|  |  |
| --- | --- |
| **ACTA- N°** | **[***Número asignado***]** |

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

**OFICINA DE TECNOLOGÍA E INFORMÁTICA**

**GRUPO DE TRABAJO DE INFORMÁTICA FORENSE Y SEGURIDAD DIGITAL**

**RADICADO [*EN NÚMERO EL RADICADO*]**

En la ciudad de Bogotá, el [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] del [*Año en letras*] ([*Año en números*]), el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante “GTIFSD”) de la Superintendencia de Industria y Comercio (en adelante “SIC”), recibe por parte del [*Grupo que realiza la solicitud*] la solicitud de realizar la revisión y preservación de (los) sitio(s) web [*Listar los sitios web o URLs a preservar*] y (Sí aplica) el (las) APP(s) [Listar las APP], correspondiente al expediente con radicado N° [*En números el número de radicado*], con el fin de preservar las pruebas que puedan llegar a ser indicios de prácticas en contra del régimen de [*Identificar el régimen*] por parte de dicho sitio web y APP (Sí aplica).

1. **DESCRIPCIÓN DEL REQUERIMIENTO**

[*Nombre de la persona que hace la solicitud*], [*Cargo*], [*Grupo de trabajo y Delegatura*] solicita al GTIFSD el día [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] del [*Año en letras*] ([*Año en números*]) la revisión y preservación de (los) sitio(s) web [*Listar los sitios web o URLs a preservar*] y (Sí aplica) el (las) APP(s) [Listar las APP],que corresponden al caso con número de radicado N° [*En números el número de radicado*] **–** [*NOMBRE DEL CASO EN MAYÚSCULA SOSTENIDA*]. Al finalizar la inspección se solicita al GTIFSD un contenedor de evidencia digital con los elementos materiales probatorios (en adelante “EMP”) necesarios para las posibles investigaciones adelantadas por la entidad.

1. **HERRAMIENTAS DE SOFTWARE Y HARDWARE UTILIZADAS**

A continuación, se relacionan las herramientas de software y hardware utilizadas para realizar la inspección del sitio web y APP objeto de la revisión y copia de esta información a un dispositivo contenedor de evidencia digital ([Identificar el tipo de dispositivo])

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOFTWARE/HARDWARE** | **PROPÓSITO** | **NOMBRE** | **VERSIÓN** | **FABRICANTE** |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |

Tabla 1 Relación de herramientas de software y hardware utilizadas en la actividad.

1. **ACTIVIDAD**

A continuación, se enuncia la actividad de Preservación para los sitios web y APP (Si aplica) a Inspeccionar según la solicitud realizada al GTIFSD por el [*Grupo de trabajo y Delegatura*], se describe la metodología y herramientas utilizadas que permitirán generar el análisis solicitado.

* 1. **BÚSQUEDA Y COMPROBACION DEL SITIO WEB**

Inicialmente se desarrolla un proceso de búsqueda y comprobación de información basada en el requerimiento definido por [*Grupo de trabajo y Delegatura*]:

* **Apertura de los enlaces a preservar.**

De acuerdo con el requerimiento, se realiza una revisión del (los) sitio(s) web [*Listar los sitios web o URLs a preservar*] utilizando el Motor de Búsqueda Web Google, realizando navegación de todos los enlaces que la componen, utilizando los navegadores [*Listar los navegadores empleados separados por comas*].

* **(SI APLICA) Revisión de Aplicaciones y/o Bases de Datos Embebidas.**

De acuerdo al requerimiento, se realiza una revisión del (los) sitio(s) web [*Listar los sitios web o URLs a preservar*] buscando aplicaciones y/o formularios que recauden algún tipo de información, revisando servicios ofrecidos y demás datos relevantes, realizando impresión por pantalla en formato Portable Network Graphics (\*.PNG) y/o Joint Photographic Experts Group (\*.JPG).

* **(APLICA PARA APP) Revisión de Aplicación Móvil.**

De acuerdo con el requerimiento, se realiza una búsqueda en google play desde el emulador de Android para PC ***BlueStacks*** y en el buscador de Google de la [*Listar las APP separadas por coma*], revisando los servicios ofrecidos, la información de la aplicación, formularios y demás datos relevantes, realizando impresión por pantalla en formato Portable Network Graphics (\*.PNG) y/o Joint Photographic Experts Group (\*.JPG).

* (APLICA PARA PRESERVACIONES DEL GRUPO DE PROTECCION DE DATOS PERSONALES)**Búsqueda de información referente al tratamiento de datos personales.**

Se explora el sitio web [*Listar las páginas web separadas por coma*] identificando: personas responsables o encargados del tratamiento de datos personales, términos y condiciones, política de tratamiento o protección de datos personales, aviso de privacidad, finalidad del tratamiento, contactos, canales de atención para la gestión de los derechos de los titulares y demás requerimientos allegados en la solicitud inicial.

* 1. **INFORMACIÓN TÉCNICA DEL SITIO WEB**

A continuación, se realiza la búsqueda de [*Información del sitio web y/o de la APP*] solicitada, mediante herramientas web gratuitas que generan un compendio de información relacionada con la búsqueda solicitada, cada herramienta web describe un aspecto informativo y técnico relacionado con el sitio web y/o APP inspeccionado(s), descrito así:

* **Búsqueda de información referente a la existencia y representación legal (RUES)** Se realiza una búsqueda en la base de datos del RUES con el fin de determinar la información relevante de la empresa. Basado en los resultados se define la actividad, estado y objeto social de la empresa.
* **Revisión de dominio**. Utilizando el dominio del sitio web solicitado se realiza la verificación de información en la base de datos WHOIS.
* **Categorización de sitio web.** Se revisa y comprueba la categoría actual de la página y la descripción resultante.
* **Reputación del Dominio.** se valida la reputación del sitio web [*Listar los sitios web separados por coma*]. La reputación online es la imagen de una empresa, persona o institución en Internet, compuesta por las noticias, comentarios y opiniones expresadas por terceros en redes sociales, foros, blogs, Trafico Spam, Tráfico malicioso y otros medios online.
* **Revisión Virus,** Se realiza el análisis de archivos y el sitio web para detectar virus, gusanos, troyanos o cualquier otro tipo de malware.
* **Revisión Certificados SSL/TLS[[1]](#footnote-1),** la verificación SSL se efectúa para evaluar parámetros de navegación segura como: uso de certificados y firmas, también explora CN, SAN, organización, OU, ciudad, número de serie, tipo de algoritmo, tamaño de clave y detalles de la cadena de certificados.
* **Escaneo Pasivo de sitio web,** Utilizando herramientas no intrusivas se genera un informe básico donde se determina la existencia de vulnerabilidades presentes en el sitio web [*Listar los sitios web separados por coma*].
  1. **PRESERVACIÓN DE SITIOS WEB**

Después de realizar las verificaciones anteriores se procede a realizar la preservación de todos los mensajes de datos y posibles EMP; de acuerdo a la siguiente actividad:

* Se realiza la descarga del sitio o sitios web explorados según la solicitud utilizando el software[*Listar el software empleado*]*,* esta aplicación captura sitios completos o elementos dentro de un sitio.
* **(SI APLICA)** Al presentarse dificultad técnica de la preservación de Banners[[2]](#footnote-2) o ventanas emergentes[[3]](#footnote-3), es necesario realizar la preservación mediante la impresión por pantalla en formato Portable Network Graphics (\*.PNG) del enlace. Para la ejecución de la toma y captura de impresión por pantalla se utiliza [*Listar el software empleado*] o la Aplicación de Microsoft Windows *Recortes*.
* Por último, todas las consultas adicionales de información realizadas anteriormente descritas se preservan con el navegador y su opción guardar como, para conservar esta información en su formato original.
  1. **ADQUISICIÓN DE IMAGEN FORENSE**

Finalmente, de acuerdo con los mensajes de datos recaudados y preservados anteriormente, se adquiere una imagen forense parcial para todos los hallazgos. Esta imagen se realiza y verifica con el software FTK Imager, lo anterior garantiza la integridad[[4]](#footnote-4) e inalterabilidad de la información mediante la Huella HASH[[5]](#footnote-5). En el desarrollo de esta actividad se encontrará la información detallada de este paso.

1. **BUSQUEDA Y COMPROBACION DEL SITIO WEB**

A continuación, se describen detalladamente las actividades realizadas en cada etapa de la búsqueda y comprobación del sitio web [*Listar los sitios web*].

* **Apertura de los enlaces a preservar**

De acuerdo al requerimiento, se realiza la revisión del sitio web [*Listar los sitios web*] y las páginas principales que lo componen, se recolecta en video la inspección general de la página y se toman las capturas de pantalla que se describen a continuación:

[*Descripción URL*]

|  |
| --- |
|  |

Imagen [Número] Index [sitio web], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

[*Descripción URL*]

|  |
| --- |
|  |

Imagen [Número] Index [Pagina web], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

[*Descripción y url N*]

|  |
| --- |
|  |

Imagen [Número] Index [Pagina web], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

(Insertar las necesarias)

* **(SI APLICA) Revisión de Aplicaciones y/o Bases de Datos Embebidas**

De acuerdo al requerimiento, se realiza una revisión del sitio web [*Pagina web*] donde se encuentra la aplicación [*Aplicación*] y/o formulario [*Formulario*] que recauda los datos, [*Listar los datos separados por comas*].

[*Descripción URL*]

|  |
| --- |
|  |

Imagen [Número] [Aplicación], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

[*Descripción URL*]

|  |
| --- |
|  |

Imagen [Número] [Formulario], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

(Insertar las necesarias)

* **(SI APLICA) Revisión De Aplicación Móvil**

De acuerdo con el requerimiento se realiza la búsqueda y descarga de la APP [*Listar las App separadas por coma*] en Google Play desde (nombrar software o hardware usado para la descarga de la APP), tomando capturas de pantalla y un video de la información general de la APP, instalación, inspección y revisión del servicio ofrecido más los componentes adicionales de la misma.

[*Descripción*]

|  |
| --- |
|  |

Imagen [Número] [App], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

[*Descripción*]

|  |
| --- |
|  |

Imagen [Número] [APP componente], obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

(Insertar las necesarias)

**(SI APLICA)**

* **Búsqueda de información referente al tratamiento de datos personales.**

Se explora el sitio web [página web] y la aplicación [Nombre de la APP] identificando: personas, responsables, encargados del tratamiento de datos personales, términos y condiciones, política de tratamiento o protección de datos personales, aviso de privacidad, finalidad del tratamiento, contactos, canales de atención para la gestión de los derechos de los titulares, otros relacionados con la solicitud inicial.

[Descripción y url N]

|  |
| --- |
|  |

<Imagen N> <página N>, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

<Descripción y url N>

|  |
| --- |
|  |

<Imagen N> <página N>, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

(Insertar las necesarias)

1. **INFORMACIÓN TÉCNICA DEL SITIO WEB**

De acuerdo con el requerimiento se realiza una revisión del sitio web [Nombre del sitio], identificando la información del registro mercantil, información del dominio y las condiciones de seguridad implementadas en la página o aplicación, para mitigar la alteración, perdida, consulta, uso o acceso no autorizado. Esta inspección se detalla a continuación:

* **Búsqueda de información referente a la existencia y representación legal (RUES)**

|  |
| --- |
|  |

<Imagen N> <página N>, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **Revisión de dominio,**

Según la consulta realizada por WHOIS del sitio web [Pagina web] se identifica [o no] el propietario y/o responsables del sitio inspeccionado así:

|  |
| --- |
|  |

<Imagen N> <página N>, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **Categorización de sitio web.**

La página revisada es [Pagina web], esta página está categorizada (o no) actualmente como:

|  |
| --- |
|  |

<Imagen N> <página N>, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **Reputación del Dominio.**

Se realiza la inspección del sitio web [Pagina web], encontrando que cuenta con reputación [buena, mala o neutra], como se muestra a continuación:

|  |
| --- |
|  |

<Imagen >, reputación del sitio web <página web> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

Se realiza inspección de la dirección ip [insertar dirección IP del sitio], relacionada al sitio web [Pagina web], encontrando que [no] cuenta reportes de bloqueos DNS, [no] cuenta con reportes de correos infectados o spam, el ISP (Ifx networks) esta IP se ubica en [Insertar ciudad y país separado por coma] como se muestra a continuación:

|  |
| --- |
|  |

<Imagen >, Revisión de la dirección IP <ip sitio web> relacionada con el sitio web <página web> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **Revisión Virus.**

Se realiza el análisis con [Inserta número de analizadores usados] analizadores que clasifican como sitio limpio de archivos y amenazas presentes al sitio web [Pagina web], como se muestra a continuación:

|  |
| --- |
|  |

<Imagen >, Revisión de virus relacionada con el sitio web <página web> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

(SI APLICA)

|  |
| --- |
|  |

<Imagen >, detecciones encontradas en virus total del sitio web <página web> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **Revisión Certificados SSL/TLS.**

Se realiza verificación SSL, se efectúa para evaluar parámetros de navegación segura en el sitio web [Pagina web], según la validación realizada se encuentra presente un certificado con las siguientes características.

|  |
| --- |
|  |

<Imagen >, Revisión certificados SSL/TLS del sitio web <página web> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

* **(SOLO PARA APP) Análisis de privacidad para Android:**

Se realiza el análisis de privacidad para la APP (Nombre de la APP), encontrando (Insertar el número de permisos) permisos potencialmente peligrosos por las acciones que la aplicación puede hacer en el sistema Android del teléfono celular donde se instala el APP analizada. Los niveles de gravedad se definen de acuerdo con los niveles de protección de Google.

[Listar los permisos]

|  |
| --- |
|  |

<Imagen >, Análisis de privacidad en las aplicaciones de Android de la APP <Nombre APP> obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.

1. **PRESERVACIÓN DE SITIOS WEB**

De acuerdo con el requerimiento y una vez hecha la inspección del sitio web [Página web] y/o la APP [Nombre de la APP], por parte del GTIFSD, se identificaron ciertos grupos de hallazgos, a continuación, su descripción:

| **Número de grupo de Hallazgo** | **Nombre del grupo del Hallazgo** | **Descripción del contenido del grupo** | **Número de sitios web preservados** |
| --- | --- | --- | --- |
| 1 | Hallazgo 1 – Preservación URL solicitada | Contiene la preservación de los enlaces web que hacen parte del sitio web:  [Página web] |  |
| 2 | Hallazgo 2 – Preservación Herramientas web adicionales | Contiene la preservación web de las consultas:   * RUES * WHOIS * Categorías * Reputación * Test Virus * Certificados SSL/TLS * Análisis de privacidad para Android |  |
| 3 | Hallazgo 3 – Otros | Preservación web según inspección y solicitud inicial. |  |

<Tabla N>: Resumen distribución hallazgos

1. **ADQUISICIÓN DE IMAGEN FORENSE PARCIAL**

De acuerdo con los EMP preservados anteriormente, se realiza una única imagen forense parcial para todos los hallazgos, esta imagen se realiza y verifica con el software FTK Imager, dicha imagen se encuentra en la carpeta “IMG\_PRESERVACION”, en la siguiente tabla se adjunta un cuadro resumen del contenido de la imagen:

| **Número de Archivos .AD** | **Número de Archivos .CSV** | **Número de Archivos .TXT** |
| --- | --- | --- |
|  |  |  |

<Tabla N>: cantidad de archivos por extensión generadas en imagen forense

El informe de adquisición de la Imagen forense que genera el software forense citado anteriormente, indica que la imagen forense inició el día [en texto (días en números)] del mes de [mes en texto] del año [Año en número] a las [hora militar] y terminó a las [hora militar] (si aplica) del mismo día ó el día [en texto (días en números)] del mes de [mes en texto] del año [Año en número], a continuación, se cita el informe de adquisición que se encuentra en formato de archivo de texto (.TXT)

|  |
| --- |
|  |

<Figura N> Contenido de hash de preservación web <nombre.txt>

La preservación de los Sitios Web en archivos de lenguaje de marcas de hipertexto (.HTML), Portable Network Graphics (\*.PNG), las páginas que lo componen y todos los hallazgos encontrados en la inspección realizada del sitio web [Página web] y la APP [Nombre de la APP], se encuentra en la siguiente estructura de carpetas según su contenido (TreeSize):

|  |
| --- |
|  |

<Figura N> Imagen de carpetas de preservación “<radicado>” obtenida con el software WinDirStat

1. **INFORMACIÓN DE CONTENEDOR DE EVIDENCIA DIGITAL FINAL**

Se realiza el traspaso de las imágenes forenses a un contenedor de evidencia digital [identificar el tipo de dispositivo] con las siguientes características técnicas:

|  |  |  |
| --- | --- | --- |
|  |  | **DISPOSITIVO DESTINO** |
| **ANÁLISIS FÍSICO** | **Radicado** |  |
| **Ubicación** |  |
| **Tipo de Dispositivo** |  |
| **Marca** |  |
| **Serial Físico** |  |
| **Estado Físico** |  |
| **ANÁLISIS LÓGICO** | **Capacidad total** |  |
| **Espacio utilizado o tamaño** |  |
| **Número Archivos** |  |
| **Número Carpetas** |  |
| **Serial Lógico** |  |
| **Estado Lógico** |  |

<Tabla > resumen de información contenedor de evidencia digital “<radicado>” preservación del sitio web <pagina web>

1. **OBSERVACIONES**

Se realizan las observaciones enumeradas a continuación.

1. **ANEXOS**

Los anexos de este documento son los siguientes:

|  |  |  |
| --- | --- | --- |
| **Descripción** | **Anexo** | **Folios** |
| Anexo 1 | Resumen de páginas Web/APP preservadas |  |
| Anexo 2 | Informe de inspección software VSO Inspector |  |
| Anexo 3 | Formato de extracción de imágenes forenses |  |
| Anexo 4 | Cadena de custodia anterior y posterior de dispositivo contenedor de evidencia digital |  |
| Anexo 5 | Contenedor digital de evidencias serial físico S/N: número |  |

<Tabla > resumen anexos acta de preservación del sitio web <página web>

La actividad termina el día [en números] del mes de [en texto] del año [en número] a la hora en [formato militar], firman los encargados de las actividades técnicos mencionados y la revisión de la presente acta por parte del GTIFSD,

|  |  |
| --- | --- |
| **Realizado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **NOMBRE**  C.C CÉDULA de CIUDAD  Servidor Público y/o Contratista – ACE Accessdata Certified Examiner | **Revisado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **NOMBRE**  C.C CÉDULA de CIUDAD  Servidor Público y/o Contratista – ACE Accessdata Certified Examiner |

**ANEXO Número de anexo**

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **CANTIDAD FOLIOS** |
| Resumen de páginas Web/APP preservadas |  |
| Informe de inspección software VSO Inspector |  |
| Formato de extracción de imágenes forenses |  |
| Cadena de custodia anterior y posterior de dispositivo contenedor de evidencia digital |  |
| Contenedor digital de evidencias serial físico S/N: número |  |

1. RESUMEN DE PÁGINAS WEB/APP PRESERVADAS

|  |  |  |  |
| --- | --- | --- | --- |
| **RAZON SOCIAL** | **NIT** | **NOMBRE COMERCIAL DEL SITIO WEB** | **URL** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. “Un certificado SSL/TLS es un objeto digital que permite a los sistemas verificar la identidad y, posteriormente, establecer una conexión de red cifrada con otro sistema mediante el protocolo Secure Sockets Layer/Transport Layer Security (SSL/TLS). Los certificados se emiten con un sistema criptográfico conocido como infraestructura de claves públicas (PKI). PKI permite que una parte establezca la identidad de otra parte mediante el uso de certificados si ambos confían en un tercero, conocido como autoridad de certificación. Por lo tanto, los certificados SSL/TLS funcionan como tarjetas de identidad digitales que aseguran las comunicaciones de red y establecen la identidad de los sitios web en Internet, así como los recursos en las redes privadas.” Fuente: Amazon: https://aws.amazon.com/es/what-is/ssl-certificate/ [↑](#footnote-ref-1)
2. Un banner es un formato estándar de publicidad en internet, desarrollado en Flash Player, con pequeñas animaciones y reclamos publicitarios. Ver Editorial Vértice, “*Técnicas avanzadas de diseño web”*, p.175. [↑](#footnote-ref-2)
3. Una ventana emergente se trata de un formato flotante que no forma parte de la página web, sino que aparecen por encima o por debajo de éstas. Ver Aparicio Marino, *“La construcción de la realidad en los medios de comunicación”*, p. 262. [↑](#footnote-ref-3)
4. Propiedad de salvaguardar la precisión y completitud de los recursos NORMA ISO 27001, Términos y definiciones. [↑](#footnote-ref-4)
5. Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash. Fuente: Agencia Española de Protección de Datos Personales: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion\_ficheros/preguntas\_frecuentes/glosario/index-ides-idphp.php [↑](#footnote-ref-5)