

 BIENESTAR FAMILIAR	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	P9.GTI	23/04/2024
	PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE MEDIOS REMOVIBLES	Versión 6	Página 1 de 8

1. OBJETIVO

Brindar orientaciones para aquellos colaboradores del ICBF que cuentan con excepciones autorizadas por parte de la Dirección de Información y Tecnología para que puedan conectar y usar medios removibles en los equipos de dominio ICBF, realizando las recomendaciones necesarias para su uso adecuado, previniendo riesgos de fuga o pérdida de información y evitando incidentes que generen afectaciones en la confidencialidad, disponibilidad e integridad de la información que maneja la Entidad.

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 Con el objeto de proteger la información de la entidad como medida preventiva la Dirección de Información y Tecnología, se activó la Política de control de puertos USB para la conexión de dispositivos USB con el fin de evitar incidentes de seguridad de la información asociados al uso estos.
- 3.2 La excepción para uso de medios removibles estará sujeta a situaciones donde la entidad no esté en capacidad de proveer medios de almacenamiento en nube como OneDrive o SharePoint a sus colaboradores o cuando por sus actividades o funciones sean desempeñadas en zonas rurales dispersas donde la entidad no tiene los medios para proveer acceso a las herramientas tecnológicas antes mencionadas.
- 3.3 La excepción de uso de medios removibles solamente serán justificados y autorizados a funcionarios y contratistas con el aval de: Directores, Subdirectores, Jefes de Oficina en el nivel nacional o Directores en el nivel Regional a través de un ticket registrado en la herramienta de gestión de la mesa de servicios.
- 3.4 La autorización de uso de medios removibles se hace una sola vez y el tiempo estará 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. Es decir, que cada vigencia el colaborador deberá renovar la solicitud de permisos especiales de portabilidad de estos medios.
- 3.5 Revisada la información generada a través del ticket y su justificación de excepcionalidad, se procederá a su aval o devolución por parte del Equipo de Seguridad Perimetral.

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

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

 BIENESTAR FAMILIAR	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	P9.GTI	23/04/2024
	PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE MEDIOS REMOVIBLES	Versión 6	Página 2 de 8

- 3.6 Una vez analizado y aprobado el caso en la herramienta de gestión, se procederá a reasignar el caso a los ingenieros regionales o soportes en sitio para que se culmine con el proceso de cifrado de información de estos medios removibles con la herramienta BitLocker, utilizando el Formato Acta de Cifrado de Información. Para aquellos casos en que sean entidades externas las que envíen información en medios extraíbles sin cifrar, en cumplimiento de alguna obligación los ingenieros o soportes en sitio procederán apoyar el colaborador en la extracción de información al equipo del colaborador y cerrarán el ticket. Es necesario mencionar que el medio extraíble queda en custodia del colaborador para su protección.
- 3.7 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, su uso y el tiempo.
- 3.8 Las Regionales o Procesos de la Sede de la Dirección General que presenten casos de excepcionalidad para el manejo de medios removibles deberán identificar un Riesgo de Seguridad de la Información y darle el correspondiente tratamiento, con el fin de que implementen medidas adicionales que permitan prevenir incidentes de seguridad de la información asociados al uso de estos dispositivos.
- 3.9 La contraseña requerida para efectuar el cifrado de información será provista por el usuario propietario del medio removable, 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.
- 3.10 En caso de olvido de la contraseña asignada para el cifrado del medio removable, 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. a acción de cifrado aplica para todo medio removable autorizado por caso de excepción o en aquellas Regiones que, por sus condiciones climáticas, tecnológicas no se ha aplicado aún la Política de control de puertos USB.
- 3.11 Se debe analizar de manera obligatoria cualquier medio removable que se conecte a los equipos con el antivirus de la entidad inmediatamente sea conectado al equipo.
- 3.12 El Colaborador se hace responsable de la información almacenada en los medios removibles en todo momento y lugar, así como de cumplir con las buenas prácticas de seguridad de la información (Contraseñas seguras, analizar los medios removibles con el antivirus de la entidad, guardarlo en un sitio seguro).

 BIENESTAR FAMILIAR	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	P9.GTI	23/04/2024
	PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE MEDIOS REMOVIBLES	Versión 6	Página 3 de 8

- 3.13 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).
- 3.14 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 (OneDrive y SharePoint).
- 3.15 El cifrado del medio removible con la herramienta BitLocker, debe realizarse antes de que el dispositivo esté en uso o contenga información para evitar la pérdida o daño de este
- 3.16 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 OneDrive o SharePoint, para luego proceder a realizar el cifrado del medio removible con la herramienta BitLocker.
- 3.17 El colaborador deberá firmar el Formato Acta de Cifrado de información, para garantizar que efectivamente se cumple con el control de cifrado de información de medios removibles. Los soportes o ingenieros regionales deberán cargar este documento como solución del ticket
- 3.18 Cuando el Colaborador ya no requiera utilizar el medio removible ya sea por una razón personal o por que se terminó su vínculo contractual con la Entidad, deberá solicitar el borrado de la información almacenada en este mediante un ticket a la mesa de servicio, así como la inactivación de la excepción.
- 3.19 El desconocimiento de la normatividad o políticas implementadas en el ICBF no exime de su cumplimiento, por lo cual el colaborador que utilice medios removibles sin cumplir con lo establecido en este documento será sujeto a investigaciones disciplinarias o llamados de atención por parte del supervisor del contrato.
- 3.20 Los proveedores (Operadores) o terceros que por motivos de requerimientos legales o contractuales entreguen información al ICBF en medios removibles, aunque estos medios no estén cifrados con BitLocker deben aplicar las demás políticas de operación establecidas en este documento.
- 3.21 Los colaboradores que cuenten con un permiso de excepción para portar medios removibles deberán firmar el formato acta de cifrado de información.
- 3.22 Con el objeto de verificar el cumplimiento de este control se realizarán visitas a la Regional o a los procesos de la Sede Dirección General.



PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

P9.GTI

23/04/2024

PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE
MEDIOS REMOVIBLES

Versión 6

Página 4 de 8

4. DESCRIPCIÓN DE ACTIVIDADES

No	Nombre de la Actividad	Descripción de la actividad	Responsable (Cargo o nivel que realiza la actividad)	Registro (evidencia de la actividad, si aplica)
		Inicio		
1	Registrar solicitud de permisos especiales para el manejo de medios removibles.	<p>Realizar la solicitud del manejo de medios removibles a través de la Herramienta de Gestión de Mesa Informática de Soluciones con la correspondiente justificación de la solicitud excepción por el director, Subdirector, jefe de oficina en el nivel Nacional o director en nivel Regional.</p> <p>Para ingresar 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:</p> <ul style="list-style-type: none">• Recursos Tecnológicos.• Recursos Informáticos.• Manejo de Medio removible.• Clic en el signo más (+). <p>Registrar en el Asunto: Autorización manejo medio Removible y en la Descripción de la solicitud se debe documentar la actividad y adjuntar la justificación de permisos especiales para el uso de medios removibles.</p>	Directores, Subdirectores, Jefes de Oficina, Director Regional	Módulo de Autogestión de la Herramienta de Gestión de Mesa de Servicio
2	Revisar la Solicitud	<p>Recibir la solicitud validar y verificar la información diligenciada.</p> <p>¿Se aprueba la solicitud?</p> <p>Si: pasa a la actividad 3</p> <p>No: Se informa al usuario las causas por las cuales no se gestiona la solicitud y pasa a la actividad 4</p>	Profesional de la Dirección de Información y Tecnología de la SDG. (Seguridad Perimetral) Ingenieros Regionales	Herramienta de Gestión de Mesa de Servicio
3	Realizar cifrado de información del medio removable	Recibir la solicitud y proceder a realizar el cifrado del medio de almacenamiento aplicando lo descrito en el IT1.P9.GTI Instructivo para Cifrado de Información a través de la herramienta BitLocker	Soporte en sitio o Profesional del Grupo de Planeación y Sistemas de la Regional	Formato Acta de Cifrado de Información 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.



BIENESTAR
FAMILIAR

PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN

PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE
MEDIOS REMOVIBLES

P9.GTI

23/04/2024

Versión 6

Página 5 de 8

No	Nombre de la Actividad	Descripción de la actividad	Responsable (Cargo o nivel que realiza la actividad)	Registro (evidencia de la actividad, si aplica)
4	Cerrar el ticket	Registrar las acciones adelantadas y cerrar el ticket.	Profesional de la Dirección de Información y Tecnología de la SDG, Soporte en sitio o 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 con la herramienta BitLocker y número de solicitud (ticket) de manejo de medios removibles, gestionado y cerrado en la herramienta de gestión de la Entidad.

6. DEFINICIONES

Medios Removibles: 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
- 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

¡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

23/04/2024

**PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE
MEDIOS REMOVIBLES**

Versión 6

Página 6 de 8

- 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.

BitLocker: Es una aplicación que asigna una contraseña al medio removible, la cual protege la información de un acceso no autorizado

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

7. DOCUMENTOS DE REFERENCIA

- Guía técnica colombiana GTC-ISO-IEC 27002
- IT1.P9.GTI Instructivo para Cifrado de Información
- Ley 1581 de 2012

8. RELACIÓN DE FORMATOS

Código	Nombre del Formato
F1.P9.GTI	Formato Acta de Cifrado de Información

9. ANEXOS: No aplica



**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

**PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE
MEDIOS REMOVIBLES**

P9.GTI

23/04/2024

Versión 6

Página 7 de 8

10. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
28/07/2022	P9.GTI V5	<p>Se realizaron los siguientes cambios:</p> <ul style="list-style-type: none">• Se ajustó el objetivo.• Se ajusta la redacción de las políticas de operación conforme a lo estipulado en la resolución 414 del 2024 "Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación".• Se incorporó la definición de Bitlocker.• Se realiza la creación del formato Acta de Cifrado de Información.• Se cambia el nombre del procedimiento para el manejo de medios removibles a procedimiento solicitud de excepción para el uso de medios removibles.
29/10/2018	P9.GTI V4	<p>Se realizan Los siguientes cambios</p> <ul style="list-style-type: none">• Se actualiza el objetivo del procedimiento.• Se actualizó la política de operación 3.2, donde se agrega que todo medio removible debe ser justificado y autorizado por el jefe inmediato o supervisor del contrato y la importancia de que antes de cifrar el medio removible si este contiene información se debe realizar una copia en el OneDrive o el SharePoint. Y se incluye política de operación 3.1• Se realizo actualización a la actividad 4, con relación a los responsables de las actividades de gestión de los tickets y cierre de estos donde se agrega al soporte en sitio• Se ajusta nombre de las actividades 1 y 3• Se ajusta descripción de las actividades 2 3 y 4
03/08/2018	P9.GTI V3	<p>Se realizan los siguientes cambios:</p> <ul style="list-style-type: none">• 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. <p>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.</p>
26/03/2018	P9.GTI V2	<p>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.</p>

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

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



BIENESTAR
FAMILIAR

**PROCESO
GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

**PROCEDIMIENTO SOLICITUD DE EXCEPCIÓN PARA EL USO DE
MEDIOS REMOVIBLES**

P9.GTI

23/04/2024

Versión 6

Página 8 de 8

Fecha	Versión	Descripción del Cambio
		En el numeral 7. DOCUMENTOS DE REFERENCIA, se asoció el IT1.P9.GTI Instructivo para Cifrado de Información.
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.
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.

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

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