.	X	X

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
	Dar cumplimiento a los lineamientos y procedimientos en la normativa legal vigente correspondiente a seguridad y privacidad de la información. Generación de conocimiento de las nuevas amenazas emergentes en el ICBF. Generar informes de los incidentes de seguridad, privacidad de la información y seguridad digital presentados en la entidad cuando se considere necesario.	Fortalecer los canales de comunicación de tal forma que sea efectiva y asertiva entre los entes de control externo, con el fin de mantener informado a éstos de los distintos ataques cibernéticos, mitigando los riesgos y previniendo incidencias. Propender por la protección de la información de la ciudadanía a través del sostenimiento de Modelo de Seguridad y Privacidad de la Información implementado a nivel nacional. Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios. Aplicar los controles de seguridad digital y seguridad de la información, establecidos para la mitigación de los riesgos en los procesos. Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad.				

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
Policía Nacional - DIJIN	Generación de conocimiento de las nuevas amenazas emergentes en el ICBF. Generar informes de los incidentes de seguridad, privacidad de la información y seguridad digital presentados en la entidad cuando se considere necesario.	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del SGSI. Fortalecer los canales de comunicación de tal forma que sea efectiva y asertiva entre los entes de control externo, con el fin de mantener informado a estos de los distintos ataques cibernéticos, mitigando los riesgos y previniendo incidencias. Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios. Aplicar los controles de seguridad digital y seguridad de la información, establecidos para la mitigación de los riesgos en los procesos. Suministro de evidencias digitales a la DIJIN, para el análisis forense por parte de este Ente.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información que contemplan análisis forense.	X	X
Contraloría	Asegurar que las fuentes de información entre el ICBF y los entes de control sea veraz oportuna y con los acuerdos de confidencialidad necesarios.	Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad.	Cumplimiento requisitos fiscales.	Evitar sanciones o hallazgos por entes de control.	X	X

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
Procuraduría	Asegurar que las fuentes de información entre el ICBF y los entes de control sean Veraces, oportunas y con los acuerdos de confidencialidad necesarios.	Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad.	Cumplimiento de requisitos sancionatorios.	Evitar sanciones o hallazgos por entes de control.	X	X
Fiscalía	Generar informes de los incidentes de seguridad, privacidad de la información y seguridad digital presentados en la entidad cuando se considere necesario.	Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios. Aplicar los controles de seguridad digital y seguridad de la Información, establecidos para la mitigación de los riesgos en los procesos.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.	X	X
Alcaldías	Sensibilización y acompañamiento en temas de delitos informáticos y riesgos de Seguridad Digital. Cooperación ante eventos catastróficos o de continuidad del negocio.	Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios. Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad.	Manual Políticas de Seguridad de la Información.	Apoyo para la implementación y ejecución de los planes de continuidad de la operación.		X
Gobernaciones	Sensibilización y acompañamiento en temas de delitos informáticos y riesgos de Seguridad Digital. Cooperación ante eventos catastróficos o de continuidad del negocio.	Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios. Cumplimiento de la normatividad legal vigente para el aseguramiento de la	Manual Políticas de Seguridad de la Información.	Apoyo para la implementación y ejecución de los planes de continuidad del negocio.	X	X

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
		infraestructura tecnológica y prestación de los servicios de la Entidad.				
ALIADOS ESTRATÉGICOS						
CSIRT - PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Dar a conocer los informes de alerta de ataques que se están presentando a nivel mundial y local, y que puedan afectar a alguna entidad estatal colombiana.	Que el ICBF dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación. Comunicación y colaboración permanente sobre el manejo de incidentes que afecten la seguridad de la información.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.	X	
CCP - Centro Cibernético Policial	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Brindar apoyo respecto a la Ciberseguridad Ciudadana.	Que el ICBF dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación. Investigación y judicialización.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.	X	X
COLCERT	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de	Que el ICBF dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.	X	

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados	Aplicación	
					Nacional	Territorial
	conocimiento e información. Brindar apoyo respecto a la Ciberseguridad de Infraestructuras Críticas del país.	Coordinación de emergencias ante incidentes.				
CCOCI - Comando Conjunto de Operaciones Cibernéticas	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Brindar apoyo respecto a la Ciberdefensa de Infraestructuras Críticas Cibernéticas Nacionales de Colombia.	Que el ICBF dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación. Participación del ICBF de las convocatorias de este ente para la implementación de controles a las infraestructuras críticas.	Manual Políticas de Seguridad de la Información.	Ser parte del Plan Nacional de Protección de Infraestructura Crítica Cibernética del país.	X	
SIC - Superintendencia de Industria y Comercio	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Registro de Base de datos en el marco de la Ley 1581 de 2012.	Que el ICBF dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación.	Cumplimento de requisito legal.	Evitar sanciones o hallazgos por entes de control.	X	X

4. EVALUACIÓN DEL DESEMPEÑO

A continuación, se muestran los indicadores del Eje de Seguridad de la Información publicados en el tablero de control del ICBF:

Nombre	Fórmula
Porcentaje de Eficacia del SGSI	Número de actividades ejecutadas al periodo de corte sobre el Número de actividades

	programadas para la vigencia del Plan de Implementación.
Porcentaje de Riesgos de Seguridad de la Información gestionados	Número de actividades ejecutadas a la fecha de corte sobre Número de actividades Programadas a la fecha de corte.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ICBF

Requisito SGSI-5.3	
Funciones, responsabilidades y autoridades de la organización	**CONTROLES RELACIONADOS** SGSI-5.1 Políticas de seguridad de la información. SGSI-5.2 Roles y responsabilidades de seguridad de la información SGSI-5.4 Responsabilidades de la dirección SGSI- 5.9 Inventario de información y otros activos asociados. SGSI-5.30 Preparación de las TIC para la continuidad de negocio SGSI-5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.
Anexos:	G7.ABS Guía para la adquisición de bienes y servicios de calidad.

Propósito:
Dictar lineamientos que permitan administrar la seguridad de la información dentro del ICBF y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades y poder aplicar las medidas de seguridad adecuadas en los accesos de terceros a la información del ICBF.

Lineamientos Generales:

- ✓ Los Roles y responsabilidades para la seguridad de la información son los dispuestos en las Resoluciones 11980 del 30 de diciembre de 2019 y 6659 del 15 de diciembre del 2020, por las cuales se adopta y modifica el Modelo de Planeación y el Sistema Integrado de Gestión o cualquiera que la adicione, modifique o derogue.
- ✓ La información deberá estar bajo la responsabilidad del Líder de Proceso para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información del ICBF.
- ✓ El Líder del Eje de Seguridad de la Información deberá mantener contacto con las autoridades Nacionales en materia de seguridad de la información.
- ✓ El Líder del Eje de Seguridad de la Información deberá mantener los contactos apropiados con los grupos de interés especial (Policía Nacional, Fiscalía, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.) u otros foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información, que requiera de asesoría externa.
- ✓ Todos los proyectos que se desarrollen en el marco del cumplimiento de los objetivos de los Procesos del Modelo de Operación por Procesos del ICBF deberán tener un componente de seguridad de la información, el cual deberá ser acompañado y asesorado por el Líder del Eje de Seguridad de la Información o a quien este delegue, de acuerdo a la especificidad técnica, teniendo en cuenta las obligaciones que están estipuladas en la -***G7.ABS Guía para la adquisición de bienes y servicios de calidad***- del proceso de ADQUISICIÓN DE BIENES Y SERVICIOS.

Control SGSI-8.1	
Dispositivos de punto final de usuario	**CONTROLES RELACIONADOS** SGSI-5.17 Información de autenticación. SGSI-8.24 Uso de la criptografía.
Anexos:	Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información

	A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información F1.P2.GTI Formato de solicitud de servicios de tecnología. F9.P2.GTI Formato verificación de equipos Personales. F10.P2.GTI Formato Verificación de Equipos Institucionales G22.GTI Guía para Uso de Dispositivos Personales BYOD. P23.GTI Procedimiento Gestión de Permisos de Propiedad Sharepoint IT1.P6.GTI Instructivo para el Cargue de Documentación en Share Point G27.GTI Guía de Políticas de Navegación

Propósito:
Establecer los lineamientos para el uso, administración, consulta y operación de los servicios en los dispositivos móviles del ICBF y a su vez controlar el acceso a los mismos, en las instalaciones del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología deberá establecer y divulgar los procedimientos para el uso de la información y los servicios tecnológicos del ICBF en los dispositivos móviles tanto de propiedad del ICBF, como aquellos suministrados por los proveedores para colaboradores en el marco de la ejecución de algún contrato o convenio, así como de propiedad de los colaboradores.
- ✓ La Dirección de Información y Tecnología deberá establecer lineamientos para el uso correcto de los dispositivos de conexión móvil, dado que éstos serán utilizados únicamente en situaciones de contingencia y en sitios donde no exista un medio de comunicación que permita el acceso a los colaboradores al servicio de internet.
- ✓ Los dispositivos móviles deberán cumplir con lo establecido en la Guía para uso de Dispositivos Personales -BYOD-.
    - Los computadores portátiles de propiedad de los colaboradores no deberán estar incluidos en el dominio *icbf.gov.co,* para conectarse a los servicios de la red de datos del ICBF deberán realizar solicitud a la mesa de servicio para la revisión de los equipos conforme a lo establecido en la Guía para uso de Dispositivos Personales -BYOD-.
    - En caso de que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con los lineamientos establecidos en la Guía para uso de Dispositivos Personales -BYOD-. Los ingenieros y soportes en sitio deberán realizar la revisión de los requisitos de seguridad en los equipos autorizados para conectarse a la red de ICBF.
- ✓ Los dispositivos móviles de propiedad del ICBF deberán cumplir con la política de control de acceso, y los colaboradores que deseen configurar sus dispositivos personales deberán acogerse a las políticas de monitoreo del dispositivo móvil, sin que esto incurra en una violación a la privacidad del colaborador.
- ✓ La red inalámbrica de funcionarios debe ser unificada en su SSID y contraseña a nivel nacional, permitiendo que únicamente se conecten los dispositivos móviles propiedad del ICBF independientemente de donde sea el colaborador.
- ✓ Aquellos dispositivos móviles que son propiedad de los colaboradores o visitantes deberán conectarse a la red de Visitantes, cumpliendo con los lineamientos de la política de seguridad de la información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos será la responsable de gestionar los riesgos que conlleva el uso de dispositivos móviles.
- ✓ La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información y el servicio de seguridad informática establecerá los lineamientos para la gestión de ciberseguridad en el marco del Sistema de Gestión de Seguridad de la Información y continuidad de la operación tecnológica del ICBF.
- ✓ Los colaboradores de terceras partes solo podrán utilizar los dispositivos asignados por el operador/contratista, para el ejercicio de las obligaciones propias del contrato suscrito con el ICBF, cumpliendo con las directrices referentes a seguridad de la información.
- ✓ Los colaboradores en modo o conectados vía VPN ZTNA se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios, y se llevará registro de su conexión.
- ✓ Todo dispositivo móvil institucional, que transmita y/o almacene información clasificada y/o reservada de la Entidad, podrá ser monitoreado a través de la herramienta de gestión tecnológica definida por la Dirección de Información y Tecnología.
- ✓ Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad, y que transmita y/o almacene información clasificada y/o reservada, podrá ser monitoreado a través de la herramienta tecnológica definida por la Dirección de Información y Tecnología.

✓ Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad deberá cumplir con la política y lineamientos definidos en la Guía para el uso de dispositivos personales.

Control SGSI-6.7	
Trabajo remoto	**CONTROLES RELACIONADOS** SGSI-5.15 Control de Acceso
Anexos:	**Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones **Resolución 6700 del 09/10/2023** "Por medio de la cual se adopta la modalidad de Teletrabajo Suplementario l en el Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras y se derogan las Resoluciones 7600 de 2016 y 4594 de 2017". A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. G22.GTI Guía para Uso de Dispositivos Personales BYOD. - F1.P2.GTI. Formato de solicitud de servicios de tecnología IT1.P2.GTI. Instructivo para gestión de solicitudes de VPN. F9.P2.GTI Formato Verificación de Equipos Personales. F10.P2.GTI Formato de Solicitud Servicios de Tecnología

Propósito:

Establecer los lineamientos en materia del Sistema de Gestión de Seguridad de la Información que tiene los colaboradores del ICBF que se acogen a la modalidad de Teletrabajo para el uso, administración, consulta y operación de los servicios en las áreas de Teletrabajo.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología deberá establecer y divulgar el uso de la información y los servicios tecnológicos necesarios para garantizar el adecuado funcionamiento de la modalidad de Teletrabajo.
- ✓ Los computadores portátiles de propiedad de los colaboradores en la modalidad de teletrabajo, se les debe realizar la verificación de los requerimientos tecnológicos del equipo mediante el formato verificación de Equipos Personales V1 F9.P2.GTI Previa solicitud a la Mesa de servicio. Los computadores portátiles propiedad de los colaboradores deberán cumplir con la política de control de acceso.
- ✓ La Dirección de Información y Tecnología será la responsable de gestionar los riesgos de seguridad de la información que se identifiquen en la modalidad de Teletrabajo y así mismo proporcionar los controles que sirvan para mitigarlos.
- ✓ La Dirección de Gestión Humana deberá verificar que los equipos personales de los colaboradores que realizan actividades **de Teletrabajo** cumplan con los lineamientos referentes a seguridad de la información, teniendo en cuenta lo enmarcado en la normativa y los procedimientos de **Teletrabajo** definidos por la Entidad, así como lo establecido en la Guía para uso de Dispositivos Personales -BYOD-.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá implementar los controles necesarios que permitan el acceso remoto a las aplicaciones o servicios tecnológicos del ICBF a los colaboradores que realicen actividades en **Teletrabajo**, así mismo se deben tener en cuenta la revocación de servicios cuando el colaborador no continué realizando actividades **de Teletrabajo**.
  Los colaboradores en modo **Teletrabajo** o conectados vía VPN ZTNA se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios y se llevará registro de su conexión.

6. SEGURIDAD DEL RECURSO HUMANO

Control SGSI-6.1	
Selección	**CONTROLES RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. Para los servidores públicos:

	- P21.GTH Procedimiento Provisión de Empleos -F3.P21.GTH Formato Relación de Documentos para Nombramiento y Posesión -F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales -F6.P21.GTH Formato Inhabilidades para ejercer Cargos Públicos -F8.P21.GTH Formato Declaración Inasistencia Alimentaria -F9.P21.GTH Formato Datos para Afiliación -F12.P21.GTH Formato Compromiso de Confidencialidad de Información -F13.P21.GTH Formato Análisis de Hoja de Vida v1 -F10.P21.GTH Formato Autorización Descuentos de Alimentación -F11.P21.GTH Formato Información Cuenta para Abono Pago Sueldo y Prestaciones Sociales Para los contratistas: P5.ABS Procedimiento para la Solicitud e Inicio del Proceso de Contratación F1.P5.ABS Formato Lista de Chequeo Contratación Directa F2.P5.ABS Formato Lista de Chequeo Proceso de Selección F3.P5.ABS Formato Estudios Previos v12 F4.P5.ABS Formato Autorización Consulta Inhabilidades por Delitos Sexuales F5.P5.ABS Formato Lista de Chequeo Contratación Directa (Aporte y Convenio) P2.ABS application/pdf Procedimiento para la Contratación de Prestación de Servicios Profesionales y de Apoyo a la Gestión F1.P2.ABS Formato Relación de Necesidades por Prestación de Servicios F3.P2.ABS Formato Certificación de no Existencia en Planta F4.P2.ABS Formato Certificado de Idoneidad y Experiencia F11.P2.ABS Formato Responsable de IVA - No Responsable de IVA F12.P2.ABS Formato Lista de Chequeo CPS con Persona Jurídica F13.P2.ABS Formato Estudio Previo y Matriz Riesgos CPSPAG y TA F14.P2.ABS Formato Lista de Chequeo CPS o TA con Persona Natural F15.P2.ABS Formato Declaración Contratista Celebración CPSP o Apoyo a la Gestión F10.P2.ABS Formato Clausulado General CPS y AG

Propósito:
Dictar lineamientos para que el personal que se contrata cumpla con las políticas del ICBF en materia de seguridad de la información.

Lineamientos Generales:

- ✓ La Dirección de Gestión Humana deberá definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación del ICBF y los que dicte la Función Pública.
- ✓ La Dirección de Contratación deberá definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la ley y la reglamentación vigente.
- ✓ Los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la política de tratamiento de datos personales del ICBF y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- ✓ Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.
- ✓ La Dirección de Gestión Humana y la Dirección de Contratación deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

Control SGSI-6.2

Términos y condiciones de empleo	**CONTROLES RELACIONADOS**
	SGSI-6.6 Acuerdos de confidencialidad o no divulgación. SGSI-5.32 Derechos de la propiedad intelectual. SGSI-5.34 Privacidad y protección de la información de identificación personal (PII). SGSI-6.4 Proceso disciplinario. SGSI-6.5 Responsabilidades después de la terminación o cambio de empleo.
Anexos:	- Resolución 2677 de 02 de mayo de 2022, Por la cual se modifica el Manual Especifico y Competencias Laborales del Instituto Colombiano de Bienestar Familiar, adoptado mediante Resolución 1818 de 2019 y modificado por las resoluciones 7444 de 2019, 4122 de 2020 y 4451 de 2020 -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. **Para los funcionarios públicos:** - Ley 734 de 2002 Código Disciplinario Único, artículo 34 Deberes. Numeral 4 " Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos" y Numeral 5 " Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos". - P21.GTH Procedimiento Provisión de Empleos - F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales. - F12.P21.GTH Formato Compromiso de Confidencialidad de Información. **Para los contratistas:** - P2.ABS Procedimiento Contrato para la Prestación de Servicios y de Apoyo a la Gestión -F15.P2.ABS Formato Declaración Contratista Celebración CPSP o Apoyo a la Gestión

Propósito:
Dictar lineamientos para que el personal que se vincula o se contrata cumpla con las políticas del ICBF en materia de seguridad de la información.

Lineamientos Generales:

- ✓ La Dirección de Contratación deberá definir los términos y condiciones del contrato, en los cuales se establecerá las obligaciones del contratista en materia de seguridad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública.
- ✓ La Dirección de Gestión Humana y la Dirección de Contratación deberán dar a conocer a los colaboradores los términos y condiciones de empleo o contrato y especificar las responsabilidades u obligaciones en materia de la seguridad de la información.
- ✓ La Dirección de Contratación deberá incluir en el pliego de condiciones o estudios previos para la contratación de terceras partes, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte el ICBF y aquellas contenidas en la -***G7.ABS Guía para la adquisición de bienes y servicios de calidad***- del proceso de ADQUISICIÓN DE BIENES Y SERVICIOS.
- ✓ La Dirección de Gestión Humana y la Dirección de Contratación deberán hacer firmar un documento de compromiso de confidencialidad de la información a los colaboradores, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.

Control SGSI-5.4	
Responsabilidades de la dirección	**CONTROLES RELACIONADOS**

	N/A
Anexos:	- Resolución 11980 de 2019, Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF - Resolución 6659 del 15/12/2020 Por la cual se modifica el modelo de Planeación y Sistema Integrado de Gestión. Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. - Acta de Comité SIGE - Revisión por Dirección
Propósito: Dictar lineamientos a todos los colaboradores del ICBF en la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. **Lineamientos Generales:** ✓ El supervisor del contrato deberá hacer seguimiento al cumplimiento de las obligaciones generales de todos los contratos en materia de seguridad de la información, sin importar su naturaleza. ✓ La Dirección de Información y Tecnología dará a conocer el Manual de Políticas de Seguridad de la Información a los colaboradores del ICBF. ✓ Una vez formalizado el proceso de vinculación, el supervisor de contrato o jefe inmediato solicitará la creación de la cuenta de usuario y apertura del inventario de vinculación del personal a través del colaborador con el rol G58. ✓ La Dirección de Contratación, la Dirección de Gestión Humana, el supervisor del contrato o el jefe inmediato deberá informar a la Mesa de servicio sobre las novedades del colaborador para tomar las acciones pertinentes.	

Control SGSI-6.3	
Conciencia de seguridad de la información, educación y formación	**CONTROLES RELACIONADOS** N/A
Anexos:	- El ICBF cuenta con un módulo SGSI inmerso en el curso virtual SIGE. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. - P10.GTH Procedimiento Inducción y Reinducción. - PIC P7.GTH Procedimiento para la Formulación y Ejecución del Plan Institucional de Capacitación. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. -PL5.GTI Plan de Apropiación de TI.
Propósito: Dictar lineamientos para que los colaboradores del ICBF sean sensibilizados en temas de seguridad de la información, buenas prácticas y toma de conciencia. **Lineamientos Generales:** ✓ La Dirección de Gestión Humana, jefe inmediato o el supervisor del contrato deberán propender que los colaboradores del ICBF y usuarios de terceras partes que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.	

- ✓ La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información, diseñará e implementará un plan con estrategias de cultura, cambio y apropiación referentes a la seguridad y privacidad de la información.
- ✓ La Dirección de Gestión Humana realizará las convocatorias para realizar el curso del Sistema Integrado de Gestión – SIGE contenido en la escuela virtual del ICBF.

Control SGSI-6.4	
Proceso disciplinario	**CONTROLES RELACIONADOS** SGSI-5.28 Recopilación de evidencias.
Anexos:	- P43.GTH Procedimiento Proceso Disciplinario – Instrucción - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. -P43.GTH Procedimiento Proceso Disciplinario -Instrucción

Propósito:
Dictar lineamientos para generar acciones a los colaboradores que hayan cometido incumplimientos a lo establecido en la Política de Seguridad de la información.

Lineamiento General:
- ✓ En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control interno disciplinario del ICBF.

Control SGSI-6.5	
Responsabilidades después de la terminación o cambio de empleo	**CONTROLES RELACIONADOS** SGSI-6.6 Acuerdos de confidencialidad o no divulgación. SGSI-6.2 Términos y condiciones de empleo.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. **Para funcionarios Públicos:** - P30.GTH Procedimiento para Entrega de Cargo por Parte de Servidores Públicos - F1.P30.GTH Formato Lista de Chequeo Entrega del Cargo - F2.P30.GTH Formato Informe Final de Entrega de Cargo - F3.P30.GTH Formato Entrevista de Retiro **Para Contratistas:** - P25.ABS Procedimiento Finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión. - F1.P25.ABS Formato lista de chequeo finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión. -F4.P30.GTH Formato Único Acta de Gestión

Propósito:
Dictar lineamientos para las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo.

Lineamientos Generales:
- ✓ El supervisor del contrato o a quien delegue deberá proteger y custodiar la información del ICBF bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

- ✓ El jefe inmediato o a quien delegue deberá proteger y custodiar la información del ICBF en el caso de retiro, investigación, inhabilidades, o cambio de funciones.
- ✓ Cuando un funcionario, colaborador, proveedor u operador se le termina su vínculo administrativo o finaliza el contrato, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo los derechos de propiedad intelectual de acuerdo con la normativa vigente.
- ✓ El jefe inmediato o el supervisor del contrato a través del G58 deberán informar a la Dirección de Información y Tecnología a través de la Mesa de servicio, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad la Dirección de Información y Tecnología deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros:
  - Si el buzón pertenece a una cuenta de correo genérica (ejemplo: info@icbf.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.
  - En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes se les entregará en cadena de custodia una copia del buzón garantizando su integridad.
  - Emitir comunicado a los proveedores y demás personal con el que el colaborador tenga contacto, indicándole que esa persona ya no labora en el ICBF e indicar quién asumirá sus funciones o responsabilidades.
  - Adicionalmente en desvinculación:
    - Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con el ICBF.
    - Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.
    - Se deben inactivar todos los accesos a los sistemas de información.
    - Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredita como colaborador del ICBF.
    - Se debe deshabilitar la cuenta de dominio y accesos a la VPN si es el caso.
    - Para los usuarios que manejen buzones genéricos deberán informarlo al supervisor para realizar la copia de información de esas cuentas adicionales.

7. GESTIÓN DE ACTIVOS

Control SGSI-5.9	
Inventario de información y otros activos asociados	**CONTROLES RELACIONADOS**
	SGSI-5.12 Clasificación de la Información. SGSI-5.10 Uso aceptable de la información y otros activos asociados
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - F1.G10.GTI Formato para levantamiento de activos de información. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional. - G11.GTI Guía para la Clasificación y Etiquetado de la Información. - Herramienta automatizada para el levantamiento de activos de información. - Sistema de Información SVE

Propósito:
Identificar los activos de información del ICBF, manteniendo un inventario de estos.

Lineamientos Generales:

- ✓ El Eje de Seguridad de la Información deberá aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de Información del ICBF.
- ✓ Los líderes de los procesos deberán mantener un inventario de sus activos de información de forma anual y serán actualizados según el evento en que se requiera.

- ✓ El ICBF deberá designar responsabilidades a los líderes de los procesos sobre sus activos de información.
- ✓ El Líder del Eje de Seguridad de la Información a través de la Dirección de Información y Tecnología, deberá reportar a la Subdirección de Sistemas Integrados de Información el inventario de activos consolidado y detallado por procesos con el fin de que estos sean publicados en los sitios designados a cada proceso en la intranet.
- ✓ El Líder del Eje de Seguridad de la Información, deberá remitir el consolidado del levantamiento de activos de información, a la Dependencia designada por la Dirección General que lidera la estrategia de la Ley de transparencia y acceso a la información pública y la estrategia de Gobierno Digital o a quien haga sus veces, con el objetivo de ser analizada, realimentada, actualizada y publicada de acuerdo a la normativa vigente colombiana teniendo en cuenta los lineamientos de legalidad emitidos por la Oficia Asesora Jurídica.

Control SGSI-5.10	
Uso aceptable de la información y otros activos asociados	**POLÍTICAS RELACIONADAS** SGSI-5.12 Clasificación de la Información.
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - PL6.GTI. Plan de cambio y cultura de seguridad y privacidad de la información -PL5.GTI Plan de Apropiación de TI - F1.P2.GTI Formato solicitud de servicios de tecnología. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional V2 - Herramienta automatizada para el levantamiento de activos de información - G22.GTI Guía para Uso de Dispositivos Personales BYOD -F10.P2.GTI Formato Verificación de Equipos Institucionales - F9.P2.GTI Formato Verificación de Equipos Personales -G11.GTI Guía para la Clasificación y Etiquetado de la Información -G23.GTI Guía Metodológica para la Anonimización de Registros -IT1.G12.GTI Instructivo Nomenclatura de Equipos -PL11.GTI Plan de Transformación Digital Visión Digital y Hoja de Ruta 2020 - 2022 - Procedimiento Control Préstamo y Devolución de Expedientes -F1. P21.SA Formato Control Préstamo y Devolución de Expedientes

Propósito:

Dictar lineamientos para identificar, documentar e implementar las reglas para el uso aceptable de información.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para el uso aceptable de los activos teniendo en cuenta lo siguiente:

- ✓ Los colaboradores y usuarios de partes externas deberán utilizar únicamente el software base aprobado y equipos de cómputo autorizados por la Dirección de Información y Tecnología.
- ✓ En caso de que el colaborador deba hacer uso de equipos personales, estos deberán cumplir con las reglas de seguridad y lineamientos establecidos en la documentación oficial para uso de dispositivos personales y solo podrá conectarse a la red del ICBF, una vez este sea avalado por los ingenieros de la Subdirección de Recursos Tecnológicos, Ingenieros Regionales o soporte en sitio.
- ✓ El único servicio de correo electrónico autorizado para el manejo de la información institucional en el ICBF es el que cuenta con el dominio *icbf.gov.co*.
- ✓ El ICBF podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado en caso de posible desacato a las leyes, decretos o reglamentación interna del ICBF.
- ✓ Las firmas de documentos oficiales que se constituyan como activos de información de acuerdo con la tabla de retención documental o acto administrativo deben reposar en original o con firma digital.
- ✓ El ICBF se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo, por solicitud expresa del coordinador, ordenador(a) del gasto, supervisor del contrato,

jefe inmediato, Director(a) General, Jefe de Oficina de Control Interno Disciplinario o Director(a) de Gestión Humana a la Dirección de Información y Tecnología, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la Entidad.

- ✓ Con el fin de mitigar la suplantación de correos electrónicos se activa el doble factor de autenticación.
- ✓ El correo institucional deberá ser usado exclusivamente para fines institucionales. Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo con la clasificación de la información establecida en la Entidad.
- ✓ Toda persona que tenga asignado correo electrónico institucional es custodio de sus credenciales de acceso, por lo cual, está expresamente prohibido el uso de su cuenta en páginas o sitios ajenos a los fines de la Entidad, siendo su responsabilidad en caso de que este sea vulnerado, asumiendo las consecuencias legales y disciplinarias a que haya lugar.
- ✓ La Dirección de Información y Tecnología deberá implementar un control de cifrado para los mensajes de correo electrónico institucional.
- ✓ La Subdirección de Recursos Tecnológicos deberá configurar el método de autenticación multifactor a los usuarios de los colaboradores al momento de iniciar la sesión para acceder a las cuentas y servicios ligadas al dominio de ICBF, con el cual se validará la identidad y se implementará el acceso seguro.
- ✓ Los servicios a los que un determinado usuario pueda acceder en internet dependerán de la categoría que se le asigne, la cual se establece a partir de la dependencia a la que pertenezca, obligaciones contractuales, funciones o roles que desempeña en el ICBF y para las cuales esté formal y expresamente autorizado.
- ✓ No está permitido el uso de botellones de agua cerca a elementos tecnológicos o archivos de gestión, lo anterior para evitar un incidente de seguridad de la información.
- ✓ No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos que sean autorizados por la Dirección Administrativa o quien haga sus veces en el nivel Regional o Zonal.
- ✓ Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los equipos de cómputo, impresoras, escáner, switches, servidores y demás recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, para desempeñar esta labor.

Control SGSI-5.11	
Devolución de activos	**CONTROLES RELACIONADOS**
	SGSI-7.14 Disposición o reutilización segura de los equipos. SGSI-8.1 Dispositivos de punto final de Usuario. SGSI-7.9 Seguridad de los activos fuera de las instalaciones.
Anexos:	Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G2.SA Guía Gestión de Bienes - F2.G2.SA Formato Devolución de Bienes al Almacén - IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo. - IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento. **Para servidores públicos:** - P30.GTH Procedimiento para Entrega de Cargo por Parte de Servidores Públicos y Contratistas. - F1.P30.GTH Formato Lista de Chequeo Entrega del Cargo.

	Para usuarios de partes externas y/o contratistas: - G7.ABS Guía para la Adquisición de Bienes y Servicios de Calidad desde el proceso de Adquisición de Bienes y Servicios. - P21.ABS Procedimiento Terminación Anticipada y/o Liquidación de Contratos de Prestación de Servicios y Apoyo a la Gestión Mutuo Acuerdo. - F1.P25.ABS Formato lista de chequeo finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión.

Propósito:
Todos los colaboradores y terceras partes deberán devolver todos los activos de información del ICBF que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

Lineamientos Generales:

- ✓ Los colaboradores y terceras partes deberán devolver todos los activos de información del ICBF que se encuentran en su poder a la terminación de su empleo, contrato, convenio o acuerdo.
- ✓ Para el traslado de equipos de cómputo al almacén o a otros colaboradores, o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre, a través de la mesa de servicio. Posterior se debe seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo, en los equipos que contengan medios de almacenamiento con el fin de propender que la información del ICBF contenida en estos medios no se pueda recuperar.
- ✓ Cuando se realice el traslado de equipos de cómputo a otros colaboradores, se deberá instalar de nuevo el sistema operativo y los programas de la línea base.
- ✓ La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Dirección de Información y Tecnología o quien haga sus veces en el nivel regional y zonal, sin embargo, cuando deba realizarse desde y hacia el almacén será la Dirección Administrativa o quien haga sus veces en el nivel regional y zonal, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.

Control SGSI-5.12	
Clasificación de la información	**CONTROLES RELACIONADOS**
	SGSI-5.15 Control de acceso
Anexos:	La Dirección de Servicio y Atención, y la Oficina de Asesoría Jurídica, revisan el levantamiento de activos para dar cumplimiento a la ley de transparencia 1712 de 2014. - El ICBF debe conocer y clasificar los activos de información. Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - Índice de Información Clasificada y Reservada. - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - G11.GTI Guía para la Clasificación y Etiquetado de la Información.

Propósito:
Clasificar la información de acuerdo con los requisitos legales, valor y criticidad de la información.

Lineamientos Generales:

La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información y la Dirección Administrativa a través del grupo de Gestión Documental desarrollarán los lineamientos para la clasificación de la información teniendo en cuenta lo siguiente:

- ✓ Los propietarios de la información son los encargados de realizar la clasificación de la información.
- ✓ El ICBF definirá los niveles adecuados para clasificar su información de acuerdo con su sensibilidad donde se valorarán por confidencialidad o integridad o disponibilidad de la información. Estos niveles deberán ser oficializados y divulgados a los colaboradores.
- ✓ Los custodios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación.
- ✓ Si la información es de carácter clasificada o reservada y es requerida por algún ente externo o ciudadano en donde opere el ICBF, su entrega está supeditada a la aprobación previa de su propietario y de las instancias jurídicas o administrativas establecidas.
- ✓ Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.
- ✓ Los colaboradores y terceras partes deberán acatar los lineamientos de la Guía para la rotulación de la información, para divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del ICBF.
- ✓ La información física y digital del ICBF deberán tener un periodo de almacenamiento que puede ser dado por requerimientos legales o misionales; este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada adecuadamente.
- ✓ La clasificación de la información del ICBF está definida de conformidad con la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), tablas de retención documental TRD, el Decreto 1080 de 2015 y lo estipulado en la Guía para el Desarrollo de Inventario y Clasificación de Activos del ICBF, regulada por la Guía de etiquetado y clasificación de la Información.

Control SGSI-5.13	
Etiquetado de la información	**CONTROLES RELACIONADOS**
	SGSI-5.12 Clasificación de la información
Anexos:	Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G11.GTI Guía para la Clasificación y Etiquetado de la Información.

Propósito:

La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información, la Dirección Administrativa a través del grupo de Gestión Documental y con el apoyo de la Oficina Asesora Jurídica, dictarán los lineamientos para desarrollar e implementar los procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por ICBF.

Lineamientos Generales:

- ✓ Los colaboradores deberán aplicar la Guía de etiquetado y clasificación de la Información.
- ✓ Las series y subseries de las Tablas de Retención Documental (TRD) deberán contener en su estructura el tipo de clasificación.
- ✓ Cada Propietario de la Información velará por el cumplimiento establecido en la Guía de etiquetado y clasificación de la Información.
- ✓ La Dirección Administrativa a través del grupo de Gestión Documental, y la Dirección de Información y Tecnología deberán establecer controles para mantener protegida la información física y electrónica durante su ciclo de vida.

Control SGSI-7.10	
Medios de almacenamiento	**CONTROLES RELACIONADOS**
	N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P9.GTI Procedimiento para el manejo de medios removibles. - IT1.P9.GTI Instructivo para cifrado de información. - IT5.P2.GTI Instructivo para Gestión de Solicitudes de Copias de Seguridad. -IT3.P2.GTI Instructivo para Gestionar Solicitudes de Borrado de Información de los Dispositivos de Cómputo -IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento

Propósito:

Dictar lineamientos para la implementación de procedimientos de gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por el ICBF, disponer de forma segura de los medios cuando estos se requieran, aplicando buenas prácticas ambientales y de seguridad de la información y, de igual manera para la protección contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, establecerá los siguientes lineamientos:

- ✓ Seguir los lineamientos de gestión de acuerdo con el Procedimiento de Solicitud de Excepciones para el Uso de Medios Removibles.
- ✓ En ninguna circunstancia se dejará desatendido los medios de almacenamiento copias de seguridad de los sistemas de información.
- ✓ Los colaboradores que hagan uso de token virtual para el desempeño de sus funciones u obligaciones deberán velar por el óptimo manejo de este.
- ✓ Deberá proveer los métodos alternativos de cifrado con los que se cuente actualmente.
- ✓ Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red del ICBF.
- ✓ Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.
- ✓ Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan información reservada o clasificada del ICBF.
- ✓ Para la disposición final de residuos de aparatos electrónicos, se debe dar cumplimiento a lo establecido en el P57.SA Procedimiento Manejo de Residuos Especiales. En caso de residuos de aparatos eléctricos y electrónicos como discos duros, se debe realizar la eliminación de la información a través de borrado seguro, antes de aplicar el Procedimiento de manejo de residuos especiales. Cuando un Disco Duro por su obsolescencia o daños irreparables se dañe y sea imposible realizar el borrado seguro se debe garantizar que la información no sea recuperable.
- ✓ El uso de medios removibles solamente será justificado y autorizado a los colaboradores del ICBF con el aval del supervisor del contrato o jefe inmediato, exceptuando situaciones donde la Entidad no esté en capacidad de proveer medios de almacenamiento en nube como OneDrive o SharePoint o cuando sus actividades o funciones sean desempeñadas en zonas rurales dispersas, donde la Entidad no tiene los medios para proveer acceso a las herramientas tecnológicas antes mencionadas o cuando sea necesario para cumplir con los objetivos en el relacionamiento con usuarios externos. Por lo anterior se requiere que en el momento que se habilite un puerto, el dueño de proceso identifique y trate el riesgo de seguridad de la información relacionado con fuga y pérdida de información e infección por Malware.

- ✓ Cuando se requiera transferir un medio de almacenamiento de información del ICBF a otras entidades se deberán establecer un acuerdo entre las partes. Dichos acuerdos deberán dirigirse a la transferencia segura de información de interés entre el ICBF y las partes.
- ✓ Cuando se requiera transferir un medio de almacenamiento se deberá tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y la entrega.
- ✓ Los colaboradores y terceras partes que interactúen en procesos de intercambio de información al exterior del ICBF deberán cumplir los lineamientos, recomendaciones o estrategias establecidas para este propósito.
  El transporte para los medios de almacenamiento deberá contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.
- ✓ Los equipos que se regresen al almacén para asignarse a otro colaborador o para dar de baja, se les deberá seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo, en caso de no poder realizar el borrado de información validar el Procedimiento manejo de residuos especiales.
- ✓ Se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los equipos que contengan medios de almacenamiento y que serán reutilizados o eliminados, con el fin de controlar que la información del ICBF contenida en estos medios no se pueda recuperar. Esta solicitud deberá ser mediante solicitud a la mesa de servicio, con aprobación del jefe inmediato o supervisor de contrato.
  - Es requisito realizar el respaldo o copia de la información contenida en el equipo, previa ejecución del borrado de información.

8. CONTROL DE ACCESO

Control SGSI-5.15	
Control de acceso	**CONTROLES RELACIONADOS** SGSI-5.2 Roles y responsabilidades en la seguridad de la información. SGSI-5.12 Clasificación de la Información. SGSI-5.13 Etiquetado de la Información. SGSI-5.16 Gestión de identidades. SGSI-5.18 Derechos de acceso. SGSI-8.2 Derechos de acceso privilegiado. SGSI-8.3 Restricción de acceso a la información. SGSI-7.5 Protección contra amenazas físicas y ambientales. SGSI-5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. -A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - G9.GTI Guía para el Control de Accesos a Centros de Cableado y Data Center. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional. - Índice de Información Clasificada y Reservada -P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. 23.GTI Procedimiento Gestión de Permisos de Propiedad Sharepoint -IT1.P23.GTI Instructivo Uso Compartido Onedrive y Sharepoint -IT2.P2.GTI Instructivo para Gestión de Solicitudes de Permiso de Firewall -F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información -G28.GTI Guía Permisos y Restricciones Microsoft 365

Propósito:
Definir parámetros para establecer, documentar controles de acceso con base en los requisitos del ICBF, así mismo establecer permisos de acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos define los lineamientos para la política de control de acceso, el acceso a redes y servicios en red teniendo en cuenta lo siguiente:

- ✓ La Subdirección de Recursos Tecnológicos suministrará a los usuarios las credenciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, de esta forma las credenciales de acceso son de uso personal e intransferible.
- ✓ Es responsabilidad de los colaboradores o terceras partes del ICBF el manejo que se les dé a las credenciales de acceso asignadas.
- ✓ Los colaboradores o terceras partes que realicen actividades administrativas sobre la plataforma tecnológica del ICBF, las deberán realizar en las instalaciones del ICBF y no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del supervisor del contrato.
- ✓ La conexión remota a la red de área local del ICBF deberá establecerse a través de una conexión VPN ZTNA suministrada por el ICBF, la cual deberá ser aprobada, registrada y auditada por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar revisiones e inactivaciones de las conexiones VPN ZTNA cada treinta (30) días o de acuerdo con las solicitudes de desactivación generadas en la mesa de servicio.
- ✓ Las conexiones remotas deberán utilizar los métodos establecidos de autenticación para el control de acceso de los usuarios.
- ✓ Deberá implantar controles adicionales para el acceso por redes inalámbricas.
- ✓ Deberá establecer una adecuada segregación de redes, separando los entornos de red de usuarios de los entornos de red de servicios.
- ✓ Deberá establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos, los recursos y servicios del ICBF.
- ✓ El control de acceso a los datos, información y servicios se deberá basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.
- ✓ Deberá crear, modificar y deshabilitar las cuentas de acceso o recursos del ICBF de acuerdo con el procedimiento establecido.
- ✓ Deberá verificar periódicamente los controles de acceso para los usuarios del ICBF y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- ✓ Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del ICBF, deberán solicitar la creación de cuenta de usuario a través del formato solicitud de servicios de tecnología.
- ✓ Los equipos personales de los colaboradores que se conecten a las redes de datos del ICBF deberán cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- ✓ No se podrá utilizar ningún tipo de utilitario para conexión remota a la red interna del ICBF, únicamente se deberá utilizar el designado por la Dirección de Información y Tecnología del ICBF.
- ✓ La Subdirección de Recursos Tecnológicos en conjunto con la Subdirección de Sistemas Integrados de Información, establecerá las configuraciones de las políticas en los sistemas de información y comunicaciones para el control de acceso a los activos de información.
- ✓ Solo los usuarios autorizados por la Dirección de Información y Tecnología podrán instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, restauración de copias de seguridad cuando se requiera y eliminar software malicioso.
- ✓ La conexión remota VPN ZTNA a la red del ICBF, debe ser justificada y solicitada por los Directores o Jefes de Oficina a través de la Mesa Informática de Soluciones y es la Dirección de Información y Tecnología en cabeza de la Subdirección de Recursos Tecnológicos quién validará la solicitud.

Control SGSI-5.16	
Gestión de la identidad	**CONTROLES RELACIONADOS**
	SGSI-5.18 Derechos de acceso.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto

	Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P2. GTI Procedimiento Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. -G28.GTI Guía Permisos y Restricciones Microsoft 365 -Depuración Directorio Activo -F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información -G28.GTI Guía Permisos y Restricciones Microsoft 365

Propósito:
Dictar lineamientos para el registro y cancelación de usuarios en el ICBF.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para el registro y cancelación de usuarios teniendo en cuenta lo siguiente:

- ✓ Deberá definir un procedimiento para el registro y la cancelación de usuarios en el ICBF, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
- ✓ Deberá definir un estándar para la creación de las cuentas de usuario institucionales.
- ✓ Deberá deshabilitar las credenciales de acceso a los colaboradores que no tengan ningún vínculo laboral o contractual con el ICBF.

Control SGSI-5.18	
Derechos de acceso	**CONTROLES RELACIONADOS**
	SGSI-5.9 Inventario de información y otros activos asociados SGSI-5.15 Control de acceso SGSI-5.3 Segregación de funciones SGSI-5.17 Información de autenticación SGSI-6.2 Términos y condiciones del empleo SGSI-6.4 Proceso disciplinario SGSI-6.6 Acuerdos de confidencialidad y no divulgación SGSI-5.20 Abordar la seguridad de la información en los acuerdos con los proveedores
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. - G27.GTI Guía Políticas Navegación. -G28.GTI Guía Permisos y Restricciones Microsoft 365 -SGSI-5.16 Gestión de identidades.

Propósito:
Dictar lineamientos para que se realice la revisión de los derechos de acceso de los usuarios a intervalos regulares. De igual manera, para el retiro o cambios de los derechos de acceso de todos los colaboradores y terceras partes a la información y a las instalaciones de procesamiento de información.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establecerá los lineamientos para el proceso de suministro de acceso formal o revocar los derechos de acceso de usuarios teniendo en cuenta lo siguiente:

- ✓ El acceso a la información del ICBF es otorgado sólo a usuarios autorizados, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios asignados.
- ✓ Definir los controles de seguridad a los tipos de usuarios dependiendo el acceso a la información que este requiera:
  - ✓ **Usuario Proveedor o Tercero:** son aquellos usuarios externos al ICBF que prestan un servicio bajo un contrato y requieren acceso a la plataforma tecnológica de la entidad.
  - ✓ **Usuario Especial:** son usuarios externos que requieren acceso a la plataforma de la entidad para una actividad específica, como los entes de control, estos usuarios deberán ser solicitados por la Oficina de Control Interno del ICBF con los respectivos permisos siguiendo el procedimiento estipulado.
  - ✓ **Usuario Administrador:** son los usuarios funcionarios, contratistas o terceros que por sus funciones u obligaciones requieren permisos de administración para el desarrollo de sus actividades en la plataforma de la entidad.
  - ✓ **Usuario Institucional:** son los usuarios estándar como son: contratistas, pasantes y funcionarios de planta entre otros que no se encuentran catalogados en ninguno de los anteriores grupos.
- ✓ No se deberá configurar el acceso a los recursos tecnológicos a usuarios que no hayan formalizado el proceso de ingreso al ICBF.
- ✓ Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica del ICBF deberá autenticarse.
- ✓ Los usuarios deberán cumplir con los lineamientos para la creación y uso de contraseñas.
- ✓ El uso de credenciales de usuarios administradores de sistemas operativos, consolas de administración y bases de datos tales como: “root”, “adm”, “admin”, “administrador”, “SQLAdmin”, “administrator” y “system”, entre otros, deberán ser administrados por parte de los especialistas del outsourcing de infraestructura de TI contratado por el ICBF.
- ✓ Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso y mantener de forma confidencial las contraseñas con la finalidad de preservar el no repudio.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá generar reportes de uso de los sistemas de información con el fin de identificar la periodicidad de uso de cada uno de los usuarios.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá revisar los derechos de acceso de los usuarios administradores por lo menos dos veces al año.
- ✓ El retiro de los privilegios se deberá hacer inmediatamente se realice la solicitud de desactivación.
- ✓ Es responsabilidad de la Dirección de Gestión Humana o a quien esta delegue, de los supervisores de los contratos o del G58 de la Dependencia o Regional dar a conocer a la Dirección de información y Tecnología el retiro, suspensión o cualquier novedad administrativa que se presente con los usuarios del ICBF, esta novedad se deberá reportar a través de la mesa de servicio.

Control SGSI-8.2	
Derechos de acceso privilegiado	**CONTROLES RELACIONADOS**
	SGSI-5.18-Derechos de acceso
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P2. GTI Procedimiento Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato de Solicitud Servicios de Tecnología. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. -G27.GTI Guía Políticas Navegación. -F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información
Propósito: Dictar lineamientos para restringir y controlar la asignación y uso de derechos de acceso privilegiado.	

Lineamientos Generales:

La Dirección de Información y Tecnología a través de sus subdirecciones desarrollarán los lineamientos para restringir y controlar la asignación y uso de derechos de acceso privilegiado teniendo en cuenta lo siguiente:

- ✓ Deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información, únicamente a aquellos colaboradores que cumplan dichas funciones.
- ✓ Deberá otorgar cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información, diferentes a los nativos y deberán ser cuentas únicas asociadas al usuario de dominio del administrador.
- ✓ Deberá restringir las conexiones remotas a los recursos de la plataforma tecnológica y se deberá permitir únicamente el acceso a los colaboradores autorizados.
- ✓ Deberán deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
- ✓ Deberá mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos del ICBF.
- ✓ Cada dependencia dentro del ICBF deberá asignar un responsable para administrar los privilegios en las carpetas asignadas en el servicio de almacenamiento con el que dispone el ICBF, este deberá ser reportado a la Subdirección de Recursos Tecnológicos.
- ✓ No se permite que los usuarios tengan carpetas compartidas en sus equipos, para ello debe hacer uso de los recursos que tiene el ICBF.
- ✓ Los administradores de carpeta serán los responsables de los accesos y asignación de permisos (lectura, escritura, modificación y eliminación) de las carpetas y subcarpetas asignadas, los cuales deberán tener sus respectivos soportes.
- ✓ La Subdirección de Recursos Tecnológicos deberá:
    - Generar registros de auditoría que contengan eventos relacionados de seguridad, teniendo en cuenta criterios tales como nombre de usuario, fechas y hora de evento, tipo de modificación sobre el objeto. Se deberá realizar un respaldo de esta información facilitando la revisión y el análisis de estos.
    - Establecer controles que permitan validar que solo cuenten con los permisos de acceso los usuarios autorizados.
    - Realizar respaldo a toda la información alojada dentro de los repositorios y herramientas oficiales de la Entidad de acuerdo con la ley 594 de 2000 Ley General de Archivo y/o cualquiera que la derogue o modifique, adicionalmente se tendrá en cuenta el programa de gestión documental del ICBF.
    - Realizar monitoreo permanente al servicio de almacenamiento esto con el fin de evitar fallas y en caso de existir reportarlas de manera oportuna.
    - Contar con herramientas que le permitan detectar fallas en la solución de almacenamiento y tomar las medidas correctivas necesarias.
    - Establecer cuotas de almacenamiento para cada recurso compartido (OneDrive, SharePoint entre otras), adicional a esto se deberá definir umbrales que permitan notificar al administrador del servicio de almacenamiento y al administrador de cada recurso que el espacio asignado ya está llegando a su límite. Cada cuota está sujeta a las necesidades de cada área y a la proyección de crecimiento de cada una de ellas.
    - Reportes mensuales en cada una de sus soluciones, evidenciando la cantidad de espacio utilizado, el que queda disponible y determinar acciones que eviten posibles fallas en la solución de almacenamiento del ICBF.
    - Restringir excepto en las dependencias que por el desarrollo de sus funciones sean necesarios almacenamiento de tipo de archivos como:
        - Audio (.avi, .mpeg, .mp3, .mid o .midi, .wav, .wma, .cda, .ogg, .ogm, .aac, .ac3, flac, .mp4, .aym)
        - Video (.avi,.mpeg, .mov, .wmv, .rm, .flv)
        - Archivos ejecutables (.exe, .bat, .com, bin)
        - Archivos de páginas web (html, xml, jsp,asp)
        - Archivos de sistema (.acm,.dll,.ocx,.sys,.vxd)
    - Generar reportes mensuales en cada una de sus soluciones, evidenciando que tipos de archivos se encuentran alojados, archivos por propietarios, archivos duplicados, archivos grandes, archivos no usados recientemente, para determinar acciones que eviten posibles fallas en la solución de almacenamiento del ICBF.

La Subdirección de Recursos Tecnológicos con apoyo de los administradores de los recursos, deberán establecer una estrategia en la que la información compartida que maneja un área con otra sea almacenada independiente de la que se maneja internamente dentro del área.

Control SGSI-5.17	
Información de autenticación	**CONTROLES RELACIONADOS**
	SGSI-6.2 Términos y condiciones del empleo. SGSI-5.18 Derechos de acceso.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G28.GTI Guía Permisos y Restricciones Microsoft 365 - Doble factor de autenticación.

Propósito:
Dictar lineamientos para definir un proceso de gestión formal para la asignación de información de autenticación, concienciando y controlando que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de contraseñas.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para la asignación de información de autenticación secreta teniendo en cuenta lo siguiente:

- ✓ La contraseña para la autenticación se deberá suministrar a los usuarios de manera segura, y el sistema deberá solicitar el cambio inmediato de la misma al ingresar.
- ✓ Se deberán establecer procedimientos para verificar la identidad de un usuario antes de reemplazar la información para la autenticación o proporcionar una nueva o temporal.
- ✓ La información para la autenticación por defecto del fabricante se deberá modificar después de la instalación de los dispositivos o del software.
- ✓ Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos del ICBF.
- ✓ El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o jefe/supervisor inmediato.
- ✓ Las contraseñas:
  - Deberán poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
  - Deberá cumplir con las siguientes recomendaciones como mínimo:
    - Tener como mínimo diez (12) caracteres alfanuméricos sin repetición.
    - No deberá contener el nombre de usuario, el nombre real o la sigla ICBF.
    - Los números que contengan no deberán ser consecutivos No se deberán usar contraseñas con los nombres de los hijos, esposo, mascotas, fechas de aniversarios, cumpleaños, años, etc.
    - Deberán ser diferentes de otras contraseñas anteriores proporcionadas, es decir las ultimas veinticuatro (24) suministradas al dominio no se deberán repetir.
    - No se deberán usar las mismas contraseñas de la autenticación para uso personal.
    - Deberán estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (), ¡, !, ¿, ?, <>…” y espacios en cualquier orden.
  - Deberán cambiarse obligatoriamente cada 30 días o cuando lo establezca la Dirección de Información y Tecnología.
  - Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado para volver a intentar, o solicitar el desbloqueo a través de la mesa de servicio.
  - Deberá cambiarse si se ha detectado anomalía o incidencia en la cuenta del usuario.
  - Deberá no ser visible en la pantalla, al momento de ser ingresada.
  - No deberán ser reveladas a ninguna persona.

- No se deberá registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos.

Control SGSI-8.3	
Restricción de acceso a la información	**CONTROLES RELACIONADOS** SGSI-5.15 Control de acceso SGSI-5.17 Información de autenticación SGSI-8.5 Autenticación segura
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología - F1.P2.GTI Formato solicitud de servicios de tecnología - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información. -G27.GTI Guía Políticas Navegación.

Propósito:
Dictar lineamientos para el acceso a la información y a la funcionalidad de las aplicaciones.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de las Subdirecciones deberán definir los lineamientos para la restricción de acceso a la información teniendo en cuenta lo siguiente:

- ✓ Deberá implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- ✓ Deberá establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, deberá implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- ✓ Deberá proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- ✓ Los desarrolladores deberán asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- ✓ Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- ✓ Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas.
- ✓ Los desarrolladores deberán asegurar que se inhabilitan las cuentas de acuerdo con lo que establece el control SGSI-5.17, estipulado en este manual.
- ✓ Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización.
- ✓ El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deberán estar restringidos y estrictamente controlados.
- ✓ Las sesiones inactivas deberán cerrarse después de un período de inactividad definido y se deberán usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.
- ✓ Deberá integrar las aplicaciones con el Directorio Activo, en el caso de usuarios externos estos deberán autenticarse mediante mecanismos de identificación única y en los procesos de criticidad de información se establecerá con el área funcional u operativa un mecanismo de autenticación.

Control SGSI-8.5	
Autenticación segura	**CONTROLES RELACIONADOS** SGSI-5.15 Control de acceso SGSI-5.16 Gestión de identidades

	SGSI-5.17 Información de autenticación
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato de Solicitud Servicios de Tecnología - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información.

Propósito:
Definir lineamientos para un proceso de ingreso seguro a los sistemas y las aplicaciones del ICBF.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de las Subdirecciones deberán definir los lineamientos para un proceso de ingreso seguro para los sistemas y las aplicaciones del ICBF teniendo en cuenta lo siguiente:

- ✓ Después de tres (3) minutos de inactividad del sistema, se considerará tiempo muerto y se deberá bloquear la sesión sin cerrar las sesiones de aplicación o de red. Para el caso de aplicaciones como el SIM y CUENTAME el sistema se bloquea después de veinte (20) minutos de inactividad. Para el caso de aplicaciones que de acuerdo con su finalidad y funcionalidad requieren el procesamiento de grandes volúmenes de información (Sistemas batch) el tiempo de sesión estará activa hasta que la información procesada finalice.
- ✓ El acceso a los sistemas o aplicaciones deberá estar protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:
  - No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
  - No suministrar mensajes de ayuda, durante el proceso de autenticación.
  - Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
  - Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos hasta un máximo de tres (3) intentos (solo aplica para los sistemas de información que se autentican a través del directorio activo).
  - No mostrar las contraseñas digitadas con anterioridad.
  - No transmitir la contraseña en texto claro.
- ✓ Se debe velar porque los accesos a los sistemas de información o un recurso informático registren el evento.

Control SGSI-8.18	
Uso de programas de utilidad privilegiados	**CONTROLES RELACIONADOS** SGSI-8.2 Derechos de acceso privilegiado.
Anexos:	Desde el Directorio activo se asignan privilegios de administrador a las personas que pueden instalar y hacer uso de programas utilitarios. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.

Propósito:
Definir lineamientos para restringir y controlar el uso de programas utilitarios privilegiados que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para el uso de programas utilitarios privilegiados teniendo en cuenta lo siguiente:

- ✓ Deberá establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.
- ✓ Deberá monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.

✓ Deberá generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información. ✓ Deberá retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información.

Control SGSI-8.4	
Acceso a código fuente	**CONTROLES RELACIONADOS**
	SGSI-8.32 Gestión de cambios
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información. -F1.P6.GTI Formato de Solicitud de Requerimiento -F14.P6.GTI Formato Documento Arquitectura de Software v2 -F15.P6.GTI Formato Especificación de Requerimientos de Software ERS -F16.P6.GTI Formato Pruebas Unitarias -F17.P6.GTI Formato Historia Usuario -F13.P6.GTI Formato Lista de Chequeo Código Fuente -F18.P6.GTI Formato Manual de Instalación y Configuración de Software -F19.P6.GTI Formato Pruebas Integrales -F6.P6.GTI Formato Escenario de Prueba -F7.P6.GTI Formato Modelo y Diccionario de Datos -F11.P6.GTI Formato Acta Verificación de Despliegue en Producción -F12.P6.GTI Formato Ficha Técnica - G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información -G21.GTI Guía de Arquitectura de Referencia de Interoperabilidad -F13.P6.GTI Formato Lista de Chequeo Código Fuente
Propósito: Definir lineamientos con respecto al acceso a los códigos fuentes de los sistemas de información del ICBF. **Lineamientos Generales:** La Dirección de Información y Tecnología a través de las subdirecciones desarrollarán los lineamientos para el control de acceso a códigos fuente teniendo en cuenta lo siguiente: ✓ El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladores y de soporte serán autorizados por la Subdirección de Sistemas Integrados de Información. ✓ Los repositorios fuentes de los sistemas de información no deberán estar contenidos en el ambiente de producción, sino en la herramienta de versionamiento definida por la Subdirección de Sistemas de Información. .	

9. CRIPTOGRAFÍA

Control SGSI-8.24	
Uso de la criptografía	**CONTROLES RELACIONADOS**
	SGSI-5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información.

	- G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información - G1.P17.GF Guía de políticas y seguridad para el manejo y control de recursos financieros administrados ICBF. - F1.P2.GTI Formato solicitud de servicios de tecnología. - B69IT1.P9.GTI Instructivo para cifrado de información.

Propósito:
Dictar lineamientos para el uso adecuado de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información del ICBF clasificada o reservada, en sistemas de información, correo electrónico y mecanismos de transferencia de información interna o externa.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para los controles criptográficos teniendo en cuenta lo siguiente:

- ✓ Se deberán utilizar controles criptográficos en los siguientes casos:
  - Para la protección de claves de acceso a sistemas, datos y servicios.
  - Para la información digital o electrónica reservada y clasificada.
- ✓ Deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada cuente con mecanismos de cifrado de datos.
- ✓ Deberá desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos.
- ✓ Deberá utilizar controles criptográficos para la transmisión de información clasificada, fuera del ámbito del ICBF.
- ✓ La Subdirección de Sistemas Integrados de Información en cabeza de los desarrolladores deberán asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Información y Tecnología, plasmados en la G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información.
- ✓ Realizar un inventario y revisión periódica de llaves criptográficas y certificados digitales actualizado (uso, protección y tiempo de vida).
- ✓ La Dirección de Información y Tecnología brindará de acuerdo con los requerimientos del ICBF, herramientas que permitan el cifrado de la información para proteger la confidencialidad, integridad y disponibilidad de la información clasificada o reservada, en sistemas de información, correo electrónico y mecanismos de transferencia de información interna o externa.

10. SEGURIDAD FÍSICA Y DEL ENTORNO

Control SGSI-7.1	
Perímetro de seguridad física	**CONTROLES RELACIONADOS** SGSI-7.2 Entrada física
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center - F1.G9.GTI Formato bitácora de ingreso

Propósito:
Dictar lineamientos para el acceso físico no autorizado, pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del ICBF, daño e interferencia para la información que se encuentren dentro o fuera de las instalaciones de procesamiento de información.

Lineamientos Generales:
La Dirección Administrativa y la Dirección de Información y Tecnología estableces los lineamientos para los controles de perímetro de seguridad física teniendo en cuenta lo siguiente:

- ✓ El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento sensible o crítico deberán estar protegidos de accesos no permitidos.
- ✓ Las áreas seguras deben estar identificadas y debidamente registradas mediante el instrumento correspondiente.
- ✓ Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- ✓ Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
- ✓ El perímetro de seguridad debe contar con vigilancia mediante CCTV y debe ser monitoreado por el personal de vigilancia del ICBF.

Control SGSI-7.2 – 7.3	
Controles de acceso físicos **Seguridad de oficinas, recintos e instalaciones**	**CONTROLES RELACIONADOS** SGSI-5.18 Derechos de acceso
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center. - F1.G9.GTI Formato bitácora de ingreso. - Contrato de Servicio de Vigilancia Vigente. - P50.SA Procedimiento Seguridad y Vigilancia Privada

Propósito:

Dictar lineamientos para la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas seguras (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Lineamientos Generales:

- ✓ La Dirección Administrativa deberá señalizar las áreas de acceso restringido.
- ✓ La Dirección Administrativa deberá establecer un sistema de control de acceso a las instalaciones del ICBF, así como a las áreas demarcadas con acceso restringido dentro y fuera de las instalaciones principales de la Entidad.
- ✓ Las áreas de acceso restringido deben estar protegidas por los controles adecuados al ingreso a ellas.
- ✓ La Dirección Administrativa en la Sede de la Dirección General y la Coordinación Administrativa en las regionales deberán controlar que los centros de cableado permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos será responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado a nivel nacional.

- ✓ La Dirección Administrativa deberá mantener en buen estado la infraestructura física de los centros de cableado a nivel nacional y centro de datos de la Sede de la Dirección general, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos en la Sede de la Dirección General y la Coordinación de Planeación y Sistemas en las regionales deberán realizar una revisión periódica del estado de los centros de cableado e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red a la Subdirección de Recursos Tecnológicos, y daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) a la Coordinación Administrativa en las regionales, y a la Dirección Administrativa en la Sede de la Dirección General.
- ✓ La Dirección Administrativa en la Sede de la Dirección General y la Coordinación Administrativa en las regionales, son los responsables del cumplimiento del protocolo de aseo en los centros de cableado y centro de datos, este último contará con el acompañamiento de la Dirección de Información y Tecnología en la Sede de la Dirección General y la Coordinación de Planeación y Sistemas en las sedes Regionales.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos en la Sede de la Dirección General y la Coordinación de Planeación y Sistemas en las regionales serán responsables de mantener organizado e identificado el cableado en los racks de los centros cableado y centro de datos.
- ✓ Se deberá establecer un plan de mantenimiento para los centros de cableado por parte de la Dirección Administrativa y la Dirección de Información y Tecnología, de tal manera que se corrijan fallas y/o establecer mejoras en los mismos.
- ✓ La Dirección Administrativa en la Sede de la Dirección General y la Coordinación Administrativa en las regionales, serán responsables de la identificación y señalización necesaria de los centros de cableado y centro de datos.
- ✓ La Dirección Administrativa deberá implementar y administrar los circuitos cerrados de televisión (CCTV) para los centros de cableado y centro de datos.
- ✓ La Dirección Administrativa y la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos en la Sede de la Dirección General la Coordinación de Planeación y Sistemas y la Coordinación Administrativa en las regionales, deberán mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado.
- ✓ La Dirección Administrativa deberá controlar y monitorear a través de CCTV el ingreso a las áreas seguras.
- ✓ La Dirección Administrativa en acompañamiento de la Dirección Financiera deberán establecer circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros (Preparador y Pagador).
- ✓ Todos los colaboradores y visitantes que se encuentren en las instalaciones físicas del ICBF deben estar debidamente identificados, con un documento, el cual deberá portarse en un lugar visible.
- ✓ Los visitantes del ICBF siempre deberán permanecer acompañados por un colaborador debidamente identificado.
- ✓ El personal de empresas contratistas que desempeñen funciones de forma permanente en las instalaciones del ICBF, deberá estar identificado con carné, o chalecos o algún distintivo que lo identifique como contratista de un operador. También deberá portar el carné de la ARL.
- ✓ El ICBF a través de la Dirección Administrativa realizará la contratación de un proveedor quien tendrá a cargo las bitácoras de ingreso/salida, sistemas de control de acceso implementados, así como los sistemas de video seguridad (Circuito cerrado de televisión CCTV), para realizar el monitoreo de seguridad en las instalaciones.

Control SGSI-7.5	
Protección contra amenazas externas y ambientales	**CONTROLES RELACIONADOS** SGSI-5.7 Inteligencia de amenazas

Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. -PL2.SA Plan de Gestión Ambiental -PT3.SA Protocolo Manejo y Atención de Emergencias Ambientales relacionadas a Derrames - PL36.SA Plan integrado de Conservación - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P29.SA Procedimiento para la Gestión Ambiental. - P22.SA Procedimiento Aspectos e Impactos Ambientales y Otros Requisitos. - PT3.SA Protocolo Manejo y Atención de Emergencias Ambientales Relacionadas con Derrames. - F4.PL36.SA Formato Monitoreo y Control de Condiciones Ambientales. - P9.GTH Procedimiento para la elaboración de planes de emergencias y contingencias.

Propósito:
Dictar lineamientos para diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Lineamiento General:
La Dirección Administrativa con el apoyo de la Dirección de Información y Tecnología y la Dirección de Gestión Humana establecerán los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad de la operación.

La Dirección de Información y Tecnología con el apoyo de la Subdirección de Recursos Tecnológicos deberá monitorear las variables de temperatura y humedad de los centros de cableado o data center y, cuando estos se vean afectados por daño o falta de mantenimiento, se deberá reportar a la Dirección Administrativa dichas eventualidades para que estos equipos sean cambiados o se haga el mantenimiento necesario para su debido funcionamiento.

Control SGSI-7.6	
Trabajo en áreas seguras	**CONTROLES RELACIONADOS**
	SGSI-7.1 Perímetro de seguridad física
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P50.SA Procedimiento Seguridad y Vigilancia Privada. - F2.G10.GTI Áreas Seguras a Nivel Nacional

Propósito:
Dictar lineamientos para trabajar en áreas seguras.

Lineamientos Generales:
La Dirección Administrativa o a quien delegue deberá:

- ✓ Realizar revisiones periódicas de las oficinas que estén vacías asegurando que estén cerradas con llave.
- ✓ Restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte del área encargada.
- ✓ El trabajo en áreas seguras debe estar monitoreado por CCTV, teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.

Control SGSI-7.8	
Ubicación y protección del equipo	**CONTROLES RELACIONADOS**

	N/A
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - IT1.P9.GTI Instructivo para cifrado de información -F3.G9.GTI Formato Monitoreo de Temperatura -P24.GTI Procedimiento para Entrega, Devolución y Uso de Dispositivos - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center - F1.G9.GTI Formato bitácora de ingreso -Señalética

Propósito:
Dictar lineamientos para la protección de la información en los equipos.

Lineamientos Generales:
La Dirección Administrativa establece los lineamientos para los controles de ubicación y protección de los equipos teniendo en cuenta lo siguiente:

- ✓ Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- ✓ Los equipos de cómputo portátiles se deberán proteger mediante mecanismos que no permitan su pérdida.

Control SGSI-7.11	
Instalaciones de suministro	**CONTROLES RELACIONADOS**
	N/A
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - PT1.SA Protocolo Cargue Combustible Plantas Eléctricas

Propósito:
Dictar lineamientos para la protección de los equipos cómputo y procesamiento contra fallas de energía u otras interrupciones causadas por fallas en los servicios de suministro.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deberán conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deberán conectarse a la red eléctrica no regulada.
- ✓ La Dirección de Información y Tecnología con el acompañamiento de la Dirección Administrativa deberán implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento.
- ✓ La Dirección Administrativa deberá suministrar plantas eléctricas a las sedes del ICBF y la Dirección de Información y Tecnología las UPS, y garantizar su mantenimiento preventivo y correctivo.

Control SGSI-7.12	
Seguridad en el Cableado	**CONTROLES RELACIONADOS**
	N/A

Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. -F3.G9.GTI Formato Monitoreo de Temperatura -F3.G10.GTI Formato Diagnóstico de las Condiciones Físicas de las Regionales

Propósito:
Dictar lineamientos para la protección de cableado de energía eléctrica y de telecomunicaciones contra interceptación, interferencia o daño.

Lineamientos Generales:
La Dirección de Información y Tecnología y la Dirección Administrativa definirán los controles de seguridad en el cableado teniendo en cuenta lo siguiente:

- ✓ El cableado que transporta datos y de suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.
- ✓ Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia.
- ✓ Deberán tener en cuenta las consideraciones técnicas de las normas vigentes y las buenas prácticas.
- ✓ Los cuartos de cableado solo podrán tener los elementos activos para su funcionamiento y no utilizarse como almacén para guardar cajas, mesas u otros equipos que no estén en uso.

Control SGSI-7.13	
Mantenimiento de equipos	**CONTROLES RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G12.GTI Guía para el Mantenimiento Preventivo de Equipos - F1.G12.GTI Formato Acta Mantenimiento Preventivo Equipos Portátiles y de Escritorio. - Anexo Estándar de Nombramiento de Estaciones - F2.G12.GTI Formato relación mantenimientos preventivos impresoras y scanner - F3.G12.GTI Formato acta mantenimientos preventivos de switches - F4.G12.GTI Formato lista de chequeo mantenimiento de Red LAN - F5.G12.GTI Formato Acta Mantenimientos Preventivos de Telefonía IP

Propósito:
Dictar lineamientos para mantener correctamente los equipos para proteger su disponibilidad e integridad.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para el mantenimiento de equipos teniendo en cuenta lo siguiente:

- ✓ Deberá definir mecanismos de soporte y mantenimiento a los equipos.
- ✓ Las actividades de mantenimiento tanto preventivo como correctivo deberán registrarse.
- ✓ Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos.
- ✓ Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.
- ✓ Los equipos que requieran salir de las instalaciones del ICBF para reparación o mantenimiento deberán estar debidamente autorizados. Cuando un dispositivo vaya a ser reasignado o retirado de servicio, deberá garantizarse la eliminación de toda información siguiendo el Instructivo para gestionar solicitudes de borrado de información de

los dispositivos de cómputo teniendo en cuenta que previo a esta actividad deberá realizar copia de seguridad de esta.

Control SGSI-7.9	
Seguridad de los equipos fuera de las instalaciones	**CONTROLES RELACIONADOS** SGSI-7.8 Ubicación y protección del equipo
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - Resolución 4594 del 15 de junio de 2017 "Por la cual se modifica la Resolución 7600 de 2016" - Resolución 7600 de 2016 "Por la cual se adopta la modalidad de Teletrabajo Suplementario a nivel nacional en el Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras y se hace una delegación" - IT1.P2.GTI Instructivo para Gestión de Solicitudes de VPN.
Propósito: Dictar lineamientos para no retirar de su sitio sin autorización previa los equipos, información o software. **Lineamientos Generales:** La Dirección Administrativa o su delegado establece los lineamientos para los controles de retiro de activos teniendo en cuenta lo siguiente: ✓ Se deberá registrar cuando los equipos de cómputo ingresan y se retiran de las instalaciones del ICBF. ✓ Se deberá llevar un control en el almacén de los equipos cuando se asignan y cuando se hace su devolución.	

Control SGSI-7.14	
Eliminación segura o reutilización de equipos	**CONTROLES RELACIONADOS** N/A
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - Anexo 4 Manual de Políticas de Seguridad de la Información A4.MS.DE. - G2.SA Guía Gestión de Bienes - F2.G2.SA Formato Devolución de Bienes al Almacén. - F3.G2.SA Formato Traslado Elementos Devolutivos - IT3.P2.GTI Instructivo para Gestionar Solicitudes de Borrado de Información de los Dispositivos de Cómputo -IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento - G12.GTI Guía para el Mantenimiento Preventivo de Equipos - F1.G12.GTI Formato acta mantenimiento preventivo equipos portátiles y de escritorio - F2.G12.GTI Formato relación mantenimientos preventivos impresoras y scanner - F3.G12.GTI Formato acta mantenimientos preventivos de switches - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología - F3.P2.GTI Formato diagnóstico de hardware.
Propósito:	

Dictar lineamientos para verificar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura antes de la disposición o reúso del equipo.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece el siguiente lineamiento:

- ✓ Todos los equipos de cómputo que vayan a ser reasignados o dados de baja, se les deberá realizar una copia de respaldo y seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo.

Control SGSI-7.7	
Escritorio despejado y pantalla despejada	**CONTROLES RELACIONADOS**
	N/A
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. -PL6.GTI Plan de Cambio, Cultura, Seguridad y Privacidad de la Información -PL5.GTI Plan de Apropiación de TI

Propósito:
Establecer mecanismos para reducir el riesgo contra pérdida, daño de información y el acceso no autorizado a los equipos del ICBF.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para los equipos desatendidos y escritorio y pantalla limpia teniendo en cuenta lo siguiente:

- ✓ Los colaboradores del ICBF, durante su ausencia no deberán conservar sobre el escritorio información propia del Instituto como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
- ✓ Los colaboradores del ICBF deberán bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el computador.
- ✓ Los colaboradores del ICBF que impriman documentos con clasificación (Clasificada – Reservada), estos deberán ser retirados de la impresora inmediatamente y no se deberán dejar en el escritorio sin custodia.
- ✓ No se deberá reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deberán ser destruidos y no deberán estar como papel reciclable.
- ✓ Los documentos impresos con clasificación (Clasificada – Reservada) o que contenga datos personales no deberán publicarse.
- ✓ Los lugares de trabajo de los colaboradores del ICBF y terceras partes que prestan sus servicios al Instituto y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.
- ✓ Todos los computadores del ICBF deberán tener configurado y en operación un protector de pantalla con tiempo máximo de tres (3) minutos para que se active cuando el equipo no esté en uso.

11. SEGURIDAD DE LAS OPERACIONES

Control SGSI-5.37	
Procedimientos operativos documentados	**CONTROLES SGSI RELACIONADOS**

	SGSI-5.1 Políticas para la Seguridad de la Información. SGSI-8.18 Uso de programas de utilidad con privilegios. SGSI-7.14 Disposición o reutilización segura de equipos. SGSI-8.13 Copias de seguridad de la información. SGSI-5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.
Anexos:	P1.MI. Procedimiento de Elaboración y Control de Documentos F1.P1.MI Formato Solicitud Elaboración Modificación o Eliminación de Documentos F2.P1.MI Formato Caracterización de Procesos F3.P1.MI Formato Plantilla Procedimiento F4.P1.MI Formato Planes Programas Protocolos F5.P1.MI Formato Guía o Manual de Usuario v4 F6.P1.MI Formato Plantilla Instructivo v5 Se encuentran publicados en la página Web e Intranet todos los procedimientos operativos de cada proceso del ICBF, para la Seguridad de la Información, los procedimientos correspondientes al Proceso de Gestión de la Tecnología e Información. -F7.P1.MI Formato Listado Maestro de Documentos

Propósito:
Dictar lineamientos para documentar los procedimientos de operación de la Dirección de Información y Tecnología del ICBF.

Lineamientos Generales:
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para la seguridad de las operaciones, de acuerdo con lo siguiente:

- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, será la encargada de la operación y administración de la plataforma tecnológica que soporta la operación del ICBF.
- ✓ La Dirección de Información y Tecnología velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, asegurando que los cambios efectuados sobre estos se realicen de manera controlada y cuenten con la autorización respectiva.
- ✓ De igual manera, la DIT deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y los sistemas de información del ICBF, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con las necesidades de la Entidad.
- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, deberá realizar y mantener copias de seguridad de la información de la Entidad, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software o de procedimientos operativos al interior de la Entidad.
- ✓ La respectiva copia de seguridad se realizará de acuerdo con el esquema definido previamente en el documento Procedimiento Gestión de Solicitudes de Tecnología de la Entidad, el cual contiene los lineamientos establecidos por la Subdirección de Recursos Tecnológicos.

Control SGSI-8.6	
Gestión de capacidades	**CONTROLES SGSI RELACIONADOS**
	N/A
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - PL1.GTI Plan de Gestión de Capacidad.

Propósito:
Dictar lineamientos para hacer el seguimiento al uso de recursos tecnológicos, para realizar ajustes y proyecciones de requisitos de capacidad futura de los servicios e infraestructura de tecnología del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá documentar una gestión de capacidad la cual le permita:
  - Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
  - Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
  - Documentar los datos de rendimiento y capacidad de la plataforma tecnológica del ICBF.
  - Documentar los acuerdos de niveles de servicio.
  - Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
- ✓ Documentar una gestión de capacidad, las recomendaciones de mejora de la infraestructura de tecnología y periódicamente deberá ser actualizado.
- ✓ Definir los indicadores de rendimiento correspondientes a la gestión de capacidad.
- ✓ Deberá asignar un responsable de la Gestión de Capacidad.

Control SGSI-8.31	
Separación de los entornos de desarrollo, prueba y producción	**CONTROLES SGSI RELACIONADOS** SGSI-8.33 Datos de prueba.
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información - G3.GTI Guía de Estándares de Especificación de Requerimientos

Propósito:

Dictar lineamientos para realizar la separación de los ambientes de desarrollo, pruebas y producción con los que cuenta el ICBF y de esta manera reducir los riesgos de cambios o cambios no autorizados.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de sistemas Integrados de Información deberá solicitar a la Subdirección de Recursos Tecnológicos la separación de ambientes de desarrollo, pruebas y producción, los cuales deberán estar separados de manera física, lógica y a nivel de segmentación de red.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá definir y documentar los lineamientos a seguir para la transferencia entre ambientes.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá utilizar datos que no sean sensibles para el ICBF en los ambientes de prueba, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad o en los casos en los que se requiera bases de datos actualizadas para garantizar que las aplicaciones funcionen correctamente en ambientes no productivos y evitar fallas de funcionamiento de la aplicación en producción.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

Control SGSI-8.7	
Controles contra el código malicioso	**CONTROLES SGSI RELACIONADOS**

	SGSI-8.13 Copias de seguridad de la información. SGSI-8.8 Gestión de vulnerabilidades técnicas. SGSI-8.19 Instalación de software sistemas en producción. SGSI-8.25 Seguridad en el Ciclo de vida de desarrollo seguro.
Anexos:	Se cuenta con el Servicio de SOC tercerizado con un proveedor y se tienen C76:N76 herramientas de seguridad perimetral como antivirus, firewall, filtros de contenido, filtro de correos, endpoint, WAF, SIEM. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información- A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información - Informe del agente y versión de la firma de virus - IT2.P2.GTI Instructivo para Gestión de Solicitudes de Permiso de Firewall - Planes de Contingencia de los Servicios de Tecnología

Propósito:
Implementar controles de detección, prevención y recuperación, así como sensibilizar a los colaboradores del ICBF para la protección contra códigos maliciosos.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá dictar los lineamientos para la instalación de software antivirus que brinde protección contra códigos maliciosos en todos los recursos informáticos del ICBF y asegurar que estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas permanentemente.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar la actualización continua de la base de firmas y parches correspondiente del software de Antivirus y actualizaciones de sistema operativo.

Todo mensaje sospechoso de procedencia desconocida deberá ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la mesa de servicio o del módulo de Autoservicio, tomando las medidas de control necesarias.

Control SGSI-8.13	
Copias de seguridad de la información	**CONTROLES SGSI RELACIONADOS**
	SGSI-8.12 Prevención de fuga de datos. SGSI-8.14 Redundancia recursos de tratamiento de la información.
Anexos:	Se cuenta con procedimientos, guías e instructivos referentes al respaldo y restauración de información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P2.GTI Procedimiento de gestión de solicitudes de tecnología - F4.P2.GTI Formato solicitud de respaldo para equipos de centros de cómputo - F5.P2.GTI Formato solicitud restauración de copias de seguridad

	- G8.GTI Guía respaldo y restauración de copias de seguridad - IT4.P2.GTI Instructivo para gestionar solicitudes de restauración de copias - IT5.P2.GTI Instructivo para gestión de solicitudes de copias de seguridad. - G15.GTI Guía Integral para el Servicio de Almacenamiento. - F2.P2.GTI Formato Acta de Entrega de Copia de Información. -IT1.P23.GTI Instructivo Uso Compartido Onedrive y Sharepoint -IT1.P6.GTI Instructivo para el Cargue de Documentación en Share Point

Propósito:
Dictar lineamientos para establecer un esquema de copias de seguridad, mediante estrategias orientadas a la protección de la información.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar y mantener copias de seguridad de la información digital solicitadas por el líder funcional o líder técnico.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá documentar un plan de copia de seguridad del ICBF donde se establezca esquemas de: qué, cuándo, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de información productiva.
- ✓ En cualquier momento la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, podrá realizar copias de información de colaboradores, producto de solicitudes que provengan de los directores, supervisores de contrato, coordinadores o jefes de área, La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir la custodia y almacenamiento de las copias.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá dar los lineamientos para la realización de las copias de seguridad de:
- ✓ Bases de datos en producción.
- ✓ Software de aplicaciones.
- ✓ Sistemas operativos.
- ✓ Software base del ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá generar mecanismos que mantengan la integridad y confidencialidad de las copias de seguridad.
- ✓ Los colaboradores son responsables de la información que resida en el computador asignado y serán los encargados de mantener copia de sus archivos más sensibles entregando al supervisor del contrato o jefe inmediato en custodia al finalizar la vinculación. En caso de que los colaboradores requieran la ejecución de un respaldo de información, lo pueden solicitar a la Subdirección de recursos tecnológico a través de la mesa de servicio.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá establecer los lineamientos y directrices para el respaldo de copias de las aplicaciones descentralizadas que se encuentran en las regionales del ICBF.
- ✓ Es responsabilidad de los funcionarios y contratistas guardar y almacenar su información institucional en OneDrive y SharePoint, con el fin de custodiar su información propendiendo por su protección y disponibilidad durante el tiempo de su vinculación laboral o contractual, y al finalizar esta con la Entidad.
- ✓ Las copias de seguridad de la información de los colaboradores deberán ser solicitadas únicamente por el jefe inmediato o quien haga las veces de supervisor del contrato y deberá tramitarse a través de la Mesa de Servicio o por requerimiento de las autoridades competentes.

Control SGSI-8.15 - 8.16	
Registros de eventos - Seguimiento de actividades	**CONTROLES SGSI RELACIONADOS** SGSI-5.28 Recopilación de Pruebas. SGSI-5.34 Privacidad y protección de la información de identificación personal (PII). SGSI-8.17 Sincronización del reloj
Anexos:	Se tiene Servicio de SOC contratado con el proveedor de servicios. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto

	Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P11.GTI Procedimiento de Gestión de Eventos y Alertas. -P25.GTI Procedimiento Gestión de Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad - F1.P5.GTI Formato Informe de Eventos Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad -F2.P25.GTI Formato Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio - F1.P11.GTI Formato Bitácora Eventos SOC

Propósito:

Dictar lineamientos que permitan registrar los eventos y evidencias, que los usuarios y administradores realizan en los sistemas de información e infraestructura tecnológica del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de sus Subdirecciones deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá salvaguardar los registros de auditoría que se generen de cada sistema.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá monitorear excepciones o los eventos de la seguridad de información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión del ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

Control SGSI-8.19	
Instalación de software sistemas en producción	**CONTROLES SGSI RELACIONADOS**
	SGSI-8.4 Acceso a código fuente. SGSI-8.31 Separación de los entornos de desarrollo, prueba y producción. SGSI-8.8 Gestión de vulnerabilidades técnicas. SGSI-5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología. - F1.P2.GT Formato de Solicitud de Servicios de Tecnología. - Software Línea Base aprobado - P4.GTI Procedimiento gestión de cambios de tecnologías de la información. -F1.P4.GTI Formato Requerimiento de Cambios Informáticos-RFC

Propósito:

Dictar lineamientos que permitan controlar la instalación de software en sistemas operativos propiedad del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios del ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá usar controles para proteger todo el software implementado y la documentación del sistema.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados deberá conservar las

versiones anteriores del software de aplicación como una medida de contingencia.

Control SGSI-8.8	
Gestión de vulnerabilidades técnicas	**CONTROLES SGSI RELACIONADOS** SGSI-5.10 Uso aceptable de la información y otros activos asociados. SGSI-5.9 Inventario de información y otros activos asociados. SGSI-8.32 Gestión de cambios. SGSI-5.26 Respuesta a incidentes de seguridad de la información.
Anexos:	Se elabora y ejecuta Test de Penetración, y se elabora Informe de resultados. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas. - F1.P1.GTI Formato registro de pruebas y remediación de vulnerabilidades -G14.GTI Guía para el Desarrollo de Pruebas de Penetración

Propósito: Dictar lineamientos para revisar de manera periódica las vulnerabilidades técnicas de los sistemas de información críticos y misionales del ICBF.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá:

- ✓ Realizar de manera periódica revisión de vulnerabilidades técnicas por medio de pruebas de penetración, a la plataforma tecnológica de la entidad.
- ✓ Documentar, informar, gestionar y corregirlos hallazgos de las vulnerabilidades adoptando las acciones preventivas y correctivas necesarias para minimizar el nivel de riesgo y reducir el impacto.
- ✓ Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.

Todo análisis de vulnerabilidad o prueba de penetración debe contar con la autorización del director de la Dirección de información y Tecnología o, a quien este delegue y estas deberán ser previamente informadas a las partes interesadas con el fin de evaluar el riesgo de la ejecución de ellas, su alcance y el cumplimiento de la normatividad vigente.

Control SGSI-8.34	
Protección de los sistemas de información durante las pruebas de auditoría	**CONTROLES SGSI RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información -F2. El Formato Plan de Auditoria v4 P2. El application/pdf Procedimiento Auditorías Internas SIGE -P7. El Procedimiento Auditorías de Control Interno -F12.El Reporte No Conformidades, respuestas y análisis OCI

Propósito:

Dictar lineamientos para revisar y auditar periódicamente los sistemas de información del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, deberá participar en las actividades de auditoría que le soliciten o involucren los sistemas en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente), determinando tareas, responsables y estas se deberán realizar fuera del horario laboral.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, deberá definir y gestionar los planes de mejoramiento que se generan de los resultados de las auditorias de los sistemas de Información del ICBF.

Control SGSI-8.20	
Seguridad de redes	**CONTROLES RELACIONADOS** SGSI-5.3 Segregación de Funciones. SGSI-8.24 Uso de Criptografía. SGSI-5.14 Transferencia de información.
Anexos:	Se cuenta con una plataforma tecnológica capaz de proteger y soportar los sistemas y aplicaciones. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - IT1.P2.GTI Instructivo para Gestión de Solicitudes de VPN - Planes de Contingencia Tecnológicos - Diagramas de Red

Propósito:

Dictar lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá:

- ✓ La Dirección de Información y Tecnología deberá segmentar la red, de modo que permita separar los grupos de servicios de información.
- ✓ Establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- ✓ Garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- ✓ Establecer la documentación necesaria para la utilización de los servicios de red restringiendo el acceso a los servicios de red y a las aplicaciones.
- ✓ Realizar revisiones y monitoreo regularmente en la gestión de los servicios de manera segura y que se encuentran en los acuerdos de servicios de red establecidos con los proveedores.
- ✓ El Oficial de Datos Personales adscrito a la Dirección de Planeación, establecerá los mecanismos y lineamientos para el intercambio de información con las entidades externas o internas.
- ✓ Los colaboradores deberán emplear los puntos de red habilitados para la conexión de equipos institucionales o personales debidamente autorizados.

Control SGSI-8.21 – SGSI-8.22	
Seguridad de los servicios de red - Segregación en redes	**CONTROLES RELACIONADOS** SGSI-5.3 Segregación de Funciones. SGSI-8.24 Uso de criptografía. SGSI-5.14 Transferencia de información.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas

	Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - Se cuenta con informes mensuales de los servicios firewall, WAN y LAN realizados por los proveedores. - P23.GTI Procedimiento Gestión de Permisos de Propiedad Sharepoint - IT1.P23.GTI Instructivo Uso Compartido Onedrive y Sharepoint - IT2.P2.GTI Instructivo para Gestión de Solicitudes de Permiso de Firewall - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información - G28.GTI Guía Permisos y Restricciones Microsoft 365

Propósito:

Dictar lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos de Información deberá disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del ICBF, teniendo en cuenta los siguientes criterios:
  - Contar con información de autenticación secreta de usuario.
  - Usar firmas o certificados digitales en caso de ser necesario.
  - Mantener protocolos seguros para la comunicación entre las partes.
- ✓ Cifrar las comunicaciones entre DMZ y los servidores de la red interna.
- ✓ Los protocolos de comunicación entre la red interna y la DMZ estén asegurados con el fin de prevenir fugas de información.
- ✓ La información almacenada de las transacciones no se encuentre pública.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información y Subdirección de Recursos Tecnológicos deberá disponer de una zona desmilitarizada o DMZ, entre la red interna del ICBF y la red externa (internet) con el objetivo de delimitar conexiones desde la red interna hacia Internet y limitar las conexiones desde Internet hacia la red interna del ICBF con los siguientes criterios:
  - El tráfico de la red externa a la DMZ está limitado.
  - El tráfico de la red externa a la red interna deberá estar controlado.
  - El tráfico de la red interna a la DMZ está limitado.
  - El tráfico de la red interna a la red externa está autorizado.
  - El tráfico de la DMZ a la red interna está prohibido.
  - El tráfico de la DMZ a la red externa está denegado.
- ✓ La DMZ se deberá implementar para ofrecer servicios que necesitan acceso desde Internet. Estos servicios deberán ser monitoreados con el fin de prevenir ataques
- ✓ La arquitectura de la DMZ deberá estar aislada de la red interna del ICBF de forma que no permita el acceso no autorizado a la red interna, por lo que se deberán diseñar redes perimetrales con los siguientes objetivos:
  - No se pueden hacer consultas directas a la red interna del ICBF desde redes externas e internet
  - Se deberá realizar la segmentación de redes y listas de acceso a los servicios del ICBF tales como servidores, administración, invitados, Etc.
  - El acceso a la red de datos del ICBF y a los sistemas de información soportados por la misma, es de carácter restringido. Se concederán permisos con base a “la necesidad de conocer” y el “acceso mínimo requerido” conforme a los criterios de seguridad de la información contemplados en la presente política.
- ✓ La conexión a la red WiFi institucional para funcionarios deberá ser administrada por la Dirección de Información y Tecnología, mediante un SSID (Service Set Identifier) único a nivel nacional. La autenticación de acceso deberá realizarse a través de un servidor RADIUS, utilizando las credenciales de los usuarios del Directorio Activo, con el fin de garantizar una gestión centralizada, segura y trazable del acceso a la red inalámbrica.
- ✓ La conexión a la red wifi institucional para visitantes deberá tener un SSID y contraseñas diferentes para cada sede administrativa (Sede de la Dirección General, Regional y Zonal), administrada por la Dirección de Información y Tecnología o quien haga sus veces en el nivel Regional y Zonal. No se podrá conectar dispositivos móviles personales a la red wifi, salvo los de la Oficina Asesora de Comunicaciones, Dirección General y los aprobados por la Dirección de Información y Tecnología o quien haga sus veces en las sedes Regionales y Zonales a través de una solicitud a la mesa de servicio.

Control SGSI-5.14	
Transferencia de información	**CONTROLES RELACIONADOS** SGSI-8.32 Gestión de cambios. SGSI-5.10 Uso aceptable de la información y otros activos asociados. SGSI-8.24 Uso de criptografía. SGSI-5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - IT1.P9.GTI Instructivo para cifrado de información - G11.GTI Guía para la Clasificación y Etiquetado de la Información. - G5. GTI Guía de recolección de evidencias de elementos informáticos - Política de tratamiento de datos personales - P14.GTI Procedimiento intercambio o suministro de información - Tablas de retención documental -PL36.SA Plan Sistema Integrado de Conservación - SIC - PL37.SA Plan de Transferencias Documentales Secundarias -PL38.SA Plan Transferencias Documentales Primarias

Propósito:

Dictar lineamientos de seguridad para la información transferida dentro del ICBF con cualquier entidad externa.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología deberá contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de esta.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá establecer mecanismos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del ICBF.
- ✓ La Dirección Administrativa o su delegada dictará directrices sobre retención, disposición y transferencia de la información física del ICBF, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- ✓ La Dirección de Información y Tecnología a través de la Dirección de Planeación y Control de Gestión - Grupo de Estadística y Gestión de Información. deberá establecer un acuerdo para la transferencia de información entre el ICBF y las partes externas.
- ✓ La Dirección de Información y Tecnología deberá definir lineamientos para la recolección de evidencias de elementos informáticos, con el fin de garantizar la autenticidad de los elementos materiales de prueba recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.

Control SGSI-6.6	
Acuerdos de confidencialidad o no divulgación	**CONTROLES RELACIONADOS** SGSI-5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información Operadores/Proveedores - G7.ABS Guía para la Adquisicion de Bienes y Servicios de Calidad.

	- F5.G7.ABS Formato Compromiso de Confidencialidad - F44.G7.ABS Formato Autorización Tratamiento Datos Personales Contratistas -F15.P2.ABS Formato Declaración Contratista Celebración CPSP o Apoyo a la Gestión Servidores Públicos -F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales -F12.P21.GTH Formato Compromiso de Confidencialidad de Información -G23.GTI Guía Metodológica para la Anonimización de Registros

Propósito:

Se deberán identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

- ✓ Como parte de sus términos y condiciones iniciales de trabajo, los colaboradores, cualquiera sea su nivel jerárquico dentro del ICBF, firmarán un compromiso de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del ICBF.
- ✓ En el caso de que sea personal externo que ejecute tareas propias del ICBF y haya sido contratado en el marco de un contrato o convenio con el ICBF, deberá reposar en la carpeta de ejecución del contrato un compromiso de confidencialidad firmado por el Representante Legal.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Control SGSI-5.8	
Seguridad de la información en la gestión de proyectos	**CONTROLES RELACIONADOS** SGSI-5.12 Clasificación de la información. SGSI-8.26 Requisitos de seguridad de las aplicaciones.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G7.ABS. Guía para la Adquisición de Bienes y Servicios de Calidad.

Propósito:

Dictar lineamientos que permitan incluir requisitos relacionados con seguridad de la información en nuevos sistemas de información y en las mejoras de los existentes.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá disponer de requerimientos para las solicitudes de nuevos sistemas de información y modificaciones a los existentes en el ICBF que cuenten con el análisis e implementación de criterios de seguridad del software.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá contar con los mecanismos para justificar, acordar y documentar en la fase de requisitos y en la fase de modificación de los sistemas del ICBF, los criterios de seguridad de la información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá contar con los componentes de seguridad de la información para los siguientes criterios:
  - El suministro de funcionalidades que permitan el acceso y la autorización para usuarios del ICBF privilegiados, técnicos y usuarios finales.
  - El suministro de funcionalidades que permitan al proceso o al usuario funcional la administración de los roles, permisos y acceso a la información de los sistemas de información.
  - Informar a los usuarios finales sobre los mecanismos de uso y apropiación de los sistemas de información, a través de la documentación que soporta las aplicaciones.
  - Proveer las aplicaciones definidas como críticas para la entidad con funcionalidades que cumplan los procesos como registro de transacciones, seguimiento y no repudio.
- ✓ La Dirección de Información y Tecnología deberá propender porque los sistemas de información o aplicativos incluyan controles de seguridad y cumplan con las políticas de seguridad de la información.

- ✓ La Dirección de información y Tecnología en conjunto con la Subdirección de Sistemas de Información deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- ✓ La Subdirección de Sistemas Integrados de Información desarrollará y/o adquirirá el software requerido para los procesos de la Sede de la Dirección General, de manera coordinada con el Área que manifieste la necesidad del software y se establecerán claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos y requisitos de seguridad de la información.
- ✓ Los desarrollos de la Entidad deberán estar completamente documentados, de acuerdo con el manual de procedimiento vigente, igualmente todas las versiones de los desarrollos se deberán preservar adecuadamente.
- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Sistemas Integrados de Información, velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información del ICBF.
- ✓ Todo nuevo hardware y software que se vaya a adquirir y conectar en la Entidad, por cualquier dependencia o proceso, deberá ser revisado y aprobado por la Dirección de Información y Tecnología, en cabeza de la Subdirección de Recursos Tecnológicos y la Subdirección de Sistemas Integrados de Información, para su correcto funcionamiento y protección de la información.
- ✓ La Dirección de Información y Tecnología implementará reglas y herramientas que restrinjan la instalación de software no autorizado o que no esté aprobada en la línea base de los activos de información del ICBF.
- ✓ El software que se adquiera a través de proyectos, programas o convenios, deberá establecer los lineamientos para la supervisión y seguimiento a las actividades de desarrollo contratado, los cuales deben quedar inmersos en las cláusulas y/o especificaciones técnicas.
- ✓ El área funcional deberá solicitar y /o autorizar la baja de cualquier software y con base en ello, la Dirección de información y Tecnología a través de la Subdirección de Recursos Tecnológicos y la Subdirección de Sistemas Integrados de Información, realizará las acciones pertinentes.
- ✓ La Subdirección de Sistemas Integrados de Información, deberá implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara, eficiente y con calidad. Cuando el desarrollo provenga de un área diferente estos deben garantizar el cumplimiento de los lineamientos de la Subdirección de Sistemas Integrados de Información.

Control SGSI-8.26	
Requisitos de seguridad de las aplicaciones	**CONTROLES RELACIONADOS**
	SGSI-8.24 Uso de criptografía. SGSI-5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología -G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información -F1.G1.GTI Formato Verificación de Estándares de Arquitectura y Desarrollo

Propósito:

Dictar lineamientos que permitan que las transferencias de información entre aplicaciones sobre redes públicas se protejan y las transacciones de los servicios de aplicación se realicen completas, sin alteraciones y/o visualización por partes no autorizadas.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información y la Subdirección de Recursos Tecnológicos deberán disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del ICBF, teniendo en cuenta los siguientes criterios:
  - Contar con información de autenticación secreta de usuario.
  - Mantener confidencialidad mediante formato establecido en el ICBF con las partes involucradas.
  - Usar cifrado en las comunicaciones cuando sea necesario.
  - Los protocolos de comunicación estén asegurados.
  - La información almacenada de las transacciones no se encuentre pública.

Control SGSI-8.25	
Seguridad en el Ciclo de vida de desarrollo seguro	**CONTROLES RELACIONADOS** SGSI-8.30 Externalización del desarrollo.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P6.GTI Procedimiento para el desarrollo y mantenimiento de los sistemas de información. - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información.

Propósito:
Dictar lineamientos que permitan establecer reglas para el desarrollo de sistemas de información dentro del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá establecer los mecanismos necesarios para la creación de software, teniendo en cuenta los siguientes aspectos:
  - Orientar sobre buenas prácticas de seguridad en el desarrollo del software.
  - Requisitos de seguridad en el control de versiones.
  - Capacidad de los desarrolladores para evitar, encontrar y resolver vulnerabilidades.
  - Establecer las condiciones para garantizar que todo el ciclo de desarrollo de software sea realizado bajo condiciones de seguridad y en ambientes controlados, que minimicen la posibilidad de materialización de riesgos que afecten la información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá tener en cuenta el punto anterior para la reutilización de códigos.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas de Integrados de Información deberá proteger los códigos ejecutables y código de desarrollo o compiladores del software operacional y aplicaciones propios del ICBF.
- ✓ Se deben seguir técnicas de programación seguras y buenas prácticas de seguridad de la información para el desarrollo de sistemas de información, por ejemplo, las recomendadas por OWASP (Proyecto Abierto de Seguridad en Aplicaciones WEB).
- ✓ Para el desarrollo contratado externamente, es necesario que el tercero cumpla con los lineamientos de desarrollo seguro que establezca el ICBF.

Control SGSI-8.32	
Gestión de cambios	**CONTROLES RELACIONADOS** SGSI-8.32 Gestión de cambios.

Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P3.GTI Procedimiento gestión de cambios de emergencia de tecnologías de la información. - P4.GTI Procedimiento gestión de cambios de tecnologías de la información. -F1.P4.GTI Formato Requerimiento de Cambios Informáticos-RFC -F2.P4.GTI Formato Calendario de Controles de Cambio -F3.P4.GTI Formato Bitácora Controles de Cambio

Propósito:

Dictar lineamientos para controlar y reducir al mínimo el impacto sobre los cambios normales, estándar y de emergencia que se generen sobre los servicios, infraestructura y aplicativos de TI administrados por la Dirección de Información y Tecnología del ICBF.

Lineamientos Generales:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá:

- ✓ Establecer un procedimiento que permita asegurar la gestión de cambios normales, estándar y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar los responsables y tareas en la gestión de cambios.
- ✓ Establecer un comité de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por un Gestor de Cambios del Operador TI. Este comité deberá estar conformado por tres integrantes del ICBF de la Dirección de Información y Tecnología, de la siguiente manera:
    - Con voz y voto: Director de Información y Tecnología (quien haga sus funciones o su delegado), Subdirector de Recursos Tecnológicos (quien haga sus funciones o su delegado) y Subdirector de Sistemas Integrados de Información (quien haga sus funciones o su delegado).
    - Con voz, pero sin voto: Representante Profesional de la Subdirección de Recursos Tecnológicos con el rol de Gestor de Cambios.
    - Ponentes: En cambios relacionados con infraestructura tecnológica el ponente es un representante de la Subdirección de Recursos Tecnológicos. En cambios relacionados con los sistemas de información el ponente es un representante de la Subdirección de Sistemas Integrados de Información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir los controles para que todo cambio a nivel de infraestructura productiva, sean documentados.
- ✓ La Dirección de Información y Tecnología a través del área de Ciberseguridad deberá tener en consideración las viabilidades técnicas de edición, creación y eliminación de VPN Site to Site, protocolos de cifrado, Protocolos de TLS-SSL–SFTP–FTPS,
  Repositorios públicos ICBF, PUERTOS PUBLICOS EN FW, IPS, SEGMENTOS PUBICOS, DNS – DOMINO ICBF, PUBLICACION DE SERVICIOS NUEVOS ICBF,
  SERVICIOS DE AUTENTICACION ICBF.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información y de la Subdirección de Recursos Tecnológicos deberá definir a través de las Pruebas Post-implementación que el cambio haya sido exitoso.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir la manera para notificar a tiempo los cambios de los sistemas, permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá evitar las modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los dados por el proveedor; limitándose únicamente a cambios necesarios, cuando se hagan, se deberán tener en cuenta los siguientes aspectos:
    - El riesgo en que se puede ver involucrado el sistema de información.
    - Verificar si se requiere consentimiento del usuario funcional.
    - Verificar la posibilidad que el proveedor realice dichos cambios.
    - El impacto en dado caso que el mantenimiento futuro recaiga en manos del ICBF.

- La compatibilidad con otro software en uso.

✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá conservar el software original cuando se hayan realizado cambios en los paquetes de este.

Control SGSI-8.27	
Arquitectura segura de sistemas y principios de ingeniería	**CONTROLES RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información -F1.G1.GTI Formato Verificación de Estándares de Arquitectura y Desarrollo - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología

Propósito:

Dictar lineamientos que permitan establecer reglas para los principios de desarrollo de sistemas de información seguros dentro del ICBF, igualmente contar con ambientes de desarrollo seguros para todo el ciclo de vida de los sistemas.

Lineamientos Generales:

✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá aplicar en los desarrollos de sistemas de información los principios y buenas prácticas de seguridad de la información.

✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá acatar las recomendaciones que se realicen por parte del Eje de Seguridad de la Información para el desarrollo seguro de sistemas de la información.

✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:

- El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Requisitos externos como reglamentaciones o políticas.
- Controles de Seguridad ya establecidos por el ICBF.
- Separación entre diferentes ambientes de desarrollo.
- Control de acceso al ambiente de desarrollo.
- Seguimiento de los cambios en el ambiente y los códigos almacenados allí.
- Control sobre el movimiento de datos desde y hacia el ambiente.

Control SGSI-8.30	
Externalización del desarrollo	**CONTROLES RELACIONADOS** SGSI-8.25 Seguridad en el Ciclo de vida de desarrollo seguro. SGSI-5.32 Derechos de propiedad intelectual.
Anexos:	Se obliga al cumplimiento a través de las cláusulas de los contratos asociados al desarrollo de software - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información.

Propósito: Dictar lineamientos que permitan establecer reglas para realizar seguimiento a los desarrollos de sistemas de información contratados externamente para funcionamiento dentro del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:
  - Acuerdos de licenciamiento, propiedad de códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
  - Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
  - Establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
  - Realizar pruebas para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.

Control SGSI-8.29	
Pruebas de seguridad en desarrollo y aceptación	**CONTROLES RELACIONADOS** SGSI-5.8 Seguridad de la información en la gestión de proyectos. SGSI-8.25 Seguridad en el Ciclo de vida de desarrollo seguro.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información donde se incluyen pruebas de funcionalidad - F6.P6.GTI Formato Escenario de Prueba

Propósito:
Dictar lineamientos que permitan establecer pruebas de seguridad y de aceptación de los sistemas del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá contemplar en los cambios y en los nuevos sistemas de información, pruebas de aceptación asociadas a los requisitos de seguridad de la información.

Control SGSI-8.33	
Datos de prueba	**CONTROLES RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información - G3.GTI Guía de Estándares de Especificación de Requerimientos

Propósito:
Dictar lineamientos que permitan establecer reglas para la protección de datos de pruebas de los Sistemas de Información del ICBF.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible del ICBF que este contenida en el ambiente de producción de las aplicaciones, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.

✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá tener en cuenta controles de acceso a los ambientes de producción y de prueba.

13. RELACIÓN CON PROVEEDORES.

Control SGSI-5.19 – 5.20 – 5.22	
Seguridad de la información en las relaciones con los proveedores. **Abordar la seguridad de la información en los acuerdos con los proveedores.** **Seguimiento, revisión y gestión de cambios de servicios de proveedores.**	**CONTROLES RELACIONADOS** SGSI-5.12 Clasificación de la información. SGSI-5.30 Preparación de las TIC para la continuidad del negocio.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la Adquisición de Bienes y Servicios de Calidad. -G3.MI Guía de Gestión de Riesgos y Peligros -F3.G3.MI Formato Matriz de Riesgos SGSI - Contratos suscritos - F43.G7.ABS Formato Seguimiento Cumplimiento Controles Seguridad Información Proveedores Servicios Tecnológicos. -P3.GTI Procedimiento Gestión de Cambios Emergencia de Tecnologías de la Información - P4.GTI Procedimiento Gestión de Cambios de Tecnologías de la Información - F1.P4.GTI Formato Requerimiento de Cambios Informático (RFC) de Infraestructura Tecnológica y Sistemas de Información - F3.P4.GTI Formato Bitácora de Controles de Cambios -Formato Calendario de Controles de Cambio

Propósito:

Dar los lineamientos de seguridad de la información para las relaciones con proveedores que trabajen con el ICBF.

Lineamientos Generales:

- ✓ La Dirección de Contratación deberá establecer lineamientos para el cumplimiento de las obligaciones contractuales del Eje de Seguridad de la Información con terceros o proveedores.
- ✓ La Dirección de Contratación deberá establecer en el momento de suscribirse contratos de apoyo a la gestión que se desarrollen dentro del ICBF, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del ICBF.
- ✓ La Dirección de Contratación deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del ICBF.
- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos deberá verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
- ✓ La Dirección de Información y Tecnología deberá establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.

- ✓ Cada dependencia del Instituto que establezca relación con proveedores y su cadena de suministro, solicitará capacitación periódica al Eje de Seguridad de la Información con el fin de dar a conocer las políticas que tiene el Instituto.
- ✓ Los operadores deberán aceptar y firmar el acuerdo de confidencialidad establecido por el ICBF.
- ✓ Los supervisores de contratos deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.
- ✓ Los supervisores de contrato deberán establecer mecanismos o condiciones con los contratistas o proveedores de servicios tecnológicos, que permitan garantizar el cumplimiento del procedimiento de gestión de cambios en los servicios suministrados a la Entidad.
- ✓ Los proveedores u operadores deberán informar y gestionar ante el supervisor del contrato, las activaciones y desactivaciones de usuarios que se deban realizar de su personal a cargo por novedades administrativas (vacaciones, permisos, incapacidades médicas, calamidad doméstica terminación del contrato u otro que supere los 8 días), con el fin de evitar posibles incidentes de seguridad de la información.

14. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Control SGSI-5.24 – 5.28	
Planificación y preparación de la gestión de incidentes de seguridad de la información. **Evaluación y decisión sobre eventos de seguridad de la información.** **Respuesta a incidentes de seguridad de la información.** **Aprender de los incidentes de seguridad de la información.** **Recopilación de Pruebas.**	**CONTROLES RELACIONADOS** SGSI-5.1 Políticas para la seguridad de la información.
Anexos:	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. -P25.GTI Procedimiento Gestión de Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad - F1.P5.GTI Formato Informe de Eventos Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad -F2.P25.GTI Formato Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio - F1.P10.GTI Formato Postulación Conocimiento Tecnológico. -P10.GTI Procedimiento Gestión del Conocimiento Tecnológico. - G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos

Propósito:

Dictar lineamientos que permitan asegurar al ICBF un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir los lineamientos para:
  - Responsables de la gestión de incidentes de seguridad de la información.
  - Los canales para que los colaboradores del ICBF puedan reportar los incidentes de seguridad de la información.
  - Para la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
  - Para la recolección de evidencia de incidentes de seguridad de la información.

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes, establecido en los lineamientos para la gestión de Incidentes.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá proporcionar los medios para el aprendizaje al ICBF de los incidentes de seguridad de la información.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá dar a conocer a los colaboradores del ICBF los lineamientos establecidos para la gestión de incidentes de seguridad de la información.
- ✓ De acuerdo con la criticidad del incidente, la Dirección de Información y Tecnología lo reportará al Equipo de respuesta a incidentes de seguridad informática, siguiendo los lineamientos y parámetros que este defina.

15. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.

Control SGSI-5.29	
Seguridad de la información durante la interrupción	**CONTROLES RELACIONADOS** SGSI-5.30 Preparación de las TIC para la continuidad del negocio
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - Planes de Contingencia de los Servicios de Tecnología - P18.DE Procedimiento Plan de Continuidad de la Operación - PL9.GTI Plan de Recuperacion de Desastres Tecnológicos - F1.PL9.GTI Formato Plan de Pruebas del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F2.PL9.GTI Formato Resultado Ejecución del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F3.PL9.GTI Formato Cronograma de Pruebas Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F4.PL9.GTI Formato Bitácora de Actividades del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F5.PL9.GTI Formato Árbol de Comunicaciones Plan de Recuperación de Desastres Tecnológicos - F6.PL9.GTI Formato Requisitos de Seguridad de la Información

Propósito:

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, deberá establecer el plan de recuperación de desastres tecnológicos de la Entidad, por medio del cual se continúe brindando el servicio durante una emergencia o desastre, y restaure los servicios críticos de tecnología identificados.

De igual manera, establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Lineamientos Generales:

- ✓ Se deben identificar y documentar los requisitos de seguridad de la información en cada una de las estrategias de recuperación de desastres identificadas en la Entidad.
- ✓ Se deberán conformar los equipos de respuesta ante incidentes de seguridad de la información.
- ✓ El ICBF, deberá elaborar un plan de recuperación de desastres tecnológicos para los servicios misionales críticos que se apoyan en las TIC para su funcionamiento identificados en el análisis de impacto al negocio.
- ✓ En caso de presentarse un incidente de seguridad de la información significativo se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.
- ✓ La Dirección de Información y Tecnología a través de sus Subdirecciones deberá documentar los procedimientos, guías o instructivos para configurar los servicios de TIC identificados en el análisis de impacto al negocio durante situaciones adversas.
- ✓ El ICBF dispondrá los planes necesarios para la implementación del proceso de continuidad de la Operación Tecnológica. La Secretaría General liderará la elaboración del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad de la Operación, así como la activación de este, cuando sea necesario.

- ✓ La Secretaría General con apoyo de la Dirección de Información y Tecnología deberá generar un Plan de Continuidad de la Operación, documentando e implementando procesos y procedimientos, para asegurar la continuidad requerida por la Entidad.
- ✓ El Plan de Continuidad de la Operación Tecnológica deberá incluirse en el Plan de Continuidad de la Operación del ICBF. Los Planes de Contingencia serán activados conforme a la operación, así como cualquier estrategia alineada a la Continuidad de la Operación dentro de la prestación del servicio del Instituto Colombiano de Bienestar Familiar.
- ✓ La Dirección de Información y Tecnología elaborará el Plan de Recuperación de Desastres, el cual deberá incluir como mínimo los procedimientos, requisitos de seguridad de la información, recuperación y retorno a la normalidad.
- ✓ La Dirección de Información y Tecnología deberá proyectar la capacidad tecnológica para la implementación y puesta en marcha del DRP en la cual se involucren las aplicaciones críticas misionales y de apoyo propias del ICBF la cual no puede ser asociada a otros ambientes diferente al antes mencionado.

Control SGSI-8.14	
Redundancia de los recursos de tratamiento de la información	**CONTROLES RELACIONADOS** N/A
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - P18.DE Procedimiento Plan de Continuidad de la Operación. - PL9.GTI Plan de recuperación de desastres tecnológicos. -F1.PL9.GTI Formato Plan de Pruebas del Plan de Recuperación de Desastres Tecnológicos -F2.PL9.GTI Formato Resultado Ejecución del Plan de Recuperación de Desastres Tecnológicos -F3.PL9.GTI Formato Cronograma de Pruebas Plan de Recuperación de Desastres Tecnológicos -F4.PL9.GTI Formato Bitácora de Actividades del Plan de Recuperación de Desastres Tecnológicos -F5.PL9.GTI Formato Árbol de Comunicaciones Plan de Recuperación de Desastres Tecnológicos -F6.PL9.GTI Formato Requisitos de Seguridad de la Información
Propósito: La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, deberá disponer de las instalaciones de procesamiento de información requeridas en el plan de recuperación de desastres tecnológicos, contemplando lo siguiente: **Lineamientos Generales:** ✓ Deberá implementar redundancia suficiente, para lo cual deberá considerar componentes o arquitecturas redundantes. ✓ Deberá poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.	

16. CUMPLIMIENTO

Control SGSI-5.31	
Requisitos legales, estatutarios, reglamentarios y contractuales	**CONTROLES RELACIONADOS** N/A
Anexos:	P4.MI - Procedimiento Identificación y Evaluación de Requisitos Legales y Otros Requisitos - Aprobación Requisitos Legales SVE - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas

	Generales de Manejo y se definen lineamientos frente al uso y manejo de la información

Propósito:
Dictar lineamientos para cumplir con los requisitos de legislación y regulación externa e interna del ICBF.

Lineamientos Generales:

- ✓ El ICBF a través de la Subdirección de Mejoramiento Organizacional, deberá definir y establecer un procedimiento y una herramienta de verificación de requisitos legales.
- ✓ La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información deberá identificar, documentar y actualizar todos los requerimientos contractuales, estatutarios y reglamentarios con el fin de salvaguardar la información de la entidad dar cumplimiento a la normatividad vigente utilizando la herramienta de verificación de requisitos legales. La Oficina Asesora Jurídica deberá asesorar al Eje de Seguridad de la Información en dicha documentación.

Control SGSI-5.32	
Derechos de propiedad Intelectual	**CONTROLES RELACIONADOS**
	N/A
Anexos:	El análisis de propiedad intelectual se encuentra desarrollado normativamente en la legislación interna mediante la Ley 23 de 1982 y en la legislación de la Comunidad Andina de Naciones (CAN) mediante la Decisión 351 de 1993. Se cuenta con el servicio de licenciamiento de software; se cuenta con un compromiso de Antipiratería ACUERDO No. 3 de 2017 del Instituto Colombiano de Bienestar Familiar; Se cuenta con una serie de obras y software registrado ante el MINISTERIO DEL INTERIOR DIRECCIÓN NACIONAL DE DERECHO DE AUTOR, de igual manera se encuentran registradas algunas marcas ante la Superintendencia de Industria y Comercio - SIC. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - Política de Tratamiento de Datos Personales -Inventarios Software Línea Base aprobado - Acta de Software Línea Aprobado

Propósito:
Dictar lineamientos para cumplir con los requisitos legislativos, reglamentarios y contractuales acerca del uso de software patentado y material con respecto al cual pueden existir derechos de propiedad intelectual.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología deberá definir controles con el objetivo de proteger adecuadamente la propiedad intelectual del ICBF, tanto propia como la de terceros, tales como derechos de autor de software, licencias y código fuente. El material registrado con derechos de autor no se deberá copiar sin la autorización del propietario.
- ✓ La Dirección de Información y Tecnología a través del Eje de Seguridad de la Información deberá generar conciencia a los colaboradores del ICBF sobre los derechos de propiedad intelectual.
- ✓ Cuando un funcionario, colaborador, proveedor u operador se le termina su vínculo administrativo o finaliza el contrato, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo los derechos de propiedad intelectual de acuerdo con la normativa vigente.
- ✓ Todos los colaboradores, proveedores y operadores deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

Control SGSI-5.33	
Protección de Registros	**CONTROLES RELACIONADOS**

	N/A
Anexos:	La Dirección Administrativa a través del grupo de Gestión Documental establece directrices de retención de registros e información contenidas en las Tablas de Retención Documental de la Entidad. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información. - PL35.SA Plan Institucional de Archivos - PINAR. - P1.SA Procedimiento Organización de Archivos. - Tablas de Retención Documental - TRD. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales.

Propósito:

Dictar lineamientos para cumplir con la protección de registros contra pérdida, destrucción y falsificación aplicando los requisitos legislativos, reglamentarios, contractuales y del ICBF.

Lineamientos Generales:

- ✓ La Dirección Administrativa a través del grupo de Gestión Documental, y la Dirección de Información y Tecnología deberán definir y establecer:
  - Directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.
  - Deberá establecer e implementar controles para proteger los registros en su confidencialidad, integridad y disponibilidad.
  - Deberá establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, deberá documentar e identificar los controles criptográficos necesarios en la infraestructura tecnológica del ICBF.
- ✓ La Dirección de Información y Tecnología brindará de acuerdo con los requerimientos del ICBF, herramientas que permitan el cifrado de la información para proteger la confidencialidad, integridad y disponibilidad de la información clasificada o reservada, en sistemas de información, correo electrónico y mecanismos de transferencia de información interna o externa.

Control SGSI-5.35 – 5.36 – 8.8	
Revisión independiente de la seguridad de la información. **Cumplimiento de políticas, normas y estándares de seguridad de la información.** **Gestión de vulnerabilidades técnicas.**	**CONTROLES RELACIONADOS** SGSI-5.1 Políticas para la seguridad de la información.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo Manual de Políticas de Seguridad de la Información - P2.EI Procedimiento Auditorías Internas SIGE y la formulación del plan de auditorías. - P7.EI Procedimiento Auditorias de Control Interno - Revisión por la Dirección.

	Se han identificado oportunidades de mejora y acciones correctivas para el incumplimiento de las políticas de seguridad de la información. - P2.MI Procedimiento Acciones Correctivas - Sistema de Información SVE Se elabora y ejecuta Test de Penetración, y se elabora Informe de resultados. - P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas. - F1.P1.GTI Formato registro de pruebas y remediación de vulnerabilidades - G14.GTI Guía para el Desarrollo de Pruebas de Penetración
Propósito: Dictar lineamientos para asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales del ICBF. **Lineamientos Generales:** ✓ La Oficina de Control Interno, deberá realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información. ✓ Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión en auditorías. ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar análisis periódicos de seguridad en los sistemas de información con ayuda de herramientas automatizadas y generar informes técnicos.	

17. CONTROLES NUEVOS

Control SGSI-5.7	
Inteligencia de Amenazas	**CONTROLES RELACIONADOS** SGSI-7.5 Protección contra amenazas externas y ambientales.
Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. La Entidad dispone de herramientas tecnológicas que analizan y automatizan las respuestas a amenazas con el fin de prepararse para este fin. Boletines de Ciberseguridad Comité de Protección de la Marca Digital Comité de Inteligencia de Amenazas -P1.GTI Procedimiento Seguimiento, Control y Atención de Vulnerabilidades Técnicas -Formato Registro de Pruebas y Remediación Vulnerabilidades
Propósito: Establecer mecanismos de recolección, análisis y uso de información sobre amenazas cibernéticas, con el fin de proteger los activos de la organización y mitigar los riesgos asociados. **Lineamientos Generales:** ✓ La Dirección de Información y Tecnología utilizará fuentes de información, tanto internas como externas, para recolectar datos sobre amenazas cibernéticas y de seguridad más relevantes para la Entidad.	

- ✓ Los datos recolectados sobre amenazas (vulnerabilidades conocidas, actividad de amenazas actuales entre otras), deben ser socializados con los Profesionales encargados de la Dirección de Información y Tecnología y/o Subdirección de Recursos Tecnológicos, con el fin de analizar e identificar patrones, tácticas, técnicas y procedimientos utilizados por diferentes vectores de ataque.
- ✓ La Dirección de Información y Tecnología implementará sistemas de monitoreo que permitan evaluar en tiempo real actividad de red, detección de intrusiones y otros indicadores de compromisos, incluyendo el seguimiento y monitoreo de logs, eventos de seguridad y vulnerabilidades.
- ✓ La Dirección de Información y Tecnología en cabeza de la subdirección de recursos tecnológicos deberá realizar evaluaciones periódicas de vulnerabilidades en sistemas y aplicaciones y conforme a los resultados priorizar las actividades de remediación y mitigación.

Control SGSI-5.23	
Seguridad de la información para el uso de servicios en la nube.	**CONTROLES RELACIONADOS** N/A
Anexos:	* Las publicaciones pasan por el WAF - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información.

Propósito:

Dictar lineamientos para el uso seguro y eficiente de los servicios de procesamiento de la información en plataformas de computación en la nube.

Lineamientos Generales:

- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos será el área encargada de mantener la seguridad y privacidad de la información, así como el uso de los servicios de procesamiento de la información en plataformas de computación en la nube que son utilizadas por el ICBF cumpliendo con los niveles de compromiso y brindando continuidad a la operación de la Entidad.
- ✓ Para la utilización de servicios de procesamiento en nube “AZURE”, No está autorizado el uso de servicios para fines personales. Todos los servicios utilizados deben ser aprobados previamente por la Dirección de Tecnología de la Información.
- ✓ Para la utilización de servicios de almacenamiento en la nube “OneDrive, SharePoint”, almacenamiento AZURE, es responsabilidad de cada colaborador garantizar que solo se almacene información de carácter institucional. El uso no autorizado de estos servicios puede resultar en sanciones disciplinarias o llamados de atención por parte del supervisor del contrato.
- ✓ Los colaboradores serán responsables que la información institucional no se almacene en servicios de nube personales y que se sigan las políticas de seguridad y privacidad establecidas para proteger la información del ICBF.
- ✓ La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, será responsable de garantizar que los servicios en la nube cumplan con todas las normativas y regulaciones aplicables, incluyendo aquellas relacionadas con la protección y privacidad de la información de la Entidad y los datos personales. Además, esta área se encargará de supervisar la implementación de medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados, pérdidas o filtraciones. También se asegurará de que los proveedores de servicios en la nube cumplan con los estándares de calidad y seguridad establecidos por la Entidad.

Control SGSI-5.30	
Preparación de las TIC para la continuidad del negocio	**CONTROLES RELACIONADOS** SGSI-5.3 Funciones, responsabilidades y autoridades de la organización. SGSI-5.19 Seguridad de la información en las relaciones con los proveedores. SGSI-5.20 Abordar la seguridad de la información en los acuerdos con los proveedores. SGSI-5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores. SGSI-5.29 Seguridad de la información durante la interrupción

Anexos:	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - PL9.GTI Plan de Recuperación de Desastres Tecnológicos - F1.PL9.GTI Formato Plan de Pruebas del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F2.PL9.GTI Formato Resultado Ejecución del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F3.PL9.GTI Formato Cronograma de Pruebas Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F4.PL9.GTI Formato Bitácora de Actividades del Plan de Recuperación de Desastres Tecnológicos y/o Contingencia - F5.PL9.GTI Formato Árbol de Comunicaciones Plan de Recuperación de Desastres Tecnológicos - F6.PL9.GTI Formato Requisitos de Seguridad de la Información - P9.GTH Procedimiento para la Elaboración de Planes de Emergencias y Contingencias BIA - Riesgos de Continuidad - Planes de contingencia Tecnológicas

Propósito:
Dictar lineamientos para la implementación del proceso de continuidad de la Operación Tecnológica.

Lineamientos Generales:

- ✓ El ICBF dispondrá los planes necesarios para la implementación del proceso de continuidad de la Operación Tecnológica. La Secretaría General liderará la elaboración del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad de la Operación, así como la activación de este, cuando sea necesario.
- ✓ La Secretaría General con apoyo de la Dirección de Información y Tecnología deberá generar un Plan de Continuidad de la Operación, documentando e implementando procesos y procedimientos, para asegurar la continuidad requerida por la Entidad.
- ✓ El Plan de Continuidad de la Operación Tecnológica deberá incluirse en el Plan de Continuidad de la Operación del ICBF. Los Planes de Contingencia de los servicios de tecnología serán activados conforme a la operación, así como cualquier estrategia alineada a la Continuidad de la Operación dentro de la prestación del servicio del Instituto Colombiano de Bienestar Familiar.
- ✓ La Dirección de Información y Tecnología lidera el Plan de Recuperación de Desastres, el cual deberá incluir como mínimo los procedimientos, requisitos de seguridad de la información, recuperación y retorno a la normalidad con el objeto de propender por la disponibilidad y el acceso a los sistemas, datos y aplicaciones de información críticos en caso de interrupciones o eventos disruptivos.

18. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
20/11/2020	Versión 10	Se ajustó la Introducción adicionando en las normativas los CONPES 3854 y 3995. En los Términos y Definiciones se incluyeron los temas relacionados con los controles nuevos de la norma técnica ISO/IEC27001:2022: actividades de seguimiento, codificación segura, eliminación de información, enmascaramiento de datos, filtrado web, gestión de la configuración, inteligencia de amenazas, monitoreo de seguridad física, prevención de fuga de datos, seguridad de la información para el uso de servicios en la nube. Se ajustaron los siguientes controles de acuerdo con la norma ISO/IEC27001:2022: Se reemplaza el Control SGSI-A.6.1 por el control 5.3, se incorporan los controles relacionados y se agrega en los lineamientos generales la Resolución 6659 del 15 de diciembre de 2020.

Fecha	Versión	Descripción del Cambio
		Se reemplaza el Control SGSI-A.6.2.1 por el control 8.1, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI-A.6.2.2 por el control 6.7, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI-A.7.1.1 por el control 6.1 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.7.1.2 por el control 6.2, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.7.2.1 por el control 5.4 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.7.2.2 por el control 6.3 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.7.2.3 por el control 6.4, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.7.3.1 por el control 6.5, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI-A.8.1.1 - A.8.1.2 por el control 5.9, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.8.1.3 por el control 5.10, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI-A.8.1.4 por el control 5.11, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI-A.8.2.1 por el control 5.12, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.8.2.2 - A.8.2.3 por el control 5.13, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de

Fecha	Versión	Descripción del Cambio
		Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.8.3.1, A.8.3.2 y A.8.3.3 por el control 7.10, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.8.3.1, A.8.3.2 y A.8.3.3 por el control 7.10, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.9.1.1 y A.9.1.2 por el control 5.15, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI-A.9.2.1 por el control 5.16, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplazan los Controles SGSI- A.9.2.2, A.9.2.5 y A.9.2.6 por el control 5.18, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.9.2.3 por el control 8.2, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.9.2.4, A.9.3.1 y A.9.4.3 por el control 5.17, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.9.4.1 por el control 8.3, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.9.4.2 por el control 8.5, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF.

Fecha	Versión	Descripción del Cambio
		Se reemplaza el Control SGSI- A.9.4.4 por el control 8.18, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.9.4.5 por el control 8.4, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.10.1.1 y A.10.1.2 por el control 8.24, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.11.1.1 por el control 7.1, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.11.1.2 y 11.1.3 por los controles 7.2 y 7.3, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.11.1.4 por el control 7.5, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.1.5 por el control 7.6, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.2.1 por el control 7.8, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.2.2 por el control 7.11 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.2.3 por el control 7.12, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.2.4 por el control 7.13, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.11.2.6 por el control 7.9, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF.

Fecha	Versión	Descripción del Cambio
		Se reemplaza el Control SGSI- A.11.2.7 por el control 7.14, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.11.2.8 y A.11.2.9 por el control 7.7, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.12.1.1 por el control 5.37, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.12.1.3 por el control 8.6 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.12.1.4 por el control 8.31, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.12.2.1 por el control 8.7, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.12.4 por los controles 8.15 y 8.16, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.12.5.1 y 12.6.2 por el control 8.19, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.12.6.1 por el control 8.8, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplazan los Controles SGSI- A.12.7.1 por el control 8.34, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.13.1.1 por el control 8.20, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF.

Fecha	Versión	Descripción del Cambio
		Se reemplazan los Controles SGSI- A.13.1.2 y A.13.1.3 por los controles 8.21 y 8.22, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.13.2.1 y A.13.2 2 por el control 5.14, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.13.2.4 por el control 6.6, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.14.1.1 por el control 5.8, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.14.1.2 y A.14.1.3 por el control 8.26, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.14.2.1 por el control 8.25, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplazan los Controles SGSI- A.14.2.2, A.14.2.3 y A.14.2.4 por el control 8.32, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.14.2.5 y A.14.2.6 por el control 8.27 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.14.2.7 por el control 8.30, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplazan los Controles SGSI- A.14.2.8 y A.14.2.9 por el control 8.29, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.14.3.1 por el control 8.33 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplazan los Controles SGSI- A.15 por los controles 5.19, 5.20 y 5.22, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.16.1.1 y A.16.1.7 por los controles 5.24 y 5.28, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la

Fecha	Versión	Descripción del Cambio
		Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.17.1.1 y A.17.1.2 por el control 5.29, se incorporan los controles relacionados, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.17.2.1 por el control 8.14 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.18.1.1 por el control 5.31 y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se reemplaza el Control SGSI- A.18.1.2 por el control 5.32, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplaza el Control SGSI- A.18.1.3 por el control 5.33, se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad y, se adicionan y ajustan lineamientos generales de acuerdo con la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar -ICBF. Se reemplazan los Controles SGSI- A.18.2 por los controles 5.35 y 5.36, se incorporan los controles relacionados y se actualizan los anexos con base en el A3.MS.DE Anexo Declaración de Aplicabilidad. Se adicionan controles nuevos con base en la norma de gestión ISO/IEC27001:2022: SGSI-5.7 Inteligencia de Amenazas SGSI-5.23 Seguridad de la información para el uso de servicios en la nube. SGSI-5.30 Preparación de las TIC para la continuidad del negocio.
21/05/2020	Versión 9	Se ajusto la Introducción, se incluyó la definición de G58 Se ajustaron los siguientes controles: Control SGSI-A.6.1 , Control SGSI-A.6.2.1 se desagrega este control y se crea el Control SGSI-A.6.2.2, Control SGSI-A.7.2.1, Control SGSI-A.7.2.2, Control SGSI-A.7.3.1, Control SGSI-A.8.1.1 – A.8.1.2 , Control SGSI-A.8.2.2 - A.8.2.3, Control SGSI-A.8.3.1, Control SGSI-A.9.2.2, Control SGSI-A.9.2.3, Control SGSI-A.9.4.1, Control SGSI A.11.1.2 – 11.1.3, Control SGSI-A.11.2.1, Control SGSI-A.11.2.3, Control SGSI-A.11.2.4, Control SGSI-A.11.2.6, Control SGSI-A.11.2.8 – A.11.2.9, Control SGSI-A.12.1.4 , Control SGSI-A.12.6.1, Control SGSI-A.12.3.1, Control SGSI-A.12.7, Control SGSI-A.13.1.1, A.13.1.2, A.13.1.3,Control SGSI-A.14.1.1, Control SGSI-A.14.2.1 , Control SGSI-A.14.1.2 SGSI-A.14.1.3, Control SGSI-A.14.2.5 – SGSI-A.14.2.6 , Control SGSI-A.14.2.7 , Control SGSI-A.14.2.8 – SGSI-A.14.2.9 , Control SGSI-A.14.3.1, Control SGSI-A.15, Control SGSI A.17.1.1, Control SGSI-A.17.1.2, Control SGSI-A.17.1.3, Control SGSI A.17.2.1, Control SGSI-A.18.1.1, Control SGSI-A.18.1.2, Control SGSI A.18.1. 3 - SGSI A.18.1.5, Control SGSI A.18.1.4, Control SGSI A.18.2
08/03/2019	Versión 8	Se realizaron los siguientes ajustes: Se actualizó la Introducción adicionando normatividades. Se incluyeron nuevos términos. Se ajustaron las Partes Interesadas. Se actualizó la evaluación del desempeño. Se cambió la palabra Continuidad del Negocio por Continuidad de la Operación. Se ajustaron los siguientes controles: A.7.1.2 Términos y condiciones del empleo

Fecha	Versión	Descripción del Cambio
		A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.3.1 Terminación o cambio de responsabilidades de empleo A.8.2.2 Etiquetado de la Información A.8.2.3 Manejo de activos A.8.3.1 Gestión de Medios removibles 8.3.2 Disposición de los Medios A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.3.1 – A.9.4.3 Uso de información secreta para la autenticación y Sistema de gestión de contraseñas A.9.4.2 Procedimiento de ingreso seguro A.9.4.5 Control de acceso a códigos fuente de programas A.11.1.2 Controles de acceso físicos A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.13.1 Gestión de la Seguridad de las redes A.13.1.1 Controles de redes A.13.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.13.1.3 Protección de transacciones de los servicios de las aplicaciones A.13.2.3 Mensajería electrónica A.14.1.1 Análisis y especificación de requisitos de seguridad de la información A.17.1.1 Planificación de la Continuidad de la Seguridad de la Información A.17.1.2 Implementación de la Continuidad de la Seguridad de la Información A.17.1.3 Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
17/08/2018	Versión 7	Se realizaron las siguientes modificaciones: - Actualización de las Partes Interesadas - A.9.1.1 – A.9.1.2 Política de control de acceso - Acceso a redes y a servicios de red, incluyendo una política de revisión e inactivación de VPN.
07/06/2018	Versión 6	Se realizaron las siguientes modificaciones: -Actualización de las resoluciones 9364 y 3600 por la resolución No. 9674 del 27 de julio de 2018 Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. - En el control A.9.2.6 Retiro o ajuste de los derechos de acceso, se elimina la opción de que los Ingenieros Regionales gestionen la activación o desactivación de usuarios del SIM cuando el supervisor del contrato no se encuentre disponible.
12/04/2018	Versión 5	Se actualizaron e incluyeron términos y definiciones (áreas seguras, CCOC, COLCERT, CSIRT, Infraestructura crítica, infraestructura crítica cibernética). Se incluyó el punto 3. Partes interesadas. Se ajustaron las siguientes políticas de acuerdo con la operación: A.6.2.1 Política para dispositivos móviles Teletrabajo A.9.2.6 Retiro o ajuste de los derechos de acceso A.8.1.3 Uso aceptable de los activos A.8.1.4 Devolución de ActivosA.11.1.4 Protección contra amenazas externas y ambientales A.11.1.4 Protección contra amenazas externas y ambientales A.13.1.1 Controles de redes A.13.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.13.1.3 Protección de transacciones de los servicios de las aplicaciones A.17.1.1 Planificación de la Continuidad de la Seguridad de la Información
17/05/2017	Versión 4	Se ajustaron las políticas de acuerdo con la operación y a la actualización de la Guía para la Rotulación de la Información. A.6.2.1 Política para dispositivos móviles, se actualizaron lineamientos. A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información, se actualizaron lineamientos generales. A.9.2.2 Suministro de acceso de usuarios, se actualizaron lineamientos generales. A.9.4.2 Procedimiento de ingreso seguro, se actualizaron lineamientos generales. A.9.4.5 Control de acceso a códigos fuente de programas, se actualizo el anexo.

Fecha	Versión	Descripción del Cambio
		A.11.2.5 Retiro de activos, se actualizo el anexo. A.11.2.7 Disposición segura o reutilización de equipos, se actualizo el anexo. A.17.1.1 Planificación de la Continuidad de la Seguridad de la Información, se actualizó el propósito y los lineamientos generales.
05/05/2017	Versión 3	Se ajustaron las políticas de acuerdo actualización de la resolución 3600 de 2017.
07/10/2016	Versión 2	Actualización de Anexos con respecto a la codificación según el nuevo modelo de procesos.
06/09/2016	Versión 1	Se ajustaron las políticas de acuerdo con la operación. Se registraron los indicadores asociados con la eficacia del SGSI, y se incluyeron responsables acordes con la resolución 10232 del 2015.