



**Informe Justificativo
Renovación de Licencias Opentext EnCase Forensic**

1. Información

1.1 Nombre de la Solución/Herramienta

Solución Opentext EnCase Forensic

1.2 Objetivo Principal

Fortalecer la seguridad cibernética de la institución mediante la renovación de soluciones y equipos integrales para la investigación, trazabilidad y realización de análisis forense digital.

1.3 Resumen del Informe

Este informe muestra la importancia y necesidad de renovar la solución Opentext EnCase Forensic, con el propósito de fortalecer la capacidad de respuesta ante incidentes y el respaldo de la integridad de las pruebas digitales de las investigaciones realizadas en el Departamento de Seguridad de la Información y Monitoreo.

A.C
E.A
M.S

2. Origen de la Necesidad

La Dirección General de Impuestos Internos (DGII) ha estado utilizando esta solución para realizar investigaciones digitales dentro del ámbito forense, ya que permite recolectar, analizar, preservar y presentar evidencias de forma estructurada, además, la solución permite recuperar datos, eliminados o encriptados desde discos duros, memorias extraíbles, entre otros dispositivos, lo cual es importante para esclarecer incidentes como fraudes internos, filtraciones de datos, actividades delictivas o incumplimientos de las políticas internas de nuestra institución.

3. Justificación de la Renovación

3.1 Necesidad de la Renovación

El Departamento de Seguridad de la Información y Monitoreo tiene como responsabilidad realizar investigaciones apegadas a procesos forenses para dar respuesta oportuna a los eventos e incidentes de seguridad presentados en la institución, esta solución facilita la capacidad de recolección, análisis y presentación de evidencias digitales en investigaciones forenses, además, es una solución confiable para el acceso a datos, incluso dañados o manipulados, archivos borrados y la visualización de cronología de eventos. En ese mismo contexto, con esta solución podemos realizar búsquedas detalladas, el cual lo hace un servicio indispensable para las investigaciones forenses. Por lo tanto, la institución debe tener la capacidad de contar con herramientas o soluciones tecnológicas que permitan que, ante cualquier incidente o evento, exista o se pueda realizar una investigación inmediata, capaz de recolectar y conservar de forma íntegra las pruebas o evidencias digitales, lo que ayuda a los ingenieros a reducir los tiempos de respuesta ante los casos que puedan surgir.

3.3 Riesgos Actuales

A continuación, la institución se expone a una serie de riesgos críticos, entre los que se destacan:

- Retraso en los tiempos de respuesta por falta de herramientas forenses.
- Fallas en la detección de comportamiento fraudulento o actividades sospechosas.





DSIM-149-2025

19 de diciembre 2025

- Falta de trazabilidad y documentación adecuada.
- Incumplimiento y fallas técnicas.
- Dificultades en recolección y trazabilidad de las evidencias presentes.
- Retraso en tiempos de respuesta a casos de urgencia.
- Creación de dependencia a herramientas temporales.

4. Beneficios de la Solución / Herramienta

Con la renovación de esta solución continuaremos con los siguientes beneficios:

- Captura de evidencia digital.
- Procesamiento rápido de grandes volúmenes de evidencia digital.
- Preservación forense confiable que garantiza la validez legal de los datos recolectados.
- Reducción significativa del tiempo por caso para los investigadores.
- Optimización del flujo de trabajo investigativo para reducir los tiempos de resolución.
- Herramientas avanzadas para examinar datos estructurados y no estructurados con precisión.
- Facilita la recolección completa de evidencia en discos duros, SSD, dispositivos móviles y otros medios digitales.

5. Conclusión

La renovación del licenciamiento de OpenText EnCase Forensic es fundamental para asegurar la integridad y efectividad de las investigaciones digitales en nuestra institución ya que la solución destaca por su confiabilidad y precisión en el análisis forense y la gestión de incidentes de ciberseguridad. Esta plataforma es conocida por su alta precisión en la preservación y análisis forense de evidencia digital, asegurando que los datos recolectados sean admisibles y confiables para procesos internos o legales. EnCase Forensic destaca por su capacidad para examinar grandes volúmenes de información de manera eficiente, identificar indicadores de compromiso, recuperar información eliminada o manipulada y generar reportes sólidos para la gestión de incidentes de ciberseguridad.

Elian M. Arias Z.

Encargado Sección de Monitoreo y Gestión de Incidentes de Seguridad

Miguel J. Santana S.

Ingeniero de Monitoreo y Gestión de Incidentes de Seguridad

Ashly C. Canelo S.

Ingeniera de Monitoreo y Gestión de Incidentes de Seguridad



Fin del documento

