



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

P9.GTI

29/10/2018

PROCEDIMIENTO PARA EL MANEJO DE MEDIOS REMOVIBLES

Versión 4

Página 1 de 5

- 1. OBJETIVO:** Orientar a los colaboradores del ICBF con respecto al uso y manejo de los medios removibles con información institucional, brindándoles las orientaciones necesarias para su uso adecuado, previniendo riesgos de fuga y pérdida de información, evitando la generación de incidentes que generen afectaciones en la confidencialidad, disponibilidad e integridad de la información del ICBF que se aloje en estos medios.
- 2. ALCANCE:** Este documento aplica en todos los niveles en donde se brinden servicios del ICBF (Sede de la Dirección General, Regional y centro Zonal, CAIVAS, CESPAS, CAVIF, Unidades Locales y Unidades Móviles).
- 3. POLÍTICAS DE OPERACIÓN:** Dentro de la operación del ICBF se prevé el manejo de medios removibles teniendo en cuenta lo siguiente:
 - 3.1 El uso de medios removibles solamente es autorizado a los funcionarios y contratistas con el aval del Profesional de la Dirección de Información y Tecnología delegado de esta labor.
 - 3.2 El Colaborador deberá registrar la siguiente información en el Módulo de Autoservicio:
 - Tipo de medio removible a usar (USB/ DD/Disco Duro externo).
 - Capacidad de almacenamiento del medio removible.
 - Tipo de información que se va a almacenar en el medio removible. (describir que información se almacenará, ejemplo actas de supervisión, informes, videos, presentaciones, etc.)
 - Tiempo de uso de la información (DD/MM/AAAA). La autorización se hace una sola vez y el tiempo de esta va ligado, para los contratistas a la fecha de finalización de su contrato y para los de planta es hasta el último día del año vigente.
 - 3.3 El manejo de la información institucional en Medios Removibles está expuesta a riesgos, como pérdida, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica del ICBF, por lo tanto, el colaborador que los use será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad del Tipo y el Tiempo de uso de la Información en estos medios.
 - 3.4 La contraseña requerida para efectuar el cifrado de información será provista por el usuario propietario del medio removible, cumpliendo lo estipulado en el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Control SGSI A.9.3.1 – A.9.4.3 Uso de información secreta para la autenticación y sistema de gestión de contraseñas dentro del Eje de Seguridad de la Información.
 - 3.5 En caso de olvido de la contraseña asignada para el cifrado del medio removible, el colaborador responsable del manejo del medio asumirá las consecuencias o perjuicios que se puedan derivar, producto de la pérdida de la información institucional que se encuentre almacenada en dicho medio.
 - 3.6 La acción de cifrado aplica para todo medio removible que transporte o contenga información del ICBF independiente de su clasificación.
 - 3.7 El Colaborador es responsable de la información en los medios removibles en todo momento y lugar.

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



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

P9.GTI

29/10/2018

PROCEDIMIENTO PARA EL MANEJO DE MEDIOS REMOVIBLES

Versión 4

Página 2 de 5

- 3.8 Los medios de almacenamiento removibles como discos duros, y dispositivos USB, que contengan información institucional, deben ser controlados (utilizar extracción segura, no forzar los conectores, escaneo con antivirus y desconectar el dispositivo cuando no se use) y físicamente protegidos (contra humedad, campos magnéticos, polvo y golpes).
- 3.9 Los medios de almacenamiento removibles deben ser de uso temporal y el colaborador deberá transferir la información institucional a los medios que el ICBF ha establecido para este propósito (computadores, NAS, fileserver u Onedrive).
- 3.10 El cifrado debe realizarse antes de que el dispositivo esté en uso, para evitar la pérdida de la información y daño de este.
- 3.11 Si el dispositivo ya contiene algún tipo de información se debe realizar respaldo de esta o transferirla a los medios que el ICBF ha establecido para este propósito (computadores, NAS, fileserver u Onedrive), para luego proceder a realizar el cifrado del medio.
- 3.12 Las fechas para el manejo de la información en medios removibles no podrán superar las fechas de vinculación laboral o contractual con el ICBF.
- 3.13 Cuando el Colaborador considere que ya no es requerida la información institucional guardada en el medio removible, o en caso de que su vinculación laboral o contractual haya finalizado, deberá realizar borrado de la información contenida en éste.

4. DESCRIPCIÓN DE ACTIVIDADES

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		Inicio		
1	Registrar solicitud de manejo medios removibles.	Realizar la solicitud del manejo de medios removibles a través del módulo de Autoservicio disponible en la Intranet http://mis.icbf.gov.co/helppeople/autoservicio/, para ingresar al módulo se deben diligenciar las mismas credenciales de acceso al equipo de cómputo que tenga asignado. Una vez ingrese debe seleccionar en el Catálogo de Servicios las siguientes opciones: • Recursos Tecnológicos. • Recursos Informáticos. • Manejo de Medio removible. • Clic en el signo más (+). Registrar en el Asunto: Autorización manejo medio Removible y en Descripción relacionar la información según la política de operación	Directores, Subdirectores, Jefes de Oficina, Asesores, Profesionales, Técnicos y Asistenciales de la Sede de la Dirección General, Regional y Centro Zonal	Módulo de Autogestión de la Herramienta de Gestión de Mesa de Servicio.

¡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**

P9.GTI

29/10/2018

PROCEDIMIENTO PARA EL MANEJO DE MEDIOS REMOVIBLES

Versión 4

Página 3 de 5

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		3.2.		
2 P.C	Revisar la Solicitud	El profesional encargado de la gestión de Incidentes de seguridad de la información recibe la solicitud, y se revisa la información diligenciada. ¿Se aprueba la solicitud? Si: pasa a la actividad 3. No: Se informa las causas por las cuales no se gestiona la solicitud y pasa a la actividad 4.	Profesional de la Dirección de Información y Tecnología de la SDG.	Herramienta de Gestión de Mesa de Servicio.
3	Gestionar la Solicitud para el cifrado	El Ingeniero de la SDG o el ingeniero regional reciben la solicitud y procede a realizar el cifrado del medio de almacenamiento aplicando lo descrito en el IT1.P9.GTI Instructivo para Cifrado de Información	Profesional de la Dirección de Información y Tecnología de la SDG. Profesional del Grupo de Planeación y Sistemas de la Regional	Herramienta de Gestión de Mesa de Servicio.
4	Cerrar el ticket	El profesional encargado de la gestión de Incidentes de seguridad de la información en el nivel SDG, el Ingeniero Regional o el ingeniero de la SDG, registra las acciones adelantadas y cierra el ticket.	Profesional de la Dirección de Información y Tecnología de la SDG. Profesional del Grupo de Planeación y Sistemas de la Regional	Herramienta de Gestión de Mesa de Servicio.
			Fin	

P.C.: Punto de Control

5. RESULTADO FINAL: Medio de almacenamiento cifrado y número de solicitud (ticket) de manejo de medios removibles, gestionado (atendido oportunamente) y cerrado.

6. DEFINICIONES

Medios Removibles: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente.

¡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	P9.GTI	29/10/2018
		Versión 4	Página 4 de 5

Los dispositivos móviles más comunes son:

- Memorias USB
- Discos duros extraíbles
- DVD
- CD
- Entre otros

Herramienta de Gestión de Servicios: Son todos los sistemas, aplicaciones, controles, soluciones de cálculo, metodología, etc., que ayudan a la gestión de una empresa; para el caso de TI para el manejo y control de servicios es el software en donde se documentan los servicios de gestión tecnológica como Incidentes, Requerimientos, Problemas, Controles de Cambios, etc. todas estas correspondientes a Tecnologías de Información.

Algunas de las Herramientas que se encuentran hoy en día en el mercado son:

- Altiris de Symantec
- IBM Service Management de IBM
- CA Service Desk Manager de CA Technologies
- Service Manager de Hewlett Packard
- Aranda's Service Desk de Aranda Software

Cifrado de información: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Profesional de la Dirección de información y Tecnología: colaborador que apoya el seguimiento y gestión de los incidentes de seguridad de la información.

Módulo de Autoservicio: Es un sistema de autoservicio y autogestión de fácil usabilidad integrado en una única interfaz mediante el cual los funcionarios de ICBF podrán crear y consultar solicitudes, realizar búsqueda a través de la base de datos de conocimiento y consultar el catálogo de servicios desde un mismo entorno sin la necesidad de recurrir a diferentes opciones. La ruta para acceder a este es: <http://mis.icbf.gov.co/helppeople/autoservicio/>

SDG: Sede de la Dirección General.

7. DOCUMENTOS DE REFERENCIA

- Guía técnica colombiana GTC-ISO-IEC 27002.
- Instructivo para Cifrado de Información.
- Ley 1581 de 2012

¡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 PROCEDIMIENTO PARA EL MANEJO DE MEDIOS REMOVIBLES	P9.GTI	29/10/2018
		Versión 4	Página 5 de 5

8. RELACIÓN DE FORMATOS: No Aplica

9. ANEXOS: No Aplica.

10. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
24/05/2014	PR15 MPA6 V1	Se migra al nuevo formato establecido como resultado del rediseño del Modelo de Procesos, lo que implica cambio de código. Se ajustan las actividades de acuerdo con el modelo de atención de las solicitudes.
02/01/2017	P9.GTI V1	Se actualiza rotulado de información de acuerdo con lo dispuesto en la Guía para la rotulación de la información.
26/03/2018	P9.GTI V2	Se ajusta el objetivo del procedimiento. Se amplía el alcance a CAIVAS, CESPAS, CAVIF, Unidades Locales y Unidades Móviles. Se realizó la numeración de las políticas de operación. Se actualizaron las políticas de operación 3.2., 3.3, 3.6, 3.9. Se incluyeron las políticas de operación 3.1, 3.10 y 3.11. Se actualiza el responsable en las actividades 2, 3 y 4. En la sección 4. DESCRIPCIÓN DE ACTIVIDADES, se actualiza la actividad No. 1, con el detalle del registro de la solicitud asociando la política de operación 3.2. En el numeral 7. DOCUMENTOS DE REFERENCIA, se asoció el IT1.P9.GTI Instructivo para Cifrado de Información.
03/08/2018	P9.GTI V3	Se realizan los siguientes cambios: • Se actualiza el objetivo del procedimiento. • Se actualizó la política de operación 3.2, la cual indica la información que se debe registrar para aprobar la solicitud. • Se actualiza la actividad 3, en la cual el ingeniero regional o el Ingeniero de la SDG procederá a realizar el cifrado del medio de almacenamiento. • Se elimina la actividad 5. • Se actualizó el resultado final. • Se realizó ajuste en los responsables de las actividades, de acuerdo con las orientaciones brindadas por la Subdirección de Mejoramiento Organizacional para el Levantamiento de Cargas.

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

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