

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 1 de 16

INTRODUCCIÓN

La Seguridad y la Privacidad de la Información constituyen un pilar estratégico para el Instituto Colombiano de Bienestar Familiar (ICBF), en la medida en que garantizan la protección de la confidencialidad, integridad y disponibilidad de la información que soporta el cumplimiento de su misión institucional, el desarrollo de sus procesos.

En el contexto actual, caracterizado por una alta dependencia de los activos de información y por la adopción acelerada de tecnologías emergentes como la computación en la nube, la inteligencia artificial, el Internet de las Cosas (IoT) y el trabajo colaborativo, las amenazas y vulnerabilidades asociadas a la seguridad y privacidad de la información se incrementan y evolucionan de manera constante. En este escenario, el factor humano se reconoce como uno de los elementos más críticos, dado que el desconocimiento, la omisión o el incumplimiento de los lineamientos, políticas y controles establecidos pueden derivar en incidentes de seguridad, fuga de información, afectaciones a la continuidad del servicio, incumplimientos normativos y riesgos reputacionales para la Entidad.

La Entidad adopta el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información como una herramienta que busca fortalecer el conocimiento, la apropiación y la responsabilidad de todos los colaboradores, contratistas, operadores y partes interesadas en el cuidado de la información.

Este Plan reúne acciones de sensibilización, capacitación, comunicación y seguimiento que permiten orientar a las personas sobre cómo proteger la información en el desarrollo de sus actividades diarias. Información sean entendidas como una responsabilidad compartida y un habilitador fundamental para el logro de los objetivos institucionales.

1. OBJETIVO

Establecer lineamientos claros para la socialización y divulgación de los temas asociados al Sistema de Gestión de Seguridad de la Información, con el propósito de fortalecer la cultura de seguridad y privacidad de la información entre los colaboradores del ICBF, mediante el uso de herramientas que faciliten la apropiación y aplicación de buenas prácticas en seguridad, ciberseguridad y privacidad de la información.

1.1. Objetivos Específicos

- Gestionar la cultura y apropiación de la Seguridad de la Información en el ICBF mediante estrategias de divulgación y formación dirigidas a los colaboradores en temas de seguridad de la información y buenas prácticas. Esto con el fin de cumplir con las políticas de seguridad, ciberseguridad y privacidad de la información de la Entidad, el modelo de seguridad y privacidad de la información del MINTIC y la normativa vigente.

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 2 de 16

- Realizar campañas de sensibilización a través de canales de comunicación y herramientas efectivas, para que los colaboradores de la Sede de la Dirección General, Regionales, Centros Zonales y Operadores puedan fortalecer sus conocimientos en seguridad y privacidad de la información.
- Aplicar buenas prácticas para fomentar el cambio y la cultura de Seguridad de la Información de manera didáctica, facilitando a los colaboradores un mayor nivel de apropiación.
- Realizar campañas para la apropiación y uso de herramientas tecnológicas, permitiendo a los colaboradores de la Sede de la Dirección General, Regionales y Centros Zonales gestionar los archivos de información, evitando su exposición y asegurando la confidencialidad, integridad y disponibilidad de la información.
- Utilizar medios tecnológicos para evaluar el nivel de apropiación adquirido por los colaboradores del ICBF a través de las campañas de sensibilización.
- Utilizar diversos medios publicitarios y de comunicación institucional para difundir temas de seguridad de la información.
- Crear una cultura que valore los principios de la Seguridad de la Información (confidencialidad, integridad y disponibilidad de la información) en la que todos los servidores públicos y contratistas del ICBF comprendan la importancia de dar un tratamiento adecuado en la protección de la información.

2. ALCANCE

El Plan inicia con promover la estrategia de miércoles de Seguridad y finaliza con atender los Incidentes de Seguridad y Privacidad de la Información o de Ciberseguridad.

Este plan aplica a nivel Sede Dirección General, Reginal y Zonal del ICBF.

3. DESARROLLO

3.1. Gobernanza Roles y Responsabilidades

Los roles en el marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información establecen las responsabilidades, niveles de participación y coordinación de los actores involucrados, con el fin de asegurar una gestión efectiva, coherente y articulada de actividades y estrategias de sensibilización, capacitación, comunicación y seguimiento. Esta gobernanza permite definir claramente quién planea, ejecuta, apoya, comunica y realiza seguimiento a las acciones del Plan, garantizando el liderazgo institucional, la rendición de cuentas y la mejora continua del Sistema de Gestión de Seguridad de la Información. Asimismo, facilita la toma de decisiones, el cumplimiento normativo y la apropiación de la seguridad y privacidad de la información como una responsabilidad compartida en todos los niveles de la Entidad.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 3 de 16

Tipo de Usuario	Objetivos de Conocimiento
Directores, subdirectores, jefes de Oficina y Coordinadores de Grupo y Coordinadores Zonales	Conocer, aplicar y promover las normas, políticas y directrices del Sistema de Gestión de Seguridad de la Información (SGSI), ejerciendo liderazgo y ejemplo en el cumplimiento de los controles de seguridad. Su rol implica impulsar la apropiación del SGSI y orientar adecuadamente las actuaciones del personal a su cargo, conforme a los principios de liderazgo y responsabilidad definidos por la ISO/IEC 27001: 2022
Colaboradores	Conocer y aplicar los controles y lineamientos establecidos por la Entidad en materia de seguridad y privacidad de la información, con el fin de proteger los activos de información y garantizar su confidencialidad, integridad y disponibilidad en el desarrollo de sus funciones.
Administradores de Sistemas	Conocer y aplicar las políticas de seguridad de la información implementadas por la Entidad, especialmente aquellos controles técnicos y operativos asociados a sus roles y responsabilidades, asegurando la protección de los sistemas de información y el cumplimiento de los requisitos del SGSI.
Administradores de infraestructura tecnológica y personal de soporte	Conocer y aplicar de manera integral las normas, políticas y procedimientos del SGSI para soportar de forma segura las operaciones críticas de la Entidad. Adicionalmente, deben estar en capacidad de orientar y apoyar el cumplimiento de estos lineamientos en los diferentes niveles de la organización.
Personal de Seguridad, Personal de Servicio Generales y conductores	Conocer y aplicar las políticas de seguridad de la información y las buenas prácticas asociadas, de acuerdo con el nivel de acceso y responsabilidad que tengan sobre la información y los activos de la Entidad.
Oficina Asesora de Comunicaciones	Conocer y aplicar los lineamientos, políticas y buenas prácticas del Sistema de Gestión de Seguridad de la Información (SGSI) para diseñar, coordinar y difundir campañas de sensibilización y comunicación relacionadas con seguridad y privacidad de la información. Debe garantizar que los mensajes sean claros, consistentes y lleguen de manera efectiva a todos los colaboradores, contratistas, operadores y partes interesadas, promoviendo la apropiación de la cultura de seguridad y fortaleciendo la confianza en la Entidad.
Oficina de Control Interno	Verificación del cumplimiento del SGSI, gestión de riesgos y controles.
Proveedores y/o Operadores	Conocer y comprender los lineamientos, principios y buenas prácticas en seguridad y privacidad de la información definidos por la Entidad, de acuerdo con el nivel de acceso e interacción que tengan con la información y los activos institucionales. Así mismo, promover comportamientos responsables y una cultura de protección de la información en el desarrollo de sus actividades, contribuyendo al fortalecimiento de la confianza y al cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información.
Partes Interesadas	Conocer y cumplir las directrices establecidas por la Entidad para el manejo, manipulación, uso y protección de la información, así como las obligaciones en materia de seguridad y privacidad de la información definidas contractualmente.

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

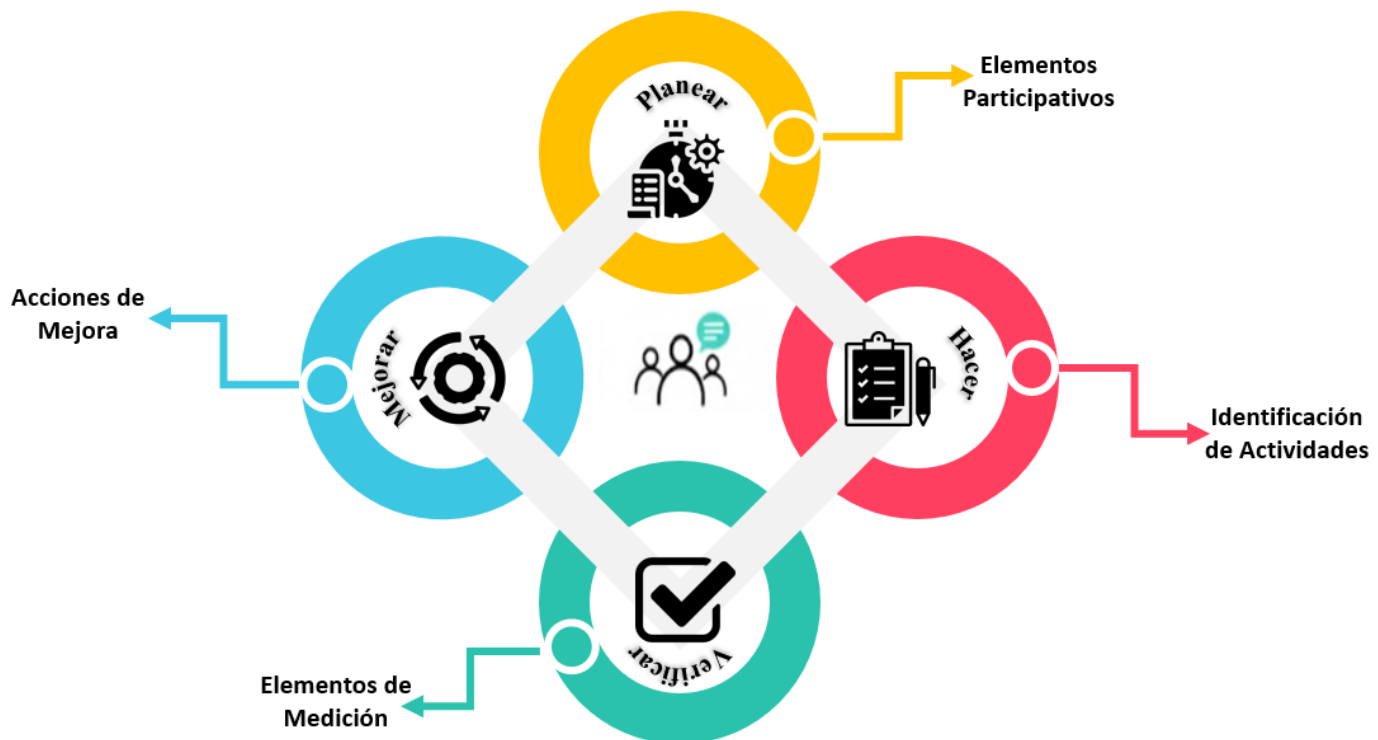
Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 4 de 16

3.2. METODOLOGÍA

La metodología utilizada para el desarrollo del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información se fundamenta en el ciclo PHVM (Planear, Hacer, Verificar y Mejorar), garantizando un enfoque sistemático, participativo y orientado a resultados. Este ciclo permite establecer acciones planificadas, ejecutarlas de manera efectiva, medir su impacto y realizar ajustes continuos para fortalecer la cultura de seguridad y privacidad en toda la Entidad

3.2.1. Gráfica PHVM- Plan de Cambio y Cultura de Seguridad y Privacidad



3.3. PLANEAR – Elementos Participativos

3.3.1. Equipo Rol y Responsabilidades

El equipo encargado de ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información está conformado por distintos actores, cada uno con funciones claras para asegurar la correcta implementación, seguimiento y apropiación de la cultura de seguridad y privacidad en toda la Entidad:

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 5 de 16

Rol	Responsabilidades
Gestor de Cambio y Cultura de Seguridad y Privacidad de la Información. (Profesional de la Dirección de Tecnologías de la Información - Seguridad de la Información)	Brindar orientaciones de ejecución, diseñar instrumentos de medición, desarrollar, dirigir, gestionar y realizar seguimiento a la ejecución del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.
Equipo de Apropiación (Profesionales de la Dirección de Tecnologías de la Información)	Apoyar en la creación de piezas gráficas, material de diseño etc. que se requiera dentro del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.
Ingenieros Regionales (Profesionales del Grupo de Planeación y Tecnología)	- Ejecutar y coordinar a nivel regional las actividades del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. - Aplicar los instrumentos de medición del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.
Equipo Promotor EPICO	- Ejecutar y coordinar en su proceso las actividades del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. - Aplicar los instrumentos de medición del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.
Equipo de Comunicaciones (Profesionales de la Oficina Asesora de Comunicaciones)	Apoyar en la aprobación, publicación y difusión de las actividades del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, en los diferentes medios de comunicación con los que cuenta el ICBF.

3.3.2 Medios y herramientas de comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información

Para la ejecución del **Plan de Cambio y Cultura de Seguridad y Privacidad de la Información**, se utilizarán diversos medios y herramientas de comunicación, con el fin de garantizar el alcance, la participación y la apropiación de los mensajes entre todos los usuarios internos y externos (colaboradores, contratistas, proveedores y operadores):

N°	Medios y Herramientas de Comunicación	Observaciones / Uso
1	Fondo de escritorio – Wallpaper	Refuerza mensajes de seguridad en el día a día del usuario.
2	Curso SIGE Teórico-Práctico Virtual	Capacitación formal en políticas y procedimientos del SGSI.
3	Micrositio SGSI	Repositorio central de recursos, guías, videos e infografías.
4	Engage – Red Social Institucional	Difusión de mensajes cortos, tips y recordatorios de seguridad.
5	Juegos / Gamificación	Actividades lúdicas para sensibilización y apropiación de buenas prácticas.
6	Charlas presenciales y virtuales	Sesiones interactivas con expertos en seguridad de la información.
7	Videos educativos	Contenidos audiovisuales sobre procedimientos y buenas prácticas.
8	Correo institucional – NoReply.DIT@icbf.gov.co	Difusión de comunicados oficiales, recordatorios y encuestas.
9	Formularios – Encuestas	Medición de conocimientos y nivel de apropiación de los usuarios.
10	Banner informativo e infografías	Refuerzo visual de mensajes clave en lugares estratégicos.
11	Herramienta colaborativa Teams	Espacio para sesiones de capacitación, reuniones y seguimiento de actividades.
12	Página Web institucional	Publicación de noticias, políticas y guías para todos los públicos.
13	Intranet	Acceso rápido a documentos, guías y recursos del SGSI.

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 6 de 16

N°	Medios y Herramientas de Comunicación	Observaciones / Uso
14	Redes Sociales Institucionales	Difusión externa e interna de campañas, buenas prácticas y eventos.
15	Pantalla de inicio de dominio	Mensajes estratégicos visibles al iniciar sesión en equipos corporativos.
16	Podcast	Contenidos de sensibilización, entrevistas y cápsulas de seguridad.
17	Boletines de la Entidad	Envío periódico de novedades, logros y alertas de seguridad.
18	Reuniones / talleres con proveedores y terceros	Difusión de políticas y seguimiento de compromisos de seguridad.
19	Material impreso (afiches, carteles)	Apoyo visual en oficinas, centros zonales y sedes regionales.

3.3.3 Eslogan: “Protección responsable, ciberseguridad resiliente”

3.3.4 Cronograma de Actividades para ejecutar dentro del marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2026.

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
1.	Promover la estrategia de miércoles de Seguridad	Gestión de usuarios Objetivo: Proveer directrices para gestionar y controlar el uso del software permitido en la Entidad, asegurando su adecuada implementación y uso.			Febrero 04,11,18 y 25	Mensual
		Uso responsable del correo electrónico Objetivo: Fomentar el uso adecuado y responsable del correo electrónico dentro de la Entidad, respetando las políticas y controles implementados			Marzo 4,11,18 y 25	Mensual
		La Seguridad en la Nube Objetivo: Implementar medidas de seguridad para proteger la información almacenada, procesada y controlada en entornos de nube			Abril 1,8,15,22,29	Mensual
		Gestión de Incidentes de Seguridad y Privacidad de la Información			Mayo 6,13,20,27	Mensual

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 7 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
		Objetivo: Desarrollar y aplicar un plan de gestión de incidentes para proteger la seguridad y privacidad de la información ante cualquier amenaza	Virtual	Correo Cartelera SGSI		
		Gestión de Contraseñas y Autenticación Multifactor Objetivo: Fortalecer las prácticas de creación, gestión y protección de contraseñas, así como promover el uso de autenticación multifactor para garantizar la seguridad de los accesos a sistemas y recursos de información.			Junio 3,10,17,24	Mensual
		Uso responsable del internet Objetivo: asegurar que las personas utilicen la red de forma segura, ética, consciente y productiva, protegiendo los activos de información			Julio 1,8,15,22,29	Mensual
		Clasificación y Etiquetado de la Información Objetivo: Establecer un sistema de clasificación y etiquetado de la información para garantizar su adecuada gestión y protección. Este proceso facilita identificar el nivel de sensibilidad y las medidas de seguridad necesarias para cada tipo de información, propendiendo su confidencialidad, integridad y disponibilidad.			Agosto 5,12,19,26	Mensual
		Seguridad en Dispositivos Móviles y Teletrabajo Objetivo: Brindar lineamientos para proteger la información en tablets, celulares y otros dispositivos de la Entidad, especialmente en escenarios de teletrabajo o trabajo remoto.			Septiembre 2,9,16,23,30	Mensual
		Control de Acceso Objetivo: Cumplir con los controles y buenas prácticas establecidas en los sistemas de información, servicios de tecnologías e infraestructura física, salvaguardando la integridad,			Octubre 7,14,21,28	Mensual

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 8 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
		disponibilidad y confidencialidad de los datos.				
		Ciberseguridad Objetivo: Establecer estrategias y medidas para proteger los sistemas y datos contra amenazas cibernéticas.			Noviembre 4,11,18,25	Mensual
		Uso seguro de la IA Fomentar una cultura organizacional donde el uso seguro y responsable de la Inteligencia Artificial sea parte de nuestros hábitos diarios, promoviendo la conciencia, el aprendizaje continuo y el compromiso colectivo para proteger la información y fortalecer la confianza en cada proceso			Diciembre 2,9,16,23,30	Mensual
2.	Celebrar el día Internacional de la Seguridad de la Información	Celebración del Día Internacional de la Seguridad de la Información Promover la concienciación y educación sobre la importancia de la seguridad de la información a través de la celebración del Día Internacional de la Seguridad de la Información. Este evento especial incluirá actividades lúdicas, juegos charlas o foros dirigidos a todos los colaboradores, para fomentar una cultura de seguridad y mantener a todos informados sobre las últimas amenazas y buenas prácticas	Virtual	Micrositio Wallpaper	27/11/2026	Anual
			Presencial	Charlas Concursos		

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 9 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
3.	Promover el Curso SIGE – Teórico Practico	Promover el Curso SIGE – Teórico Práctico Fomentar la participación en el Curso SIGE (Sistema Integrado de Gestión de la Entidad) – Teórico Práctico, dirigido a todos los colaboradores del ICBF. Este curso está diseñado para proporcionar una comprensión integral y práctica de las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información. A través de sesiones teóricas y ejercicios prácticos, los participantes adquirirán las habilidades necesarias para aplicar buenas prácticas en seguridad, ciberseguridad y privacidad de la información, contribuyendo así a la creación de una cultura de seguridad robusta dentro de la Entidad	Virtual	Escuela Virtual	30/06/2026 18/12/2026	Según convocatoria realizada por la Dirección de Gestión Humana
4.	Realizar Feria Épico	Apoyar y participar en este evento interactivo dedicado a la concienciación y educación sobre la seguridad de la información. Esta feria incluirá actividades prácticas, demostraciones en vivo, videos, juegos y charlas de expertos en seguridad, ciberseguridad y privacidad de la información. El propósito es fomentar una cultura de seguridad sólida entre los colaboradores del ICBF, proporcionando un entorno dinámico y atractivo para aprender y aplicar buenas prácticas en la protección de la información.	Virtual Presencial	Herramienta Teams Estrategias innovadoras enmarcadas en Seguridad de la información	30/11/2026	Anual

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 10 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
5.	Realizar charlas a Nivel Nacional	Organizar una serie de charlas a nivel nacional dirigidas a todos los colaboradores del ICBF. Estas charlas abordarán temas claves de seguridad, ciberseguridad y privacidad de la información, proporcionando conocimientos y herramientas prácticas para la protección de la información en la organización. Con la participación de expertos en la materia, estas charlas se llevarán a cabo en diferentes regionales y centros zonales, asegurando una cobertura amplia y efectiva de la concienciación a nivel país.	Presencial Virtual	Materiales Concursos Videos Presentaciones Herramienta para llevar el control de colaboradores que asisten a las charlas	30/04/2026 18/12/2026	Cuatrimestral
6.	Socializar en temas a la vanguardia de Seguridad de la información	Organizar sesiones de socialización y sensibilización sobre los temas más avanzados y actuales en el ámbito de la seguridad de la información. Estas sesiones incluirán discusiones sobre las últimas tendencias, tecnologías emergentes, nuevas amenazas y estrategias innovadoras para la protección de la información.	Virtual	Microsoft Teams	30/06/2026 18/12/2026	Semestral
7.	Realizar inducciones dirigidas al personal que ingresa a la Entidad	Llevar a cabo sesiones de inducción específicas para el personal que ingresa a la Entidad, con el fin de familiarizarlos con las políticas, procedimientos y buenas prácticas en seguridad de la información. Estas inducciones, tanto presenciales como virtuales, asegurarán que los nuevos colaboradores comprendan la importancia de proteger la información desde su primer día, promoviendo así una cultura de seguridad y privacidad.	Presencial Virtual	Presentaciones Videos	03/02/2026 27/11/2026	Según convocatoria realizada por la Dirección de Gestión Humana
8.	Utilizar el Micrositio SGSI	Micrositio SGSI en la Intranet del ICBF Este espacio digital está diseñado para proporcionar a los colaboradores acceso fácil y rápido a recursos, políticas, procedimientos y buenas prácticas en seguridad, ciberseguridad y privacidad de la información. Además, incluirá herramientas interactivas, noticias actualizadas, videos y piezas graficas facilitando así la concienciación y formación continua.	Micrositio	Intranet ICBF/Sistema Integrado de Gestión/Eje Seguridad de la Información	28/02/2026 21/12/2026	Permanente

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 11 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
9.	Organizar y preparar la mesa de comunicaciones SIGE	Mesa de Comunicaciones SIGE Establecer una Mesa de Comunicaciones SIGE (Sistema Integrado de Gestión de la Entidad) para diseñar estrategias de comunicación efectivas, gestionar la divulgación de información relevante, organizar eventos y campañas de sensibilización, y asegurar que todos los colaboradores del ICBF estén informados y comprometidos con las políticas y prácticas de seguridad de la información.	Presencial Virtual	Temas SIGE	03/03/2026 28/11/2026	Según convocatoria realizada por la Subdirección de Mejoramiento organizacional
10.	Realizar espacios con los Operadores o Terceros	Espacio para Compartir Piezas Gráficas SGSI con los Operadores o Terceros Crear un espacio para compartir piezas gráficas relacionadas con el Sistema de Gestión de Seguridad de la Información (SGSI) con los operadores y terceros. Este espacio permitirá la distribución de material educativo y de concienciación, como infografías, carteles y presentaciones, que refuercen las buenas prácticas en seguridad de la información, ciberseguridad y privacidad. Al facilitar el acceso a estos recursos, se promoverá una cultura de seguridad robusta y colaborativa entre las partes interesadas.	Virtual	Correo	30/06/2026 18/12/2026	Semestral
11.	Ejecutar pruebas de Ingeniería Social	Pruebas de Ingeniería Social Realizar pruebas de ingeniería social para evaluar la capacidad de los colaboradores del ICBF para evaluar la capacidad de reacción y respuesta ante ataques de ingeniería social. Estas pruebas incluirán simulaciones de correos electrónicos de phishing, llamadas telefónicas fraudulentas y otros escenarios comunes de ataques de ingeniería social. El propósito es identificar áreas de mejora y fortalecer la capacidad de los colaboradores para proteger la	Virtual Presencial	Correo y/o Telefonía	30/06/2026 18/12/2026	Semestral

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 12 de 16

N.º	Actividad	Descripción	Canal	Herramienta	Fecha de Ejecución	Frecuencia
		información y minimizar el riesgo de incidentes de seguridad.				
12.	Realizar encuestas de medición	Encuestas de Medición SGSI Realizar encuestas de medición para evaluar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) dentro del ICBF. Estas encuestas serán diseñadas para recolectar datos sobre el nivel de concienciación, cumplimiento de políticas, y percepción de los colaboradores y operadores respecto a las prácticas de seguridad de la información.	Virtual	Correo Cuestionario Forms	31/03/2026 18/12/2023	Semestral
13.	Atender incidentes de seguridad y privacidad de la Información o ciberseguridad	Realizar Piezas Gráficas con el fin de generar alertas y prevenir Incidentes o eventos de Seguridad y privacidad de la Información o ciberseguridad.	Virtual	Herramienta Correo- Redes Sociales	03/02/2026 31/12/2026	Cuando se requiera

3.4 HACER - Ejecución de Actividades

En esta fase se lleva a cabo la implementación del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, desarrollando las actividades planificadas a nivel nacional según el cronograma establecido. Cada actividad se ejecuta utilizando los medios, herramientas y canales de comunicación definidos, con el objetivo de garantizar la difusión, sensibilización y apropiación efectiva de los temas de seguridad y privacidad de la información entre todos los usuarios internos y externos (colaboradores, contratistas, proveedores y operadores). Durante esta fase se desarrollan y ejecutan a nivel nacional las actividades propuestas dentro del cronograma de actividades, cumpliendo con las fechas y frecuencias establecidas, utilizando las herramientas y medios necesarios para impartirlas y divulgarlas

Las evidencias de cumplimiento de las Regionales y Procesos del Plan de Cambio y Cultura de Seguridad y privacidad de la Información se verán reflejadas dentro del Plan Operativo SGSI.

3.5 VERIFICAR - Elementos de Medición

3.5.1 Medición del cumplimiento del plan

En esta fase se realiza el seguimiento al cumplimiento del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, verificando que las actividades se ejecuten según el cronograma y los responsables definidos. Se registran evidencias en el **Plan Operativo SGSI**, como asistencia, participación en cursos y resultados de encuestas, para evaluar la cobertura, efectividad y nivel de

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 13 de 16

apropiación. Esta información permite identificar oportunidades de mejora y fortalecer continuamente la cultura de seguridad y privacidad en la Entidad.

3.5.2 Medición de Conocimiento Adquirido

Para medir el nivel de apropiación adquirido por los colaboradores del ICBF en las directrices y buenas prácticas impartidas y aplicadas al plan de cambio y cultura de Seguridad y Privacidad de la Información, se realizan diferentes estrategias de apropiación a través de encuestas, actividades de Ingeniería social e incidentes presentados en las Regionales, Centros Zonales y Sede de la Dirección General.

Actividad	Frecuencia	Evidencia
Encuesta	Semestral	Informe Medición
Prueba Interna de Ingeniería Social	Semestral	Informe Medición
Incidentes SGSI	Mensual	Reportes Incidentes

3.6 ACTUAR – Oportunidades de Mejora

En esta fase se analizan los resultados obtenidos de los instrumentos de medición, las lecciones aprendidas de incidentes de seguridad de la información y los hallazgos de auditorías internas y externas. A partir de este análisis se identifican ajustes, cambios y oportunidades de mejora para fortalecer el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información en la próxima vigencia.

Actividad	Frecuencia	Evidencias	Estrategias
Registrar oportunidades de mejora en SVE	Anual	Seguimiento y monitoreo a las oportunidades de mejora cargadas en SVE	Plan de Implementación SGSI

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 14 de 16

4. ANEXOS

No aplica

5. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
17/02/2025	V8	Se actualizó la introducción y objetivos del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. En el ítem 3. Desarrollo, se actualizo el nombre como Gobernanza Roles y Responsabilidades En el ítem 3.3.2 Se actualizan los medios y herramientas de comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, se agrega Pantalla Inicio de Dominio. 3.3.3 Personaje del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información Se actualiza el Eslogan " Protección responsable, ciberseguridad resiliente" Se realizó la actualización del ítem 3.3.5 Cronograma de Actividades a ejecutar dentro del marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2026 Se actualizó el ítem 3.6 ACTUAR – Oportunidades de Mejora
22/03/2024	V7	Se actualizó la introducción y objetivos del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información En el ítem 3.3.2 Se actualizan los medios y herramientas de comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información se agrega Pantalla Inicio de Dominio 3.3.3 Personaje del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información Se actualiza el Eslogan ""El protagonista de Seguridad de la Información eres tú, soy yo, somos todos" Se realizó la actualización del ítem 3.3.5 Cronograma de Actividades a ejecutar dentro del marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2025 Se actualizó el ítem 3.6 ACTUAR – Oportunidades de Mejora
18/04/2022	V6	En el ítem 3.3.2 Medios y herramientas de comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información se agrega Pantalla Inicio de Dominio 3.3.3 Personaje del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información Se cambia el Eslogan ""El protagonista de Seguridad de la Información eres tú, soy yo, somos todos" 3.3.5 Cronograma de Actividades a ejecutar dentro del marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2024 Se actualiza los temas y fechas de miércoles de seguridad
02/03/2022	V5	Se adiciona en el ítem 1.1 Objetivos Específicos: Utilizar diferentes medios de comunicación institucionales con el objeto de realizar la difusión de temas de seguridad de la información Se ajusta el ítem 3.3.2 Medios y Herramientas de Comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, conforme a las herramientas de difusión que cuenta el eje de seguridad de la información para la vigencia 2023

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

Plan de Cambio y Cultura de Seguridad y Privacidad de la
Información

PL6.GTI

04/03/2026

Versión 9

Página 15 de 16

Fecha	Versión	Descripción del Cambio
		Se actualizan los temas y fechas de ejecución en el ítem 3.3.5 Cronograma de Actividades a ejecutar dentro del marco del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información para la vigencia 2023
04/01/2021	V4	En el punto 1 Objetivo, se modificó su redacción En el punto 1.1 Objetivos Específicos, Se agrega el siguiente objetivo específico "Crear una cultura respecto a los principios de la Seguridad de la Información; confidencialidad, integridad y disponibilidad de la información en donde todos los servidores públicos y contratistas del ICBF comprendan la importancia de dar un tratamiento adecuado a la información" En el punto 3.1 Usuarios y Necesidades se modifica redacción y se agregó el Tipo de Usuario Personal de Seguridad, Personal de Servicio Generales y conductores En el punto 3.2 Metodología, se modificó el gráfico PHVM (Planear, Hacer, Verificar y Mejorar). En el punto 3.3 Planear en el punto 3.3.1 Equipo inicial encargado del programa se agrega como responsable al Equipo Promotor Épico 3.3.2 Medios y herramientas de comunicación y difusión para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, se ajustan las herramientas de comunicación (Se agrega el correo institucional apropiacionDIT@icbf.gov.co y se agrega como medios y herramientas infografías En el punto 3.3.5. Cronograma de actividades a ejecutar dentro del Plan de Cambio y Cultura de Seguridad y privacidad de la Información: Este punto como se trata del cronograma se traslada a las actividades de Planear del Plan, Por sugerencia de la auditoría externa. Adicionalmente se incluyen (4) cuatro actividades • Espacio SGSI • Pruebas de Ingeniería Social • Encuestas • Incidentes. En el punto 3.4 se realizan ajustes para informar que dentro del plan operativo SGSI de la vigencia es donde se van a almacenar las evidencias del este. En el punto 3.5. Se realizan ajustes a la tabla de actividades de medición y se agrega una columna de Evidencia. En el punto 3.6 Se realizan ajustes a la tabla de lecciones aprendidas y se agrega una columna de evidencias
30/12/2019	V3	En el punto 1 Objetivo, se modificó el objetivo. En el punto 3.1 Objetivos Específicos, Se modificaron los objetivos específicos. Se adicionó el punto 3.2 Usuarios y Necesidades donde se hizo necesario ajustar la numeración a partir de este ítem. En el punto 3.2 que pasa a ser el punto 3.3 Metodología, se modificó la redacción, dado que el ciclo estaba en términos de PHVA y se alineó al ciclo definido en el ICBF- PHVM (Planear, Hacer, Verificar y Mejorar). En el punto 3.3.2 que pasa a ser el punto 3.4.2 Medios y herramientas de comunicación para el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, se ajustan las herramientas de comunicación (Se modifica protector de pantalla por Boletín ICBF, Pendones – Afiches por Podcast, Micrositio por Micrositio SGSI y se agregan Correo Seguridaddigital@icbf.gov.co; Correo NoReply.DIT@icbf.gov.co) y se elimina la tabla de premios. En el punto 3.3.4 que pasa a ser el 3.4.4 se modifica el eslogan para el eje de seguridad de la información: "El protagonista de la Política de Seguridad de la Información del ICBF es Usted" cambia por "El protagonista de Seguridad de la Información del ICBF eres tú". En el punto 3.4 que pasa a ser el punto 3.5 y se realizan ajustes en la tabla que contiene las actividades donde en el ítem 1 de "Miércoles de Seguridad" el campo "Tema" cambia y en el campo "Canal" se agrega "Virtual". Se adiciona la fila 10: la estrategia de "Red Social". En el punto 3.5.2 que pasa a ser el punto 3.6.2 Medición de Conocimiento Adquirido, se ajustó en la redacción "Para medir el conocimiento adquirido por los colaboradores del ICBF" por "Para medir el nivel de apropiación adquirido por los colaboradores del ICBF" En el punto 3.6 que pasa a ser el punto 3.7 ACTUAR - Actividades de Mejora, se modificó en la tabla el campo "Frecuencia" pasa de "Semestral" a "Anual" y se agregó la columna "Estrategias"
27/02/2019	V2	Se realizan actualizaciones y ajustes a los ítems: introducción, 2. Alcance y 3. Desarrollo.

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	PL6.GTI	04/03/2026
		Versión 9	Página 16 de 16

Fecha	Versión	Descripción del Cambio
		En el punto 3.3 se realiza modificación del nombre del Plan, el cual se renombra como: Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. En el punto 3.3.2 se realizan ajustes adicionando una fila a la tabla de medios y herramientas de comunicación. En el punto 3.4.3 se ajusta el nombre del eslogan para el eje de seguridad de la información. En el punto 3.4 se realizan las actualizaciones frente a temas y fechas a ejecutar en el plan y se elimina la estrategia de Yammer En el ítem 3.6 se realizan ajustes al texto y se adiciona una tabla En todo el documento se modifica el nombre del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, remplazándolo por Plan de Cambio y Cultura de Seguridad y Privacidad de la Información.
11/02/2019	V1	Se realizan actualizaciones y ajustes a los ítems: introducción, 1. Objetivo, 2. Alcance y 3. Desarrollo. En el punto 3.4 se realizan las actualizaciones frente a temas y fechas a ejecutar en el plan. En el ítem 3.5.2 se realizan ajustes al texto.
19/10/2018	N/A	Elaboración del documento.

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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.