1. OBJETIVO. Suministrar orientaciones para el manejo, recolección y disposición de evidencias digitales asociadas a una situación judicial o incidente de seguridad de la información, que involucre dispositivos electrónicos del ICBF.

2. ALCANCE. El documento está orientado a los profesionales y colaboradores que participan en la gestión de incidentes de seguridad de la información, y debe ser aplicado en las Regionales y Centros Zonales por los Ingenieros Regionales, y en la Sede de la Dirección General por los Ingenieros de soporte de la Subdirección de Recursos Tecnológicos. Abarca el nivel Centro Zonal, Regional y Sede de la Dirección General.

3. DEFINICIONES.

Autenticidad. Propiedad de que una entidad es lo que afirma ser [ISO/IEC 27000:2009].
Confidencialidad. Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados [ISO/IEC 27000:2009].
Cadena de custodia: Es el procedimiento que garantiza la autenticidad de los elementos materiales de prueba recolectados y examinados asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.
Evidencia. Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información [ISO/IEC 27000:2009].
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

Incidente de seguridad de la información. Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009].
Integridad. Propiedad de exactitud e integridad [ISO/IEC 27000:2014].
Ticket /Número de Servicio. Número consecutivo suministrado por una Herramienta de Gestión durante el reporte de una Solicitud de Servicio, para facilitar a través del mismo el seguimiento y control.

4. DESARROLLO

En el marco de la gestión de incidentes de seguridad de la información, uno de los aspectos importantes y que requiere asegurar una adecuada gestión es la recopilación de información almacenada en medios electrónicos, con el fin de garantizar su adecuada recolección, transporte y almacenamiento, de tal manera que esta permanezca inalterable para cuando una entidad competente lo requiera. A continuación, se detallan aspectos a tener en cuenta y actividades que deben ejecutarse de manera detallada, incluyendo fechas y horas.

4.1. Solicitud de creación de ticket en la Herramienta de Gestión

A nivel regional el Director Regional o Coordinador de área y en la Sede de la Dirección General el Director, Subdirector o Jefe de Oficina, deben solicitar un ticket en la Herramienta de Gestión de Servicios del ICBF, requiriendo la recolección de evidencia en dispositivos electrónicos. Para la solicitud de creación de dicho ticket se pueden utilizar los siguientes medios:

- Enviando un mensaje de correo electrónico con la solicitud a MIS@icbf.gov.co.
- Llamando a la Mesa de Servicio a la extensión IP 8080.
- Llamando a la línea de atención 018000913434.

La mesa de servicio asignará el ticket teniendo en cuenta las siguientes condiciones:

- La solicitud efectuada por una regional se escala al Ingeniero de esa regional.
- En la Sede de la Dirección General se escala a uno de los ingenieros de Soporte en Sitio o un Profesional de la Subdirección de Recursos Tecnológicos.

4.2. Identificar la información a recolectar.

El Profesional de la Subdirección de Recursos Tecnológicos, el Ingeniero Regional o el Ingeniero de Soporte en Sitio debe establecer los elementos que pueden contener información para identificar claramente que se debe recolectar, es importante resaltar que se debe obtener la mayor cantidad de información existente asociada a la situación presentada, esto sin afectar algún tipo de evidencia potencial, igualmente cualquier medio que pueda contener información para un posible análisis forense o entrega a un ente competente.

4.3. Elementos para recolectar información.

Se debe contar con elementos necesarios que permitan realizar las actividades de recolección de información de una manera segura, efectiva y eficiente, sin improvisaciones. Estos elementos deben estar plenamente identificados para su utilidad en caso de necesitarse, evitando así interrupciones en el proceso de recolección de evidencias.

Para la recolección de evidencias se recomienda tener a la mano los siguientes elementos:

- Cajas de cartón liso
- Plástico embalaje
- Láminas de plástico de burbuja
- Espuma moldeada
- Cinta industrial
- Grapas para cerrar cajas de cartón.
- Guantes de látex en caso de que la evidencia pueda verse afectada por la estática.

- Rótulos y/o sellos de seguridad, para marcar la caja.

4.4. Involucrados en la recolección de evidencias.

Esta actividad la ejecuta quien tiene asignado el ticket (Profesional de la Subdirección de Recursos Tecnológicos, Ingeniero Regional o Ingeniero de Soporte en Sitio) acompañado mínimo de una persona y máximo tres, vinculadas al ICBF (empleado o contratista), quienes necesariamente no están obligadas a tener conocimiento técnico, su función es únicamente de acompañamiento y verificación del estado final de la evidencia recolectada, con el fin de minimizar las probabilidades de corromperla. Las personas que se involucren en el proceso deben estar en todo el transcurso de recolección de la evidencia, desde su hallazgo hasta su correcto almacenamiento y suscribir como testigos en el F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales; estos participantes deben prepararse para testificar (quizá años más adelante) y posiblemente exponer todas las acciones que vieron que se tomaron y en qué momento. Por ningún motivo se debe realizar este proceso de manera individual.

4.5. Recolectar evidencia.

Para realizar el levantamiento de evidencia y diligenciamiento del F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales se debe tener en cuenta las siguientes recomendaciones:

- Realizar el proceso con mínimo un (1) testigo, de acuerdo con las orientaciones indicadas en el punto 4.4. Involucrados en la recolección de evidencias.
- El o los acompañantes que participan como testigos deben estar presente(s) de principio a fin en el proceso de recolección de evidencias.
- Describir el proceso detalladamente:
    - Descripción del escenario.
    - Estado en el que se encontró el elemento electrónico.
    - El paso a paso de las actividades realizadas.
- Adjuntar evidencias fotográficas de todo el proceso realizado, es importante que en ellas se pueda observar los acompañantes que participan como testigos.
- Se debe salvaguardar únicamente los elementos que cuenten con información, en caso de un ratón o teclado no es necesario que se almacenen como evidencia.
- Es importante tener en cuenta que el acta debe ser firmada por todos los participantes en el proceso de recolección de evidencias.

4.6. Asegurar la integridad de la Información.

Una vez recolectada la evidencia, se debe garantizar su integridad, procediendo de la siguiente manera:

- Debe guardarse en un elemento que garantice no sea alterado en su almacenamiento, ejemplo: un elemento de cartón, plástico y similares (tener en cuenta lo mencionado en el punto 4.3. Elementos para recolectar información).
- Debe sellarse de tal manera que en dado caso que alguien intente o afecte el embalaje, se evidencie la alteración.
- En la medida de lo posible debe guardarse en un empaque de plástico para evitar daños por efectos ambientales como polvo, temperatura, humedad y salinidad.
- Al sellar se debe incluir sellos de seguridad con logos del ICBF.

4.7. Almacenar la información en sitio seguro.

Se debe almacenar la evidencia obtenida del paso anterior en un sitio con medidas de seguridad como: un espacio con llave que pueda garantizar que las personas con acceso a ella sea limitado, evitando que la evidencia sea alterada y/o borrada por usuarios no autorizados.

4.8. Cierre del Ticket

El Profesional de la Subdirección de Recursos Tecnológicos, Ingeniero Regional o Ingeniero de Soporte en Sitio debe cerrar en la Herramienta de Gestión de servicios el ticket que le fue asignado, adjuntando allí el acta con la información recolectada (se recomienda reducir el tamaño de los archivos, para dicha actividad remitirse al soporte de Windows (https://support.office.com/es-es/article/Reducir-el-tama%C3%B1o-del-archivo-631d1d48-a56b-4fd4-ad66-091dd201db10), es importante incluir como adjunto del caso toda la información recolectada en estas guía.

4.9. Entrega de la Evidencia

El Coordinador de Planeación y Sistemas en el nivel regional, o el Subdirector de Recursos Tecnológicos en la Sede de la Dirección General, son los responsables de establecer en cadena de custodia las evidencias recolectadas antes de realizar la entrega de la evidencia digital a un tercero, el cual debe ser un ente autorizado como la Fiscalía o la Policía Nacional. Independiente del tercero que requiera la entrega de las evidencias, se debe diligenciar el F2.G5.GTI Formato Acta de Entrega de Evidencias Digitales identificando los elementos entregados.

4.10. Listado de actividades:

No.	Actividad	Responsable
1	Solicitar creación de ticket en la herramienta de gestión.	Directores, Subdirectores, Jefes de Oficina de la SDG Directores, Coordinadores de la Dirección Regional.
2	Identificar la información a recolectar.	Profesional de la Subdirección de Recursos Tecnológicos, Profesional del Grupo de Planeación y Sistemas / Ingeniero o Técnico del Operador de Mesa de Servicio.
3	Convocar involucrados en la recolección de evidencias.	Profesional de la Subdirección de Recursos Tecnológicos, Profesional del Grupo de Planeación y Sistemas / Ingeniero o Técnico del Operador de Mesa de Servicio.
4	Recolectar evidencia.	Profesional de la Subdirección de Recursos Tecnológicos, Profesional del Grupo de Planeación y Sistemas / Ingeniero o Técnico del Operador de Mesa de Servicio / Profesional, Técnico o asistencial de la Sede de la Dirección General, Regional o Centro Zonal.

No.	Actividad	Responsable
5	Asegurar la integridad de la información.	Profesional de la Subdirección de Recursos Tecnológicos, Profesional del Grupo de Planeación y Sistemas / Ingeniero o Técnico del Operador de Mesa de Servicio.
6	Almacenar la información en sitio seguro.	Coordinador de Planeación y Sistemas de la Sede Regional, o el Subdirector de Recursos Tecnológicos de la Sede de la Dirección General.
7	Cerrar el ticket.	Profesional de la Subdirección de Recursos Tecnológicos, Profesional del Grupo de Planeación y Sistemas / Ingeniero o Técnico del Operador de Mesa de Servicio
8	Entregar la evidencia.	Coordinador de Planeación y Sistemas de la Sede Regional, o el Subdirector de Recursos Tecnológicos de la Sede de la Dirección General.

5. ANEXOS:

F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales
F2.G5.GTI Formato Acta de Entrega de Evidencias Digitales

6. NATURALEZA DE LOS CAMBIOS:

Fecha	Versión	Descripción del Cambio
10/02/2016	G13.MPA6	Se migra al nuevo formato establecido como resultado del rediseño del Modelo de Procesos, lo que implica cambio de código.
04/11/2016	G5.GTI V1	Se actualiza rotulado de información de acuerdo con lo dispuesto en la Guía para la rotulación de la información.
06/03/2018	G5.GTI V2	Se modifica la rotulación pasándola de Clasificada a Pública. Se adiciona el numeral 4.10 LISTADO DE ACTIVIDADES, con la identificación de los responsables de las actividades que se ejecutan, de acuerdo con las orientaciones brindadas por la Subdirección de Mejoramiento Organizacional para el Levantamiento de Cargas.