

¿Cómo responder de manera efectiva a solicitudes regulatorias o litigios? ¿Cómo administrar grandes volúmenes de evidencia digital?

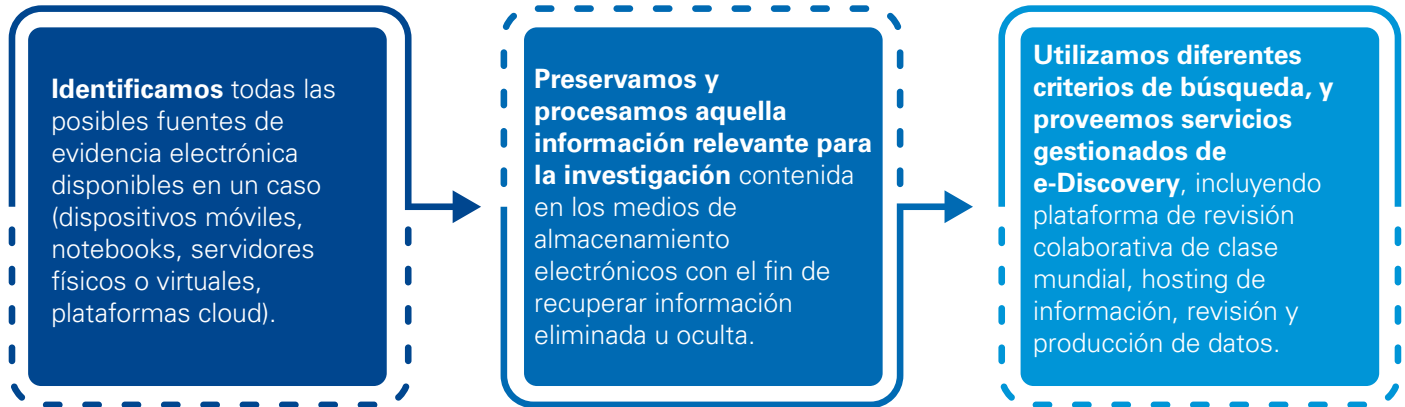
La integración entre nuestras herramientas y tecnologías nos permite mantener el control de los datos a través de cada fase del proceso de e-Discovery, mientras respondemos de manera ágil a los cambios de requisitos, alcance y prioridades de nuestros clientes.

Computer forensic | Identificación, preservación y procesamiento de evidencia

e-Discovery | Gestión, análisis y protección de grandes volúmenes de datos

Los servicios de e-Discovery y Computer forensic son un componente clave para resolver asuntos regulatorios o litigios de manera ágil.

En KPMG contamos con las capacidades para brindar asistencia a nuestros clientes durante las seis etapas del proceso de e-Discovery.



- Trabajamos respetando protocolos de cadena de custodia y utilizamos técnicas que permiten garantizar la no contaminación de la prueba electrónica preservada, para que la misma pueda ser aportada como evidencia válida en un proceso judicial.

- Utilizamos las herramientas de tecnología forense más actuales y reconocidas.

- Utilizamos técnicas que aplican la Inteligencia Artificial, además de diferentes criterios de búsqueda y procesamiento de evidencia digital para limitar el universo de archivos exclusivamente relacionados al asunto que se investiga.



Diego Bleger
Socio Líder de Advisory
dbleger@kpmg.com.ar



Ana López Espinar
Socia Líder de Forensic Services
ablopez@kpmg.com.ar

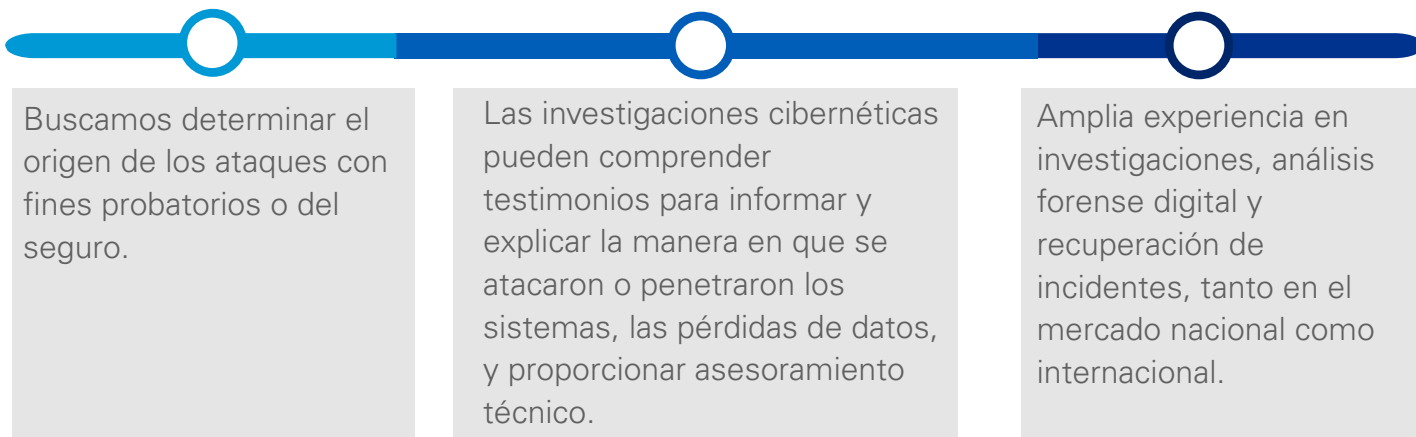


Hernán Carnovale
Socio de Forensic Services
hcarovale@kpmg.com.ar

Ayudamos a los clientes a responder de forma rápida y eficiente ante incidentes de ciberseguridad, acompañándolos durante todas las fases del proceso:



Los beneficios son: limitar el nivel de impacto de los incidentes, lograr una pronta recuperación y obtener retroalimentación para mejorar la postura de ciberseguridad, junto con la capacidad de detección y respuesta a incidentes futuros.



Podemos responder o investigar ante los siguientes tipos de amenaza:

- Ransomware
- Ingeniería social
- Robo de identidad
- Phishing
- Fuga de información
- Ataques a la cadena de suministro de software
- Denegaciones de servicio (DoS/DDoS)
- Ciberacoso
- Ciber extorsión
- Acceso indebido o intrusiones de seguridad
- Fraude
- Amenazas internas (Insider Threats)



Diego Bleger
Socio Líder de Advisory
dbleger@kpmg.com.ar



Ana López Espinar
Socia Líder de Forensic Services
ablopez@kpmg.com.ar



Hernán Carnovale
Socio de Forensic Services
hcarovale@kpmg.com.ar