Detection and Response Readiness

Transforma tu capacidad de defensa: anticipa, responde y evoluciona frente a las amenazas.

El reto de estar preparados en un entorno de amenazas constante

En un panorama digital cada vez más complejo, las organizaciones enfrentan amenazas cibernéticas más frecuentes, sofisticadas y persistentes. La transformación digital, la adopción de nuevas tecnologías y la creciente interconexión entre sistemas han ampliado la superficie de ataque, exponiendo a las empresas a riesgos operativos, reputacionales y legales. La detección tardía, la falta de entrenamiento práctico y la ausencia de planes de respuesta efectivos agravan esta situación. Prepararse no es solo una cuestión de tecnología, sino de estrategia, personas y procesos. La preparación efectiva en detección y respuesta se ha convertido en un imperativo para garantizar la resiliencia organizativa y la continuidad del negocio.

¿Tu organización está preparada para responder?

Las cifras hablan por sí solas. La falta de preparación ante incidentes de ciberseguridad es una de las principales vulnerabilidades de las organizaciones:

81,6%
de las organizaciones sufrieron al menos un ciberataque exitoso en el último año.

267
días es el tiempo medio que tarda una organización en completar el ciclo de respuesta a un incidente.

66%
de las organizaciones reportan carencias críticas en habilidades de ciberseguridad.

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

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

Nuestra visión de una preparación efectiva sobre capacidades de detección y respuesta

Una preparación eficaz permite anticiparse a las amenazas, responder con agilidad y evolucionar continuamente. Las organizaciones más resilientes se apoyan en prácticas consolidadas que incluyen la evaluación continua de sus capacidades, el diseño adaptado de arquitecturas de respuesta y la optimización operativa de procesos y herramientas. La formación especializada de los equipos, la simulación realista de escenarios críticos y el benchmarking frente a estándares del sector completan un enfoque integral que permite justificar inversiones y priorizar acciones de mejora.

Evaluación continua

Las organizaciones líderes revisan periódicamente el nivel de madurez de sus capacidades de detección y respuesta, identificando brechas en procesos, tecnología y personas mediante marcos reconocidos.

Diseño adaptado

Las arquitecturas de respuesta deben estar alineadas con el contexto operativo, regulatorio y de amenazas, incorporando modelos de gobernanza, flujos de trabajo y estructuras organizativas claras.

Optimización operativa

La mejora continua implica redefinir roles, automatizar procesos, ajustar reglas de detección y asegurar la integración efectiva de herramientas para maximizar la eficacia operativa.

Formación especializada

Los programas formativos deben incluir entrenamientos prácticos, certificaciones reconocidas y planes de desarrollo adaptados al nivel de cada profesional.

Simulación realista

Las simulaciones de respuesta, tanto estratégicas como técnicas, permiten validar la preparación real, identificar áreas de mejora y fortalecer la coordinación entre equipos.

Benchmarking estratégico

Comparar capacidades frente a estándares y organizaciones del sector, ayuda a justificar inversiones, demostrar madurez y priorizar acciones de mejora.

Nuestros servicios

Diseñamos y activamos capacidades de detección y respuesta adaptadas a cada organización, combinando evaluación, formación y simulación.

Diseño e Implementación de SOC / CERT / CSIRT

Definimos e implantamos capacidades de detección y respuesta adaptadas al contexto del cliente, asegurando su alineación con los objetivos de negocio.

- Diseño de arquitectura técnica y operativa.
- Modelos de gobernanza.
- Planes de despliegue y transición.
- Integración con herramientas existentes.
- Procedimientos operativos.

Evaluaciones de Madurez de SOC / CERT / CSIRT

Realizamos diagnósticos detallados del estado actual de las capacidades de detección y respuesta, identificando fortalezas y oportunidades de mejora.

- Análisis de procesos, tecnología y roles clave.
- Evaluación frente a marcos internacionales.
- Entrevistas y revisión documental.
- Roadmap de evolución.
- Comparativa sectoriales y mejores prácticas.

Optimización de SOC / CERT / CSIRT

Mejoramos las capacidades existentes para maximizar su eficacia, eficiencia y alineación con las amenazas actuales.

- Revisión de casos de uso y reglas de detección.
- Automatización de procesos de análisis y respuesta.
- Redefinición de roles y responsabilidades.
- Evaluación de métricas.
- Mejora de flujos de escalado, coordinación y reporting.

Diseño de Planes de Respuesta a Incidentes

Diseñamos planes prácticos, accionables y alineados con el negocio para gestionar incidentes de forma eficaz.

- Identificación de escenarios de riesgo.
- Definición de flujos de actuación, roles y responsabilidades.
- Integración con equipos legales, de negocio y comunicación.
- Alineación regulatoria.
- Validación mediante simulacros y table tops.

Ejercicios Table Top de Respuesta a Incidentes

Facilitamos simulaciones estratégicas para validar la preparación organizativa ante incidentes críticos.

- Diseño de escenarios.
- Moderación de sesiones con equipos técnicos y de negocio.
- Evaluación de decisiones y coordinación.
- Identificación de oportunidades de mejora.
- Informe de lecciones aprendidas y plan de acción.

Entrenamientos y Certificaciones

Capacitamos a los equipos defensivos mediante programas formativos técnicos y prácticos.

- Cursos y certificaciones especializadas en defensa.
- Evaluación de competencias y simulaciones prácticas.
- Planes de formación continua y desarrollo profesional.
- Laboratorios virtuales y ejercicios hands-on.

Ejercicios de Capture The Flag y Cyber Range

Diseñamos y ejecutamos simulaciones técnicas avanzadas para entrenar habilidades defensivas.

- Escenarios gamificados y realistas adaptables.
- Retos de detección, forense y respuesta.
- Evaluación y métricas de evolución de desempeño individual y grupal.
- Feedback y recomendaciones de mejora personalizado.

Benchmarking de Soluciones

Evaluamos la eficacia de las herramientas de detección y respuesta frente a amenazas reales.

- Análisis funcional y técnico de soluciones (SIEM, EDR, XDR, NDR, SOAR, etc.).
- Comparativa frente a estándares y mejores prácticas.
- Evaluación de cobertura, eficiencia y capacidades.

Beneficios potenciales

- Reducción del riesgo ante incidentes críticos.
- Optimización de inversiones en tecnología y procesos.
- Equipos entrenados y coordinados para responder.
- Mejora continua de la postura defensiva.

¿Por qué KPMG?

Presencia global

Contamos con más de 265.000 profesionales multidisciplinares en 143 países, siendo 9.300 expertos en ciberseguridad y 45.000 basados en riesgos.

Diferencial

Combinamos una amplia experiencia, con profundos conocimientos del negocio y sector, con profesionales que les apasiona ayudar a proteger y fomentar la confianza entre las partes interesadas.

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