

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

San Borja, 11 de Julio del 2023

INFORME TEC PREVIO EVALUACION DE SW N° 000010-2023-OTI-

A : **SAUL ENRIQUE VASQUEZ ARTEAGA**
Jefe de la Oficina de Tecnologías de la Información

DE : **MARIA SOFIA CASTILLO QUISPE**
Unidad de Operaciones y Soporte de Tecnologías de la Información

ASUNTO : Informe Técnico Previo de Evaluación de Software para
recuperación, extracción y análisis forense de dispositivos móviles

REFERENCIA: HOJA DE TRAMITE N° 000249-2023-OTI-UTI/INDECOPÍ
(22JUN2023)

1. NOMBRE DEL ÁREA

Oficina de Tecnologías de la Información - OTI

2. RESPONSABLE DE LA EVALUACIÓN

María Sofía Castillo Quispe

3. CARGO

Especialista 2

4. FECHA

La que se indica en la parte superior.

5. JUSTIFICACIÓN

Mediante la Ley de Represión de Conductas Anticompetitivas (D.Leg. N°1034), se facultó a la Dirección Nacional de Investigación y Promoción de la Libre Competencia - DLC a "realizar inspecciones, con o sin previa notificación, en los locales de las personas naturales o jurídicas, sociedades irregulares y patrimonios autónomos y examinar los libros, registros documentación y bienes, pudiendo comprobar el desarrollo de procesos productivos y tomar la declaración de las personas que en ellos se encuentren. En el acto de la inspección podrá tomarse copia de los archivos físicos, magnéticos o electrónicos, así como de cualquier documento que se estime pertinente o tomar las fotografías o filmaciones que se estimen necesarias. Para ingresar podrá solicitarse el apoyo de la fuerza pública", por lo que requieren contar con herramientas forenses adecuadas para la recolección, transferencia, procesamiento y análisis de evidencia electrónica de dispositivos móviles recabada durante las visitas de inspección.

5. ALTERNATIVAS

Los productos de software alternativo a ser comparados son:

- CELLEBRITE UFED 4PC
<https://cellebrite.com/es/cellebrite-ufed-es/>

- OXYGEN FORENSICS Detective
<https://oxygenforensics.com/en/products/oxygen-forensic-detective/>
- Avilla Forensics <https://github.com/AvillaDaniel/AvillaForensics>

El presente informe aplica para adquisición, renovación, mantenimiento y suscripción de Software para recuperación, extracción y análisis forense de dispositivos móviles.

7. ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N°139-2004-PCM.

7.1. Propósito de la evaluación

Producto final: Seleccionar un producto entre productos alternativos

7.2. Tipo de producto

Software de recuperación, extracción y análisis forense de dispositivos móviles

7.3. Modelo de Calidad

Se ha aplicado el modelo de calidad de software ISO/IEC 9126 descrito en la Guía Técnica sobre Evaluación de Software para la Administración Pública.

7.4. Selección de métricas

Las métricas fueron identificadas de acuerdo con los requerimientos de la DLC y a la información técnica de los productos señalados en el punto 6.

ITEM	ATRIBUTOS INTERNOS Y EXTERNOS
1	Debe soportar como mínimo los siguientes dispositivos: - o Teléfonos tradicionales. - o Teléfonos inteligentes (smartphone). - o Tarjetas SIM.
2	Debe permitir extraer y revisar como mínimo los siguientes datos: - o Registro de llamadas. - o Mensajes SMS. - o Libreta de contactos. - o Calendario. - o Correo electrónico. - o Archivos multimedia (imágenes y audios). - o Datos de aplicaciones de tercero.
3	Debe permitir extraer la información. - o Extracción física. - o Extracción lógica.
4	Debe permitir el desarrollo de los siguientes procesos: - o Extracción de evidencia en dispositivos Android, IOS y BlackBerry. - o Lectura de tarjetas SIM. - o Extracción o bypass de password de bloqueo. - o Recuperación de datos borrados o eliminados. - o Compatible con backups de Android, IOS y BlackBerry.
5	Debe soportar las siguientes técnicas de búsqueda: - o Búsqueda avanzada en texto abierto. - o Búsqueda avanzada basada en parámetros específicos.
6	Debe permitir la visualización de base de datos SQLite.
7	Debe permitir eludir bloqueos de pantalla.
8	Debe ser de licenciamiento perpetuo o suscripción

ITEM	ATRIBUTOS INTERNOS Y EXTERNOS
9	Debe mostrar alertas que hay actualizaciones disponibles.
10	Debe permitir instalaciones en alta disponibilidad activo-pasivo y la activación es con el dongle.
11	Debe permitir exportar y personalizar informes en mínimo los siguientes formatos: o PDF. o XLS. o HTML.
12	Debe permitir crear mínimamente HASH MD5 por cada extracción.
13	Debe estar en idioma español o inglés.
14	Manuales incluido en la aplicación (instalación y configuración) en formato electrónico o en línea
15	Debe contar con soporte, vía telefónica o correo electrónico.
16	Con interfaz gráfica intuitiva
17	Debe permitir guardar con opción de visor para la revisión de otras áreas o entidades.
18	Debe permitir realizar vista gráfica y análisis de la información mediante: o Vista de conversación. o Lista de archivos. o Datos de geolocalización. o Cronología o Líneas de tiempo. o Creación de etiquetas
19	Requisitos mínimos de funcionamiento: Core i7, 32GB RAM y 1TB SSD.
20	El fabricante debe haber sido evaluado por terceros y no estar calificado como "participante" o "niche player".
21	El fabricante debe proveer actualizaciones frecuentes no menores de 3 meses.
22	Opción de nuevas versiones, parches y actualizaciones.
23	El fabricante publica en su portal seguro las versiones anteriores del software.
24	Debe permitir instalaciones en un mínimo de 2 computadoras y la activación es con el dongle.
25	Debe contar con mantenimiento de software (ISO 27001).
26	Debe soportar como mínimo los siguientes sistemas: o Android. o iOS. o BlackBerry
27	Debe ser compatible con Windows de 64 bits.
28	Debe de poder abrir múltiples ventanas.
29	Debe permitir hacer upgrade sin necesidad de cambiar el hardware.
30	El software no debe estar "amarrado" a un hardware específico.
ITEM	ATRIBUTOS DE USO
31	Permite etiquetar los resultados para que se pueda usar como filtro en las siguientes búsquedas.
32	Posee recursos y opciones de fácil manejo para ahorro potencial en el tiempo de procesamiento y análisis de la información, permitiendo lograr las metas especificadas con exactitud e integridad.
33	Licencia a través de dongle.
34	Interface gráfica intuitiva con figuras en los íconos fáciles de reconocer por el usuario.

7.5. Niveles/Escalas para las métricas

Se estableció niveles de calificación cualitativa en base a los siguientes puntajes:

MÉTRICAS	PUNTAJE
No cumple	0
Cumple parcialmente	2
Cumple Completamente	4

Considerando que la suma de los puntajes máximos es 100%, se considera la siguiente tabla de aceptación de alternativas:

NIVEL %	DESCRIPCIÓN
[0 - 90]	No califica No cumple con los requerimientos.
[91 - 100]	Califica Cumple total o aceptablemente con los requerimientos.

7.6. Comparación de criterios de calidad

Los criterios de valoración y toma de medidas de los productos de software, según las métricas definidas, se encuentran en el **anexo A** de la presente.

El software con mayor puntaje lo obtuvo OXYGEN con 99 puntos y en segundo lugar CELLEBRITE con 96 puntos. El software AVILLA no calificó.

8. ANÁLISIS COMPARATIVO DE COSTO BENEFICIO

En el presente análisis solo participan los productos de software que calificaron en el análisis comparativo técnico y se tomó en cuenta los siguientes conceptos:

* **Licenciamiento:** Se solicitaron cotizaciones (**ver anexo B**), pero solo se cotizó CELLEBRITE. Para OXYGEN se utilizó fuente histórica.

* **Hardware necesario para su funcionamiento:** Todos los productos se adaptan y son compatibles con la plataforma informática de hardware.

* **Soporte y mantenimiento externo:** La adquisición de la licencia debe contemplar el soporte y mantenimiento (derecho a actualizaciones) durante el periodo solicitado.

* **Personal y mantenimiento interno:** El Laboratorio Forense del Indecopi cuenta con el personal especializado realizar el mantenimiento (actualizaciones).

* **Capacitación:** El personal del Laboratorio Forense de Indecopi tiene conocimiento en el uso de los programas.

SOFTWARE	Precio unitario S/	1-% del total
CELLEBRITE	65100	39%
OXYGEN	40900	61%
Total	111060	100%

Nota: Los montos están expresados en Nuevos Soles e incluyen el IGV. Las cotizaciones se encuentran en el **anexo B** de la presente.

Para determinar el puntaje total se aplicó la siguiente fórmula:

$$PT = c_1P_t + c_2P_e$$

Donde:

PT = Puntaje total

P_t = Puntaje por evaluación técnica

P_e = Puntaje por evaluación económica

c₁ = Coeficiente de ponderación para la evaluación técnica (0.80)

c₂ = Coeficiente de ponderación para la evaluación económica (0.20)

De la aplicación de la fórmula se obtienen los resultados siguientes:

SOFTWARE	Puntaje de evaluación técnica (Pt)	Puntaje de evaluación económica (Pe)	PT = (0.80 x Pt) + (0.20 x Pe)
CELLEBRITE	96%	39%	84%
OXYGEN	99%	61%	91%

El software con mayor puntaje total es OXYGEN.

9. CONCLUSIONES

9.1. Del análisis comparativo técnico realizado, se observa que tanto el software Cellebrite y Oxygen cumplen con los requerimientos de la Dirección Nacional de Investigación y Promoción de la Libre Competencia para la recuperación, extracción y análisis forense de dispositivos móviles.

9.2. Del análisis comparativo costo beneficio realizado, se observa que el software Oxygen es el más conveniente.

10. FIRMAS

Atentamente,

MARIA SOFIA CASTILLO QUISPE

Unidad de Operaciones y Soporte de Tecnologías de la Información

Cc:

(MCQ)