

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

San Borja, 24 de Julio del 2023

INFORME TEC PREVIO EVALUACION DE SW N° 000012-2023-OTI-

A : **ENITH GIANCARO MATIAS HERRERA**
Jefa de la Oficina de Tecnologías de la Información(e)

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

ASUNTO : Informe Técnico Previo de Evaluación de Software para
extracción, recuperación, procesamiento y análisis forense de evidencia
digital

REFERENCIA: HOJA DE TRAMITE N° 000303-2023-OTI-UTI/INDECOPI
(18JUL2023)

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 extracción, recuperación, procesamiento y análisis forense de evidencia digital recabada durante las visitas de inspección.

3. ALTERNATIVAS
Los productos de software alternativo a ser comparados son:

- NUIX WORKSTATION <https://www.nuix.com/technology/nuix-workstation>

- NUIX DISCOVER <https://www.nuix.com/technology/nuix-discover>
- MAGNET AXIOM COMPUTER
<https://www.magnetforensics.com/products/magnet-axiom/computer/>
- MAGNET AXIOM CYBER
<https://www.magnetforensics.com/products/magnet-axiom-cyber/>

El presente informe aplica para cualquier modalidad de aprovisionamiento como adquisición, renovación, mantenimiento y suscripción de software.

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 extracción, recuperación, procesamiento y análisis forense de evidencia digital.

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 sistemas de archivos: - o FAT32. - o NTFS. - o EXT2.
2	Debe permitir adquirir, procesar y analizar como mínimo: - o Procesar grandes volúmenes de datos a alta velocidad. - o Correos electrónicos. - o Archivos de ofimática - o Permitir analizar mediante la creación de casos portables y/o la colaboración de forma segura en la nube. - o Permitir identificar y categorizar rápidamente la información de interés en un caso.
3	Debe permitir la adquisición de evidencias de manera remota o física
4	Debe permitir el desarrollo de los siguientes procesos: - o Procesar mínimo los siguientes formatos: E01, L01, DD, RAW - o Debe identificar datos duplicados - o Debe recuperar archivos eliminados - o Debe mostrar la visualización detallada del procesamiento.

ITEM	ATRIBUTOS INTERNOS Y EXTERNOS
5	Debe permitir extraer y revisar como minimo los siguientes tipos de archivos: o Correos (pst, ost, msg, nsf, dbx, mbox, eml). o Documentos (pdf, doc, docx, xls, xlsx, ppt, pptx, html). o Imagen (png, jpg, jpeg, tiff, bmp, gif). o Compresión (zip, rar, tar). o Otros (iso, xml, vhd).
6	Debe permitir analizar evidencias usando modelos de aprendizaje automático (IA) y/o algoritmos especializados. o Seguridad de datos. o Recolección de datos confiable. o Actualizaciones y mantenimiento
7	El fabricante debe emitir constantemente actualizaciones para evadir las vulnerabilidades por falta de mantenimiento.
8	Debe ser de licenciamiento perpetuo o suscripción
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	Toda información procesada debe ser accesible a través de la licencia (Dongle)
12	Debe permitir crear mínimamente el HASH MD5 en la 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 visualizaciones gráficas como: o Lista de archivos. o Vista conversación o Creación de etiquetas o Visualización cronológico o líneas de tiempo.
19	Requisitos mínimos de funcionamiento: Core i7 2.1GHz, 32GB RAM y 1TB SSD.

ITEM	ATRIBUTOS INTERNOS Y EXTERNOS
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 permitir la colaboración de usuarios mediante la creación de casos portables y/o la colaboración de forma segura en la nube. Para trabajar en diferentes dispositivos
27	Debe ser compatible con Windows de 64 bits.
28	Debe poder abrir múltiples ventanas
29	Debe permitir hacer upgrades sin necesidad de cambiar el hardware.
30	El software no debe estar "amarrado" a un hardware específico.
ITEM	ATRIBUTOS DE USO
31	Debe permitir la búsqueda por palabras clave y filtrado.
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	Interfaz 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.

Como resultado de la comparación técnica, los 4 productos de software superan el 90%.

El software con mayor puntaje lo obtuvo MAGNET AXIOM CYBER con 95.59%.

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:** Los precios se obtuvieron en primer lugar de cotizaciones actualizadas, luego de precios históricos y finalmente de páginas webs.

SOFTWARE	Precio unitario S/	1-Pu/ΣPu (%)
NUIX WORKSTATION	120,360.00	65.80%
NUIX DISCOVER	0.00	FALTA PRECIO
MAGNET AXIOM COMPUTER	94,568.00	73.13%
MAGNET AXIOM CYBER	136,980.00	61.08%
ΣPu	351,908.00	

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

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

* **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 para realizar el mantenimiento (actualizaciones).

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

Para el análisis comparativo de costo beneficio 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)
NUIX WORKSTATION	92.65%	65.80%	87.28%
NUIX DISCOVER	92.65%	0.00%	74.12%
MAGNET AXIOM COMPUTER	94.12%	73.13%	89.92%
MAGNET AXIOM CYBER	95.59%	61.08%	88.69%

El software con mayor costo beneficio total es MAGNET AXIOM COMPUTER, seguido de MAGNET AXIOM CYBER.

9. CONCLUSIONES

9.1. Del análisis comparativo técnico realizado, se observa que los 2 productos de software de NUIX y los 2 productos de software de MAGNET cumplen con los requerimientos de la Dirección Nacional de Investigación y Promoción de la Libre Competencia para la extracción, recuperación, procesamiento y análisis forense de evidencia digital.

9.2. Del análisis costo beneficio el software con mayor fue MAGNET AXIOM COMPUTER.

10. FIRMAS

Atentamente,

MARIA SOFIA CASTILLO QUISPE

Unidad de Operaciones y Soporte de Tecnologías de la Información

Cc:

(MCQ)