Contenido

## 1. INTRODUCCIÓN

El presente manual hace parte integral de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, la cual se encuentra publicada en la página web 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”.
- ✓ Ley 734 de 2002 “Por la cual se expide el Código Disciplinario Único”.
- ✓ Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- ✓ Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- ✓ CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- ✓ 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 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- ✓ 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.
- ✓ CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano
- ✓ 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)
- ✓ Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- ✓ 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.
- ✓ Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

## 2. TÉRMINOS Y DEFINICIONES

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

- **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.
- **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.
- **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.

- **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.
- **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.
- **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.

- **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.
- **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.
- **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 de las Partes Interesadas que se encuentra en el portal web 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.<br>Dar cumplimiento a los lineamientos y procedimientos en la normativa legal vigente correspondiente a seguridad y privacidad de la información.<br>Generación de conocimiento de las nuevas amenazas emergentes en el ICBF.<br>Generar informes de los incidentes de | Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del SGSI.<br>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.<br>Propender por la protección de la | 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 |
| | seguridad, privacidad de la información y seguridad digital presentados en la entidad cuando se considere necesario. | información de la ciudadanía a través del sostenimiento de Modelo de Seguridad y Privacidad de la Información implementado a nivel nacional.<br>Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios.<br>Aplicar los controles de seguridad digital y seguridad de la información, establecidos para la mitigación de los riesgos en los procesos.<br>Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad. | | | | |
| **Policía Nacional - DIJIN** | Generación de conocimiento de las nuevas amenazas emergentes en el ICBF.<br>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.<br>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. | Manual Políticas de Seguridad de la Información. | Respuesta oportuna a incidentes de Seguridad de la Información que contemplan análisis forense. | X | X |

| Parte interesada | Necesidades | Expectativas | Requisitos en el sistema de gestión | Logros y resultados esperados | Aplicación | |
|---|---|---|---|---|---|---|
| | | | | | Nacional | Territorial |
| | | Articulación eficiente entre el ICBF y entidades, con el fin de intercambiar información que permita la prestación efectiva de los servicios.<br>Aplicar los controles de seguridad digital y seguridad de la información, establecidos para la mitigación de los riesgos en los procesos.<br>Suministro de evidencias digitales a la DIJIN, para el análisis forense por parte de este Ente. | | | | |
| **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 |
| **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.<br>Aplicar los controles de seguridad digital y seguridad de la Información, establecidos para la mitigación de los | Manual Políticas de Seguridad de la Información. | Respuesta oportuna a incidentes de Seguridad de la Información. | X | X |

| Parte interesada | Necesidades | Expectativas | Requisitos en el sistema de gestión | Logros y resultados esperados | Aplicación | |
|---|---|---|---|---|---|---|
| | | | | | Nacional | Territorial |
| | | riesgos en los procesos. | | | | |
| **Alcaldías** | Sensibilización y acompañamiento en temas de delitos informáticos y riesgos de Seguridad Digital.<br>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.<br>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.<br>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.<br>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 del negocio. | X | X |
| **ALIADOS ESTRATÉGICOS** | | | | | | |
| **CSIRT - PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática** | Articulación, cooperación, información y comunicación Interinstitucional.<br>Implementar estrategias y herramientas para el intercambio de conocimiento e | 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 |
| | información.<br>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. | Comunicación y colaboración permanente sobre el manejo de incidentes que afecten la seguridad de la información. | | | | |
| **CCP - Centro Cibernético Policial** | Articulación, cooperación, información y comunicación Interinstitucional.<br>Implementar estrategias y herramientas para el intercambio de conocimiento e información.<br>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.<br>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.<br>Implementar estrategias y herramientas para el intercambio de conocimiento e información.<br>Brindar apoyo respecto a la Ciberseguridad de Infraestructuras Críticas del país. | 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.<br>Coordinación de emergencias ante incidentes. | Manual Políticas de Seguridad de la Información. | Respuesta oportuna a incidentes de Seguridad de la Información. | X | |
| **CCOCI - Comando Conjunto de Operaciones Cibernéticas** | Articulación, cooperación, información y comunicación Interinstitucional.<br>Implementar estrategias y herramientas para el intercambio de conocimiento e información.<br>Brindar apoyo respecto a la | 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.<br>Participación del ICBF de las convocatorias de este | Manual Políticas de Seguridad de la Información. | Ser parte del Plan Nacional de Protección de Infraestructura Crítica Cibernética del país. | X | |

| Parte interesada | Necesidades | Expectativas | Requisitos en el sistema de gestión | Logros y resultados esperados | Aplicación | |
|---|---|---|---|---|---|---|
| | | | | | Nacional | Territorial |
| | Ciberdefensa de Infraestructuras Críticas Cibernéticas Nacionales de Colombia. | ente para la implementación de controles a las infraestructuras críticas. | | | | |
| **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

| **Control SGSI-A.6.1** | |
|---|---|
| **Organización interna** | **CONTROLES RELACIONADOS** |
| | SGSI-A.5.1.1 Políticas para la seguridad de la información.<br>SGSI-A.8.1.2 Propiedad de los activos. |

| | |
|---|---|
| | SGSI-A.17. Aspectos de Seguridad de la Información de la gestión de Continuidad de Negocio.<br>SGSI-A.16 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 la Resolución 11980 del 30 de diciembre de 2019, por la cual se adopta 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, y los boletines que estas entidades emitan deberán ser publicados en el Micrositio de SGSI en la Intranet del ICBF.
- ✓ El Líder del Eje de Seguridad de la Información deberá mantener los contactos apropiados con los grupos de interés especial (Policía Nacional, 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-A.6.2.1** | |
|---|---|
| **Política para dispositivos móviles** | **CONTROLES RELACIONADOS** |
| | SGSI-9.2.4. Gestión de información secreta para la autentificación de usuarios.<br>SGSI-10. Criptografía. |
| **Anexos:** | F1.P2.GTI Formato de solicitud de servicios de tecnología.<br>F9.P2.GTI Formato verificación de equipos Personales |

**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.
- ✓ Los dispositivos móviles que se pueden utilizar en el ICBF son: computador portátil, celular Smartphone, Tablet. En el caso de los computadores portátiles estos deberán contar con software licenciados y antivirus actualizado, para los Smartphone y Tablet deberán utilizar la suite Microsoft Office 365 con las credenciales del ICBF.
    - 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 y cumplir con los lineamientos referentes a seguridad de la información.
    - En caso de que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del ICBF una vez esté avalado por los ingenieros de la Subdirección de Recursos Tecnológicos a nivel Central e Ingenieros Regionales en el nivel Regional y Zonal. La Subdirección de Recursos Tecnológicos deberá realizar la revisión de los requisitos antes mencionados de manera periódica en los equipos autorizados para conectarse a la red de ICBF.
- ✓ Los dispositivos móviles 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 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 trasmita 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.

| **Control SGSI-A.6.2.2** | |
|---|---|
| **Política para teletrabajo** | **CONTROLES RELACIONADOS** |
| | SGSI-A9 Control de Acceso |
| **Anexos:** | F1.P2.GTI Formato de solicitud de 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, 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.
- ✓ 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 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-A.7.1.1** | |
|---|---|
| **Selección** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | F2.P5.ABS Formato Lista de Chequeo Proceso de Selección<br>P21.GTH Procedimiento Provisión de Empleos |

**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-A.7.1.2** | |
|---|---|
| **Términos y condiciones del empleo** | **CONTROLES RELACIONADOS**<br>SGSI-A.13.2.4 Acuerdos de confidencialidad o de no divulgación.<br>SGSI-A.18.1.2 Derechos de Propiedad intelectual.<br>SGSI-A.18.1.4 Privacidad y protección de información de datos personales.<br>SGSI-A.8 Gestión de Activos.<br>SGSI-A.7.2.3 Proceso disciplinario.<br>SGSI-A.7.3 Terminación y cambio de empleo. |
| **Anexos:** | F1.P2.GTI Formato de solicitud de servicios de tecnología.<br>G7.ABS Guía para la adquisición de bienes y servicios de calidad. |

**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 y aclarar que estas se extienden más allá de los límites del ICBF y del horario normal de trabajo o de ejecución del objeto contractual.
- ✓ 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-A.7.2.1** | |
|---|---|
| **Responsabilidades de la dirección** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | F1.P2.GTI Formato de solicitud de servicios de tecnología. |

**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-A.7.2.2** | |
|---|---|
| **Toma de conciencia, educación y formación en la seguridad de la información** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | P10.GTH Procedimiento Inducción y Reinducción |

**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-A.7.2.3** | |
|---|---|
| **Proceso disciplinario** | **CONTROLES RELACIONADOS** |
| | SGSI-A.16.1.7 Recolección de evidencia. |
| **Anexos:** | P2.GTH Procedimiento Proceso Disciplinario Ordinario |
| **Propósito:**<br>Dictar lineamientos para generar acciones a los colaboradores que hayan cometido un desacato a la seguridad de la información.<br><br>**Lineamiento General:**<br>✓ 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 del ICBF. | |

| **Control SGSI-A.7.3.1** | |
|---|---|
| **Terminación o cambio de responsabilidades de empleo** | **CONTROLES RELACIONADOS** |
| | SGSI-A.13.2.4 Acuerdos de confidencialidad o de no divulgación.<br>SGSI-A.7.1.2 Términos y condiciones del empleo. |
| **Anexos:** | P10.SA Procedimiento egreso por entrega o suministro de elementos.<br>P19.ABS Procedimiento terminación anticipada y /o liquidación de contratos PS y AG mutuo acuerdo.<br>G7.ABS Guía para la adquisición de bienes y servicios de calidad.<br>F7.P2.ABS Formato Compromiso de Confidencialidad de Información – Contratistas<br>P30.GTH Procedimiento para entrega de cargo por parte de servidores públicos.<br>F12.P21.GTH Formato compromiso de confidencialidad<br>P25.ABS Procedimiento para la finalización del contrato de prestación de servicios profesionales y de apoyo a la gestión |
| **Propósito:**<br>Dictar lineamientos para las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo.<br><br>**Lineamientos Generales:**<br>✓ El supervisor del contrato o a quien delegue deberá recoger 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 recoger y custodiar la información del ICBF en el caso de retiro, investigación, inhabilidades, o cambio de funciones.
- ✓ 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. Se deben inactivar los accesos biométricos o de tarjetas de proximidad de los sistemas de control de acceso.
  - 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-A.8.1.1 – A.8.1.2** | |
|---|---|
| **Inventario y propiedad de los activos** | **CONTROLES RELACIONADOS** |
| | SGSI-A.8.2.1 Clasificación de la Información. |
| **Anexos:** | G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. |
| **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, deberá reportar a la Subdirección de Mejoramiento Organizacional 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-A.8.1.3** | |
|---|---|
| **Uso aceptable de los activos** | **POLÍTICAS RELACIONADAS** |
| | SGSI-A.8.2.1 Clasificación de la Información |
| **Anexos:** | PL6.GTI Plan de cambio y cultura de seguridad y privacidad de la información<br>F1.P2.GTI Formato solicitud de servicios de tecnología.<br>P2.GTI Procedimiento de gestión de solicitudes de tecnología. |

**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 los aplicativos y equipos de cómputo autorizados por la Dirección de Información y Tecnología.
- ✓ En caso de que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado,

actualizado y solo podrá conectarse a la red del ICBF una vez esté avalado por la Subdirección de Recursos Tecnológicos a nivel Central e Ingenieros Regionales en el nivel Regional y Zonal.

- ✓ 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 a la tabla de retención documental o acto administrativo deben reposar en original o con firma digital ,en ningún caso se debe utilizar firmas digitalizadas o escaneadas, salvo en aquellos que se autorice por resolución de la Dirección General, indicando para qué fin y porqué medios (comunicados masivos individuales a los aportantes, comunicaciones masivas individuales a colaboradores u operadores, etc.).
- ✓ 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 prohíbe suministrar acceso directo a los buzones de correo asignado a cada colaborador. En caso de ser necesario realizar la gestión del correo institucional, se debe solicitar a la mesa de servicio listando los colaboradores que tendrán los permisos para escribir correos en nombre del colaborador solicitante.

| **Control SGSI-A.8.1.4** | |
|---|---|
| **Devolución de activos** | **CONTROLES RELACIONADOS** |
| | SGSI-A.11.2.7 Disposición segura o reutilización de equipos. |
| **Anexos:** | IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo |

**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-A.8.2.1** | |
|---|---|
| **Clasificación de la información** | **CONTROLES RELACIONADOS** |
| | SGSI-A.9.1.1. Política de Control de Acceso |
| **Anexos:** | G11.GTI Guía para la rotulación 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.

| **Control SGSI-A.8.2.2 - A.8.2.3** | |
|---|---|
| **Etiquetado de la información manejo de activos** | **CONTROLES RELACIONADOS** |
| | SGSI-A.8.2.1 Clasificación de la información |
| **Anexos:** | IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo.<br>G11.GTI Guía para la rotulación 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 para la rotulación 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 para la rotulación 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-A.8.3.1** | |
|---|---|
| **Gestión de medios removibles** | **CONTROLES RELACIONADOS** |
| | N/A |

| | |
|---|---|
| **Anexos:** | P9.GTI Procedimiento para el manejo de medios removibles.<br>IT1.P9.GTI Instructivo para cifrado de información.<br>IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo.<br>P57.SA Procedimiento de manejo de residuos especiales |

**Propósito:**

Dictar lineamientos para implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por el ICBF.

**Lineamientos Generales:**

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

- ✓ Un procedimiento 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 para el desempeño de sus funciones u obligaciones deberán velar por la custodia y buen manejo de estos.
- ✓ Deberá proveer los métodos de cifrado de la información además de suministrar el software o herramienta utilizado para tal fin.
- ✓ 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.

| **Control SGSI-A.8.3.2** | |
|---|---|
| **Disposición de los medios** | **CONTROLES RELACIONADOS** |
| | SGSI-11.2.7 Disposición segura o reutilización de equipos |
| **Anexos:** | G2.SA Guía gestión de bienes |

| | |
|---|---|
| | P9.GTI Procedimiento para el manejo de medios removibles<br>IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo.<br>P57.SA Procedimiento manejo residuos especiales |

**Propósito:**
Disponer de forma segura de los medios cuando estos no se requieran, aplicando buenas prácticas ambientales y de seguridad de la información.

**Lineamientos Generales:**
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos desarrollará lineamientos para la disposición de medios teniendo en cuenta lo siguiente:

- ✓ 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.

| **Control SGSI-A.8.3.3** | |
|---|---|
| **Transferencia de medios físicos** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**Propósito:**
Dictar lineamientos para proteger 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 lineamientos para mantener la seguridad de la información que se transfiere dentro del ICBF y con cualquier entidad externa teniendo en cuenta lo siguiente:

- ✓ 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.

## 8. CONTROL DE ACCESO

| **Control SGSI-A.9.1.1 – A.9.1.2** | |
|---|---|
| - **Política de control de acceso**<br>- **Acceso a redes y a servicios de red** | **CONTROLES RELACIONADOS**<br>SGSI-A.6.1.1 Roles y responsabilidades para la seguridad de la información.<br>SGSI-A.8.2 Clasificación de la Información.<br>SGSI-A.8.2.2 Etiquetado de la Información.<br>SGSI-A.9.2 Gestión de Acceso de usuarios.<br>SGSI-A.9.2.1 Registro y cancelación del registro de usuarios.<br>SGSI-A.9.2.2 Suministro de acceso de usuarios.<br>SGSI-A.9.2.3 Gestión de derechos de acceso privilegiado.<br>SGSI-A.9.2.5 Revisión de los derechos de acceso de usuarios.<br>SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso.<br>SGSI-A.9.3 Responsabilidades de los usuarios.<br>SGSI-A.9.4 Control de acceso a sistemas y aplicaciones.<br>SGSI-A.11 Seguridad física y del entorno.<br>SGSI-A.18.1 Cumplimiento de requisitos legales y contractuales. |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología<br>P2.GTI Procedimiento de gestión de solicitudes de tecnología. |

**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 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 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.

| **Control SGSI-A.9.2.1** | |
|---|---|
| **Registro y cancelación del registro de usuarios** | **CONTROLES RELACIONADOS**<br>SGSI-A.9.2.2 Suministro de acceso de usuarios.<br>SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso. |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología |

**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-A.9.2.2** | |
|---|---|
| **Suministro de acceso de usuarios** | **CONTROLES RELACIONADOS**<br>SGSI-A.8.1.2 Propiedad de los activos<br>SGSI-A.9.1 Requisitos del negocio para control de acceso<br>SGSI-A.6.1.2 Separación de deberes<br>SGSI-A.9.2.5 Revisión de los derechos de acceso de usuarios<br>SGSI-A.9.2.4 Gestión de información de autenticación secreta de usuarios<br>SGSI-A.7.1.2 Términos y condiciones del empleo<br>SGSI-A.7.2.3 Proceso disciplinario<br>SGSI-A.13.2.4 Acuerdos de confidencialidad o de no divulgación<br>SGSI-A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología |

| | |
|---|---|
| | P2.GTI Procedimiento de gestión de solicitudes de tecnología. |

**Propósito**:
Definir los lineamientos para el proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para los sistemas y servicios del ICBF.

**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 controladas, monitoreadas, vigiladas y custodiadas por los líderes de los servicios de la Subdirección de Recursos Tecnológicos de la Dirección de Información y Tecnología.

- ✓ 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.

| **Control SGSI-A.9.2.3** | |
|---|---|
| **Gestión de derechos de acceso privilegiado** | **CONTROLES RELACIONADOS** |
| | SGSI-A.9.1-Política de control de acceso |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología. |

**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 auditoria 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 las carpetas y subcarpetas 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, adicional a esto se deberá definir umbrales que permitan notificar al administrador del servicio de almacenamiento y al administrador de carpeta 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 las carpetas, 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-A.9.2.4** | |
|---|---|
| **Gestión de información de autenticación secreta de usuarios** | **CONTROLES RELACIONADOS**<br>SGSI-A.7.1.2 Términos y condiciones del empleo. |

| | |
|---|---|
| | SGSI A.9.3.1 – A.9.4.3. Uso de información secreta para la autenticación. Sistema de gestión de contraseñas. |
| **Anexos:** | N/A |

**Propósito**:
Dictar lineamientos para definir un proceso de gestión formal para la asignación de información de autenticación secreta.

**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 secreta para la autenticación o proporcionar una nueva o temporal.
- ✓ La información secreta para la autenticación por defecto del fabricante, se deberá modificar después de la instalación de los dispositivos o del software.

| **Control SGSI-A.9.2.5** | |
|---|---|
| **Revisión de los derechos de acceso de usuarios** | **CONTROLES RELACIONADOS** |
| | SGSI-A.9.2.1 Registro y cancelación del registro de usuarios.<br>SGSI-A.9.2.2 Suministro de acceso de usuarios.<br>SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso.<br>SGSI-A.7 Seguridad de los recursos humanos. |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología |

**Propósito**: Dictar lineamientos para que se realice la revisión de los derechos de acceso de los usuarios a intervalos regulares.

**Lineamientos Generales:**
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá generar reportes de uso de cada uno 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.

| **Control SGSI-A.9.2.6** | |
|---|---|
| **Retiro o ajuste de los derechos de acceso** | **CONTROLES RELACIONADOS** |
| | N/A |

| | |
|---|---|
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología<br>P4.GTH Procedimiento para la activación, actualización y desactivación de las cuentas de usuario institucionales |

**Propósito**:
Dictar lineamientos 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 que se realice el retiro y cambios de los derechos de acceso a todos los colaboradores y terceras partes a la información y a las instalaciones de procesamiento de información teniendo en cuenta lo siguiente:

- ✓ 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 A.9.3.1 – A.9.4.3** | |
|---|---|
| - **Uso de información secreta para la autenticación**<br>- **Sistema de gestión de contraseñas** | **CONTROLES RELACIONADOS**<br>SGSI-A.9.2.2 Suministro de acceso de usuarios.<br>SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso. |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología<br>P2.GTI Procedimiento de gestión de solicitudes de tecnología |

**Propósito**:
Dictar lineamientos para la asignación de información de autenticación secreta, 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:

- ✓ 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 (10) 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, etc.
    - Deberán ser diferentes de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (10) 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 60 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-A.9.4.1** | |
|---|---|
| **Restricción de acceso a la información** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología<br>P2.GTI Procedimiento de gestión de solicitudes de tecnología |

**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 A.9.3.1 – A.9.4.3, 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.
- ✓ Los desarrolladores deberán establecer que periódicamente se revalide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.
- ✓ 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-A.9.4.2** | |
|---|---|
| **Procedimiento de ingreso seguro** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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.
  - No mostrar las contraseñas digitadas con anterioridad.
  - No transmitir la contraseña en texto claro.
- ✓ Todo acceso a un sistema de información o a un recurso informático deberá registrarse y mantenerse respaldado.

| **Control SGSI-A.9.4.4** | |
|---|---|
| **Uso de programas utilitarios privilegiados** | **CONTROLES RELACIONADOS** |
| | SGSI-A.9.2.3 Gestión de derechos de acceso privilegiado. |
| **Anexos:** | F1.P2.GTI Formato solicitud de servicios de tecnología |

| | |
|---|---|
| | P2.GTI Procedimiento de gestión de solicitudes de tecnología |

**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-A.9.4.5** | |
|---|---|
| **Control de acceso a códigos fuente de programas** | **CONTROLES RELACIONADOS** |
| | SGSI-A.14.2.2 Procedimiento de control de cambios en sistemas |
| **Anexos:** | P4.GTI Procedimiento gestión de cambios de tecnologías de la información<br>P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información |

**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-A.10.1.1 – A.10.1.2** | |
|---|---|
| - **Política sobre el uso de controles criptográficos**<br>- **Gestión de llaves** | **CONTROLES RELACIONADOS**<br>SGSI-A.15.2 Gestión de la prestación de servicios de proveedores.<br>SGSI-A.18.1.5 Reglamentación de controles criptográficos. |
| **Anexos:** | G1.P17.GF Guía de políticas y seguridad para el manejo y control de recursos financieros administrados ICBF.<br>F1.P2.GTI Formato solicitud de servicios de tecnología. |

**Propósito:**

Dictar lineamientos para el uso adecuado de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información del ICBF, así mismo implementar el uso, protección y tiempo de vida de las llaves criptográfica durante todo su ciclo de vida.

**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.
- ✓ Deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada que 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.

| |
|---|
| ✓ La Subdirección de Recursos Tecnológicos deberá disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.<br>✓ Realizar un inventario y revisión periódica de llaves criptográficas y certificados digitales actualizado (uso, protección y tiempo de vida). |

## 10. SEGURIDAD FÍSICA Y DEL ENTORNO

| **Control SGSI-A.11.1.1** | |
|---|---|
| **Perímetro de seguridad física** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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 establece 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 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 A.11.1.2 – 11.1.3** | |
|---|---|
| **Controles de acceso físicos**<br>**Seguridad de oficinas, recintos e instalaciones** | **CONTROLES RELACIONADOS**<br>SGSI-A.9.2.5 Revisión de los derechos de acceso de usuarios.<br>SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso. |
| **Anexos:** | F1.G9.GTI Formato bitácora de ingreso |

**Propósito:**

Dictar lineamientos para proteger a través de controles de acceso para que solo se permita el ingreso a personal autorizado a las áreas seguras.

**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 o a quien ella asigne, será responsable de administrar el ingreso y salida del personal a los centros de cableado y centros de datos de la Sede de la Dirección General. En las regionales estará a cargo de la Coordinación Administrativa o quien esta delegue.
- ✓ La Dirección Administrativa en la Sede de la Dirección General y la Coordinación Administrativa en las regionales autorizarán el ingreso a personal ajeno al ICBF a los centros de cableado para fines laborales y se harán responsables de la estadía de estos durante el tiempo que permanezcan en las instalaciones brindándoles el correspondiente acompañamiento.
- ✓ Todo el personal que ingrese al Centro de Datos y centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso, como también registrarse en la bitácora de ingreso.
- ✓ 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).

| **Control SGSI-A.11.1.4** | |
|---|---|
| **Protección contra amenazas externas y ambientales** | **CONTROLES RELACIONADOS** |
| | N/A |

| | |
|---|---|
| **Anexos:** | PL1.P9.GTH Plan de emergencia y contingencia sede de la dirección general |

**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-A.11.1.5** | |
|---|---|
| **Trabajo en áreas seguras** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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-A.11.1.6** | |
|---|---|
| **Áreas de despacho y carga** | **CONTROLES RELACIONADOS** |
| | SGSI-A.8 Gestión de activos. |
| **Anexos:** | N/A |

**Propósito:**
Dictar lineamientos para controlar los puntos de acceso tales como áreas de despacho y de carga, así como otros puntos donde pueda entrar personal no autorizado.

**Lineamientos Generales:**
La Dirección Administrativa o a quien delegue establece los lineamientos para los controles de área de despacho y carga teniendo en cuenta lo siguiente:

- ✓ Las áreas de cargue y descargue deberán estar señalizadas.
- ✓ Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante CCTV.
- ✓ El material que ingresa se deberá inspeccionar y examinar para determinar la presencia de materiales peligrosos.

| **Control SGSI-A.11.2.1** | |
|---|---|
| **Ubicación y protección de los equipos** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | IT1.P9.GTI Instructivo para cifrado de información |

**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-A.11.2.2** | |
|---|---|
| **Servicio de suministro** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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-A.11.2.3** | |
|---|---|
| **Seguridad en el Cableado** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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-A.11.2.4** | |
|---|---|
| **Mantenimiento de equipos** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | F1.G12.GTI Formato acta mantenimiento preventivo equipos portátiles y de escritorio<br>F2.G12.GTI Formato relación mantenimientos preventivos impresoras y scanner<br>F3.G12.GTI Formato acta mantenimientos preventivos de switches |

| | |
|---|---|
| | F4.G12.GTI Formato lista de chequeo mantenimiento de Red LAN<br>F3.P2.GTI Formato diagnóstico de hardware |

**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-A.11.2.5** | |
|---|---|
| **Retiro de activos:** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | G2.SA Guía gestión de bienes<br>F3.G2.SA Formato traslado elementos devolutivos |

**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-A.11.2.6** | |
|---|---|
| **Seguridad de equipos y activos fuera de las instalaciones** | **CONTROLES RELACIONADOS** |
| | SGSI-A.6.2 Dispositivos móviles y teletrabajo. |
| **Anexos:** | 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 |

**Propósito:**
Dictar lineamientos para aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización.

**Lineamiento General:**
La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establece los lineamientos para que los equipos y medios retirados de las instalaciones no se dejen sin vigilancia en lugares públicos y se protejan adecuadamente.

- ✓ Deberá informarse al jefe inmediato sobre la salida de los elementos de cómputo de las instalaciones del ICBF.

| **Control SGSI-A.11.2.7** | |
|---|---|
| **Disposición segura o reutilización de equipos** | **CONTROLES RELACIONADOS** |
| | SGSI-A.10. Criptografía |
| Anexos: | G2.SA Guía gestión de bienes<br>P5.SA Procedimiento para definir la destinación de bienes muebles<br>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-A.11.2.8 – A.11.2.9** | |
|---|---|
| **Equipos de usuarios desatendidos**<br>**Política de escritorio y pantalla limpia** | **CONTROLES RELACIONADOS**<br>SGSI-A.8.2 Clasificación de la información. |
| **Anexos:** | G11.GTI Guía para la rotulación de la información |

**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-A.12.1.1** | |
|---|---|
| | **CONTROLES SGSI RELACIONADOS** |

| | |
|---|---|
| **Procedimientos de Operación Documentados** | SGSI-A.5.1.1 Políticas para la Seguridad de la Información.<br>SGSI-A.8.3 Manejo de medios.<br>SGSI-A.9.4.4 Uso de programas utilitarios privilegiados.<br>SGSI-A.11.2.7 Disposición segura o reutilización de equipos.<br>SGSI-A.12.3 Copias de respaldo.<br>SGSI-A.12.4 Registro y seguimiento.<br>SGSI-A.16.1.1 Responsabilidades y procedimientos. |
| **Anexos:** | P2.GTI. Procedimiento de gestión de solicitudes de tecnología.<br>F4.P2.GTI Formato solicitud de respaldo para equipos de centros de cómputo<br>G8.GTI Guía respaldo y restauración de copias de seguridad<br>IT5.P2.GTI Instructivo para gestión de solicitudes de copias de seguridad<br>P4.GTI Procedimiento gestión de cambios de tecnologías de la información.<br>P6.GTI Procedimiento para desarrollo y mantenimiento de sistema de información.<br>P7.GTI Procedimiento de gestión de problemas de tecnología<br>P3.GTI Procedimiento gestión de cambios de emergencia de tecnologías de la información.<br>P5.GTI Procedimiento gestión de incidentes de seguridad de la información.<br>P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas.<br>P9.GTI Procedimiento para el manejo de medios removibles<br>F5.P2.GTI Formato solicitud restauración de copias de seguridad<br>IT4.P2.GTI Instructivo para gestionar solicitudes de restauración de copias<br>G8.GTI Guía respaldo y restauración de copias de seguridad |

**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 las Subdirecciones de Recursos Tecnológicos ySistemas Integrados de Información con el apoyo de la Subdirección de Mejoramiento Organizacional deberán:

- ✓ Documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
- ✓ Poner a disposición de todos los colaboradores los procedimientos de operación.

| **Control SGSI-A.12.1.2** | |
|---|---|
| **Gestión de cambios** | **CONTROLES SGSI RELACIONADOS** |
| | SGSI-A.14.2.2 Procedimiento de control de cambios en sistemas.<br>SGSI-A.16.1 Gestión de incidentes de seguridad de la información. |
| **Anexos:** | P4.GTI Procedimiento gestión de cambios de tecnologías de la información.<br>F1.P4.GTI Formato requerimiento de cambios informáticos - RFC.<br>F2.P4.GTI Formato calendario de controles de cambio.<br>P3.GTI Procedimiento gestión de cambios de emergencia de tecnologías de la información.<br>G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información<br>F1.G1.GTI Formato verificación de estándares de arquitectura y desarrollo |

**Propósito:**

Dictar lineamientos para controlar y reducir al mínimo el impacto sobre los cambios normales 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 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.

| **Control SGSI-A.12.1.3** | |
|---|---|
| **Gestión de capacidad** | **CONTROLES SGSI RELACIONADOS** |
| | N/A |
| **Anexos:** | 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-A.12.1.4** | |
|---|---|
| **Separación de los ambientes de desarrollo, pruebas y producción** | **CONTROLES SGSI RELACIONADOS** |
| | SGSI-A.14.3 Datos de prueba. |
| **Anexos:** | N/A |
| **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 y lógica.
- ✓ 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.
- ✓ 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-A.12.2.1** | |
|---|---|
| **Controles contra códigos maliciosos:** | **CONTROLES SGSI RELACIONADOS**<br>SGSI-A.12.3 Copias de respaldo.<br>SGSI-A.12.6 Gestión De la vulnerabilidad técnica.<br>SGSI-A.12.6.2 restricciones sobre la instalación de software.<br>SGSI-A.14.2 Seguridad en los procesos de desarrollo y de soporte. |
| **Anexos:** | Informe del agente y versión de la firma de virus (data). |

**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-A.12.3.1** | |
|---|---|
| **Respaldo de la información:** | **CONTROLES SGSI RELACIONADOS** |
| | SGSI-11. Seguridad física y del entorno |
| **Anexos:** | P2.GTI Procedimiento de gestión de solicitudes de tecnología<br>F4.P2.GTI Formato solicitud de respaldo para equipos de centros de cómputo<br>F5.P2.GTI Formato solicitud restauración de copias de seguridad<br>G8.GTI Guía respaldo y restauración de copias de seguridad<br>IT4.P2.GTI Instructivo para gestionar solicitudes de restauración de copias<br>IT5.P2.GTI Instructivo para gestión de solicitudes de copias de seguridad |

**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.
- ✓ 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.

| **Control SGSI-A.12.4** | |
|---|---|
| **Registro (Logging) y Seguimiento** | **CONTROLES SGSI RELACIONADOS** |
| | SGSI-16.1.7 Recolección de evidencias.<br>SGSI-18.1.4 Privacidad y seguridad de la información de datos personales. |
| **Anexos:** | N/A |
| **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-A.12.5** | |
|---|---|
| **Instalación de software en sistemas operativos** | **CONTROLES SGSI RELACIONADOS**<br>SGSI-9.4.5 Control de acceso a códigos fuente de programas.<br>SGSI-12.1.4 Separación de ambientes de desarrollo pruebas y producción.<br>SGSI-12.6 Gestión de la vulnerabilidad técnica.<br>SGSI-15.2.1 Seguimiento y revisión de los servicios de los proveedores. |
| **Anexos:** | N/A |

**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-A.12.6.1** | |
|---|---|
| **Gestión de vulnerabilidad técnica** | **CONTROLES SGSI RELACIONADOS** |
| | SGSI-8. Gestión de activos.<br>SGSI-8.1.1. Inventario de activos.<br>SGSI-12.1.2 Gestión de cambios.<br>SGSI-13.1 Seguridad de las comunicaciones.<br>SGSI-14.2.2 Procedimientos de control de cambios en sistemas.<br>SGSI-16.1.5 Respuesta a incidentes de seguridad de la información. |
| **Anexos:** | P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas.<br>F1.P1.GTI Formato registro de pruebas y remediación de vulnerabilidades |

**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-A.12.6.2** | |
|---|---|
| **Restricciones sobre la instalación de Software** | **CONTROLES SGSI RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**Propósito:**

Dictar lineamientos para las restricciones sobre la instalación de Software.

**Lineamientos Generales:**

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá monitorear que la Infraestructura tecnológica del ICBF no sea utilizada para actividades comerciales o para propósitos de entretenimiento, acceso o uso a material no autorizado.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá establecer que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole derechos de autor.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos designará y autorizará al personal para instalar, configurar y dar soporte a los equipos de cómputo del ICBF.
- ✓ Sólo está permitido el uso de software licenciado por el ICBF y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos. Las aplicaciones generadas por el ICBF, en desarrollo de su misión institucional, deberán ser reportadas a la Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, para su administración.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales.

| **Control SGSI-A.12.7** | |
|---|---|
| **Consideraciones sobre auditorias de sistemas de información** | **CONTROLES SGSI RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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 planificar actividades que involucren auditorias de los sistemas críticos 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.

## 12. SEGURIDAD DE LAS COMUNICACIONES

| **Control SGSI A.13.1** | |
|---|---|
| **Gestión de la Seguridad de las redes** | **CONTROLES RELACIONADOS**<br>SGSI-A.6.1.2 Separación de deberes.<br>SGSI-A.10 Criptografía.<br>SGSI-A.13.2 Transferencia de información. |
| **Anexos:** | N/A |

**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:

- ✓ Proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta deberá estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes de terceros y del servicio de acceso a internet. La división de estos segmentos deberá ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
- ✓ Realizar segmentación de redes para colaboradores y visitantes del ICBF.
- ✓ 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.

| **Control SGSI-A.13.1.1 – SGSI-A.13.1.2 – SGSI-A.13.1.3** | |
|---|---|
| **Controles de redes**<br>**Seguridad de servicios de las aplicaciones en redes públicas**<br>**Protección de transacciones de los servicios de las aplicaciones** | **CONTROLES RELACIONADOS**<br>SGSI-A.6.1.2 Separación de deberes.<br>SGSI-A.10 CRIPTOGRAFÍA.<br>SGSI-A.13.2 Transferencia de información. |
| **Anexos:** | IT1.P9.GTI Instructivo para cifrado de información |

**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:
  - o Contar con información de autenticación secreta de usuario.
  - o Usar firmas o certificados digitales en caso de ser necesario.
  - o 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:
  - o El tráfico de la red externa a la DMZ está limitado.
  - o El tráfico de la red externa a la red interna deberá estar controlado.
  - o El tráfico de la red interna a la DMZ está limitado.
  - o El tráfico de la red interna a la red externa está autorizado.
  - o El tráfico de la DMZ a la red interna está prohibido.
  - o 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 desde la Dirección de Información y Tecnología mediante un SSID (Service Set Identifier) único a nivel nacional, la autenticación deberá ser con usuario y contraseña de directorio activo.
- ✓ 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-A.13.2.1 -A.13.2 2** | |
|---|---|
| **Políticas y Procedimientos de Transferencia de información**<br>**Acuerdos sobre transferencia de información** | **CONTROLES RELACIONADOS**<br>SGSI-A.12.2.1 Gestión de cambios.<br>SGSI-A.8.1.3 Uso aceptable de los activos.<br>SGSI-A.10. criptografía.<br>SGSI-A.18.1 Cumplimiento de requisitos legales y contractuales. |
| **Anexos:** | IT1.P9.GTI Instructivo para cifrado de información<br>G11.GTI Guía para la rotulación de la información<br>G5. GTI Guía de recolección de evidencias de elementos informáticos<br>TRD versión 1999<br>TRD versión 2005<br>TRD versión 2009<br>TRD versión 2010<br>TRD versión 2012<br>TRD versión 2019<br>Política de tratamiento de datos personales |

| | |
|---|---|
| | P14.GTI Procedimiento intercambio o suministro de información |

**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-A.13.2.3** | |
|---|---|
| **Mensajería electrónica** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | IT1.P9.GTI Instructivo para cifrado de información<br>G11.GTI Guía para la rotulación de la información<br>G5. GTI Guía de recolección de evidencias de elementos informáticos<br>TRD versión 1999<br>TRD versión 2005<br>TRD versión 2009<br>TRD versión 2010<br>TRD versión 2012<br>TRD versión 2019<br>Política de tratamiento de datos personales |
| **Propósito:** | |

Proteger adecuadamente la información incluida en la mensajería electrónica.

**Lineamientos Generales:**

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá implementar controles para el direccionamiento y transporte correcto del mensaje, así como la confiabilidad y disponibilidad del servicio.
- ✓ La Dirección de Información y Tecnología otorgará la aprobación a los colaboradores o terceros que requieran usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información, estos serán monitoreados y revocados en caso de ser necesario.

| **Control SGSI-A.13.2.4** | |
|---|---|
| **Acuerdos de confidencialidad o de no divulgación:** | **CONTROLES RELACIONADOS**<br>SGSI-A.18.1 Cumplimiento de requisitos legales y contractuales. |
| **Anexos:** | G7.ABS Guía de adquisición de bienes y servicios de calidad |

**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.

## 13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

| **Control SGSI-A.14.1.1** | |
|---|---|
| **Análisis y especificación de requisitos de seguridad de la información** | **CONTROLES RELACIONADOS**<br>SGSI-A.8.2 Clasificación de la información.<br>SGSI-A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.<br>SGSI-A.14.1.3 Protección de transacciones de los servicios de las aplicaciones (*Application Services*). |
| **Anexos:** | G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información.<br>G3.GTI Guía de estándares de especificación de requerimientos. |

**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.

| **Control SGSI-A.14.1.2 SGSI-A.14.1.3** | |
|---|---|
| **Seguridad de servicios de las aplicaciones en redes públicas**<br>**Protección de transacciones de los servicios de las aplicaciones** | **CONTROLES RELACIONADOS**<br>SGSI-A.10 Criptografía.<br>SGSI-A.18.1.5 Reglamentación de controles criptográficos. |
| **Anexos:** | N/A |

**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-A.14.2.1** | |
|---|---|
| **Política de desarrollo seguro:** | **CONTROLES RELACIONADOS** |
| | SGSI-A.14.2.7 Desarrollo contratado externamente. |
| **Anexos:** | 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-A.14.2.2 - SGSI-A.14.2.3 - SGSI-A.14.2.4** | |
|---|---|
| **Procedimientos de control de cambios en sistemas**<br>**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**<br>**Restricciones en los cambios a los paquetes de software** | **CONTROLES RELACIONADOS**<br>SGSI-A.12.1.1 Procedimiento de operación documentados.<br>SGSI-A.12.1.2 Gestión de cambios.<br>SGSI-A.12.6.1 Gestión de las vulnerabilidades técnicas.<br>SGSI-A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de la operación. |
| **Anexos:** | P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información. |

**Propósito:**

Dictar lineamientos que permitan establecer procedimientos y revisión de los cambios de las aplicaciones críticas del ICBF y desalentar los cambios en los paquetes de estos.

**Lineamientos Generales:**

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá definir controles para que los cambios de los Sistemas de Información en el ICBF sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá definir un proceso formal para el desarrollo, mantenimiento, inclusión y cambios importantes de los sistemas de información involucrando pruebas, control de calidad e implementación.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información en los entornos definidos para el desarrollo y mantenimiento del software y la Subdirección de Recursos Tecnológicos en los entornos de producción deberá definir para los cambios en los sistemas del ICBF los siguientes aspectos:
  - Niveles de autorización acordados.
  - Presentar los cambios a los usuarios autorizados.
  - Revisar la integridad para asegurar que no se vean comprometidos los cambios.
  - Identificar y validar el código para minimizar la posibilidad de existencia de vulnerabilidades conocidas.
  - Antes de cualquier cambio, asegurar que los usuarios autorizados aceptan los cambios.
  - Mantener un control de versiones para las actualizaciones de los sistemas.
  - Mantener un rastro de auditoria de los cambios.
  - Asegurar que los cambios se hagan en momentos adecuados y que no afecten los procesos del ICBF.

- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas de Integrados de Información deberá guardar en un repositorio, las versiones anteriores de cada sistema de información que es actualizado.
- ✓ La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información deberá definir la manera de revisar después de un cambio importante que el sistema de información alterado no se haya comprometido.
- ✓ 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-A.14.2.5 – SGSI-A.14.2.6** | |
|---|---|
| **Principios de construcción de sistemas seguros**<br>**Ambiente de desarrollo Seguro** | **CONTROLES RELACIONADOS**<br>SGSI-A.7.1.1 Selección. |
| **Anexos:** | P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información. |

**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-A.14.2.7** | |
|---|---|
| **Desarrollo contratado externamente** | **CONTROLES RELACIONADOS**<br>SGSI-A.14.2.1 Política de desarrollo seguro.<br>SGSI-A.18.1.2 Derecho de propiedad intelectual. |
| **Anexos:** | N/A |

**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-A.14.2.8 – SGSI-A.14.2.9** | |
|---|---|
| **Pruebas de seguridad de sistemas**<br>**Prueba de aceptación de sistemas** | **CONTROLES RELACIONADOS**<br>SGSI-14.1.1 Análisis y especificación de requisitos de Seguridad de la Información.<br>SGSI-14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.<br>SGSI-14.2.1 Política de desarrollo seguro. |
| **Anexos:** | N/A |
| **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-A.14.3.1** | |
|---|---|
| **Protección de datos de Prueba** | **CONTROLES RELACIONADOS** |
| | N/A |
| **Anexos:** | N/A |

**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.

## 14. RELACIÓN CON PROVEEDORES.

| **Control SGSI-A.15** | |
|---|---|
| **Política de seguridad de la información para las relaciones con proveedores**<br>**Tratamiento de la seguridad dentro de los acuerdos con proveedores**<br>**Cadena de suministro de tecnología de información y comunicación**<br>**Seguimiento y revisión de los servicios de los proveedores** | **CONTROLES RELACIONADOS**<br>SGSI-A.8.2 Clasificación de la información.<br>SGSI-A.17 Aspectos de seguridad de la información de la gestión de Continuidad de negocio. |

| | |
|---|---|
| **Gestión de cambios en los proveedores** | |
| **Anexos:** | G7.ABS Guía para la adquisición de bienes y servicios de calidad |

**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.

## 15. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

| **Control SGSI-A.16.1.1 – A.16.1.7** | |
|---|---|
| | **CONTROLES RELACIONADOS** |

| | |
|---|---|
| **Responsabilidad y procedimientos**<br>**Reporte de eventos de seguridad de la información**<br>**Reporte de debilidades de seguridad de la información**<br>**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**<br>**Respuesta a incidentes de seguridad de la información**<br>**Aprendizaje obtenido de los incidentes de seguridad de la información**<br>**Recolección de evidencia** | SGSI-A.5.1.2 Revisión de políticas para la seguridad de la información. |
| **Anexos:** | P5.GTI Procedimiento gestión de incidentes de seguridad de la información.<br>F1.P5.GTI Formato informe incidente de seguridad de la información.<br>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. |

## 16. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.

| **Control SGSI A.17.1.1** | |
|---|---|
| **Planificación de la continuidad de la seguridad de la información** | **CONTROLES RELACIONADOS**<br>N/A |
| **Anexos:** | PL9.GTI Plan de recuperación de desastres tecnológicos |
| **Propósito:**<br>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.<br><br>**Lineamientos Generales:**<br>✓ 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. | |

| **Control SGSI-A.17.1.2** | |
|---|---|
| **Implementación de la continuidad de la seguridad de la información** | **CONTROLES RELACIONADOS**<br>SGSI-17.1.1 Planificación de la Continuidad de la Seguridad de la Información |
| **Anexos:** | P4.GTI Procedimiento gestión de cambios de tecnologías de la información<br>F1.P4.GTI Formato requerimiento de cambios informáticos-RFC<br>G8.GTI Guía Respaldo y restauración de copias de seguridad<br>PL9.GTI Plan de recuperación de desastres tecnológicos<br>F1.PL9.GTI Formato plan de pruebas del plan de recuperación de desastres tecnológicos<br>F2.PL9.GTI Formato Rresultado ejecución del plan de recuperación de desastres tecnológicos<br>F3.PL9.GTI Formato cronograma de pruebas plan de recuperación de desastres tecnológicos<br>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<br>F6.PL9.GTI Formato requisitos de seguridad de la información |
| Esta política pretende 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.<br><br>**Lineamientos Generales:**<br>✓ Se deberán conformar los equipos de respuesta ante incidentes de seguridad de la información.<br>✓ 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.<br>✓ 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.<br>✓ 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. | |

| **Control SGSI-A.17.1.3** | |
|---|---|
| **Verificación, revisión y evaluación de la continuidad de la seguridad de la información** | **CONTROLES RELACIONADOS**<br>N/A |
| **Anexos:** | F1.P4.GTI Formato requerimiento de cambios informáticos-RFC<br>P18.DE Plan de continuidad de la operación<br>PL9.GTI Plan de recuperación de desastres tecnológicos<br>F1.PL9.GTI Formato plan de pruebas del plan de recuperación de desastres tecnológicos<br>F2.PL9.GTI Formato resultado ejecución del plan de recuperación de desastres tecnológicos<br>F3.PL9.GTI Formato cronograma de pruebas plan de recuperación de desastres tecnológicos<br>F4.PL9.GTI Formato bitácora de actividades del plan de recuperación de desastres tecnológicos<br>F5.PL9.GTI Formato árbol de comunicaciones plan de recuperación de desastres tecnológicos<br>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 verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Se deberá verificar que las pruebas realizadas sean consistentes con el alcance y el objetivo del Plan de recuperación de desastres tecnológicos y minimicen la interrupción de las operaciones.

**Lineamientos Generales:**

- ✓ Se debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
- ✓ Para el Plan de recuperación de desastres se deberá establecer un programa de pruebas, teniendo en cuenta los requerimientos técnicos necesarios. Las pruebas deberán ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación.
- ✓ Se deben documentar las pruebas y se deben generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan.
- ✓ Se deberá contar con planes de contingencia de los servicios de tecnología.
- ✓ Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que los planes de recuperación de desastres tecnológicos se mantengan actualizados.
- ✓ La Dirección de Información y Tecnología deberá revisar y aprobar el plan de recuperación de desastres tecnológicos.

| **Control SGSI A.17.2.1** | |
|---|---|
| **Disponibilidad de instalaciones de procesamiento de información** | **CONTROLES RELACIONADOS** |
| | N/A |
| Anexos: | PL9.GTI Plan de recuperación de desastres tecnológicos |

**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.

## 17. CUMPLIMIENTO

| **Control SGSI-A.18.1.1** | |
|---|---|
| **Identificación de la legislación aplicable y de los requisitos contractuales** | **CONTROLES RELACIONADOS**<br>N/A |
| **Anexos:** | P4.MI Procedimiento identificación y evaluación de requisitos legales.<br>IT1.P4.MI Instructivo matriz de verificación de requisitos legales. |

**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-A.18.1.2** | |
|---|---|
| **Derechos de propiedad Intelectual:** | **CONTROLES RELACIONADOS**<br>N/A |
| **Anexos:** | N/A |

**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.

| **Control SGSI A.18.1. 3 - SGSI A.18.1.5** | |
|---|---|
| **Protección de Registros**<br>**Reglamentación de controles criptográficos** | **CONTROLES RELACIONADOS**<br>N/A |
| **Anexos:** | N/A |

**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.

| **Control SGSI A.18.1.4** | |
|---|---|
| **Privacidad y protección de información de datos personales** | **CONTROLES RELACIONADOS**<br>P15.GTI Procedimiento para la consulta, actualización, revocación y supresión de datos personales<br>P14.GTI Procedimiento para el intercambio o suministro de información |
| **Anexos:** | Política de Tratamiento de Datos Personales |

**Propósito:**

Dictar lineamientos para cumplir con la protección de datos personales.

**Lineamientos Generales:**

| |
|---|
| La Dirección de Planeación y Control de Gestión con el apoyo de la Dirección de Información y Tecnología y la Oficina Asesora Jurídica, deberá definir una política de tratamiento de datos personales, para la protección de los derechos fundamentales en su tratamiento. |

| **Control SGSI A.18.2** | |
|---|---|
| **Revisión independiente de la seguridad de la información**<br>**Cumplimiento con las políticas y normas de seguridad**<br>**Revisión del cumplimiento técnico** | **CONTROLES RELACIONADOS**<br>SGSI-5.1.1 Políticas para la seguridad de la información.<br>SGSI-12.4 Registro y Seguimiento. |
| **Anexos:** | P2. El Procedimiento auditorías internas SIGE |

**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.

## 18. CONTROL DE CAMBIOS

| Fecha | Versión | Descripción del Cambio |
|---|---|---|
| 21/05/2020 | Versión 9 | Se ajusto la Introducción, se incluyó la definición de G58<br>Se ajustaron los siguientes controles:<br>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, |

| Fecha | Versión | Descripción del Cambio |
|---|---|---|
| | | 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:<br>Se actualizó la Introducción adicionando normatividades.<br>Se incluyeron nuevos términos.<br>Se ajustaron las Partes Interesadas.<br>Se actualizó la evaluación del desempeño.<br>Se cambió la palabra Continuidad del Negocio por Continuidad de la Operación.<br>Se ajustaron los siguientes controles:<br>A.7.1.2 Términos y condiciones del empleo<br>A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información<br>A.7.3.1 Terminación o cambio de responsabilidades de empleo<br>A.8.2.2 Etiquetado de la Información<br>A.8.2.3 Manejo de activos<br>A.8.3.1 Gestión de Medios removibles<br>8.3.2 Disposición de los Medios<br>A.9.2.1 Registro y cancelación del registro de usuarios<br>A.9.2.2 Suministro de acceso de usuarios<br>A.9.3.1 – A.9.4.3 Uso de información secreta para la autenticación y Sistema de gestión de contraseñas<br>A.9.4.2 Procedimiento de ingreso seguro<br>A.9.4.5 Control de acceso a códigos fuente de programas<br>A.11.1.2 Controles de acceso físicos<br>A.11.1.3 Seguridad de oficinas, recintos e instalaciones<br>A.13.1 Gestión de la Seguridad de las redes<br>A.13.1.1 Controles de redes<br>A.13.1.2 Seguridad de servicios de las aplicaciones en redes públicas<br>A.13.1.3 Protección de transacciones de los servicios de las aplicaciones<br>A.13.2.3 Mensajería electrónica<br>A.14.1.1 Análisis y especificación de requisitos de seguridad de la información<br>A.17.1.1 Planificación de la Continuidad de la Seguridad de la Información<br>A.17.1.2 Implementación de la Continuidad de la Seguridad de la Información<br>A.17.1.3 Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información<br>A.17.2.1 Disponibilidad de instalaciones de procesamiento de información |
| 17/08/2018 | Versión 7 | Se realizaron las siguientes modificaciones:<br>- Actualización de las Partes Interesadas<br>- 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:<br>-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.<br>- 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).<br>Se incluyó el punto 3. Partes interesadas.<br>Se ajustaron las siguientes políticas de acuerdo con la operación:<br>A.6.2.1 Política para dispositivos móviles<br>Teletrabajo<br>A.9.2.6 Retiro o ajuste de los derechos de acceso<br>A.8.1.3 Uso aceptable de los activos<br>A.8.1.4 Devolución de ActivosA.11.1.4 Protección contra amenazas externas y ambientales |

| Fecha | Versión | Descripción del Cambio |
|---|---|---|
| | | A.11.1.4 Protección contra amenazas externas y ambientales<br>A.13.1.1 Controles de redes<br>A.13.1.2 Seguridad de servicios de las aplicaciones en redes públicas<br>A.13.1.3 Protección de transacciones de los servicios de las aplicaciones<br>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.<br>A.6.2.1 Política para dispositivos móviles, se actualizaron lineamientos.<br>A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información, se actualizaron lineamientos generales.<br>A.9.2.2 Suministro de acceso de usuarios, se actualizaron lineamientos generales.<br>A.9.4.2 Procedimiento de ingreso seguro, se actualizaron lineamientos generales.<br>A.9.4.5 Control de acceso a códigos fuente de programas, se actualizo el anexo.<br>A.11.2.5 Retiro de activos, se actualizo el anexo.<br>A.11.2.7 Disposición segura o reutilización de equipos, se actualizo el anexo.<br>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. |
| 06/09/2016 | Versión 1 | Elaboración del manual |