Preservación de Evidencia Digital en la Nube

Lic. Gastón Semprini, Lic. Gerardo Nilles, Lic. Gaston Silva

Departamento de Informática Forense del Poder Judicial de la Provincia de Rio Negro.
Argentina
gsemprini@jusrionegro.gov.ar
gnilles@jusrionegro.gov.ar
gsilva@jusrionegro.gov.ar

Abstract. La computación en la nube es la tendencia, en el proceso de transformación digital, más adoptada por organizaciones de todos los tamaños.
El objetivo del análisis forense en la nube es obtener evidencia digital manteniendo la seguridad e integridad de la información almacenada en la nube.
Este artículo aborda el aspecto metodológico y las buenas prácticas referidas a la obtención de evidencia digital almacenada en la nube.

Keywords: Nube, análisis, forense, evidencia.

1 Introducción

De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST) [1], la ciencia de la informática forense en la nube se define como "la aplicación de principios científicos, prácticas tecnológicas y métodos derivados y probados para reconstruir los eventos pasados de computación en la nube a través de la identificación, recolección, preservación, examen, interpretación y reporte de la evidencia digital."

En el caso de la informática forense tradicional, el investigador sigue pautas y metodologías bien definidas. En este caso, el proceso abarca el secuestro, la copia de imágenes forenses y el análisis digital para producir un reporte.

La adquisición de evidencia digital de entornos en la nube es más restrictivo porque las infraestructuras y los recursos no son propiedad de los usuarios de la nube sino que son proporcionados por los proveedores de servicios en la nube (CSP) Cloud Service Provider. Los usuarios tienen acceso limitado a los datos y no tienen conocimiento de dónde se encuentran físicamente [2].

2 Guía de buenas prácticas

En función del estudio y pruebas realizadas en el Área de informática forense del poder judicial de Rio Negro elaboró una guía de buenas prácticas para la obtención de evidencia digital de proveedores de servicios en la nube. El objetivo de esta guía es otorgar un marco formal adecuado que permita ofrecer rigurosidad y control de calidad en la

integración de métodos y técnicas utilizadas. Para la elaboración de esta guía se siguieron los lineamientos propuestos por Scientific Working Group on Digital Evidence (SWGDE) [3].

2.1 Limitaciones

Esta guía no es exhaustiva para las personas que no tienen experiencia en la adquisición de evidencia digital, para su utilización el investigador debe poseer una comprensión básica de la metodología.

Dada la gran cantidad de plataformas y proveedores de servicios en la nube, no es posible establecer un conjunto preciso de procedimientos para cubrir cada situación. El investigador debe seleccionar las acciones apropiadas en función de los recursos disponibles y su conocimiento y comprensión del caso investigado.

2.2 Datos en la nube

El almacenamiento en la nube se utiliza frecuentemente para aumentar la capacidad de almacenamiento, sincronizar información entre dispositivos u ofrecer servicios informáticos remotos.

Los dispositivos informáticos pueden sincronizar o hacer una copia de seguridad de los datos y configuraciones de los usuarios a los proveedores de la nube de forma predeterminada, lo que requiere poca interacción del usuario. Algunos dispositivos tienen por defecto una sincronización automática con servicios en la nube, como ser WhatsApp, Redes Sociales, imágenes, videos, documentos del dispositivo, etc. El investigador debe tener en cuenta que los datos pueden existir en varios lugares.

Puede haber diferencias en el estado de cifrado entre un dispositivo local y los datos sincronizados con la nube. Los datos en el dispositivo local pueden estar encriptados o ser difíciles de decodificar, sin embargo, al solicitar datos al proveedor de la nube podría proporcionarlos de forma no encriptada o legible.

Un proveedor puede proporcionar información adicional asociada con esa cuenta, como dispositivos históricos, actividad del dispositivo y registros de usuario. Los datos históricos almacenados en la nube pueden ser más extensos y valiosos que los encontrados en un dispositivo local.

2.3 Métodos de adquisición

Acceso por credenciales

La evidencia se obtiene ingresando las credenciales aportadas por la parte interesada, típicamente un nombre de usuario o cuenta de correo electrónico y su contraseña. También se pueden obtener credenciales de los dispositivos físicos que se encuentren bajo investigación. Algunos proveedores de servicios en la nube permiten el acceso a los datos almacenados con ellos y los metadatos asociados a través de aplicaciones cliente o API. Es posible que el acceso a los datos a través de estas API se pueda obtener desde un dispositivo en investigación que utiliza los servicios en la nube. En los casos que las

credenciales no sean aportadas por las partes interesadas es necesario contar con la correspondiente autorización legal.

Oficio a las compañías

La evidencia se obtiene solicitando información a los distintos proveedores de servicios. Se puede obtener información valiosa como por ejemplo número de teléfonos y correos electrónicos asociado, horarios e IP de Conexión, etc. Por lo general no se obtienen contenidos, como mensajes enviados y recibidos y/o publicaciones realizados. Se deben consultar las secciones de Legales de los proveedores para conocer cómo realizar el pedido y que información se puede obtener.

Pasos anteriores a la adquisición

Identificar los datos particulares buscados, los períodos de tiempo relevantes, los proveedores de servicios en la nube involucrados y los servicios utilizados.

Los registros de facturación y la información de la cuenta pueden identificar el proveedor y los servicios específicos.

La mayoría de los proveedores publican políticas de privacidad en su sitio web que detallan los servicios que brindan, los tipos de información que recopilan y las circunstancias bajo las cuales recopilan esa información.

Si corresponde, solicitar al proveedor que preserve los datos buscados.

Pasos durante la adquisición

Documentar el proceso de adquisición, los métodos utilizados, cómo se reciben los datos. Tomar fotografías, filmar y capturas de pantalla o en algunos casos realizar una grabación de la sesión utilizada.

Determinar si los datos relevantes pueden adquirirse utilizando el método de adquisición planificado.

Obtener los datos utilizando el método de adquisición seleccionado.

Si surgen problemas para obtener los datos a través de métodos planificados, intentar métodos alternativos. Si todos los métodos fallan, considerar las capturas de pantalla o fotografías de los datos relevantes.

Pasos posteriores a la adquisición

Calcular y registrar valores hash para los datos adquiridos. Si un proveedor provee información firmada digitalmente o proporciona valores hash, verificar la firma o los valores hash.

Verificar que se hayan adquirido todos los datos.

Si los datos se proporcionaron en medios físicos documentar como se recibió.

Seguir los procedimientos del área para almacenar los datos adquiridos, transferir los datos adquiridos a un medio adecuado de almacenamiento de evidencia, para ser entregados al área correspondiente.

3 Marco Normativo

Resulta necesario establecer un marco normativo comprensible y viable de buenas prácticas respecto a la extracción de evidencia digital almacenada en la nube.

En el caso del Poder Judicial de Río Negro, el marco normativo es establecido por la Acordada 8/2019 Superior Tribunal de Justicia. [4]

La intención de la Acordada es garantizar que la preservación de la evidencia se realice bajo un procedimiento metodológico y riguroso siguiendo los protocolos, procedimientos estándares y guías de buenas prácticas para ello.

Dentro de los considerandos, se establece que:

- Las preservaciones se realizan utilizando las credenciales de acceso a las correspondientes plataformas que pueden ser obtenidas de los dispositivos o aportadas por el propietario.
- Al no requerir acceso al dispositivo la preservación de evidencia se puede realizar a distancia independiente del dispositivo en el cual se haya originado, recibido o almacenado el dato pudiendo en determinadas circunstancias recuperar datos eliminados.
- La evidencia preservada de esta manera puede ser analizada utilizando las mismas técnicas y herramientas que para la evidencia tradicional.

En el contexto de la Acordada se brindó una capacitación a los operadores de justicia sobre la importancia de la obtención de este tipo de evidencia, se generó un protocolo de actuación en el cual se establecen los pasos a seguir por el operador que requiere el servicio. También se dotó a las oficinas de acceso a internet por WI-FI para los casos en que se requiera la sincronización de datos de un dispositivo con la nube.

4 Conclusiones

El objetivo de este trabajo es aportar una guía de buenas prácticas para la obtención de la información almacenada en la nube, generando el marco normativo comprensible y viable de buenas prácticas respecto de la extracción de evidencia digital almacenada en la nube.

En el caso de la provincia de Rio Negro, que cuenta con un laboratorio de informática forense en la ciudad capital, brindando servicios a toda la provincia, la adquisición de evidencia digital almacenada en la nube ha permitido obtener evidencia aportada por una víctima, un testigo o cualquier persona que se encuentre realizando una denuncia en cualquier ciudad de la Provincia, sin importar la distancia a la que se encuentre del laboratorio optimizando los tiempos y obteniendo evidencia que en algunos casos se perdía por no ser aportada.

Este servicio permitió al Poder Judicial de Rio Negro no solo darle celeridad al proceso, sino también validación de información documental como así también obtención de información de testigos, victimas y/o denunciantes en el momento.

Referencias

1. N. C. C. F. S. W. Group. NIST cloud computing forensic science challenges. Draft NISTIR 8006, 2014.
2. Stavros Simou, Christos Kalloniatis, Stefanos Gritzalis, Haralambos Mouratidis: A survey on cloud forensics challenges and solutions. Security and Communication Networks, Noviembre 2016.
3. SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers Versión: 1.0 (Julio, 2019) .
4. Superior Tribunal de Justicia de la provincia de Rio Negro. Acordada 8/2019. https://digesto.jusrionegro.gov.ar/bitstream/handle/123456789/9351/Ac008-19.pdf?sequence=1&isAllowed=y