

CyberSOC  
Seguridad 24/7



# Una nueva realidad

## Escenario actual

Las organizaciones se enfrentan hoy en día a un amplio catálogo de amenazas de seguridad que pueden materializarse tanto dentro como fuera del perímetro establecido.

La rápida evolución de estas amenazas complica asimismo la implantación de controles eficaces que, con el paso del tiempo, deberán ser revisados y actualizados para garantizar un nivel de seguridad aceptable.

En este contexto, es necesario combinar de manera inteligente los diferentes elementos que componen la estrategia de seguridad de una organización: operaciones, tecnología, equipos humanos, elementos de gestión del riesgo y procedimientos de trabajo.

Solamente con un enfoque holístico respecto a los elementos anteriores puede una organización mantener las capacidades de seguridad elementales con un rendimiento adecuado, entre ellas: capacidad de respuesta a incidentes, gestión de vulnerabilidades, control y protección de la reputación de la marca o la prevención de casos de fuga de información.

## La problemática existente

Muchas organizaciones que realizan significativas inversiones en seguridad manifiestan la ausencia del retorno esperado. Esta circunstancia se produce incluso cuando existe tecnología adecuada y personal con cierto grado de especialización.

Es asimismo frecuente la ausencia de controles adecuados para un amplio abanico de amenazas que hasta el momento no presentaban un nivel de riesgo significativo, o que ni siquiera habían sido consideradas en la estrategia de seguridad.

Por último, elementos tales como la capacidad de operar en 24x7, la disponibilidad de plataformas tecnológicas de seguridad con enfoque colaborativo, las sinergias derivadas del trabajo para múltiples clientes o la capacidad de financiar una infraestructura compleja y creciente quedan fuera del alcance de la mayor parte de la organizaciones, reduciendo la eficacia de sus planteamientos en materia de seguridad TI.

**Deloitte.**

### Applications for Security Management.

- Static Application Security Testing**  
The CyberSOC platform provides the most sophisticated technology to detect vulnerabilities in the source code with an automated process, suitable for any type of software applications, as well as managing their resolution in a collaborative way.
- Ethical Hacking Managed Services**  
These services provide the required resources to detect, document, manage and mitigate the risks associated with technological vulnerabilities found in the IT infrastructure of an organization. The web portal includes the features required to implement all the steps in the vulnerability management process.
- Intelligence Service**  
CyberSOC's advanced drawing technology provides relevant and useful information about global threats for all cybercrime's variants: phishing, malware, brand abuse, DDoS, sensitive information theft, etc.
- Phishing Protection Service**  
The team of highly skilled professionals responsible for accurately detecting and resolving this type of security incidents guarantee the best approach to threat management in an organization.

User:

Password:

I accept legal notice

[Request access](#) [Login](#)

#### News

**bugScout**  
Presentación  
Bienvenidos al nuevo canal RSS de bugScout Update

Minimum resolution is: 1280x800. Deloitte © 2012. All rights reserved. [Privacy policy](#) | [Terms of use](#)

# Servicios de seguridad de extremo a extremo

## Nuestra propuesta

Los servicios gestionados del CyberSOC se integran dentro de la solución global de Deloitte para ciberseguridad: preparar, conocer y responder; ayudando a consolidar la transformación de la organización desde una postura tradicional reactiva a una situación que permita anticiparse a los ataques y reducir los impactos que puedan causar de manera rápida.

La propuesta de Deloitte se fundamenta en la existencia de un SOC propio, con un enfoque cloud, con equipos de trabajo de alto rendimiento y con una plataforma tecnológica probada e integrada que permite resolver cualquier escenario corporativo en el que las operaciones de seguridad tengan un papel clave.

Deloitte permite a las organizaciones gestionar el riesgo tecnológico y reputacional a través de un portfolio de servicios que responden a necesidades reales, empleando las herramientas más eficaces y unos procedimientos de trabajo orientados al cliente.

Para la puesta en marcha del SOC, Deloitte ha considerado la problemática existente en clientes de los principales sectores del mercado, y ha enfocado su conocimiento en seguridad hacia los requerimientos específicos de un entorno crítico de operaciones.

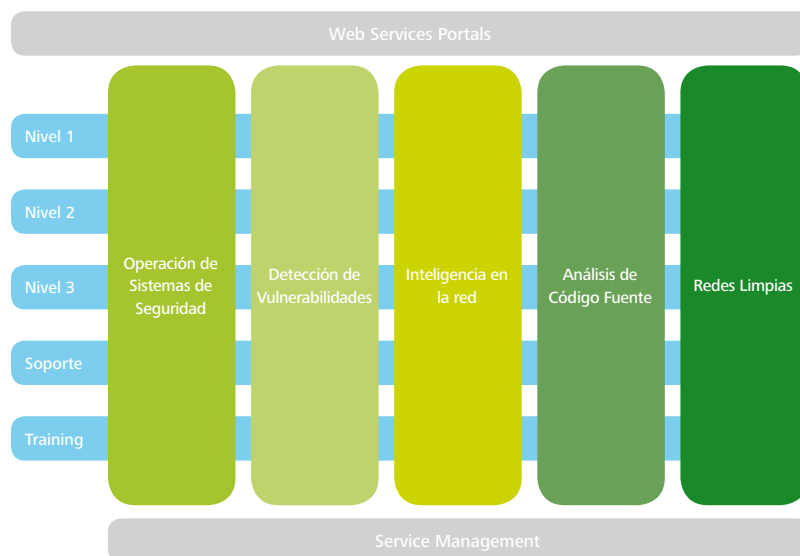
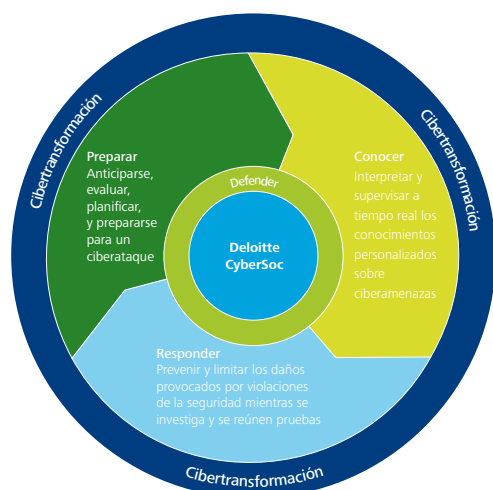
## El CyberSOC de Deloitte

Ubicado en Madrid, en unas instalaciones dedicadas, el CyberSOC está formado por casi 100 profesionales que trabajan en modalidad 24x7 para la prestación de un amplio conjunto de servicios de operaciones de seguridad.

El CyberSOC cuenta asimismo con una plataforma tecnológica que integra la tecnología de los fabricantes más exitosos del mercado, proporcionando un único punto de gestión a través del que los clientes pueden conocer el estado del servicio, obtener métricas e indicadores de su evolución, e interactuar con los equipos responsables de cada actividad.

El CyberSOC constituye el punto de referencia de servicios SOC a nivel internacional en Deloitte. En la actualidad, empresas de todo el mundo están empleando sus capacidades para resolver de manera eficaz sus necesidades en materia de seguridad y disponer de un modelo de operación eficiente, fiable, integral y efectivo.

Por último, esta aproximación global permite asimismo disponer de procedimientos de trabajo con un elevado grado de optimización, lo que desencadena un modelo de costes mucho más eficiente y competitivo.



# Una plataforma integrada

## Portfolio de servicios

El portfolio de servicios del CyberSOC comprende las principales áreas de actividad en un equipo de operaciones de seguridad, atendiendo a un amplio abanico de necesidades que incluye:

### Vulnerability Management

Focalizado en la detección y gestión de vulnerabilidades, en modalidad de vulnerability assessment, penetration testing, hacking gestionado, hacking on demand o hacking pasivo, a través del servicio de alerta temprana.

### Managed Security Services

Focalizado en la administración, monitorización y correlación de equipamiento de seguridad, con el objetivo de explotar al máximo las capacidades de la infraestructura y extraer información relevante para la gestión de incidentes o la toma de decisiones.

### Brand Services

Focalizados en la identificación, clasificación y procesamiento de información relevante publicada

en Internet, incluyendo phishing, malware, amenazas a la marca, reputación de la marca y reputación de directivos.

### Static Application Security Testing

Focalizado en la detección de vulnerabilidades en código fuente a través de una sofisticada tecnología que automatiza gran parte del proceso y la orquestación de las tecnologías involucradas en la aplicación revisada.

### Clean Pipes

Focalizado en la protección del correo electrónico corporativo y la navegación en Internet de los empleados, a través de una plataforma en la nube que evita la instalaciones de equipamiento on premises.

## Enfoque cloud

Todos los servicios del portfolio han sido diseñados para su prestación en modalidad cloud, sin necesidad de despliegue de equipamiento en la organización y con una capa de gestión de servicio que garantiza la interacción eficaz con el cliente y el control de los resultados.



# Servicios corporativos 24x7 en la nube

## Correlación de seguridad

Una plataforma de correlación en la nube capaz de detectar incidentes de seguridad en procesos de negocio, entornos sujetos a auditoría, despliegues DLP y otros sistemas cuya sofisticación va más allá de los sistemas de seguridad tradicionales.

## Static Application Security Testing

Una plataforma de revisión de código fuente en la nube con soporte para aplicaciones web, aplicaciones de escritorio, aplicaciones móviles y tecnologías de bases de datos, con un entorno de colaboración que optimiza los procesos de resolución asociados.

## Gestión de vulnerabilidades

Un equipo de profesionales en España y Argentina capaces de arrancar un trabajo de hacking en menos de 8 horas, conforme a nuestra capacidad On Demand, y un portal web de gestión desde el que abordar los procesos de resolución reduciendo los costes de documentación de resultados.

## Cyber Watch

Una plataforma de monitorización en Internet y un equipo de analistas capaces de identificar información sensible publicada en foros de cibercrimen, credenciales robadas, menciones difamatorias o casos de fraude vinculadas a las marcas de nuestros clientes.

## Brand 3.0

Un servicio de análisis de la presencia en la red que permite a las empresas conocer el sentimiento de sus consumidores respecto a la marca y sus productos, su posición respecto a sus competidores y el grado de posicionamiento de sus sitios web.

## Mobile Device Management

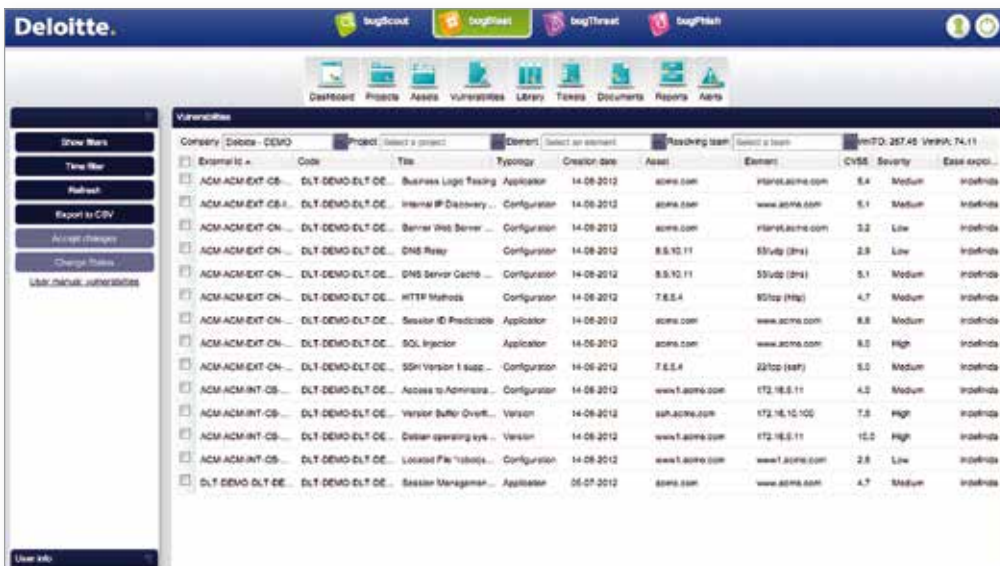
Una plataforma en la nube orientada a la gestión eficaz de los dispositivos móviles bajo la filosofía BYOD, con capacidades de prevención de fuga de información e implantación de las políticas de seguridad corporativas.

## Protección frente al fraude

Un equipo de especialistas capaces de eliminar sitios web fraudulentos vinculados a una organización en menos de 48 horas, detectar binarios maliciosos que afectan a una marca o analizar el comportamiento de los mismos para determinar el grado de impacto de un incidente de seguridad.

## Ingeniería social

Una metodología probada para identificar el grado de madurez de la organización respecto a los ataques de ingeniería social, con indicadores fáciles de interpretar y acciones correctivas que previenen la ocurrencia de los mismos y la concienciación de los empleados de la organización.



The screenshot shows the Deloitte Vulnerability Management interface. The main area displays a table of vulnerabilities with columns for Company, Code, Title, Typology, Creation date, Asset, Element, CVE, Severity, and Ease of exploit. The table lists various vulnerabilities such as Business Logic Testing, Insecure IP Discovery, Banner Spoof Server, DNS Relay, DNS Server Cache, HTTP Methods, Session ID Predictable, SQL Injection, SSH Version 1 supp, Access to Adminarea, Vendor Buffer Overf, Custom operating sys, Locked File System, and Session Management.

Company	Code	Title	Typology	Creation date	Asset	Element	CVE	Severity	Ease of exploit
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	Business Logic Testing	Application	14-06-2012	acme.com	http://acme.com	5.4	Medium	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	Insecure IP Discovery	Configuration	14-06-2012	acme.com	www.acme.com	5.1	Medium	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	Banner Spoof Server	Configuration	14-06-2012	acme.com	http://acme.com	3.2	Low	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	DNS Relay	Configuration	14-06-2012	8.8.10.11	55/tcp (DNS)	2.9	Low	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	DNS Server Cache	Configuration	14-06-2012	8.8.10.11	53/tcp (DNS)	5.1	Medium	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	HTTP Methods	Configuration	14-06-2012	7.8.5.4	80/tcp (HTTP)	4.7	Medium	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	Session ID Predictable	Application	14-06-2012	acme.com	www.acme.com	8.8	Medium	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	SQL Injection	Application	14-06-2012	acme.com	www.acme.com	8.0	High	Infinite
ACM-ACM-EXT-CS	DLT-DEMO-ELT-DE	SSH Version 1 supp	Configuration	14-06-2012	7.8.5.4	22/tcp (SSH)	5.0	Medium	Infinite
ACM-ACM-INT-CS	DLT-DEMO-ELT-DE	Access to Adminarea	Configuration	14-06-2012	www.f.acme.com	172.16.5.11	4.0	Medium	Infinite
ACM-ACM-INT-CS	DLT-DEMO-ELT-DE	Vendor Buffer Overf	Version	14-06-2012	sa.acme.com	172.16.10.100	7.0	High	Infinite
ACM-ACM-INT-CS	DLT-DEMO-ELT-DE	Custom operating sys	Version	14-06-2012	www.f.acme.com	172.16.5.11	10.0	High	Infinite
ACM-ACM-INT-CS	DLT-DEMO-ELT-DE	Locked File System	Configuration	14-06-2012	www.f.acme.com	www.f.acme.com	2.8	Low	Infinite
DLT-DEMO-ELT-DE	DLT-DEMO-ELT-DE	Session Management	Application	06-07-2012	acme.com	www.acme.com	4.7	Medium	Infinite

## Contactos

### **Alfonso Mur**

Socio Riesgos Tecnológicos  
amur@deloitte.es  
Telf.: +34 91 514 5000

### **Fernando Picatoste**

Socio Riesgos Tecnológicos  
fpicatoste@deloitte.es  
Telf.: +34 91 514 5000

### **César Martín**

Socio Riesgos Tecnológicos  
cmartinlara@deloitte.es  
Telf.: +34 91 514 5000

### **Luis Carro**

Socio Riesgos Tecnológicos  
lcarro@deloitte.es  
Telf.: +34 91 514 5000

### **Marta García**

Socio Riesgos Tecnológicos  
martgarcia@deloitte.es  
Telf.: +34 91 514 5000

### **Mercedes Gutiérrez**

Socio Riesgos Tecnológicos  
megutierrez@deloitte.es  
Telf.: +34 91 514 5000

### **Ricardo Martínez**

Socio Riesgos Tecnológicos  
rmartinezmartinez@deloitte.es  
Telf.: +34 91 514 5000

### **Fernando Pons**

Socio Riesgos Tecnológicos  
fepons@deloitte.es  
Telf.: +34 93 280 4040

### **Carmen Sánchez Tenorio**

Socio Riesgos Tecnológicos  
csancheztenorio@deloitte.es  
Telf.: +34 91 514 5000

Si desea información adicional, por favor, visite [www.deloitte.es](http://www.deloitte.es)

Deloitte se refiere a Deloitte Touche Tohmatsu Limited, (*private company limited by guarantee*, de acuerdo con la legislación del Reino Unido) y a su red de firmas miembro, cada una de las cuales es una entidad independiente. En [www.deloitte.com/about](http://www.deloitte.com/about) se ofrece una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, asesoramiento fiscal y legal, consultoría y asesoramiento en transacciones corporativas a entidades que operan en un elevado número de sectores de actividad. Con una red de firmas miembro interconectadas a escala global que se extiende por más de 150 países, Deloitte aporta las mejores capacidades y un servicio de máxima calidad a sus clientes, ofreciéndoles la información que necesitan para abordar los complejos desafíos a los que se enfrentan. Deloitte cuenta en la región con más de 200.000 profesionales, que han asumido el compromiso de convertirse en modelo de excelencia.

Esta publicación contiene exclusivamente información de carácter general, y Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, la Verein Deloitte Touche Tohmatsu, así como sus firmas miembro y las empresas asociadas de las firmas mencionadas (conjuntamente, la "Red Deloitte"), no pretenden, por medio de esta publicación, prestar servicios o asesoramiento en materia contable, de negocios, financiera, de inversiones, legal, fiscal u otro tipo de servicio o asesoramiento profesional. Esta publicación no podrá sustituir a dicho asesoramiento o servicios profesionales, ni será utilizada como base para tomar decisiones o adoptar medidas que puedan afectar a su situación financiera o a su negocio. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado. Ninguna entidad de la Red Deloitte se hace responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.

© 2013 Deloitte Advisory, S.L.

Diseñado y producido por CIBS, Dpto. Comunicación, Imagen Corporativa y Business Support, Madrid.