CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Adriana Cetina Hernández Cargo: Jefe Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2025-01-28

1 OBJETIVO

Establecer las directrices generales para la ejecución de actividades técnicas, administrativas, probatorias y tecnológicas relacionadas con los mensajes de datos y/o evidencias digitales mediante la descripción de las etapas para atender y tramitar solicitudes según el modelo API, del mismo modo, gestionar solicitudes complementarias, y asegurar la custodia del material probatorio, en el marco de los trámites y procesos administrativos de la Superintendencia de Industria y Comercio. (en adelante **SIC**).

2 DESTINATARIOS

Este procedimiento debe ser conocido y aplicado por aquellos servidores públicos y contratistas que participen directa o indirectamente en las actividades del Grupo de Trabajo de Informática Forense y Seguridad Digital de la Superintendencia de Industria y Comercio.

3 GLOSARIO

ADQUISICIÓN: En esta etapa se lleva a cabo la identificación y adquisición de información relevante para cualquier proceso administrativo o judicial. Asimismo, es fundamental garantizar que la recolección de los mensajes de datos de acuerdo con los criterios establecidos por el Artículo 11 de la Ley 527 de 1999.

CADENA DE CUSTODIA: Registro que garantiza la autenticidad de las evidencias materia de prueba que han sido recolectadas en el transcurso de la actuación administrativa –averiguación preliminar o investigación- que permite asegurar la integridad y confidencialidad de los elementos probatorios en todas las etapas procesales. (FGN[1])

CONTENEDOR DE EVIDENCIA DIGITAL: Es el elemento o dispositivo en el que se guardan las evidencias digitales y los mensajes de datos de forma permanente o temporal. Existe variedad importante de contenedores entre los que se encuentran el CD, el DVD. el Blu-ray, el USB y el disco duro. En tanto. la cadena de custodia registra la ubicación y los procedimientos hechos a la evidencia que se encuentra en estos contenedores[2].

[1] Tomado del Manual de Cadena de Custodia de la Fiscalía General de la Nación.
[2] B, Prieto (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales.

CUSTODIO: Persona que vigila y guarda con cuidado y responsabilidad un Elemento Material Probatorio y Evidencia Física o un lugar de los hechos. (FGN[3])

ELEMENTO MATERIAL PROBATORIO: Es cualquier objeto que demuestre una conducta en contra de la ley. Según el literal g del artículo 275 de la ley 906 de 2004, un mensaje de datos puede ser considerado un elemento material probatorio una vez haya sido aportado a un proceso legal, y debe estar protegido garantizando su integridad, confidencialidad y disponibilidad, es decir, que el mensaje de datos recolectado en campo es el mismo mensaje de datos presentado ante una autoridad legal. Adicionalmente, debe haber un registro en el cual se evidencie quién ha sido responsable de custodiar y transportar el mensaje de datos o el contenedor donde éste se encuentre, y así mismo quién o quiénes han sido los investigadores y han tenido contacto con el mismo. (Ley 906 de 2004 artículo 275)

EMBALAR: Es el procedimiento técnico utilizado para empacar, preservar y proteger los Elementos Materiales Probatorios y Evidencia Física en el contenedor adecuado con el fin de ser enviados para análisis o almacenamiento.

EVIDENCIA DIGITAL: Cualquier dato o conjunto de datos de información generado, almacenado o transmitido en formato binario (digital) que evidencien elementos propios que pueden ser susceptibles de recaudo durante la práctica de una visita administrativa y entre otras actividades.

INVESTIGACIÓN: Los mensajes de datos son identificados y analizados para cumplir con su propósito dentro de la actuación que se esté desarrollando. De acuerdo con su relevancia pueden adquirir la categoría de Elemento Material Probatorio,

INFORMÁTICA FORENSE: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información. (MINTIC[4])

MENSAJE DE DATOS: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax (Definición de acuerdo con Ley 527 de 1999 Artículo 2º)

[3]Ibidem
[4] Tomado de la Guía de Evidencia Digital del Ministerio de la Tecnologías de la Información y las Comunicaciones - MINTIC.

MODELO EDRM: El Modelo de referencia de descubrimiento electrónico, también conocido como EDRM o el diagrama de EDRM, describe los procesos y etapas clave del proceso de descubrimiento electrónico en forma de nueve fases interrelacionadas: Gobernanza de la información, identificación, conservación, recolección, procesamiento, revisión, análisis, producción y presentación. Cada fase representa una etapa central del proceso de descubrimiento electrónico. Al dividir el proceso de descubrimiento electrónico en fases, los profesionales pueden aprovechar los recursos básicos (es decir, personas, tecnología y procesos) de una manera más organizada para lograr los resultados deseados. http://www.edrm.net/resources/glossaries/glossary.

MODELO API (Adquisición Procesamiento Investigación): Este modelo surge a partir de la flexibilidad y versatilidad del modelo EDRM, ya que, por su naturaleza, es posible realizar cambios o modificaciones a su estructura base sin afectar su finalidad. Gracias a esta característica, pueden surgir modelos derivados como el API el cual simplifica su entendimiento y puesta en práctica[5].

PROCESAMIENTO: Esta actividad implica transferir la información adquirida a un contenedor donde pueda ser conservada por el tiempo establecido por las políticas y/o el exigido por la Ley. Asimismo, en este punto se realizan las labores necesarias para poder revisar y analizar la información, esto incluye actividades como extraer la información de mensajes de datos contenidos, convertir archivos para visualizar la información, indexar los mensajes de datos, extraer el texto de imágenes, entre otras.

PUESTA A DISPOSICIÓN: Presentación del resultado de la fase de procesamiento, los mensajes de datos se exponen a personal autorizado a través de herramientas especializadas que permiten visualizar la información impidiendo que pueda ser modificada o alterada, garantizando así su integridad en todo momento.

RECOLECTAR: Obtención de cosas u objetos determinados que guardan un vínculo directo con la escena o lugar del hecho materia de investigación. (FGN[6])

REGISTRO DE CADENA DE CUSTODIA: Es la historia exhaustiva y documentada de cada traspaso y traslado del material físico de prueba, durante el desarrollo del proceso de cadena de custodia. Permite verificar la identidad, el estado y condiciones originales de los elementos físicos de prueba, así como las

[5] La información ampliada de este modelo se encuentra en el documento GS04-I01 Instructivo Informática Forense.
[6] Ibidem

modificaciones realizadas a estos, establece la ruta seguida por dichos elementos; determina su lugar de permanencia y la persona responsable de la custodia en cada lapso del tiempo. (FGN)

RÓTULO: Formato diligenciado que se adhiere al contenedor con fines de identificación del elemento material probatorio y Evidencia física. (FGN)

SISTEMA INFORMÁTICO: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. (Definición de acuerdo con Ley 527 de 1999 Artículo 2º)

4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
Constitución Política de Colombia	1991	Derecho a la intimidad	Artículo 15	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar
Decreto	092 de 2022	Por el cual se modifica la estructura de la Superintendencia de Industria y Comercio, y se determinan las funciones de sus dependencias		Aplicación total
Ley	57 de 1985	Por la cual se ordena la publicidad de los actos y documentos oficiales		Aplicación total
Ley	527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.		Aplicación total
Ley	599 de 2000	Por la cual se expide el Código Penal	Artículo 195	Acceso abusivo a un sistema informático
Ley	906 de 2004	Por la cual se expide el Código de Procedimiento Penal.	Título I -La indagación y la investigación Título II - Medios cognoscitivos en la	Capítulo V - Cadena de custodia Capítulo único - Elementos materiales probatorios, evidencia física e información.

Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
			indagación e investigación	
Ley	1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.		Aplicación total
Ley	1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones	Artículo 58	Conductas punibles se utilicen medios informáticos, electrónicos o telemáticos
Decreto Ley	4886 de 2011	Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones	Artículo .5	Funciones de la Oficina de Tecnología e Informática
Ley	1581 de 2012	Por medio la cual se contempla la reglamentación para la protección del derecho fundamental que todas las personas naturales a dar autorización de información para la recolección, tratamiento y almacenamiento que contenga datos personales		Aplicación total
Ley	1564 de 2012	Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones	Artículos 165, 175, 251	Medios de Prueba, Desistimiento de Pruebas, Documentos en Idioma Extranjero y otorgados en el extranjero
Decreto Ley	1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015		Aplicación total
ACUERDO	SAA06-3334 de 2006	Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia		Aplicación total
ISO/IEC	27037 de 2012	Guía por la cual se determina los lineamientos para la identificación, recopilación, adquisición y preservación de evidencia digital		Aplicación total

Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
NTC	6231 de 2017	Valor probatorio y admisibilidad de la información electrónica. Especificaciones		Aplicación total
Resolución	62538 de 2018	Por la cual se crea y organiza el Grupo de Trabajo de Informática Forense y Seguridad Digital adscrito a la Oficina de Tecnología e Informática		Aplicación total

Tabla 1 Referencias Normativas

5 GENERALIDADES

El Grupo de Trabajo de Informática Forense y Seguridad Digital, atiende entre otras las solicitudes relacionadas con el servicio de apoyo a las diferentes áreas de la SIC, en las técnicas de Adquisición, Procesamiento e Investigación de mensajes de datos y/o evidencias digitales, garantizando el valor probatorio de la información mediante herramientas de hardware y software especializado.

Solicitudes mediante Sistema de Trámites

Para la atención de solicitudes de carácter técnico, administrativo, probatorio y tecnológico de los mensajes de datos y/o evidencias digitales, se establece que las comunicaciones deben realizarse mediante el Sistema de Trámites de acuerdo con los perfiles establecidos.

Solicitudes mediante Correo Electrónico

De manera análoga al Sistema de Tramites, las comunicaciones pueden ser planteadas por este medio. No obstante, este tipo de solicitudes deben ser enviadas por coordinadores o por cargos semejantes o superiores.

Manejo de los documentos

El servidor público y/o contratista que recibe la documentación de los procedimientos técnicos realizados, firmará recibido en una copia de la primera hoja como soporte de la entrega, por lo anterior, toda documentación física que se genere en el desarrollo de las actividades es responsabilidad del área o dependencia destinataria, quienes deben tomar las medidas necesarias para resguardar los documentos originales que le sean entregados en los respectivos expedientes y determinar la digitalización y condiciones de consulta que debe quedar, tanto para el usuario interno como externo.

Teniendo en cuenta lo manifestado, el GTIFSD no cuenta con copia de los documentos físicos, los mismos son entregados en formato original a las dependencias destinatarias.

5.1 CONTROLES DE ACCESO

Los controles de acceso son todos los mecanismos físicos y digitales empleados para salvaguardar la confidencialidad de la información, adicional a ello, los permisos otorgados deben ser únicos para el funcionario y/o contratista en ejercicio de sus funciones. Esto debe aplicar para todas las labores que se desempeñan en el desarrollo del marco de trabajo ya que esto permite incrementar los niveles de seguridad de acceso y no repercute negativamente en la confidencialidad e integridad de los datos.

5.1.1 ACCESO A LA INFORMACIÓN

Todo el acceso a información digital de manera física (dispositivos de almacenamiento digital) o virtual (almacenamiento en la nube), debe tener la autorización previa del Coordinador del GTIFSD, en ningún escenario se permite el acceso a funcionarios y/o contratista sin autorización. El acceso únicamente se dará para ejecución de las funciones del funcionario y/o contratista si su actividad así lo requiere.

Cuando por medio de solicitud formal y bien, cuando la ley lo estipule, se dará acceso a la información a terceros, todo ello con la autorización del Coordinador del GTIFSD. Estas solicitudes deben ser realizadas por medio del sistema de trámites o por correo electrónico y radicadas en la SIC.

Es relevante resaltar que cuando se trate de los contenedores de evidencia digital, debe hacerse el respectivo registro en el sistema de cadena de custodia al cual se encuentre anclado dicho elemento, ya que esto puede afectar su validez probatoria.

5.2 CONFIDENCIALIDAD

Por motivo del ejercicio de sus funciones todo funcionario y/o contratista que recaude, almacene, procese, analice, observe o tenga cualquier interacción con información o evidencia digital, tiene el compromiso desde su vinculación con la SIC a salvaguardar la confidencialidad de la misma, por lo tanto, está prohibida su copia o distribución, excepto que sus funciones así lo requieran y esté debidamente

autorizado por el Coordinador del GTIFSD atendiendo una solicitud del coordinador del área a la cual pertenece la información.

A continuación, se cita un ejemplo de cláusulas de confidencialidad en los contratos de los contratistas y/o funcionarios: "**(…)***Dar cumplimiento al procedimiento de Administración de Bienes devolutivos y de consumo de la CONTRATANTE, velar por el buen uso de los bienes y elementos entregados por la Contratante, para el ejercicio de las actividades relacionadas con a la ejecución del objeto contractual. Abstenerse de utilizarlos para fines y lugares diferentes a los convenidos, y entregarlos a la finalización del vencimiento del plazo pactado.*(…)", De igual manera, en otro de los numerales se manifiesta **"**(…) *mantener y garantizar total confidencialidad sobre la información que le sea entregada para el cumplimiento del objeto del contrato, durante la ejecución del mismo y con posterioridad a su finalización, la cual no será compartida o divulgada a terceras personas no relacionadas con el desarrollo de las labores encomendadas por la CONTRATANTE. Cualquier información que sea requerida sólo será suministrada previa autorización escrita y expresa dada por la CONTRATANTE. Así mismo, deberá cumplir lo estipulado en el documento: Acuerdo de seguridad y privacidad para contratistas, publicado en el Sistema Integral de Gestión Institucional – SIGI, el cual se entiende conocido y aceptado con la suscripción del presente contrato. (…)".*

En ese orden de ideas, los funcionarios y contratistas que hacen parte de la SIC y las entidades públicas con facultades otorgadas por la Ley, en cumplimiento de sus funciones, pueden solicitar autorización de acceso a la información digital cumpliendo con los reglamentos que garanticen la confidencialidad de los datos.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**ATENDER SOLICITUD**	Solicitudes de acompañamiento de visita formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la SIC	En esta etapa los servidores públicos y/o contratistas del GTIFSD reciben y responden las solicitudes formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la Superintendencia de Industria y Comercio. A través de las siguientes actividades: - Tramitar solicitud - Responder solicitud	El Coordinador y servidor público del GTIFSD Servidores públicos y/o contratistas de las áreas o dependencias solicitantes	Requerimiento de información (si es necesario) Asignación de la Solicitud para pasar a Etapa 2 o Etapa 3

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
2	**TRAMITAR SOLICITUDES SEGÚN MODELO API**	Solicitud y autorización para el Procesamiento y/o Investigación, enviada por el servidor público y/o contratista del área o dependencia solicitante	En esta etapa el Grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD emplea el modelo API basado en la modelo E-Discovery el cual se enfoca en las actividades de Adquisición, Procesamiento e Investigación de evidencias digitales, como estándar de buenas prácticas para las investigaciones digitales. A través de las siguientes actividades: - Planear y ejecutar la Adquisición. - Planear y ejecutar el Procesamiento - Planear y ejecutar la Investigación	El Coordinador y/o servidor público del GTIFSD	Ejecución de actividades según GS04-I01 Instructivo Informática Forense: Entrega GS04-F06 Acta de Unificación de Evidencias Digitales, documentos y medios de almacenamiento con la evidencia digital recolectada, GS04-F01 Registro Cadena de Custodia, GS04-F02 Vr1 Formato de Adquisición de Imágenes Forenses, GS04-F03 Rotulo Elemento Materia de Prueba o Evidencia Física, Informe de Copia, Anexos Digitales o Lista de Investigación (Si aplica)
3	**TRAMITAR SOLICITUDES COMPLEMENTARIAS**	Asignación de la Solicitud complementaria	En esta etapa el GTIFSD recibe y da respuesta a las solicitudes formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la Superintendencia de Industria y Comercio, que no estén relacionadas con el Modelo API. A través de las siguientes actividades: - Recibir y dar respuesta a las solicitudes complementarias.	El Coordinador y/o servidor público del GTIFSD	Respuesta a la solicitud
4	**CUSTODIAR MATERIAL PROBATORIO**	Designación del servidor público y/o contratista para la custodia de las evidencias digitales Solicitudes de préstamo de material probatorio	En esta etapa el Coordinador del GTIFSD designa a un servidor público y/o contratista para que realice la custodia de las evidencias digitales (no incluye material físico ya que éste es de custodia del área o dependencia solicitante de la SIC), y tome las medidas para garantizar la originalidad, autenticidad e inalterabilidad de la	El Coordinador y servidor público del GTIFSD	Atención a la solicitud y anotación en el GS04-F01 Registro Cadena de Custodia posterior

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
			información que se custodia. A través de la actividad de: - Custodiar evidencias digitales		

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

7.1 ETAPA 1. ATENDER SOLICITUD

En esta etapa los servidores públicos y/o contratistas del grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD reciben y responden las solicitudes formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la Superintendencia de Industria y Comercio.

7.1.1 Tramitar solicitud

Los servidores públicos y/o contratistas de las áreas o dependencias solicitantes, tramitan la solicitud mediante el sistema de trámites y correo electrónico de la entidad. Los requisitos mínimos de entrada para la solicitud son:

- Tipo de Solicitud.
- Descripción de la Solicitud.
- Número de Radicado.
- Nombre del Caso (opcional).

El Coordinador del GTIFSD recibe la solicitud y la asigna al Servidor Público y/o Contratista del GTIFSD.

7.1.2 Responder solicitud

El servidor público y/o contratista del GTIFSD analiza la solicitud de acuerdo con el GS04-I01 Instructivo Informática Forense, evaluando las herramientas que necesita para resolverla y determinando el tiempo que tardará en atenderla dependiendo de su criticidad.

En caso de que se requiera información adicional, el Coordinador del GTIFSD realiza el requerimiento al área o dependencia solicitante.

El servidor público y/o contratista designado para atender el requerimiento solicita al personal designado por el Coordinador del GTIFSD para la administración y supervisión del inventario físico, que le sean asignados los equipos y herramientas necesarias para poder dar cumplimiento a la solicitud realizada. Estas herramientas hacen parte del inventario físico del GTIFSD, el cual será verificado de manera periódica o extemporánea según solicitud del Coordinador. Para lo cual se llevará control del inventario y del préstamo de los equipos mediante el uso de la plantilla denominada INVENTARIO DEL LIF.

Todos los elementos físicos puestos a disposición en el Inventario del GTIFSD se encuentran cubiertos por la póliza todo riesgo puesto a disposición por la Entidad, en caso que se llegue a presentar algún siniestro se deberá remitir al documento GA02-I01 Instructivo para la reclamación en caso de siniestro.

El uso de los equipos dispuestos por la Entidad para el GTIFSD se debe realizar única y exclusivamente para los fines pertinentes en el ejercicio de las funciones propias del grupo, y nunca para uso privado o personal de uno de los integrantes del GTIFSD o de algún otro funcionario y/o contratista de la SIC.

Una vez se recibe la información correspondiente, se consolida la información necesaria para dar inicio al trámite y se continúa con la siguiente etapa, teniendo en cuenta que:

- Si es un requerimiento de acompañamiento de visita administrativa, se continúa con la etapa “TRAMITAR SOLICITUDES SEGÚN MODELO API”.
- Si es otro tipo de trámite se continúa con la etapa “TRAMITAR SOLICITUDES COMPLEMENTARIAS”.

7.2 ETAPA 2. TRAMITAR SOLICITUDES SEGÚN MODELO API

En esta etapa el Grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD emplea el modelo API basado en la modelo e-Discovery el cual se enfoca en las actividades de Adquisición, Procesamiento e Investigación de evidencias digitales, como estándar de buenas prácticas para las investigaciones digitales.

7.2.1 Planear y ejecutar la Adquisición

La adquisición inicia con la identificación, preservación y recolección de los mensajes de datos que pueden llegar a ser caracterizados como elementos materiales probatorios ante las autoridades competentes o para ejecutar controles internos de la SIC, lo anterior siempre y cuando se tengan en cuenta las siguientes consideraciones:

- Un mensaje de datos está contenido dentro de la evidencia digital adquirida para el desarrollo de una investigación.
- Cada evidencia digital contiene una cantidad determinada de mensajes de datos.
- Para que un mensaje de datos sea considerado un elemento material probatorio válido ante autoridades competentes debe permanecer en un dispositivo de almacenamiento el cual garantice su integridad, confidencialidad y disponibilidad en concordancia con los criterios establecidos por la Ley.

Es importante tener presente que el funcionario y/o contratista designado para esta actividad debe estar preparado para cualquier eventualidad que se pueda presentar en medio de la diligencia con relación a los dispositivos desde los cuales debe realizar la adquisición de mensajes de datos, en consecuencia, podrá acudir al repositorio forense establecido en la unidad de almacenamiento compartido en la plataforma dispuesta por la Entidad, asimismo, tendrá equipos especializados que le permitan la adquisición de cualquier tipo de evidencia digital contenida en los diferentes medios de almacenamiento posibles, así como la disposición de los diferentes mecanismos de aislamiento de la evidencia en caso de que la diligencia deba ser suspendida por los diferentes motivos que pueda adoptar el líder de la visita administrativa.

Asimismo, el experto forense es quien determina qué tipo de información es relevante y la manera apropiada para realizar la adquisición, ya que puede encontrarse situaciones fuera de las habituales que afecten el transcurso normal de su desarrollo. En consecuencia, el experto definirá el tipo de imagen forense es más adecuado para cada caso, procurado no exceder la duración total del acto administrativo.

Para dar continuidad a la Adquisición de elementos de evidencia digital, se establecen los lineamientos y las diferentes actividades que pueda llevar a cabo el funcionario y/o contratista que realiza la actividad según la situación a la que se vea expuesto, las cuales se encuentran descritas en el GS04-I01 Instructivo Informática Forense.

7.2.2 Planear y ejecutar el Procesamiento

Esta etapa se encuentra compuesta por diferentes acciones como: (i) unificación de evidencias, en la cual se agrupan los mensajes de datos provenientes de diferentes fuentes y se almacenan en un contenedor de evidencia digital el cual reposa en el Cuarto de Evidencias del Laboratorio de Informática Forense, (ii) copia en servidor,

(iii) creación de lista de procesamiento, (iv) procesamiento de evidencias digitales y (v) la puesta a disposición de los mensajes de datos.

Es importante resaltar que para cada una de las etapas mencionadas anteriormente se realizan las respectivas anotaciones en el sistema de cadena de custodia y se soporta con la debida documentación. Adicional para el desarrollo de las etapas (iii), (iv) y (v) debe contar con la autorización del coordinador, jefe, director o delegado del área o dependencia solicitante vía correo electrónico al Coordinador del GTIFSD para la gestión pertinente.

Por otro lado, el especialista forense designado para la actividad de procesamiento informará periódicamente al Coordinador del GTIFSD cualquier novedad o situación que se pueda presentar en torno a esta labor y se tomaran las acciones y medidas que se consideren pertinentes para su culminación exitosa.

7.2.3 Planear y ejecutar la Investigación

El servidor público y/o contratista designado para la investigación, desarrolla esta actividad teniendo como fundamento el propósito del requerimiento legal. Dependiendo del análisis e inspección de los mensajes de datos se puede definir si éstos se pueden considerar elementos materiales probatorios o no. Se continúa con la Gestión de las Investigaciones, descrita en el GS04-I01 Instructivo Informática Forense.

7.3 ETAPA 3. TRAMITAR SOLICITUDES COMPLEMENTARIAS

En esta etapa el GTIFSD recibe y da respuesta a las solicitudes formuladas por los servidores públicos y/o contratistas de las áreas o dependencias solicitantes de la Superintendencia de Industria y Comercio, que no estén relacionadas con el Modelo API.

7.3.1 Recibir y dar respuesta a las solicitudes complementarias

El servidor público y/o contratista del área o dependencia solicitante, envían solicitud al Coordinador del GTIFSD para la atención de alguna de las siguientes actividades:

- Copia de Contenedores de Evidencias Digitales.
- Preservación de Páginas Web.
- Informe Técnico.
- Traslado de Contenedores de Evidencias Digitales.
- Depuración de Mensajes de Datos.
- Exportación de Elementos de Evidencia Digital.

El Servidor Público y/o Contratista designado por el Coordinador del GTIFSD recibe la solicitud y la asigna para su atención. La gestión de la solicitud se hace de conformidad con lo estipulado en el GS04-I01 Instructivo Informática Forense.

7.4 ETAPA 4. CUSTODIAR MATERIAL PROBATORIO

En esta etapa el Coordinador del GTIFSD designa a un servidor público y/o contratista para que realice la custodia de las evidencias digitales (no incluye material físico ya que éste es de custodia del área o dependencia solicitante de la SIC), y tome las medidas para garantizar la originalidad, autenticidad e inalterabilidad de la información que se custodia.

7.4.1 Custodiar evidencias digitales

El servidor público y/o contratista designado para la custodia de material probatorio debe preservar y salvaguardar todos los elementos adquiridos y vincularlos debidamente al sistema de cadena de custodia durante los actos administrativos.

Previo al almacenamiento de los elementos materiales probatorios, se llevan a cabo labores de unificación de evidencias que se encuentren asociadas a un mismo radicado, con el objetivo de optimizar los recursos del Laboratorio de Informática Forense. Estas labores son registradas en el documento de cadena de custodia y se conserva el registro histórico al realizar el traslado de contenedor y se hace apertura de un nuevo documento de cadena de custodia.

De igual manera, es necesario garantizar que cada uno de los dispositivos que ingresan al cuarto de evidencias, se encuentren debidamente embalados y rotulados, debido a que el almacenamiento de los dispositivos contenedores de evidencia digital, en el cuatro de evidencia o el sitio designado para tal fin, se efectúa por medio del número de radicado en orden ascendente y en caso de haber más de un contenedor con el mismo número de radicado, estos se organizan por orden alfabético de acuerdo con el serial físico del dispositivo.

Por otro lado, las copias controladas de dispositivos contenedores de evidencia digital y/o cualquier otra solicitud deben contar con la autorización del coordinador, jefe, director o delegado del área o dependencia solicitante y debe ser aprobado por el Coordinador del GTIFSD. Una vez se cuente con la autorización del caso, el servidor público y/o contratista designado para la custodia de material probatorio, atiende la respectiva solicitud dejando constancia en el GS04-F01 Registro Cadena de Custodia posterior, documento que reposa en el expediente del área o

dependencia solicitante. Para mayor detalle ver GS04-I01 Instructivo Informática Forense.

Es importante resaltar que, si bien cada área solicitante es el dueño de la información recolectada, la custodia debe ser conservada por el GTIFSD, ya que de este modo es posible proteger la integridad, disponibilidad y confidencialidad de los datos. Adicional, el Laboratorio de Informática Forense cuenta con el personal idóneo para realizar cada una de las labores relacionadas con la evidencia digital y cuentan con los controles acceso suficientes, medios físicos necesarios y las herramientas de software para salvaguardar la información.

Nota: Es necesario que cada persona que interactúe con el contenedor de evidencia digital registre adecuadamente en la cadena de custodia, todas las interacciones y actividades que se realicen entorno a las evidencias digitales que reposan en él o al dispositivo en sí mismo.

8 DOCUMENTOS RELACIONADOS

GS04-I01 Instructivo Informática Forense
GS04-F01 Registro Cadena de Custodia
GS04-F02 Formato de Adquisición de Imágenes Forenses
GS04-F03 Rotulo Elemento Materia de Prueba o Evidencia Física
GS04-F06 Acta de Unificación de Evidencias Digitales

8.1 DOCUMENTOS EXTERNOS

N.A.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se reemplaza el concepto del modelo ATI por el modelo API. Se realizan ajustes de conceptos Se elimina la noción de “tratamiento” Se agrega la noción de “procesamiento” Correcciones generales

Fin documento