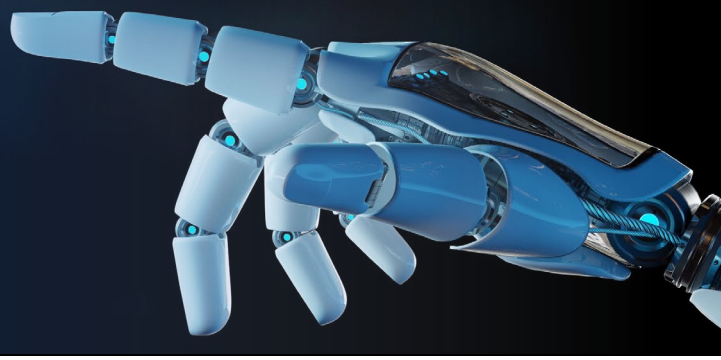
Incident Response

Recupera el control, minimiza el impacto y fortalece tu resiliencia.



Cuando cada minuto cuenta, la respuesta lo es todo

En un entorno digital cada vez más hostil, los incidentes de seguridad no son una posibilidad, sino una certeza. La capacidad de responder con rapidez, coordinación y eficacia es clave para proteger la continuidad del negocio, cumplir con las exigencias regulatorias y preservar la confianza de clientes y socios.

Además, la presión reputacional y la velocidad con la que se propagan los ataques exigen una reacción inmediata, estructurada y respaldada por expertos. Cada minuto sin control puede traducirse en pérdidas operativas, legales y de imagen.

Lo que está en juego

Los ataques son cada vez más frecuentes, sofisticados y con mayor impacto. Las organizaciones enfrentan el reto de responder con rapidez y eficacia, pero muchas carecen de los recursos, procesos y capacidades necesarias. La falta de preparación, coordinación y visibilidad puede amplificar las consecuencias operativas, legales y reputacionales de un incidente. Sin una estrategia clara, los equipos internos se ven superados, lo que dificulta la contención y recuperación.

83%
de las organizaciones sufrieron al menos un incidente significativo en el último año.

287
es el tiempo medio para contener y recuperar completamente de un incidente.

72%
de las empresas no cuentan con un plan de respuesta formal ni roles definidos.

58%
de los incidentes generan impacto reputacional o legal.

46%
de los equipos internos no logran coordinarse eficazmente en situaciones de crisis.

Nuestra visión sobre un servicio eficaz de respuesta a incidentes

En un entorno marcado por ataques disruptivos, presión regulatoria y falta de preparación interna, las organizaciones requieren una capacidad de respuesta rápida, coordinada y experta para minimizar el impacto y recuperar la normalidad.

Activación inmediata y flexible

Capacidad de desplegar equipos expertos en minutos, adaptándose al tipo de incidente, su gravedad y el entorno afectado. La rapidez en la activación es clave para contener el daño y evitar su propagación.

Coordinación multidisciplinar

Uso de telemetría enriquecida, correlación de eventos y análisis contextual para identificar patrones de ataque, incluso aquellos que evaden controles tradicionales.

Análisis forense y contextual

Investigación profunda del incidente para entender su origen, alcance y posibles implicaciones. Incluye preservación de evidencias, reconstrucción de eventos y análisis de impacto.

Gestión legal y regulatoria

Soporte experto en cumplimiento normativo, notificación a autoridades y comunicación con terceros. Ayuda a minimizar riesgos legales y proteger la reputación corporativa.

Recuperación segura y validada

Restauración de sistemas y servicios afectados, con validación técnica y funcional. Se asegura que la recuperación no reintroduzca vulnerabilidades ni afecte la operación.

Aprendizaje y mejora continua

Evaluación post-incidente con recomendaciones accionables para fortalecer la postura defensiva. Incluye talleres, simulacros y ajustes en procesos y tecnologías.

Nuestros servicios

KPMG ofrece un servicio integral que permite contener, erradicar y recuperar rápidamente, con soporte experto en todas las dimensiones del incidente. Está estructurado en cinco bloques clave:

Incident Response Ad-hoc

Activación inmediata de un equipo experto para contener y gestionar incidentes específicos.

- Identificación de vectores de ataque y activos comprometidos.
- Coordinación técnica y comunicación con stakeholders.
- Soporte en decisiones críticas y recuperación operativa.
- Documentación del incidente para fines regulatorios (evidencias, trazabilidad, etc.).
- Recomendaciones iniciales para evitar recurrencia.

Incident Response Retainer

Modelo de servicio continuo que permite activar la respuesta en cualquier momento, sin necesidad de contratación ad-hoc.

- SLAs predefinidos.
- Activación prioritaria y acceso a equipo multidisciplinar.
- Cobertura flexible según tipo de incidente.
- Revisión del plan de respuesta y capacidades internas.
- Acompañamiento en la mejora de procesos y roles internos.
- Formación y simulacros.

Threat Detection & Response

Monitorización continua y capacidad de respuesta inmediata ante eventos críticos.

- Monitorización de activos clave y correlación de eventos.
- Activación de contención automatizada o manual.
- Escalado a equipo de respuesta en tiempo real.
- Alertas priorizadas y contextualizadas para facilitar la toma de decisiones.
- Soporte en la gestión de falsos positivos y tuning de reglas.

Forensics, Legal & Crisis Support

Análisis profundo del incidente y acompañamiento en todas sus implicaciones.

- Investigación forense digital para identificar el origen, alcance y técnicas utilizadas, preservación de evidencias e informes periciales para proceso legal.
- Asesoramiento legal en notificación a autoridades y comunicación pública.
- Apoyo en gestión de crisis con planes de comunicación y coordinación con stakeholders.
- Soporte en la relación con medios, clientes y terceros afectados.

Post-Incident Review

Revisión integral del incidente para extraer aprendizajes y fortalecer la postura defensiva.

- Elaboración de informes técnicos y ejecutivos.
- Revisión de tiempos de respuesta, decisiones tomadas y coordinación interna.
- Identificación de brechas en procesos, tecnología y capacidades y propuesta de mejoras estructurales.

Beneficios potenciales

- Reducción del impacto operativo, legal y reputacional.
- Mayor rapidez y eficacia en la contención de amenazas.
- Cumplimiento normativo y tranquilidad frente a auditorías.
- Fortalecimiento de la resiliencia organizacional.
- Aprendizaje continuo y mejora de procesos internos.
- Confianza reforzada ante clientes, socios y reguladores.

¿Por qué KPMG?

Capacidad y experiencia

Combinamos capacidades globales con experiencia multidisciplinar para transformar la seguridad tras cada incidente.

Líderes por el enfoque

KPMG ha sido reconocido como líder global en respuesta a incidentes, gracias a su enfoque integral que cubre todo el ciclo de gestión de crisis.

Comprometida

Las relaciones con nuestros clientes se basan en la confianza mutua y el compromiso a largo plazo para proporcionar estrategias eficaces y eficientes.

Contactos

Sergi Gil
Partner
MDR Lead
T: +34 636 189 222
E: sergigil@kpmg.es

Paúl Martínez
Senior Manager
MDR BD Lead
T: +34 699 410 959
E: paulricardomartinez@kpmg.es

José Sosa
Senior Manager
MDR Tech Lead
T: +34 636 739 221
E: josemiguelsosa@kpmg.es

Sergio Galán
Senior Manager
Threat Intel, Hunting & IR Tech Lead
T: +34 606 286 219
E: sgalan1@kpmg.es

kpmg.es