

Contactos

KPMG en España



Marc Martínez
Socio Ciberseguridad
T: 91 451 31 39
E: marcmartinez@kpmg.es



Javier Santos
Director Ciberseguridad
T: 91 456 59 04
E: javiersantos@kpmg.es



Alejandro Rivas-Vásquez
Director Ciberseguridad
T: 91 456 59 74
E: arivasvasquez@kpmg.es



Sergi Gil
Director Ciberseguridad
T: 93 254 27 41
E: sergigil@kpmg.es



Juan Antonio Calles
Senior Manager Ciberseguridad
T: 91 451 30 25
E: jcalles@kpmg.es



Daniel González
Manager Ciberseguridad
T: 608 018 423
E: danielgonzalez3@kpmg.es

kpmg.es



© 2018 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la red KPMG de firmas independientes afiliadas a KPMG International Cooperative ("KPMG International"), sociedad suiza. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Cooperative ("KPMG International"), sociedad suiza.

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.



Ciberinteligencia. Anticípate a los riesgos

**Servicio avanzado de
vigilancia integral**

Ciberseguridad

www.kpmgciberseguridad.es



Detectar ciberamenazas en tiempo real

La **Ciberseguridad** requiere actuar antes, durante y después de un ataque. Solo una **monitorización continua en la superficie y en lo más profundo de la Web, en tiempo real y con información histórica, permite detectar a tiempo posibles amenazas.**

Nuestros servicios rastrean en todo Internet para detectar y prevenir potenciales amenazas.

Podemos ayudarle a identificar:

- » Detectar fugas de información
- » Robo de identidades
- » Phishing o suplantación de identidad
- » Registro malicioso de dominios
- » Campañas fraudulentas
- » Falsas APPs y perfiles
- » Ataques potenciales (DDoS, etc.)
- » Detención de vulnerabilidades
- » Ataques a la reputación de la marca

Todo esto lo logramos gracias a nuestro **equipo multidisciplinar** de profesionales y a una herramienta que hemos desarrollado internamente, K-CIT basada en **Open Source Intelligence (OSINT)** y permite identificar alertas tempranas de riesgos. Según destacados servicios nacionales de inteligencia, como la CIA estadounidense o la británica GCHQ, los sistemas basados en OSINT juegan un papel clave en el mundo de la ciberseguridad para obtener una visión global a un coste relativamente bajo.

Ejemplos de uso



Preguntas clave



¿Quién amenaza su organización?



¿Hay sistemas comprometidos?



¿Quién publica información maliciosa sobre la compañía?



¿Existen filtraciones de datos?



¿Le están suplantando?

Niveles de Internet

Clear web

1 Páginas a las que se puede acceder fácilmente desde un buscador y navegador corriente

Usuarios de Internet

2 Páginas no indexadas por buscadores y cuyo acceso requiere del conocimiento previo de su URL

Universidades, departamentos IT

3 Información alojada en redes de tipo P2P (peer-to-peer) y similares, para las que es necesario acceder mediante determinados protocolos

Gente que descarga contenidos

Deep web

4 Páginas alojadas en redes de tipo TOR, i2p, Freenet y similares para las que es necesario conectarse a través de nodos específicos de tipo proxy

Hackers, policías, fuerzas de seguridad, investigadores

5 Páginas alojadas en redes de tipo TOR, i2p, Freenet y similares, que además de requerir el uso de proxys específicos, cuentan con mayores niveles de seguridad y anonimato

Delincuentes y perfiles opacos

Dark web

Fuente: KPMG