Abecé del Sistema de Gestión de Seguridad de la Información

Abril de 2025 - Diseño por la DIT

Este es el abecé del Sistema de Gestión de Seguridad de la Información; su contenido presenta aspectos básicos con conceptos generales y está reglamentado bajo la normatividad vigente para el cumplimiento y la aplicabilidad de las políticas de seguridad de la información en el **Bienestar Familiar.**

Eje de Seguridad de la Información

Su propósito es salvaguardar la confidencialidad, integridad y disponibilidad de la información, aplicando la mejora continua y los controles adecuados en los entornos donde es tratada, gestionada, administrada y custodiada, sí como la continuidad de la operación del Bienestar Familiar, promoviendo con ello la gestión del conocimiento institucional con base en la norma **ISO/IEC 27001:2022**

¿Qué es la seguridad de la información?

Es un conjunto de medidas y buenas prácticas que protegen la información del Bienestar Familiar, asegurando su confidencialidad, integridad y disponibilidad.

¿Por qué es importante?

Evita fraudes, pérdida de información y filtraciones.

Garantiza el cumplimiento normativo ISO 27001:2022.

BIENESTAR FAMILIAR

Protege la reputación del Bienestar Familiar.

Previene incidentes de seguridad.

Política General SGSI

Sistema de Gestión de Seguridad de la Información

El ICBF protege, preserva y administra la integridad, confidencialidad, disponibilidad de la información, así como la ciberseguridad y la gestión de la continuidad de la operación, conforme al mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios.

Así mismo, la entidad previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, ciberseguridad y continuidad del negocio, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con el fin de prestar servicios con calidad y transparencia, partiendo de las necesidades y expectativas de las partes interesadas (stakeholders), promoviendo la protección integral de los derechos de los niños, niñas, adolescentes, familias y colaboradores del ICBF.

Consulta nuestra resolución por la cual se adopta la ***«Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación»***, las ***«Políticas generales de manejo»*** y se definen lineamientos frente al uso y manejo de la información en el micrositio del Eje de Seguridad en la intranet ICBF.

https://intranet.icbf.gov.co/sistema-integrado-de-gestion/eje-seguridad-de-la-informacion

Sé nuestra primera línea de defensa y cumple con nuestros objetivos del Sistema de Gestión de Seguridad de la Información

1. Desarrollar e implementar **mecanismos de aseguramiento** para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información de la entidad, utilizando controles robustos.

2. **Mitigar los incidentes** relacionados con la seguridad y privacidad de la información, así como con la ciberseguridad, mediante la implementación de controles preventivos y correctivos y la adopción de medidas de respuesta de manera efectiva, eficaz y eficiente.

3. **Gestionar los riesgos relacionados con la seguridad y privacidad de la información, ciberseguridad y continuidad de la operación,** de acuerdo con los requisitos de la norma ISO 27001:2022, a través de la identificación, evaluación y tratamiento de riesgos, así como la implementación de controles adecuados para mitigar posibles amenazas y asegurar la resiliencia operativa de establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.

4. **Fortalecer las capacidades de cambio y cultura en seguridad de la información** entre las partes interesadas (stakeholders), mediante programas de capacitación, concienciación y la implementación de mejores prácticas en ciberseguridad y privacidad de la información.

5**. Establecer lineamientos** necesarios para el manejo de la información y los recursos tecnológicos del ICBF.

6. **Cumplir con los requisitos legales, reglamentarios y regulatorios**, así como con las normas técnicas colombianas en materia de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación. Esto incluye la implementación de políticas y procedimientos que aseguren la conformidad con las leyes y estándares aplicables, garantizando la protección de la información y la resiliencia operativa de la entidad.

¿Cómo proteger la seguridad y privacidad de la información?

Aplicando estos principios fundamentales lo lograrás...

1. **Confidencialidad:** se refiere a la protección de la información de ser revelada a personas no autorizadas. Por ejemplo, la información de identificación personal, como los números telefónicos, direcciones de residencia o los números de tarjetas de crédito, es información confidencial que no debe ser compartida con cualquier persona que no tenga autorización para acceder a ella.

2. **Integridad:** se refiere a la protección de la información; no debe ser alterada por personas no autorizadas. Por ejemplo, una persona no autorizada puede modificar un registro de un sistema de información, causando daños a la integridad del archivo y posiblemente causando pérdida de datos.

3. **Disponibilidad:** la disponibilidad se refiere a la capacidad de los usuarios autorizados de acceder a la información cuando lo necesiten. Por ejemplo, si el portal web está bajo un ciberataque, los usuarios no podrán acceder al sitio web y la información no estará disponible.

Buenas prácticas para todos

Cuando se habla de mejores prácticas debemos tener en cuenta algunos aspectos fundamentales que es necesario conocer para poder ser aplicadas en nuestro día a día.

Protección de la confidencialidad

1. **Contraseñas seguras** usa contraseñas fuertes y cámbialas regularmente. No compartas tus contraseñas con nadie.

2. **Bloquea tu equipo** cuando te ausentes de tu puesto de trabajo.

3. **Evita divulgar información** sensible o datos personales.

4. **No compartas tu correo institucional** en páginas de comercio, foros, entidades bancarias o para asuntos personales.

5. **La actualización de software y sistemas operativos** es esencial para mantener la seguridad de los sistemas informáticos, para corregir las vulnerabilidades y errores conocidos en el software.

6. **Accede a la información que necesitas** para tu trabajo. No intentes acceder a datos que no te corresponden.

7. **Protección contra amenazas:** implementar controles para proteger la información contra accesos no autorizados, alteraciones y destrucción.
   Actualmente existen muchas amenazas y vulnerabilidades en nuestro entorno digital por lo que se han implementado varios controles que, con tu ayuda, aportan al fortalecimiento de la seguridad y privacidad de la información.

8. **Doble factor:** la autenticación de dos factores es una medida de seguridad adicional que requiere que los usuarios proporcionen una segunda forma de autenticación además de la contraseña, como un código de seguridad enviado a un teléfono móvil.

9. **Administración de usuarios y permisos:** gestiona de manera controlada y segura el acceso a la información, garantizando que cada colaborador u operador disponga únicamente de los permisos necesarios para realizar sus actividades o funciones.

10. **Antivirus:** es una herramienta esencial que analiza, identifica y neutraliza código malicioso que podría comprometer la seguridad de la información.

11. **Respaldo y recuperación:** asegurar que, en caso de pérdida, daño o incidente, la información pueda ser restaurada de manera eficiente.

12. **Planes de contingencia:** contar con planes de contingencia de los servicios garantiza que en caso de algún evento o interrupción, se pueda dar continuidad a la operación.

Protección de la integridad

1. **No alteres, registros, datos e información sin autorización.**

2. **Verifica siempre la fuente de la información** antes de usarla.

3. **No instales software no autorizado** en el equipo.

4. **Clasifica y etiqueta la información** (Pública, Clasificada y Reservada).

Protección de la dispónibilidad

1. **Almacena la información en OneDrive y SharePoint**, no en el disco de tu computador, medios extraíbles o correos personales.
2. **No abras o descargues archivos** o enlaces de correos desconocidos o sospechosos.
3. **Usa redes seguras**, evitando conectarte a WIFI públicas desconocidas.
4. **Cierra sesión en sistemas de información, correos, VPN, etc.** cuando termines de usarlos.
5. **Aprende a identificar amenazas de ataques de ingeniería social.**
6. **Reporta cualquier evento** relacionado a la afectación de la confidencialidad, disponibilidad e integridad de la información.

Roles y responsabilidades:

Liderar y gestionar los riesgos de seguridad de la información que afecten el proceso.

Propender porque los colaboradores cumplan con las políticas y lineamientos de seguridad de la información.

Promover para que se realicen actividades de formación en temas de SGSI en sus procesos o áreas.

Atender todos los requisitos de seguridad de la información.

Identificar y comunicar los requisitos y necesidades de seguridad de la información.

Reportar los incidentes de seguridad de la información o incumplimientos de políticas de seguridad de la información.

Los roles y responsabilidades del Eje de Seguridad de la Información se encuentran enmarcados en las resoluciones ***11980 de 2019 y 6659 del 2020,*** por las cuales se adopta el modelo de Planeación y Sistema Integrado de Gestión del ICBF.

Resolución 11980 de 2019:

https://www.icbf.gov.co/system/files/resolucion_11980_de_dic_de_2019_-_adopta_modelo_de_planeacion_y_sistema_integrado_de_gestion_del_icbf_0.pdf

Resolución 6659 del 2020:

https://www.icbf.gov.co/system/files/resolucion_6659_de_dic_2020-_modifica_modelo_de_planeacion_y_sistema_integrado_de_gestion_1.pdf

Activos SGSI:

En el contexto de seguridad digital son elementos tales como **aplicaciones de la organización**, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Utiliza la «Guía para la clasificación y etiquetado de la información para proteger la privacidad y seguridad de la información»

Presenta la metodología para realizar el clasificado y etiquetado de la información física y digital producida por los procesos, colaboradores, pasantes, judicantes y terceros del Instituto Colombiano de Bienestar Familiar, con el fin de aplicar los niveles adecuados de protección de acuerdo con la clasificación interna del instituto, dando cumplimiento a la *Ley 1712 de 2014, Ley 1581 de 2012 y la norma ISO/ IEC 27001- Clasificación de la Información.*

Pública

Es información que puede ser divulgada sin ningún tipo de restricción.

Clasificada

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.

Reservada

Es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712/2014.

Protección de datos personales

¿Sabes qué son los datos personales?

Consiste en toda información de una persona que permite su identificación. Por ejemplo: su identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, formación académica, experiencia laboral, o profesional.

Tipos de datos personales

Sensibles:
Datos que afectan la intimidad de las personas o cuyo uso indebido puede generar discriminación.
(Ej.: origen racial, convicciones filosóficas o religiosas, videos, fotografías, salud).

Semiprivados:
Datos que son de carácter privado, no tienen naturaleza íntima, reservada, que solamente le interesan al titular y a un grupo determinado de personas.
(Ej.: datos financieros, crediticios).

Privados:
Datos que son, por su naturaleza íntima o reservada, relevantes solamente para el titular de la información.
(Ej.: fotografías, videos, datos relacionados con su estilo de vida) .

Públicos:
son todos aquellos datos que conciernen a un interés general. Son los que la Constitución y la ley determinen como tales.
(Ej.: nombre, cédula, estado civil, sentencias judiciales).

Riesgos y oportunidades

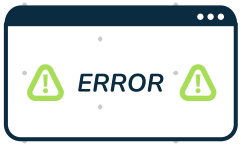
¿Qué son los riesgos en seguridad de la información?

Los riesgos son eventos que pueden afectar la confidencialidad, integridad y disponibilidad de la información del Bienestar Familiar, generando impactos negativos como:

Filtraciones o pérdidas de datos personales o sensibles.

Accesos no autorizados.

Alteración o corrupción de información.



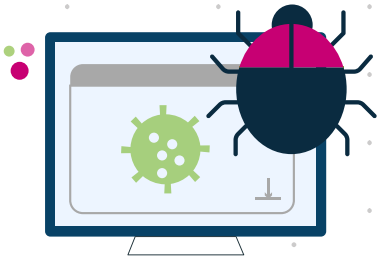
Indisponibilidad de servicios o aplicativos misionales.

Pérdida de confianza y sanciones legales.

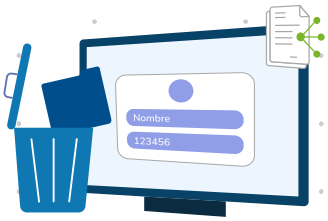
Ejemplos de riesgos de seguridad de la información

Phishing:
Correos falsos que buscan engañar a los colaboradores del ICBF para robar información.

Vishing:
Llamadas telefónicas con el fin de capturar información sensible o financiera para luego proceder a fraudes.



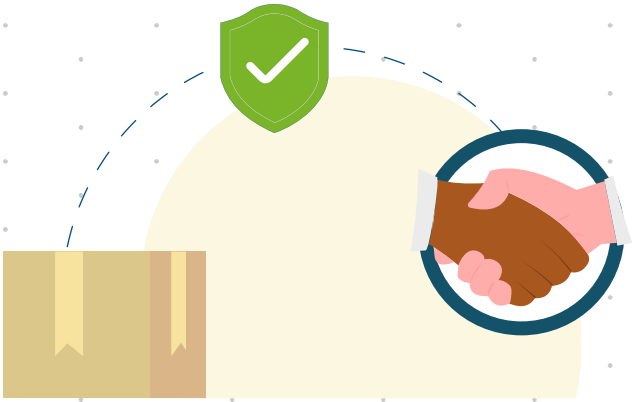
Malware o ramsonware:
Software malicioso que puede bloquear, secuestrar o robar información sensible o datos personales.



Errores humanos:
Eliminación accidental de información, uso de contraseñas; compartir información de la entidad sin autorización.

Ataques cibernéticos:
intentos de ciberdelincuentes por vulnerar los servicios o sistemas de información de la entidad.

Uso indebido de información:
acceso, modificación o eliminación de datos sin autorización.



Gestión de seguridad con proveedores

Los requisitos de seguridad de la información deben ser acordados con el proveedor antes de firmar los contratos y deben quedar documentados.

¿Sabías que en la «Guía para la adquisición de bienes y servicios de calidad» están consignadas las obligaciones contractuales del Eje de Seguridad de la Información?

Conoce las obligaciones contractuales que, conforme al objeto contractual de cada proveedor operador o tercero, deben cumplir y que están establecidas en su contrato.

1. **Certificar el cumplimiento, seguimiento y revisión** de los asuntos correspondientes a seguridad de la información, enmarcado en la normativa interna del ICBF vigente durante la ejecución del contrato.

2. Suscribir un documento de **compromiso de confidencialidad** con el representante legal, el cual deberá ser entregado al supervisor una vez se firme el contrato o convenio.

3. Suscribir un documento de **autorización de tratamiento de datos personales** con el representante legal, el cual deberá ser entregado al supervisor una vez se firme el contrato.

4. **Informar al supervisor,** en el momento que ocurran incidentes de seguridad o se materialice un riesgo de seguridad de la información que afecte la disponibilidad, integridad o confidencialidad de la información del ICBF, en el marco de la ejecución del objeto establecido.

5. **Certificar el cumplimiento de la cadena de suministro TIC**, de acuerdo

con lo establecido en la Política de la Seguridad de la Información del ICBF.

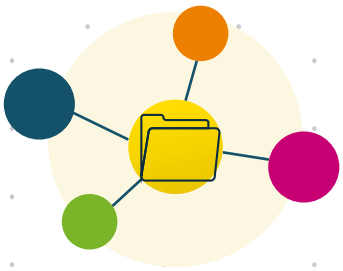
5 **Prever el plan de recuperación y contingencia** del servicio contratado ante los eventos que puedan afectar el cumplimiento de la ejecución de este.

6 **Cumplir con lo establecido en la G22.GT** «Guía para el uso de dispositivos personales -BYOD»- cuando se requiera conexión de equipos que no son propiedad de ICBF a la red institucional.

7

8 **Identificar, documentar y evaluar los riesgos de seguridad** de la información relacionados con los procesos, sistemas y servicios que estén dentro del alcance de objeto contractual, conforme a las mejores prácticas internacionales, tales como las establecidas en la norma ISO/IEC 27001:2022 o su equivalente, alineadas con la Política de Seguridad de la información definidas con el operador de servicios de tecnología.

Guía BYOD



Protección de la información compartida con proveedores, operadores y terceros.

1 Los sitios compartidos con los proveedores o terceros se deben restringir solo a la información necesaria.

2 Los proveedores deben sensibilizarse en los controles establecidos en la «Política de seguridad y privacidad, ciberseguridad y continuidad de la operación y buenas prácticas».

3 Los proveedores deben cumplir los lineamientos y controles del Sistema de Gestión de Seguridad de la Información.

4 Los incidentes asociados a la gestión de seguridad de la información en los que se tenga alguna afectación en la confidencialidad, disponibilidad e integridad de la información de Bienestar Familiar, se deben reportar al supervisor del contrato, quien será el encargado de seguir con los lineamientos estipulados en el procedimiento.

Aplica a dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información; son utilizados por servidores públicos, pasantes, practicantes, contratistas de prestación de servicios profesionales y de apoyo a la gestión para el ejercicio de sus funciones u obligaciones en el ICBF en la Sede de la Dirección General, regionales, centros zonales y, si aplica, a CAIVAS, CESPAS, CAVIF, SRPA, casas de Justicia y unidades locales.

¿Cómo reportar un incidente asociado a la gestión de seguridad de la información?

Un incidente de seguridad de la información es aquel que afecta la integridad, confidencialidad o disponibilidad de la información.

Si identificas un incidente de seguridad de la información:

Canales para reportar los incidentes:

MIS WEB y ChatBot MISI

No tomes decisiones sin consultar.

Reporta de inmediato el incidente a través de los canales de atención de Bienestar Familiar.

Realiza capturas de pantalla o registra información relevante.

No compartas información del incidente con terceros.

Apóyanos en la investigación.

A través de estos medios podrás registrar sus solicitudes las 24 horas al día de lunes a domingo.

Horario de Mesa de Servicio:
Lunes a viernes de 7:00 a. m. a 7:00 p. m.

Otros canales disponibles:

MIS WEB: **https//mis.icbf.gov.co/login**

Extensión: **8080 dentro del ICBF**

Línea gratuita: **018000112880**

Línea en Bogotá: **6017666755**

Correo electrónico: **mis@icbf.gov.co**

Conoce el micrositio SGSI

Espacio donde podrás encontrar:
- Documentos SGSI
- Material de apoyo
- Gestiones
- Miércoles de seguridad

Plan de Continuidad de la Operación

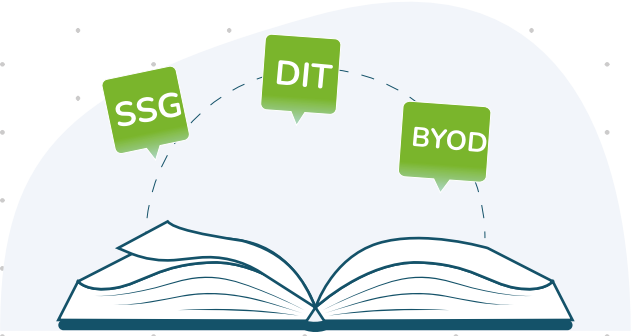
Clic aquí: Intranet ICBF - Instituto Colombiano de Bienestar Familiar ICBF

Definir las actividades a implementar ante un incidente, desastre natural, crisis de emergencias, situación de orden público u otros eventos inesperados que interrumpan la ejecución de la operación de los procesos que prestan los servicios críticos misionales de la entidad.

Plan de Recuperación de Desastres

El Plan de Recuperación de Desastres (DRP) es una estrategia documentada y probada que comprende una serie de actividades que le permiten al Instituto Colombiano de Bienestar Familiar prepararse y responder ante posibles eventos de desastres inesperados y recuperarse a través del restablecimiento de los servicios críticos misionales frente a situaciones de emergencia.

Información:
Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas,



Glosario

cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Política:
Controles que describen la posición de la entidad sobre un tema específico.

Activo:
Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (software, hardware, servicio, recurso humano, soporte, etc.) que tienen un valor para la entidad.

Activo crítico:
Instalaciones, sistemas y equipos los cuales, si son destruidos o no se encuentran disponibles, afectarán el cumplimiento de los objetivos misionales del 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 de forma periódica.

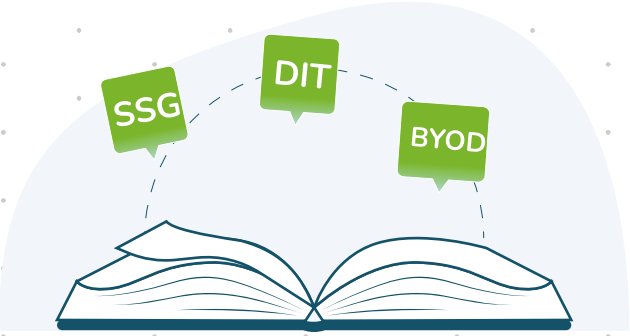
Amenaza:
Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la entidad.

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).

Evaluación de riesgos:
Es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento, la probabilidad de que



Glosario

ocurran y su potencial impacto en la operación de la entidad.

Incidente de seguridad:
Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Medio removible:
Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador 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 Servicios 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.

Partes interesadas (stakeholders):
Corresponden a las personas naturales o jurídicas con la cuales se 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).

Requisitos de seguridad de la información:
Se identifican mediante una evaluación metódica de los riesgos de seguridad.

BYOD:
Bring Your Own Device (BYOD)- Trae tu propio dispositivo.