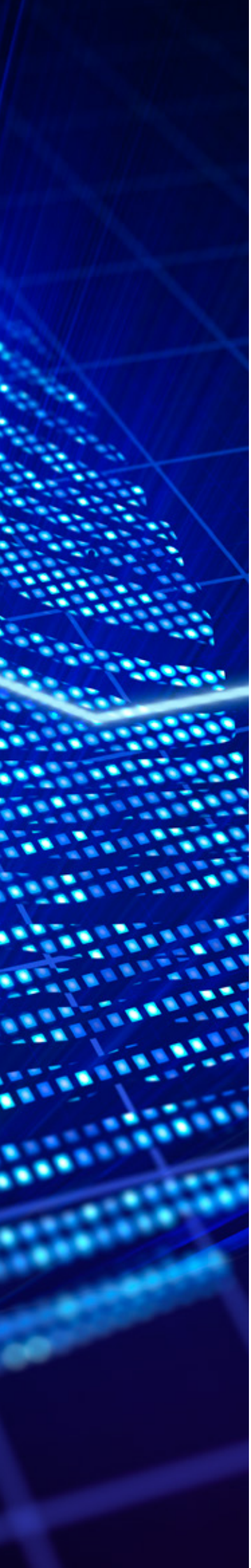
KPMG

Una perspectiva 360º de la ciberseguridad

Servicios

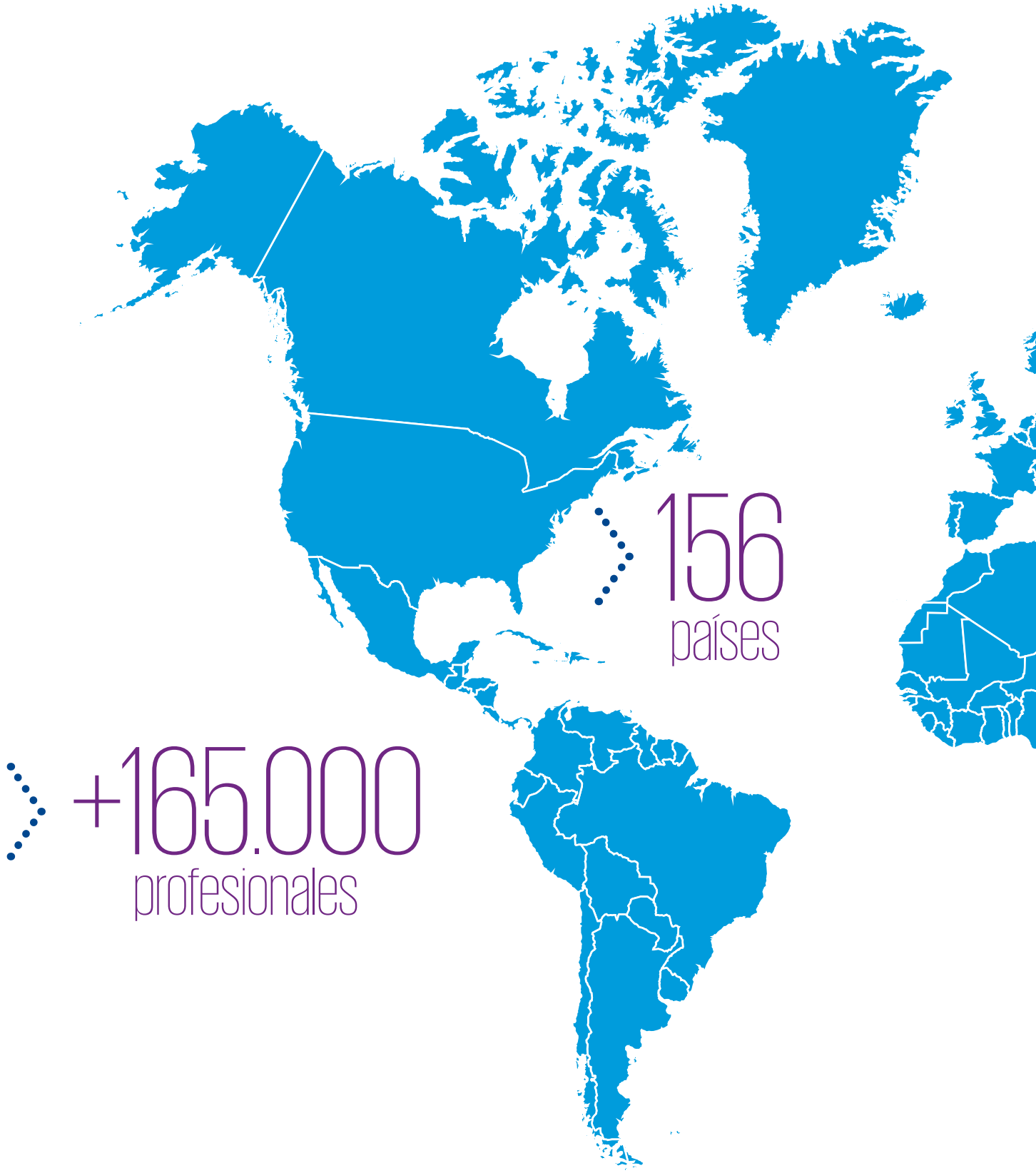
Marzo 2016

kpmg.es



Índice

Red Global de KPMG



156
países

+165.000
profesionales

1917
año de fundación

Servicios de auditoría, fiscales y de asesoramiento legal, financiero y de negocio

El estado de la ciberseguridad hoy

Atacantes más listos con más recursos, mejores herramientas y con objetivos más peligrosos.

Aumento de los miedos, incertidumbres y dudas –especialmente sobre los sistemas integrados / sistemas de control industrial–.

Evolución de las amenazas

Aumento de la repercusión de medios y redes sociales

Principales ciberriesgos

Nuestro principal riesgo para la seguridad: la mala asignación de los escasos recursos –tiempo y dinero–

Cambios en los modelos de servicios de IT

Nuevas capacidades de IT, desde BYOD al cloud y al Big Data, han tenido un tremendo impacto en los controles de seguridad necesarios y que se pueden usar.

Proliferación de proveedores de soluciones

Según IDC, en 2014 sólo en el mercado estadounidense, los productos y servicios de seguridad alcanzaron los $58bn. Según INCIBE en España el mercado fue de 5700 M€.

Nuestra aproximación

La aproximación a los servicios de seguridad se ha diseñado para ser simple y efectiva –alineada a las necesidades de nuestros clientes resolviendo sus servicios de seguridad, siguiendo el modelo de Buscar / Resolver / Operar.

Alineado con las prioridades de los clientes y las necesidades de cumplimiento

Buscar

Ayudando a los clientes a detectar y responder los Ciber incidentes, entendiendo las amenazas a su negocio, sus vulnerabilidades y riesgos.

Resolver

Ayudando a los clientes a construir y mejorar su ciberseguridad, soportada por las personas, organización y tecnologías adecuadas.

Operar

Ayudando a los clientes a permanecer seguros en todo su negocio y evolucionando y madurando sus programas tecnológicos.

Buscar

Grupo de servicios		Qué hacemos
Test & Ejercicios	**Red Teaming**	Verificar las ciberdefensas de las organizaciones desde la perspectiva de un atacante mediante la evaluación de las huellas en Internet de la organización y de sus vulnerabilidades; evaluar la seguridad alrededor de sus sitios claves y explotando la confianza del personal mediante ingeniería social.
	Penetration Testing	Evaluaciones estructuradas de la seguridad de la red y los sistemas de TI utilizando escenarios conocidos de ciber ataques, incluyendo la explotación de las vulnerabilidades actuales mediante exploits.
	Descubrimiento de activos	Revisiones iniciales de TI y de los activos de comunicación para determinar el estado de configuración y de parches, y para detectar dispositivos no autorizados conectados a las redes.
	Diseño de escenarios de ciber ejercicios y soporte	El desarrollo de escenarios de ciberejercicios adaptados a las necesidades de los clientes. Diseño y ejecución de ejercicios ciber diseñados para poner a prueba la madurez y eficacia de las ciberdefensas de las organizaciones.
Respuesta	**Security Analytics**	Asesoramiento en la adquisición e integración de análisis de seguridad en la gestión de incidentes y la gestión de eventos de la organización. Adaptación de la analítica de seguridad para cumplir con las necesidades de negocio de las organizaciones, incluyendo su entorno de cumplimiento.
	Planificación de la respuesta a incidentes y su coordinación	Diseño e implantación de los procedimientos y sistemas de respuesta a incidentes en las organizaciones.
	Gestión de amenazas y vulnerabilidades	Diseño e implantación de metodología de gestión de amenazas y vulnerabilidades de las organizaciones a la medida de sus necesidades de negocio y entorno de amenazas, incluido el asesoramiento sobre la selección e integración de herramientas.
	Diseño e implantación de inteligencia de amenazas	Diseño e implantación de procesos de ciber inteligencia y sistemas dentro de las organizaciones, incluido el asesoramiento sobre la selección e integración de proveedores de inteligencia.
	Gestión de incidentes y eventos de seguridad incluyendo soporte a análisis forens	Ayudar a los clientes en su respuesta a incidentes y eventos de seguridad, proporcionando conocimientos especializados y el asesoramiento, la capacidad de reacción y el acceso a las habilidades forenses y de investigación especializados.

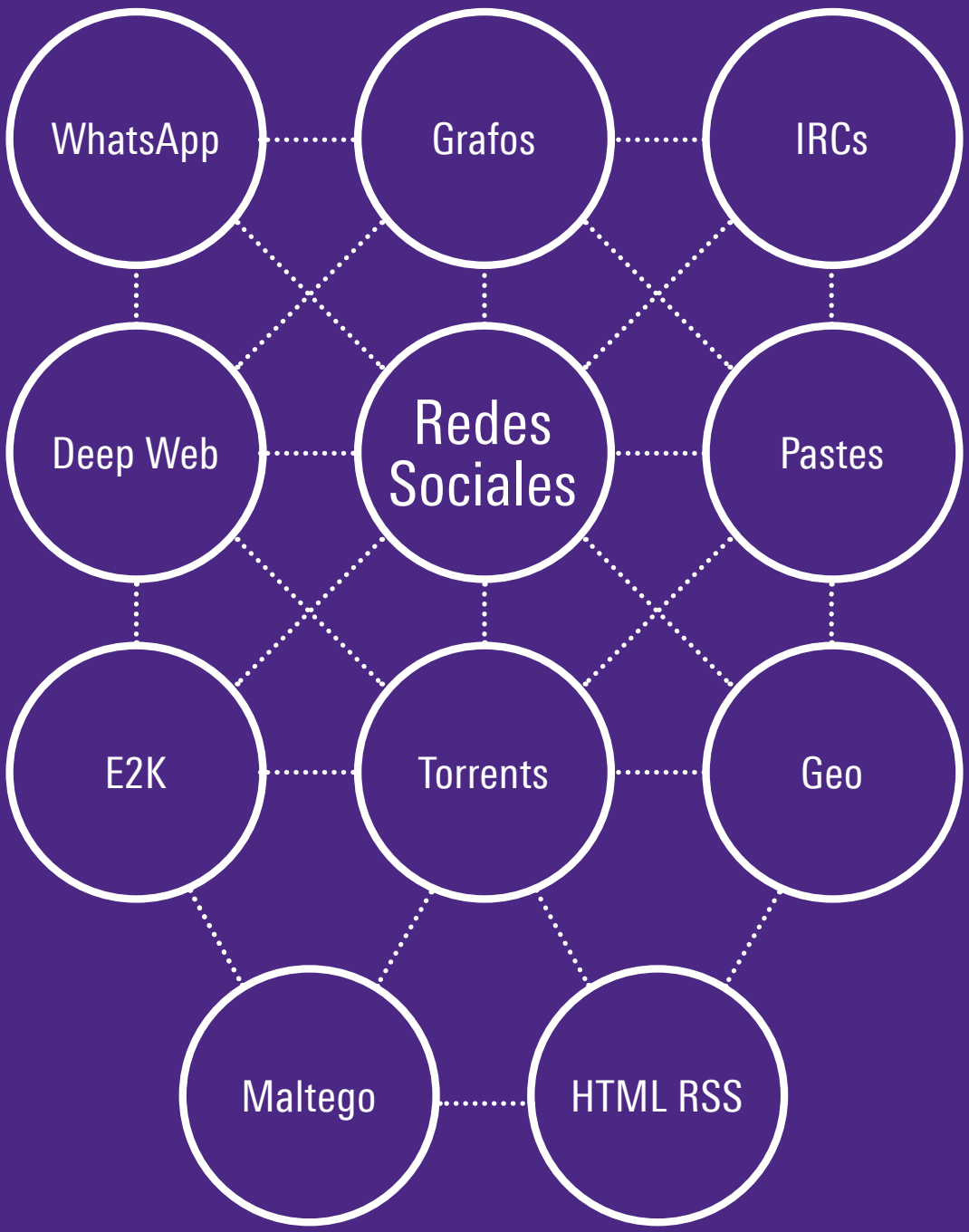
Resolver

Grupo de servicios		Qué hacemos
Transformar	**Modelo operativo objetivo**	Asesoramiento en el diseño de modelos operativos objetivo para las funciones de seguridad dentro de las organizaciones, incluyendo las mejores prácticas y la selección de los enfoques óptimos industria
	Diseño de arquitectura	Asesoramiento neutral de proveedores en el diseño de arquitecturas de seguridad y su integración en los sistemas de TI de la organización. Asesoramiento en el bastionado de los sistemas de movilidad y de cloud computing.
	Gestión del cambio	Apoyo en el diseño y ejecución de los programas de transformación de seguridad, garantizando que la mejora en seguridad sea sostenible y esté alineada con los objetivos de los clientes.
	Program Management	Ayudar a los programas de seguridad y ayudar a los clientes en la entrega incluyendo la provisión de una oficina de gestión de programas (PMO) cuando sea necesario.
	Benchmarking & Challenge	Desarrollar benchmarks de mejores practicas y trabajar con las principales comunidades para recoger los datos de interés para los intereses de los clientes.
	Peer Support & Networking	Gestión de la conferencia internacional I-4 que permite oportunidades de networking para el personal clave, así como una red de liderazgo de seguridad dirigido a los principales CISOs de la industria.
Diseñar	**Gestión de riesgos de la información**	Diseño e implantación de soluciones de gobierno, gestión de riesgos y cumplimiento (GRC). Consultoría en la integración y personalización de soluciones de GRC.
	Gestión de identidades y accesos	Definir requisitos de gestión de identidades y accesos, desarrollar pruebas de concepto y asesorar en la selección de herramientas, desarrollar e implantar proyectos de IAM integrándolos con las aplicaciones existentes.
	Gestión de logs	Asesorar en los riesgos de los sistemas de logs, diseñando e implantado sistemas de gestión de eventos que incluyan los registros actuales.
	Gestión de métricas y rendimiento	Desarrollar métricas y marcos de gestión de seguridad de la información para realizar un seguimiento de la eficacia del sistema y programas de transformación.
	Campañas de concienciación y educación, gestión del cambio cultural de seguridad	Evaluar la cultura de seguridad de las organizaciones, diseñar estrategias para cambiar esa cultura incluyendo campañas de educación y sensibilización.
	Gestión interna y formación especilizada	Disponibilidad de expertos de la seguridad de alto nivel para ayudar en las transiciones del personal o aumentar las habilidades internas en áreas clave

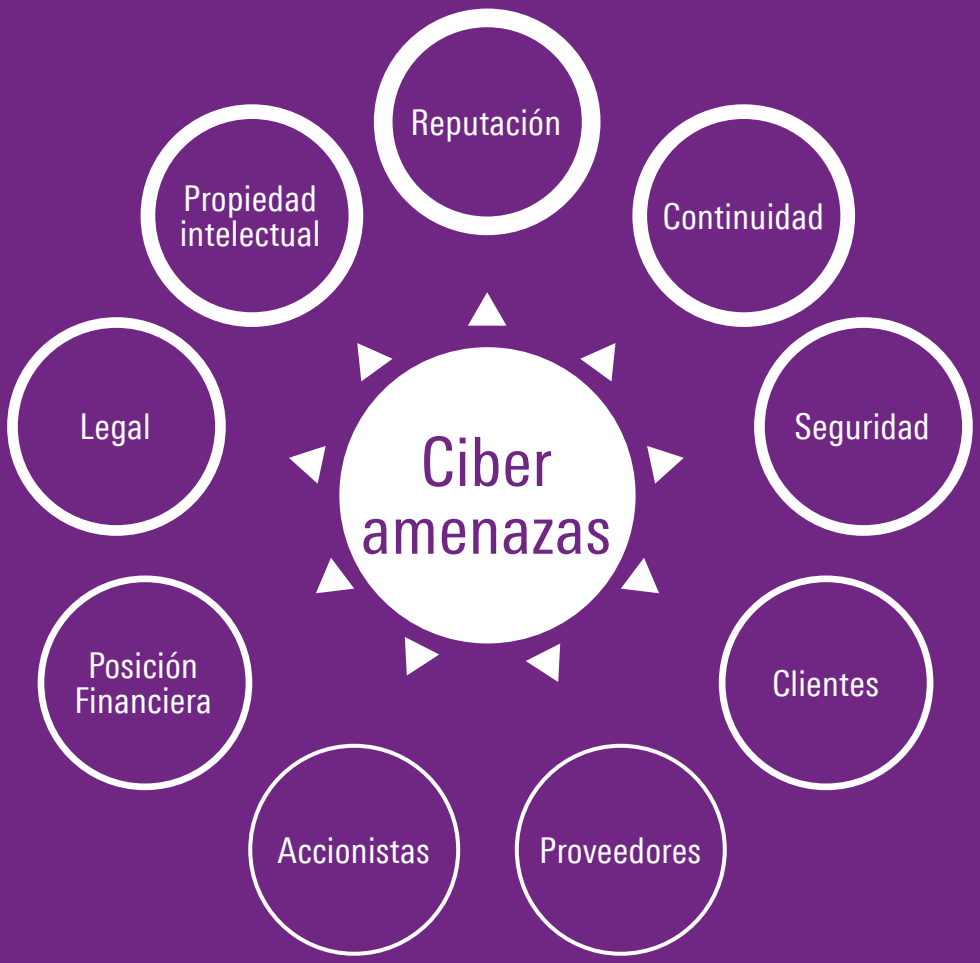
Operar

Grupo de servicios		Qué hacemos
Estrategia y Gobierno	**Estrategia de seguridad de la información**	Asesoramiento en el desarrollo e implantación de estrategias de seguridad de la información que reflejan las mejores prácticas de la industria, las necesidades de reglamentación legal y asesoramiento sobre el aprovechamiento de las oportunidades digitales, incluyendo la movilidad segura
	Gobierno de la información y privacidad	Asesoramiento sobre riesgos para la privacidad y la información. Analizar el riesgo para la privacidad y hacer evaluaciones de impacto. Contribuir al cumplimiento normativo, incluida la adopción de normas corporativas vinculantes.
	Continuidad de negocio y gestión de crisis	Asesoramiento en continuidad del negocio y gestión de crisis que ofrece un enfoque integrado y resiliente tanto a amenazas físicas como ciber
Aseguramiento	**Valoración de la madurez de seguridad y análisis de gap**	Evaluación estructurada y repetible de la madurez en los procesos de ciberserguridad, controles y cultura de una organización, incluyendo un análisis de gap para evaluar acciones correctivas.
	Consultoría de cumplimiento	Asesoramiento en la aplicación e implantación de una amplia variedad de estándares de seguridad y de cumplimientos regulatorios como el PCI/DSS
	Certificaciones ISO 27001	Evaluación y apoyo en la certificación de la ISO 27001 y servicio de asesoramiento para cumplir con las necesidades de firmas a todos los niveles.
	Certificaciones especiales	Servicios de certificación en toda una amplia variedad de estándares como firma electrónica o continuidad de negocio.
	Evaluación de proveedores	Asesoramiento y soporte en la definición de estrategias de revisión de los servicios proporcionados por proveedores y la ejecución de las revisiones.
	Gestión de incidentes y eventos de seguridad incluyendo soporte a análisis forense	Ayudar a los clientes en su respuesta a incidentes y eventos de seguridad, proporcionando conocimientos especializados y el asesoramiento, la capacidad de reacción y el acceso a las habilidades forenses y de investigación especializados.
	Monitorización cumplimiento de seguridad	Diseñar y realizar exámenes y evaluaciones de supervisión de cumplimiento de medidas y controles de seguridad , incluyendo la adaptación y uso de sistemas analíticos para realizar su vigilancia.
	Cyber soporte a auditorías internas y externas	Diseñar y realizar auditorías de ciberseguridad como parte de los programas de auditoría interna así como realizar auditorías de ciberseguridad externas para verificación y control de la seguridad de las organizaciones.
	Servicios gestionados para clientes	Provisión de servicios gestionados de seguridad de valor añadido que permiten la automatización y entrega de servicios de inteligencia, ciberamenazas, vigilancia de proveedores, etc

Fuentes de información K-IT



Cybersecurity Intelligence



VIGILANCIA ONLINE

Servicio selectivo y permanente de captar información, para convertirla en conocimiento.

CYBINVEST / CYBINT

Ciberinvestigación.

Ciberinteligencia.

SERVICIOS 24x7

SISTEMA ALERTA TEMPRANA

Detección en tiempo real e identificación de factores críticos, riesgos, amenazas y oportunidades.

REPORTING

Servicio de informes periódicos.

Ad-Hoc.

Análisis.

Dashboards (Visual Analytics).

Compliance

Cumplimiento normativo y legal

Los servicios gestionados de cumplimiento legislativo, permiten a las organizaciones demostrar a los auditores el cumplimiento de regulaciones y normativas de una manera eficiente y proactiva. KPMG enfoca estas acciones combinando las necesidades de seguridad y del entorno de TI con los requisitos para el cumplimiento de la legislación a aplicar.

Nuestros servicios

– LOPD: Ley Orgánica de Protección de Datos de Carácter Personal y Reglamento de Medidas de Seguridad.

– LSSI/CE: Ley de Servicios de el Grupo de la Información y Comercio Electrónico.

– Cambios regulatorios (código penal, etc.) y revisión de líneas éticas.

– Normativas propias de cada empresa o de legislaciones específicas.

– Externalización de servicios: mantenimiento de Documentos de Seguridad.

– Estudios de impacto de la adopción de nuevas tecnologías.

– Asesoría en Firma y Facturación Electrónica.

– Cumplimiento de requisitos SCIIF.

– Cumplimiento de requisitos SOX.

– Adecuación de sistemas y procedimientos a recomendaciones de Secure Pay.

Plan Director de Seguridad

El Plan Director de Seguridad es el resultado de la definición y priorización de un conjunto de proyectos en materia de seguridad dirigido a minimizar los riesgos a los que está expuesta la organización hasta lograr unos niveles aceptables para garantizar y respaldar las acciones y procesos de negocio de la misma.

Nuestros servicios

Definición de un objetivo de protección que permita acotar y establecer el alcance.

– Realización de estudios comparativos GAP y propuesta de mejoras.

– Valoración de hitos de riesgo con niveles de aceptación.

– Análisis de cumplimientos.

– Gestión y evaluación de mecanismos de control.

– Definición de proyectos e iniciativas.

– Clasificación y priorización en función de necesidades reales de negocio.

– Adecuación de una hoja de ruta de aplicación.

– Planificación de un horizonte de desarrollo del PDS.

– Maduración de un Plan Global de Seguridad.

– Supervisión y revisión continua del PDS en tanto en cuanto el negocio se actualiza.

– Sistema de gestión de seguridad de la información. ISO 27001, PCI, ENS, Magerit.

Gobierno de TI

Un modelo de Gobierno de TI habilita sinergias entre tecnología, seguridad y procesos de negocio en pos de facilitar la toma de decisiones. Alineando dichas iniciativas con la estrategia del negocio, y los requisitos cambiantes propios de los ámbitos tecnológico y legislativo.

Nuestros servicios

- Establecimiento de un marco de actuación.
- Gestión de la estrategia de TI y alineamiento con la estrategia de negocio.
- Estructuración de procesos de TI.
- Optimización de recursos de TI.
- Definición de indicadores de desempeño y cuadros de mando organizativos.
- Monitorización y seguimiento de acciones.
- Metodología de Gobierno TI propia de KPMG, basada en:
  - Metodología COBIT. Definición de Objetivos de Control para la Información y las Tecnologías Relacionadas
  - Metodología ITIL. Enfoque orientado al proceso para la entrega de la infraestructura IT como un conjunto de servicios y el soporte directo de esos servicios.

Plan Director de Seguridad

Servicios de consultoría encaminados a garantizar la continuidad de los procesos de negocio de la compañía. Identificación de procesos y funciones claves del negocio, relacionando los sistemas y comunicaciones críticos sobre los que se sustentan. Definición y revisión de planes de continuidad y gestión de crisis.

Nuestros servicios

- Análisis de Impacto en el Negocio. (BIA)
- Plan de Contingencia y recuperación ante desastres. (DRP)
- Plan de Continuidad de Negocio. (BCP)
- Gestiones de Crisis y Gabinete de Ejecución.
- Sistemas de Gestión de Continuidad de Negocio en base a la norma ISO 22301.
- Cálculo continuo de impacto y riesgo en los procesos de negocio.
- Plan de gestión del riesgo actualizado de manera permanente.
- Valoración y recomendación de las estrategias de recuperación alternativas más adecuadas.
- Metodología de Gestión de Crisis y Criterios y condiciones de activación de un BCP.
- Planes de pruebas y de auditoría de la BCM.

Privacidad

Realizar un correcto control sobre los activos de una compañía es de vital importancia. Una correcta gestión de los mismos hace que se pueda saber cuantos hay, quién accede a ellos, qué importancia tienen y así, poder centrar los esfuerzos para protegerlos de forma inteligente y reduciendo costes.

Nuestros servicios

- Gestión continuada de la Privacidad.

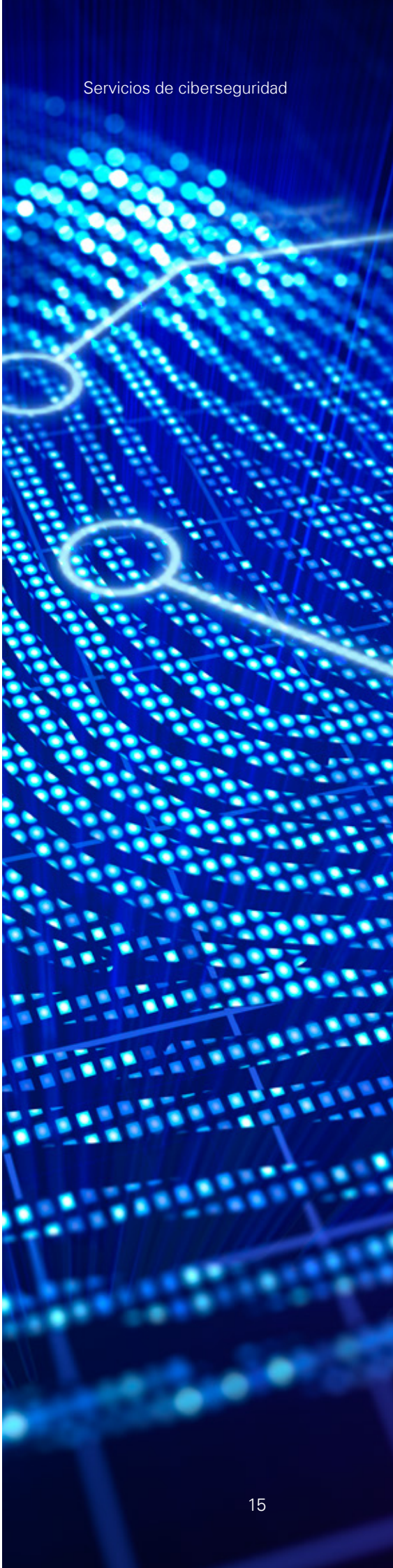
- Control del flujo de la información en los procesos de negocio:
  - Clasificación de la información
  - Protección de la Alta Dirección
  - Protección de la información soportada en la tecnología
  - Protección de Infraestructuras Críticas
  - Banco Cooperativo

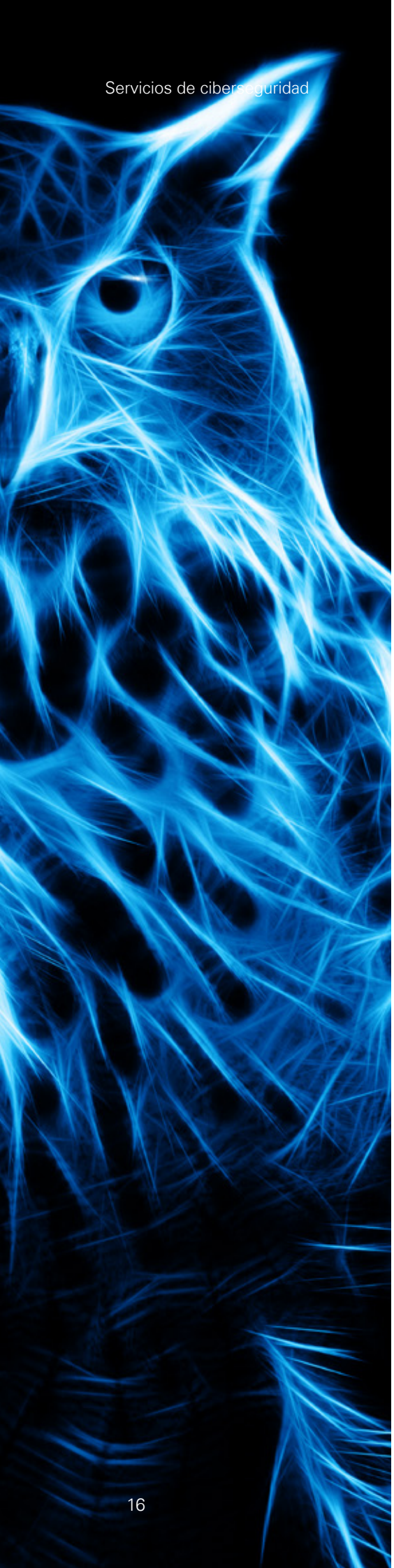
- Destrucción de la Información

- Definición de medidas de Seguridad para la información tanto a nivel lógico como físico para todo el ciclo de vida.

- Correcta gestión de los dispositivos móviles, inventarios de activos, flujos de aprobación, etc.

- Controles de seguridad Cloud.





Hacking Ético

Los Servicios de auditoría de seguridad tratan de proporcionar información sobre el grado de la integridad de los sistemas de información con la finalidad de eliminar accesos ilegales, prevenir robos de información y pérdidas de productividad.

Nuestros servicios

– Auditoría de seguridad y test de intrusión internos y externos.

– Revisión de Infraestructuras de sistemas de control: SCADA, MPLS, etc.

– Revisión de Seguridad Mainframes, SOs, BBDD, Red, etc.

– Revisión de la fortaleza de la infraestructura ante ataques (DoS y DDoS).

– Análisis Aplicaciones Móviles: Android, iOS & Blackberry.

– Análisis Tecnologías de comunicación: WiFi, NFC, VoIP, etc.

– Auditoría de código fuente.

– Gestión del fraude y ciberdelitos.

– Análisis de entornos: SAP, Navision, ERP, etc.

– Auditoría de aplicativos web.

– Análisis Concienciación en Seguridad.

Privacidad

Plan de pruebas ejecutado con el fin de identificar las posibles vulnerabilidades de los aplicativos web de un organismo.

El proceso de auditoría incluirá distintas pruebas de intrusión con el objetivo de identificar vulnerabilidades a través de una revisión de las técnicas de ataque actuales, realizando un hacking ético de las aplicaciones identificadas y reproduciendo estos ataques mediante un plan de pruebas:

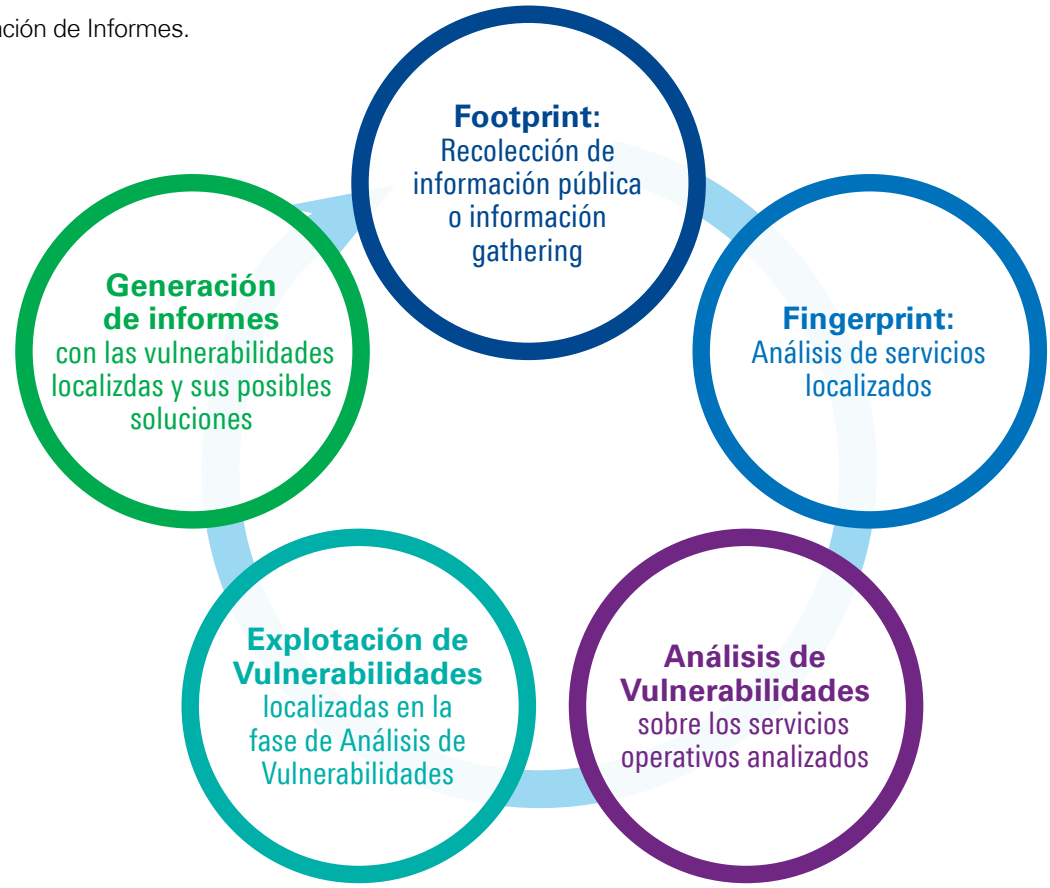
– Footprint.

– Fingerprint.

– Análisis de Vulnerabilidades.

– Explotación de Vulnerabilidades.

– Generación de Informes.



Auditoría Interna de Sistemas de Información

Plan de pruebas ejecutado con el fin de identificar las posibles vulnerabilidades la red interna de un organismo. Su objetivo se centra en simular posibles ataques hacker externos que hayan logrado alcanzar la intranet o ataques provenientes de personal interno:

- Pruebas de caja negra automáticas y manuales.
- Pruebas de caja blanca automáticas.
- Informe de las pruebas realizadas y del éxito de las mismas.
  - Impacto/Riesgo de las vulnerabilidades detectadas.
  - Recomendación para solucionar la vulnerabilidad.
  - Descripción de la vulnerabilidad.

Test de intrusión

Plan elaborado de pruebas para evaluar la seguridad de los sistemas de la compañía tanto de manera interna como externa.

- Pruebas de caja negra automáticas y manuales.

- Pruebas de caja blanca automáticas.

- Informe de las pruebas realizadas y del éxito de las mismas.
  - Impacto/Riesgo de las vulnerabilidades detectadas.
  - Recomendación para solucionar la vulnerabilidad.
  - Descripción de la vulnerabilidad.

Auditoría de aplicaciones móviles

Pruebas llevadas a cabo con el objetivo de identificar posibles vulnerabilidades en Aplicaciones de movilidad.

Se realizarán pruebas de intrusión y se identificarán vulnerabilidades mediante una revisión de las técnicas de ataque actuales, realizando un hacking ético de los aplicativos identificados y reproduciendo estos ataques mediante un plan de pruebas:

- Pruebas de caja negra automáticas y manuales.

- Pruebas de caja blanca automáticas.

- Informe de las pruebas realizadas y del éxito de las mismas.
  - Impacto/Riesgo de las vulnerabilidades detectadas.
  - Recomendación para solucionar la vulnerabilidad.
  - Descripción de la vulnerabilidad.

Los Servicios de auditoría de seguridad tratan de proporcionar información sobre el grado de la integridad de los sistemas de información con la finalidad de eliminar accesos ilegales, prevenir robos de información y pérdidas de productividad

Metodologías de trabajo en auditoría

OWASP

OWASP (Open Web Application Security Project) representa el conjunto de proyectos, llevados a cabo por una comunidad abierta, y sin ánimo de lucro, dedicados a encontrar y combatir las causas de la inseguridad del software.

Su objetivo es ayudar a las empresas a entender y mejorar la seguridad de sus aplicaciones y servicios web.

Proyecto OWASP

Un proyecto OWASP es una colección de tareas relacionadas, las cuales tienen definido un plan de actuación y un equipo de trabajo.

Los proyectos liberados más significativos son:

- OWASP Top Ten: Documento que describe las 10 vulnerabilidades más comunes en aplicaciones Web.
- OWASP Testing Guide: Documento diseñado para ayudar a las organizaciones a entender qué comprende la realización de un programa de pruebas, y ayudarlas a identificar los pasos necesarios a realizar para construir y operar dicho programa de pruebas sobre sus aplicaciones web.
- OWASP Guide Project: Manual para desarrollar aplicaciones y servicios web seguros, convertido en un estándar a nivel internacional.

KPMG-IA

La metodología KPMG-IA establece las pautas para la realización de pruebas de intrusión y búsqueda de vulnerabilidades sobre auditorías de seguridad interna, y detallando cómo realizar la comprobación de cada vulnerabilidad.

Para ello, divide el conjunto de pruebas en siete categorías:

- Recolección de información.
- Análisis de vulnerabilidades.
- Ataques en redes de datos.
- Pruebas de autenticación y autorización.
- Pruebas de malware.
- Pruebas de redes inalámbricas.
- Pruebas de disponibilidad de servicios.

Cada una de estas categorías establece una serie de controles específicos cuyo objetivo es la revisión global de la seguridad. La metodología KPMG-IA se basa en establecer un marco para la verificar la seguridad de los sistemas de información.

KPMG-MS

La metodología KPMG-MS establece las pautas para la realización de pruebas de intrusión sobre auditorías de aplicaciones móviles, y detallando cómo realizar la comprobación de cada vulnerabilidad.

Para ello, divide el conjunto de pruebas en siete categorías:

– Pruebas Cliente-Servidor.

– Privacidad.

– Almacenamiento local de datos.

– Ingeniería inversa.

– Esquemas URL.

– Notificaciones

KPMG-CA

Una auditoría de código fuente es un proceso de hacking ético, a través del cual se ejecutará un completo plan de pruebas para identificar las posibles vulnerabilidades existentes en el código fuente de un aplicativo:

Plan de pruebas KPMG-CA:

– Autenticación.

– Autorización

– Gestión de Cookies.

– Validación de datos de entrada.

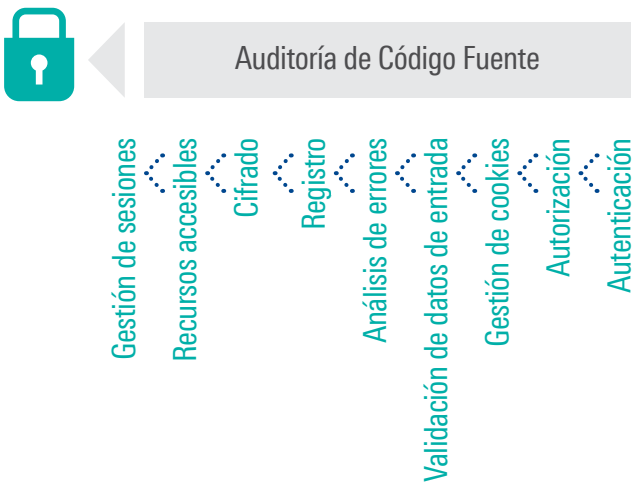
– Análisis de errores.

– Registro.

– Cifrado.

– Recursos accesibles.

– Gestión de Sesiones.



Fortificación

Hardening

Un proceso de hardening permite bastionar los sistemas de información con el fin de protegerlos ante posibles acciones maliciosas.

El proceso de aseguramiento de un sistema de información suele ir precedido de un proceso de hacking ético, donde se identifican las distintas fallas de seguridad existentes, y se desarrolla un plan de acción con las medidas que se deberán aplicar para fortificar la infraestructura.

El proceso de hardening contempla desde la instalación y configuración de dispositivos hardware, como elementos de seguridad perimetral, sistemas de copia de seguridad o backup hasta el despliegue de elementos software, como sistemas antivirus y antispyware o soluciones avanzadas de detección y prevención de intrusos.

En KPMG tenemos una dilatada experiencia integrando soluciones de distintos fabricantes con el fin de ayudar a nuestros clientes a estar protegidos ante el mayor número de amenazas posibles.

Fortificación de sistemas basada en estándares de mercado

Desde KPMG tenemos una dilatada experiencia en la fortificación de sistemas de información basándonos en estándares de mercado, normativas y metodologías de reconocimiento nacional e internacional y mejores prácticas indicadas por los respectivos fabricantes, como por ejemplo las guías CCN-STIC, publicadas de forma regular por el Centro Criptológico Nacional del Centro Nacional de Inteligencia de España.

- **Serie 400** (Ej. 406 Seguridad en Redes Inalámbricas, 407 Seguridad en Telefonía Móvil, 408 Seguridad Perimetral – Cortafuegos, 412 Requisitos de Seguridad en Entornos y Aplicaciones Web, 442 Seguridad en VMWare ESXi, 480H Seguridad en Sistemas SCADA – Establecer una dirección permanente).

- **Serie 500** (Ej. 521A Seguridad en Windows 2008 Server (controlador de dominio), 560A Seguridad en Windows 2012 Server R2 (controlador de dominio).

- **Serie 600** (Ej. 625 Seguridad en Sun Solaris 10 para Oracle 10g, 626 Guía de Securización de Sun Solaris 10 con NFS, 644 Seguridad en Equipos de Comunicaciones. Switches Cisco, 661 Seguridad en Firewalls de Aplicación, 672 Seguridad en Servidores Web Tomcat, 692 Guía de Securización de Oracle Application Server 10gR2 para Solaris 9 y 10).

- **Serie 800** (Ej. 812 Seguridad en Servicios Web en el ENS, 814 Seguridad en Servicio de Correo en el ENS, 816 Seguridad en Redes Inalámbricas en el ENS, 830 Seguridad en Bluetooth en el marco del ENS).

Ciberinteligencia

Nuevo enfoque de gestión de riesgos de ciberseguridad

Futuro

Capacidad de Respuesta en tiempo real

Evitar daños -> **Prevenir**

Tradicional

Reacción

Minimizar daños

Retomar control

PREVENTIVO

FOCO EN LOS NUEVOS CANALES

ANTICIPACIÓN

REDUCCIÓN DE INCERTIDUMBRE

RESILENCIA

SUPERANDO LÍMITES

INTELIGENCIA DE CONTEXTO

REACTIVO

OBSOLETO

COSTOSO E INEFICIENTE

SIEMPRE POR DETRÁS

SIN CONTEXTO

FRACASO

LIMITADO

Percepción global

Percepción parcial

Áreas de cobertura

Digital Network Intelligence (DNINT)

– Movimientos/ Revueltas Sociales.

– Individuos/Usuarios.

– Redes/Participación.

– Congegraciones.

– Sin objeto particular.

Criminal Intelligence (CRIMINT)

– Movimientos/ Revueltas Sociales.

– Individuos/Usuarios.

– Redes/Participación.

– Congegraciones.

– Sin objeto particular.

Brand Protection

– Defensa y protección de la marca.

– Tráfico de productos ilícitos.

– Propiedad intelectual, industrial y tecnológica.

Protección VIP

– Evaluación de Exposición Virtual.

– WEBINT – Web Intelligence.

– Web signature / Footprint.

– Firma / Huella Digital.

Contrainteligencia

– Contraespionaje.

– Protección de información.

– Amenazas exteriores.

– Incremento de la Seguridad.

Criminalística Digital

– Pruebas / Evidencias Digitales.

– Asegurar la escena Online.

– Laboratorio Forense.

Corporate (CI)

– Intel- Competitiva/ Tecnológica / Estratégica.

– Empleados/ Servicios / Productos.

– Reputación Corporativa.

– Vigilancia legal, jurídica, Normativa.

Diplomacia Digital

– Nuevos escenarios / Canales.

– Relaciones / Diplomacia Corporativa.

– Gobernanza Digital.

– Reducción de Riesgos.

Seguridad y prevención

Disponer de información relevante proveniente de fuentes abiertas, que nos permita:

– Identificar los canales utilizados para cometer los abusos o ataques. **(Canales)**

– Mejorar el entendimiento de los nuevos métodos de ataque. **(Patrones de Conducta)**

– Detectar las amenazas que se originan en Internet y que pueden poner en Riesgo a los clientes de su compañía, en el transcurso de la utilización de los servicios. **(Riesgos y Amenazas)**

– Detectar de forma temprana las amenazas a las infraestructuras. **(Alerta Temprana)**

– Identificar concentraciones sociales que puedan tener implicaciones en la prestación del servicio de su compañía, en la circulación de las personas por las instalaciones o en el uso. **(CRIMINT)**

Identificar información relevante sobre acciones de realización en instalaciones o material de la compañía:

– Identificación de acciones.

– Material visual: fotografías y videos.

– Apodos y firmas.

– Nombre de usuario o perfil.

– Grupo al que pertenece.

– Ubicación, datos de localización del individuo o de los datos localizados.

– Lugares de reunión o encuentro, para levar a cabo las acciones de vandalismo, etc.

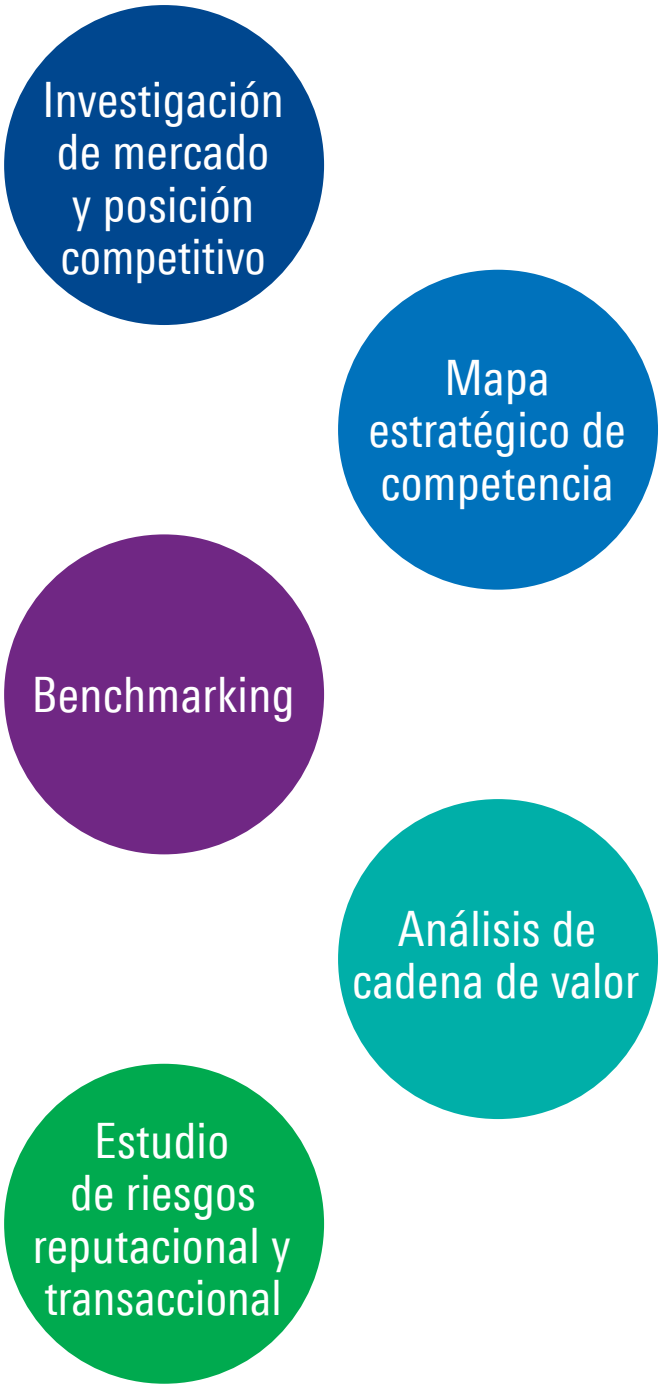
– Realizar investigaciones sobre hechos acaecidos, sobre los cuales se ha generado información en Internet y que haya sido recabada por el servicio o que pueda ser recabada por el mismo. **(Investigación)**

– Detectar la revelación de información confidencial o sensible por parte del personal que presta el servicio de vigilancia de seguridad. **(Contrainteligencia)**

– Generar y aportar la documentación como "prueba de cargo". **(Investigación y Criminalística: Pruebas y Evidencias)**

Disponer de información relevante que nos permita responder las siguientes preguntas:

- ¿Cuáles son los riesgos planteados por los posibles nuevos socios?
- ¿Qué vendedores o proveedores tienen la capacidad de poner mi negocio en Riesgo?
- ¿Quiénes son los competidores potenciales que no se ven en mi Mercado?
- ¿Cómo va afectar a la adquisición de mi participación en el Mercado?
- ¿Qué alianzas tienen sentido para mi negocio o empresa?
- ¿Qué eventos o asuntos políticos suponen un Riesgo para mi negocio?



Personal directivo/negocio

Disponer de información relevante que nos permita:

– Identificar la aparición de nuevas tecnologías críticas. **(Vigilancia Tecnológica)**

– Identificar la aparición de nuevos proveedores. **(Inteligencia Competitiva)**

– Identificar nuevos procesos productivos. **(Vigilancia Tecnológica)**

– Detectar posibles alianzas con fabricantes y/o proveedores. **(Inteligencia Competitiva)**

– Identificar las actuaciones de la Competencia en el mercado. **(Inteligencia Competitiva)**

– Detectar el desarrollo y lanzamientos de productos. **(Inteligencia Competitiva)**

– Identificar las acciones de Comunicación y comercial. **(Inteligencia Competitiva)**

– Identificar Personal Clave. **(Inteligencia Empresarial)**

– Identificar Datos económicos/Financieros/Sectoriales/ Consumidores/Competencia. **(Inteligencia Empresarial)**

– Detectar amenazas sobre clientes y/o áreas geográficas. **(Inteligencia Empresarial)**

Disponer de la información relevante proveniente de fuentes abiertas en Internet, que nos permita:

– Identificar información de interés para el ámbito de la comunicación de su compañía. **(Communication Intelligence)**

– Identificar la situación y el posicionamiento en el mercado de los productos. **(Market Intelligence)**

– Identificar aquellas materias sobre las que se vierten quejas o reclamaciones sobre una mala prestación del servicio. **(ORM, Online Reputation Management)**

– Identificar los usuarios más activos y potenciales líderes de opinión en blogs, foros o redes sociales, relacionados con los intereses de su compañía. **(Social Media)**

– Identificar aquellas materias que generan descontento de la compañía. **(Social Media Research)**

Disponer de información relevante que nos permita responder las siguientes preguntas:

– ¿Cuáles son los riesgos planteados por los posibles nuevos socios?

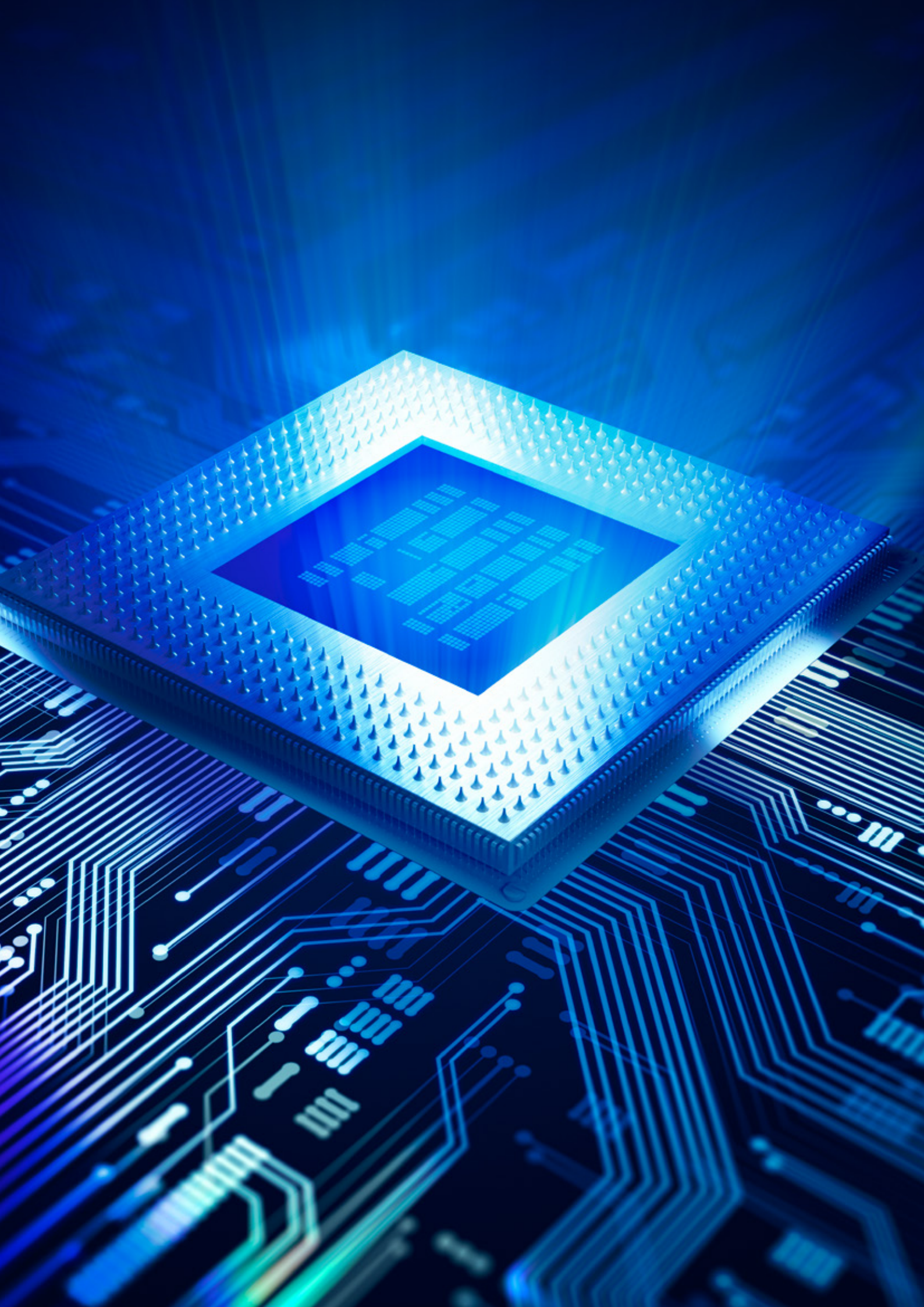
– ¿Qué vendedores o proveedores tienen la capacidad de poner mi negocio en Riesgo?

– ¿Quiénes son los competidores potenciales que no se ven en mi Mercado?

– ¿Cómo va afectar a la adquisición de mi participación en el Mercado?

– ¿Qué alianzas tienen sentido para mi negocio o empresa?

– ¿Qué eventos o asuntos políticos suponen un Riesgo para mi negocio?



Comunicación, Marca y Publicidad

Otras informaciones que puntualmente o coyunturalmente, sean de interés para el Negocio del en su conjunto o de un área en particular, esta inteligencia debe permitimos afrontar los siguientes retos:

– Evolución continúa de amenazas que provienen de fuera del perímetro de la empresa.

– Entender las metodologías de ataque.

– Identificar los canales utilizados para cometer los abusos.

– Rastreo del gran volumen de información y fuentes abiertas (blogs, foros, webs, redes sociales).

– Detección temprana y análisis del potencial del impacto negativo.

– Definir estrategias que permitan evitar que los ataques llegue a producirse.

Disponer de la información relevante que nos permita:

– Detectar las modificaciones en la **normativa** internacional, nacional y/o sectorial.

– Identificar los **proyectos de ley** que influyen en el devenir de la marca/empresa.

– Identificar **grupos de presión/lobby** de la empresa/marca.

– Detectar **licencias y patentes** en relación a tecnologías o procesos productivos.

– Identificar **Subvenciones, ayudas** y proyectos de desarrollo.

– Identificar amenazas para la **identidad legal digital**.

– Detectar la **usurpación** de perfiles corporativos. (Suplantación de identidad).

– **Phising**. (Usurpación de identidad de la empresa).

– **Pharming**. (Modificación del nombre de dominio).

Legal – Jurídico - Normativo

Disponer de la información relevante que nos permita:

– Detectar el registro abusivo de nombres de dominio o usuarios:
  – **Typosquatting**. (Registro de nombre de dominio similares a los de una marca)

– Detectar la utilización no consentida de derechos de propiedad intelectual o industrial: **(Brand Protection)**

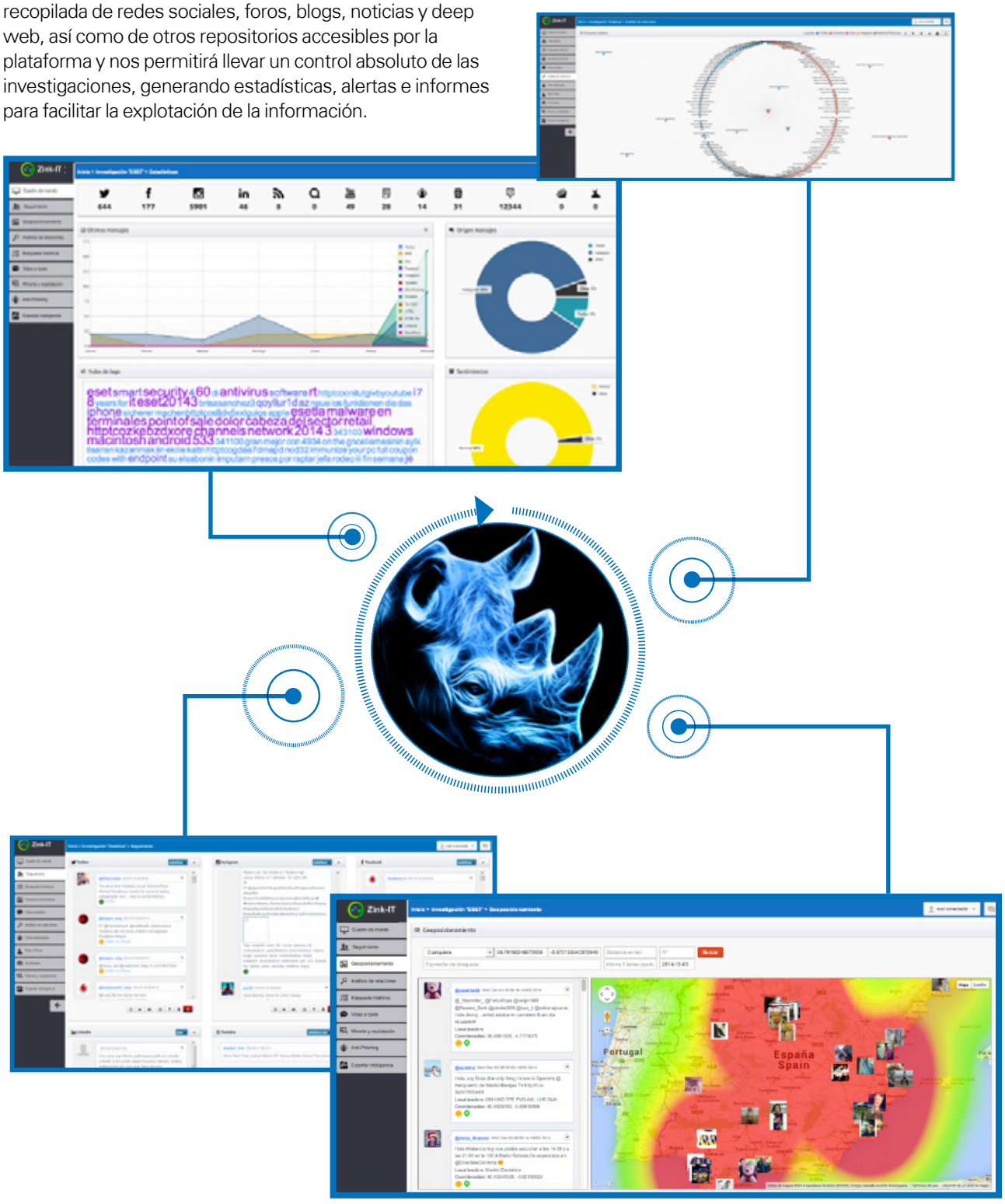
– Utilización no consentida de contenidos de terceros.

– Vulneración de derechos de marca y signos distintivos.

– Generar y aportar la documentación legal como "prueba y evidencia de cargo". **(Criminalística)**.

KPMG Intelligence Tool: K-IT

Esta herramienta nos permitirá investigar y monitorizar eventos, fugas de información, relaciones entre personas, grupos, entidades, etc. a través de la información recopilada de redes sociales, foros, blogs, noticias y deep web, así como de otros repositorios accesibles por la plataforma y nos permitirá llevar un control absoluto de las investigaciones, generando estadísticas, alertas e informes para facilitar la explotación de la información.



Investigación

Análisis de un suceso

Análisis de un sistema tras un suceso sospechoso con el objetivo de averiguar:

– ¿Qué ha ocurrido? ¿dónde? ¿cuándo? ¿cómo? ¿por qué?

Servicios de investigación:

– Análisis de dispositivos móviles y smartphones (iOS, Android, Windows Phone, etc.)

– Análisis de tarjetas SIM

– Análisis de malware.

– Análisis de logs.

– Análisis de discos duros y tarjetas de memoria.

– Análisis de memoria RAM.

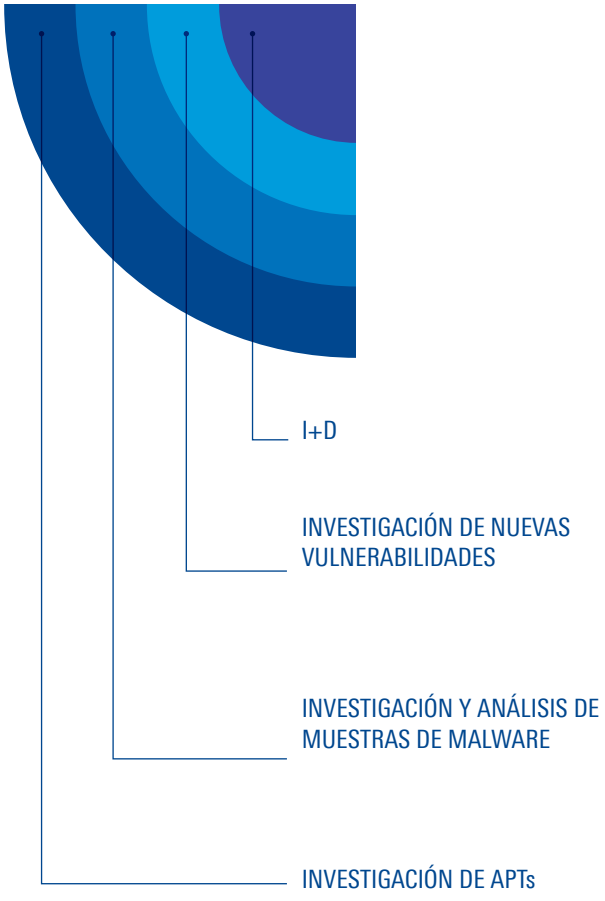
– Análisis de correo electrónico.

– Análisis de servidores de ficheros.

– Análisis de operaciones administrativas.

– Análisis de accesos no autorizados.

Laboratorio de amenazas



PERSONAL CERTIFICADO

CHFI	ITIL	DLINK
CISA	FTSAI	ANCITE
CISM	FCSI	PMP

Contactos

Marc Martínez Marce
Partner – IT Advisory
91 456 38 31
marcmartinez@kpmg.es

Javier Santos
Director – Cyber Security
91 456 59 04
666 48 26 51
javiersantos@kpmg.es

Juan Antonio Calles
Senior Manager - Cyber Security
608 91 95 03
jcalles@kpmg.es

kpmg.es

kpmgciberseguridad.es