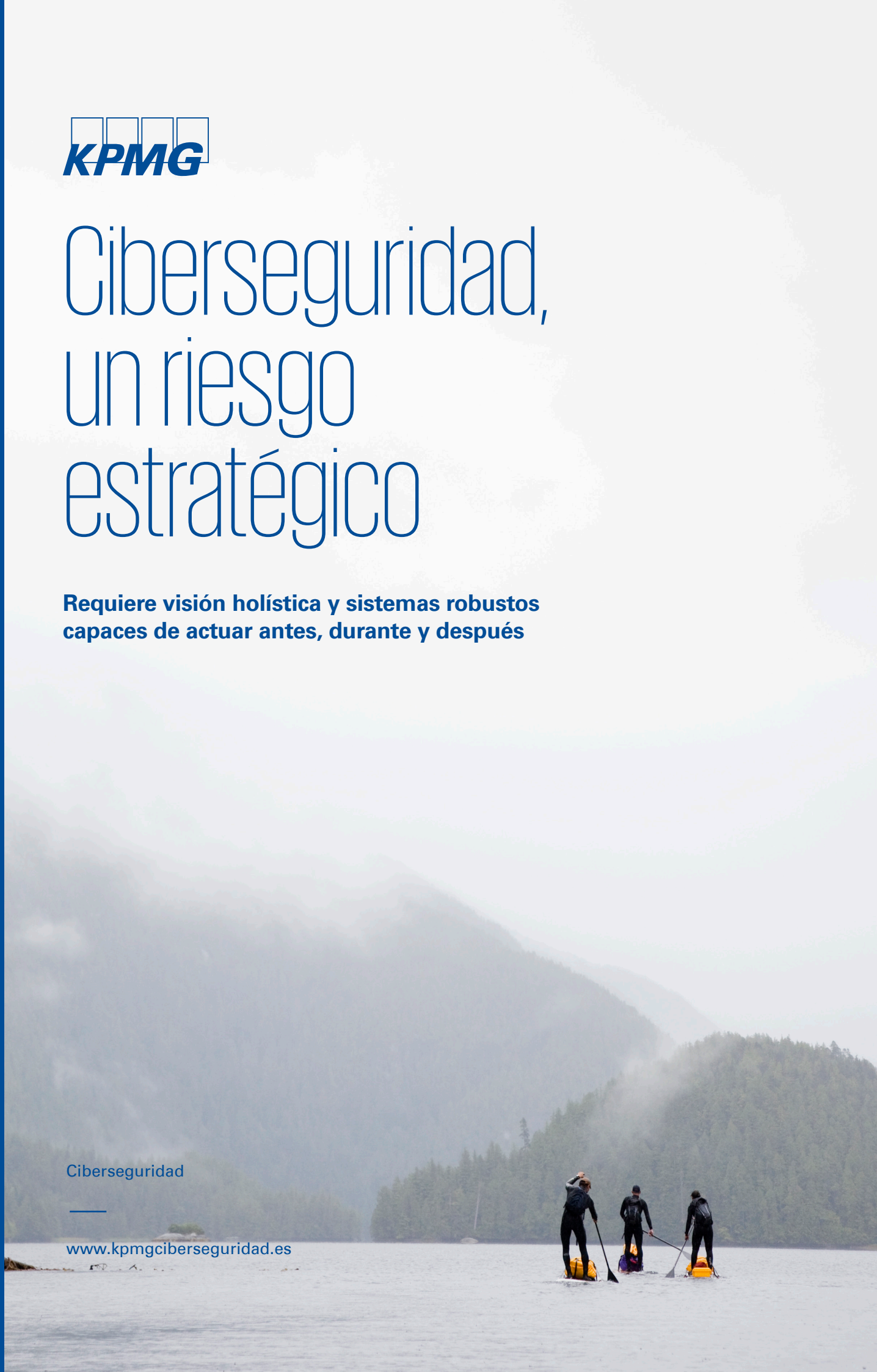
Ciberseguridad, un riesgo estratégico

Requiere visión holística y sistemas robustos capaces de actuar antes, durante y después



Ciberseguridad

www.kpmgciberseguridad.es

Nadie puede quedarse fuera del proceso de digitalización. Sería aislarse del mundo. Pero la digitalización, que abre enormes oportunidades, también implica riesgos que hay que saber gestionar. Uno de ellos es la Ciberseguridad.

En un mundo dominado por la imparable conectividad de las personas, las organizaciones y las cosas (Internet of Things), las vulnerabilidades se multiplican.

La ciberseguridad implica dotarse de sistemas robustos capaces de actuar antes, durante y después. No solo para prevenir. También para aumentar la confianza de los clientes y del mercado, minimizando cualquier riesgo reputacional que pueda tener un impacto reseñable en el negocio.

Contar con sólidos sistemas de ciberseguridad no es hoy una opción. Es una exigencia de todos: consumidores, inversores, reguladores y el conjunto de la sociedad. Y en su gestión deben implicarse todas las esferas de la organización ¿Está tu compañía preparada?

"Cualquier CEO que realmente sepa cómo es hoy la gestión de riesgos, sabe que la ciberseguridad es el más impredecible de todos"

Marc Martínez
Socio y responsable de Ciberseguridad
KPMG en España

Nuestros servicios

KPMG ha hecho de la ciberseguridad uno de sus pilares estratégicos. Miles de profesionales multidisciplinares integran y colaboran en nuestra red global prestando servicios que cubren todos los aspectos clave.

Estrategia y Gobierno

- **Modelos de referencia y marco de control de seguridad**
- **Gestión de la continuidad de negocio**
- **Privacidad (GDPR)**
- **Seguridad del dato y clasificación de la información**
- **Gestión del riesgo**
- **Gobierno de la Seguridad de terceros/proveedores**
- **Compliance**

Transformación de la Seguridad

- **Oficina de Transformación de la seguridad**
- **Formación y concienciación**
- **Cuadros de mandos de seguridad**
- **Gestión de identidades**
- **Arquitecturas de seguridad**

Ciber Defensa

- **Ciberinteligencia**
- **Segmentación de entornos y DMZs**
- **Integración de soluciones de seguridad**
- **SSDLC**
- **Análisis de amenazas internas**
- **Análisis y estrategia de LOGS**

Ciber Respuesta

- **Respuesta ante incidentes**
- **Seguridad ofensiva (Red Team)**
- **Seguridad defensiva (Blue Team)**

Estrategia y Gobierno

Los servicios de estrategia y gobierno están diseñados para proporcionar a las organizaciones un marco de control de riesgos de ciberseguridad, incluyendo desde la evaluación de la madurez de la organización en materia de ciberseguridad hasta la concienciación, formación y sensibilización de la capa directiva.

- **Modelos de referencia y marco de control de seguridad:** Diseño de estrategias y desarrollo de planes de Ciberseguridad
- **Gestión de la continuidad de negocio:** Organización de las capacidades de resiliencia
- **Privacidad (GDPR):** Asesoría en el cumplimiento del Nuevo Reglamento Europeo de Protección de Datos (GDPR), incluyendo Seguridad en Privacidad (Privacy by design y Privacy Impact Assessments)
- **Seguridad del dato y Clasificación de la información**
- **Gestión del Riesgo**
- **Gobierno de la Seguridad de terceros/proveedores:** Modelos para clasificar y taxonomizar a prestadores de servicio y establecimiento de modelos de revisión y priorización de los mismos
- **Compliance:**
  - PSD2 / PCI-DSS
  - Cloud Security Alliance
  - ISAE 3402
  - ISO 27001 / ISO 22301
  - Directiva NIS

CASO DE ÉXITO

Sector textil:
Análisis del estado de seguridad de los datos para mejorar los controles y conocer al detalle por dónde y cómo fluye la información crítica y los sistemas de información y bases de datos implicados en los procesos de negocio y su ciclo de vida.

La ciberseguridad va mucho más allá de un problema técnico. Requiere nuevas políticas y un enfoque distinto, porque el ciberespacio se rige por reglas diferentes a las del mundo físico.

Transformación de la Seguridad

En el actual entorno competitivo, todas las organizaciones están inmersas en programas de transformación digital de sus negocios. Esta transformación, unida a la continua evolución de ciberamenazas, supone un reto adicional a las empresas, que deben simultanear la evolución tecnológica con una transformación de la seguridad acorde a nuevos estándares de desarrollo, arquitectura, control y gestión que cubran los requisitos de seguridad en el ciberespacio.

- **Oficina de Transformación de la Seguridad:** Evolución y transformación hacia modelos proactivos de la función de la Seguridad de la Información
- **Formación y concienciación:** Diseño de planes para sensibilización de empleados y formación específica
- **Cuadros de mandos de seguridad:** Definición de Marcos de control de Ciberseguridad y representación mediante cuadros de mando
- **IAM:** Gestión de identidades
- **Arquitecturas de Seguridad:** Modelado de patrones de seguridad para la estandarización de arquitecturas seguras

CASO DE ÉXITO

Sector utilities:
Acompañar el proceso de transformación digital de la empresa con un enfoque proactivo de la seguridad, aumentando su nivel de madurez y desarrollando un modelo de gobierno de la seguridad más efectivo.

Las tecnologías emergentes, como Inteligencia Artificial, Robótica, Internet of Things (IoT), vehículos autónomos o impresión 3D, están redefiniendo las infraestructuras físicas, creando una interdependencia que incrementa considerablemente el riesgo de ciberataques.

Ciber Defensa

Las brechas de ciberseguridad rara vez están fuera de los medios de comunicación. A medida que aumenta la sofisticación de los atacantes, muchas organizaciones reaccionan cuando ya es demasiado tarde: el ataque está en marcha. Pocas organizaciones tienen la capacidad de anticipar amenazas cibernéticas e implementar estrategias preventivas, a pesar de que la prevención es más rentable y enfocada al cliente. Los servicios de Ciber Defensa de KPMG en España permiten a las organizaciones desarrollar capacidades y disponer de servicios que garanticen la identificación de las amenazas y les protejan de ellas.

- **Ciberinteligencia**
  - Monitorización de fugas de información
  - Seguridad de proveedores mediante rating y evaluación de sus ciberamenazas
  - Due Diligence
  - Vigilancia de marca
  - Monitorización de VIPs y directivos
  - Vigilancia de ciber amenazas (hacktivismo, phishing y pharming)
  - Seguimiento y respuesta ante amenazas técnicas (malware, apps maliciosas, fraude online, etc.)
- **Segmentación de entornos y DMZs**
- **Integración de soluciones de seguridad:** DLPs, SIEMS, AntiVirus, AntiRansomware, etc.
- **SSDLC: Implantación de metodologías y tecnologías de desarrollo seguro**
- **Análisis de Amenazas internas**
- **Security Analytics**

CASO DE ÉXITO

Sector bancario:
Servicio para monitorizar en tiempo real ciberamenazas existentes en Internet y Deep Web. Implica identificación de patrones de conducta y perfiles, continuo rastreo y análisis de la información para detectar amenazas como apps falsas, suplantación de identidad, fugas o robo de datos y credenciales, etc.

La ciberseguridad se ha convertido en un elemento clave de la reputación de las empresas. Las que gestionen bien este riesgo contarán con la confianza de clientes, empleados, aliados y reguladores.

Ciber Respuesta

Diseño, implantación y limitación de los daños ocasionados por brechas de seguridad. Evaluamos la capacidad de respuesta ante incidentes testeándola frente a modelos de respuesta predefinidos o contra modelos de ciberejercicios técnicos (Blue y Red Teaming) ayudando a identificar debilidades, mejorar procesos, implantar herramientas, seleccionar partners estratégicos y formar a los equipos.

Respuesta ante incidentes:

- Análisis de amenazas (malware, DDoS, intrusiones, APTs...)
- Evaluación y contención de un incidente
- Soporte forense para la toma de evidencias (cadena de custodia, copiado seguro, análisis en entorno seguro...)
- Planes técnicos de contingencia y continuidad

Seguridad ofensiva (Red Team):

- Test de intrusión y auditorías de seguridad de hacking ético para:
  - Redes y sistemas internos
  - Servicios y aplicaciones externas e internas
  - Revisiones código fuente
  - Elementos de red y protección perimetral (firewalls)
  - Dominios y servicios de Directorio
  - Puestos de usuario
  - Dispositivos móviles y soluciones MDM
  - TPVs y pasarelas de pago
  - IIOT. Sistemas de control en la industria 4.0

Seguridad defensiva (Blue Team):

- Bastionado (hardening):
  - Sistemas Operativos y maquetas seguras

Concienciación y formación:

- Formación en ciberseguridad
- Ciber escenarios de formación simulando escenarios de amenazas externas e internas

CASO DE ÉXITO

Sector seguros:
Definición de los mecanismos de defensa, predictiva y reactiva. Evaluación continua de los sistemas, aplicaciones y servicios críticos para identificar vulnerabilidades, riesgos y desviaciones frente al baseline definido para cada una de ellos. Metodología de control del desarrollo seguro de las aplicaciones con seguimiento y soporte.

El concepto de resiliencia se ha convertido en el eje de las estrategias de ciberseguridad. La capacidad de defensa es un criterio crítico para garantizar la supervivencia de las organizaciones en un entorno cambiante de ciberamenzas.

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

kpmg.es