Deloitte.

La solución ante las ciberamenazas

Cybex One to One

Ciberseguridad

Contenidos

Conocer para responder

Probar, evaluar, reforzar

¡Atención!

Los procesos de negocio críticos de su organización dependen directamente del buen funcionamiento de servicios que se soportan sobre tecnologías de la información. ¿Está preparado para afrontar la ciberamenaza? ¿Lo ha comprobado desde un punto de vista práctico? ¿Los que toman las decisiones en su organización disponen de esta información?

Las tecnologías de la información proporcionan unas facilidades incuestionables para las entidades: acceso inmediato a la información, interconexión de sedes, teletrabajo, un escaparate ante todo el mundo donde publicitarse y comunicarse directamente con sus clientes. Esta ubicuidad de la información y de los servicios conlleva una mayor complejidad a la hora de mitigar los riesgos, ya que éstos pueden provenir tanto de un empleado descontento como de una organización dedicada al cibercrimen situada en la otra punta del planeta.

¿Qué puede implicar la materialización de una ciberamenazas?

La creciente dependencia de las tecnologías de la información implica que, en caso de materializarse una ciberamenaza, el impacto será mucho mayor. Pueden producirse pérdidas de información, daño a la imagen corporativa, indisponibilidad de servicios esenciales para el correcto funcionamiento del negocio, etc.

¿Es vulnerable su entidad ante ciberamenazas?

La complejidad y el alcance de los ciberataques han aumentado en los últimos años, así como las pérdidas que han supuesto para las entidades. Éstas pérdidas en un año se han visto incrementadas en un 56%, pasando de una media de $5,9 millones a una de $8,4 millones[1].

Ante el alto coste que supone la materialización de una ciberamenaza cobra mayor sentido preguntarse e indagar hasta qué punto las medidas de protección de su entidad son suficientes como para estar protegido ¿Las medidas técnicas de protección son las adecuadas? ¿Es correcta la organización del equipo de seguridad? ¿Son correctos los procedimientos de gestión de incidentes de seguridad? ¿La formación del personal es la adecuada?

[1] Ponemon Institute, «Second Annual Cost of Cyber Crime Study - Benchmark Study of U.S Companies,» 2011.

Ciberejercicios: de lo público a la privado

Algunos casos de éxito

Los ciberejercicios empiezan a cobrar mayor importancia en la actualidad gracias al valor añadido que aportan al permitir evaluar de forma global la respuesta de una entidad ante ciberataques además del carácter colaborativo que se genera entre los distintos participantes permitiendo que compartan experiencias y conocimientos adquiridos.

En el 2010 ENISA (European Network and Information Security Agent) organizó un ciberejercicio que incluyó a veintidós estados miembros de la Unión Europea (UE) como participantes y otros ocho como observadores. Del total un 95% consideró que el ciberejercicio había ayudado a comprender cómo tratar un ciberincidente de seguridad[2].

Posteriormente en el 2011, con el soporte del DHS (Department of Homeland Security) por parte de los EEUU y nuevamente de ENISA por parte de la UE se realizó otro ciberejercicio orientado a probar la reacción de infraestructuras críticas ante ciberataques. El 100% de los participantes consideró como útil su participación[3].

Con el objetivo de analizar y mejorar la capacidad de respuesta de las organizaciones ante posibles ciberataques a sus sistemas informáticos e infraestructuras críticas, la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum), junto al Instituto Nacional de Tecnologías de la Comunicación (INTECO), en colaboración con Deloitte, llevó a cabo la iniciativa CYBEX 2012, consistente en la simulación de ciberataques a determinadas empresas pertenecientes a distintos sectores estratégicos, para evaluar su nivel de preparación y su capacidad de respuesta ante ciberamenazas. Como resultado se obtuvo una valoración de las capacidades de dichas empresas de reaccionar ante un ciberataque y permitió elaborar un benchmarking comparativo de los distintos parámetros que fueron evaluados.

Desde Deloitte consideramos la participación en ciberejercicios una herramienta excelente para mejorar la protección frente a ciberataques y aumentar la concienciación interna en ciberseguridad.

¡Atrévete y pon a prueba tus capacidades!

[2] ENISA, «CYBER EUROPE 2010 – EVALUATION REPORT,» 2010.

[3] BIC – Networking ICT Trust and security researchers around the globe, «CYBER ATLANTIC 2011 - 1st joint EU-US Cyber Exercise,» 2011.

Ciberejercicios One to One

Su organización a prueba

Las pruebas, que serán diseñadas con el alcance y profundidad que requiera su organización, permitirán determinar el nivel de madurez en la gestión de la ciberamenaza permitiendo cubrir aspectos tan variados como los procedimientos gestión de incidentes, la gestión del conocimiento y las lecciones aprendidas ante vulnerabilidades o incidentes detectados previamente, las habilidades y conocimientos de las personas dedicadas a la ciberseguridad y la calidad de los planes de formación asociados, la idoneidad y suficiencia de las arquitecturas de seguridad implantadas.

Sus servicios a prueba

Ponga a prueba sus servicios Web, Correo Electrónico, Acceso Remoto y Específicos (DNS, VoIP,…) con una batería de pruebas diseñada específicamente para su organización, que le permitirán conocer su estado real de seguridad, no solamente desde el punto de vista técnico sino también desde el punto de vista funcional y organizativo.

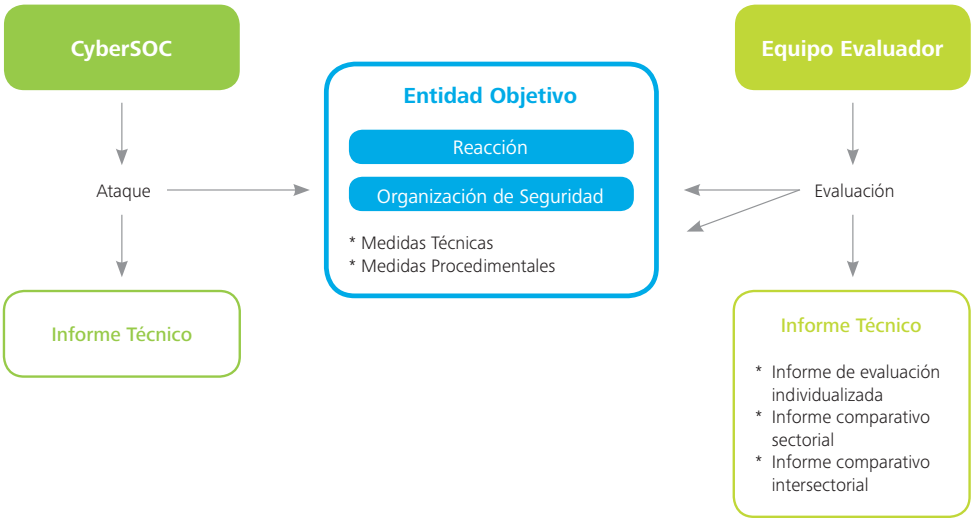
De esta manera, la batería de pruebas técnicas contempla, entre otras, la búsqueda y recopilación de información pública y análisis de metadatos, escaneos perimetrales, análisis de vulnerabilidades, pruebas de intrusión y diferentes APTs (ingeniería social, infección, phishing,…), abarcando prácticamente la totalidad de los posibles vectores de ataque que pueden ser generados por un atacante real.

Como elemento diferenciador, incorporamos la generación de escenarios de ciberataques, una tarea durante la fase de Planificación que permitirá definir vectores de ataque específicos contra su organización, en función de su estructura, negocio y visibilidad de activos.

Los ciberejercicios one to one permiten evaluar la madurez en la respuesta y recuperación ante los ciberincidentes, identificando líneas de mejora.

Por último, diseñamos la batería de pruebas para que su organización valide, en la medida de lo posible, el cumplimiento técnico de las diferentes legislaciones y normativas que le son de aplicación, de ámbito nacional e internacional, generando un enorme valor añadido la realización del ciberejercicio

Los resultados obtenidos tras un ciberejercicio, son la mejor herramienta para mejorar el nivel de concienciación de la dirección y de las distintas áreas de negocio de la organización sobre la importancia de estar preparados ante las ciberamenazas.



Evaluación a medida

¿Qué ofrecemos?

En función de las necesidades de su entidad dispondrá de un ciberejercicio adaptado que le permitirá evaluar las capacidades de respuesta ante ciberamenazas. Además existe la posibilidad de incluir dentro del alcance más de una entidad permitiendo así conocer su grado de seguridad en comparación con el resto, compartir experiencias y conocimientos.

Evaluación en profundidad

Evalúe todos los elementos de su entidad que entran en juego a la hora de responder ante ciberataques; no solo las configuraciones técnicas sino también las respuestas de las personas.

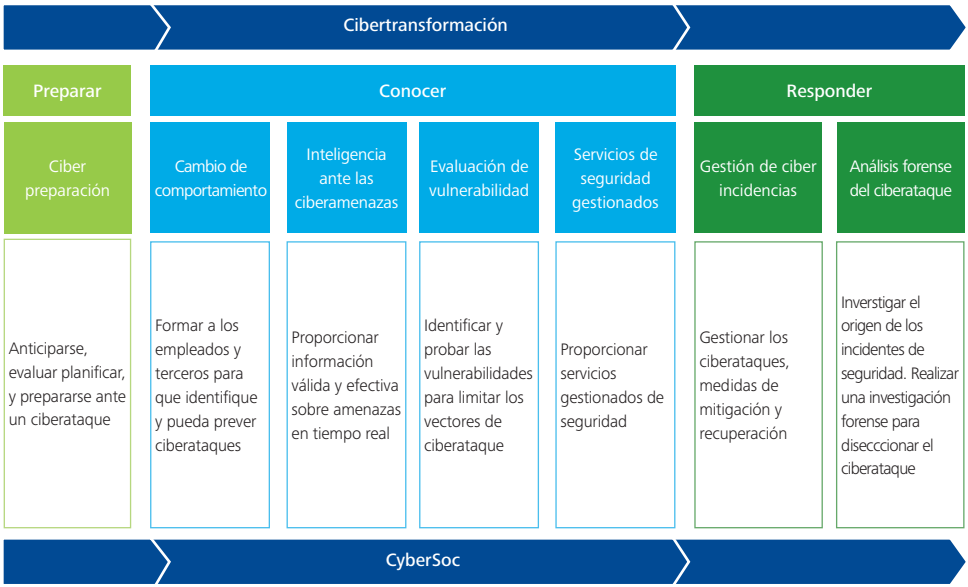
Conozca, ante distintos ciberataques, sus capacidades de prevención, detección, contención, recuperación, análisis forense, formación, gestión de crisis y coordinación con terceros. Con este enfoque podrá evaluar en detalle cómo responde su entidad de principio a fin: se materializa una ciberamenaza, se detectada por los sistemas de monitorización y se gestionada por un equipo especializado. Incluso podrá evaluar casos excepcionales como aquellos en los cuales entra en juego los procedimientos de respuesta ante crisis, interacción con otras entidades u organismos y análisis posterior al ciberataque.

	Alcance	One to One
Aspectos Técnicos	Web	✓
	Correo Electrónico	✓
	Acceso Remoto (VPN, TS,...)	✓
	Servicios Específicos (VoIP, DNS,...)	✓
	Información Pública	✓
	Escaneos Perimetrales	✓
	Análisis de Vulnerabilidades	✓
	Pruebas de Intrusión	✓
	APTs	✓
	Generación de Escenarios	✓
	Diseño para Cumplimiento	✓
Aspectos organizativos	Gestión de Incidentes: Prevención	✓
	Gestión de Incidentes: Detección	✓
	Gestión de Incidentes: Contención	✓
	Recuperación	Opcional
	Análisis Forense	Opcional
	Formación	Opcional
	Gestión de Crisis	Opcional
	Intercomunicaciones: Proveedores de Servicios	Opcional
	Intercomunicaciones: Autoridades u otros	Opcional

¿Cómo puede ayudar Deloitte?

¿Cómo puede ayudar Deloitte?
La capacidad de preparación de Deloitte permite a las empresas comprender realmente sus riesgos de sufrir ciberataques. Nosotros evaluamos procedimientos de gestión de crisis en escenarios controlados pero realistas, en vez de basarnos en planes hipotéticos. La demora a la hora de responder eficazmente a un incidente informático puede suponer un coste significativo para la organización, además del daño a su reputación.

- **Talleres de Preparación contra ciberataques:** Poner a prueba su estrategia y elaborar un inventario de los perfiles de riesgos informáticos a través de una prueba pautada personalizada en dos escenarios para informar de la naturaleza de la amenaza informática, considerar el impacto para la empresa y lograr una mayor comprensión de los procedimientos de respuesta implantados.



- **Simulaciones de Ciberpreparación:** Evaluar la capacidad de respuesta, tanto tecnológica como estratégica, e identificar las áreas de mejora. Los participantes pueden practicar los distintos roles y procedimientos involucrados en la gestión de la ciberamenazas (simulado) de tal forma que adquieran confianza y mejoren el conocimientos de los planes y procedimientos involucrados.

¿Por qué Deloitte?

Nuestro personal está capacitado y cuenta con una gran experiencia en la preparación de simulacros y ejercicios de gestión de crisis basados en diferentes metodologías.

El equipo lleva a cabo pruebas que permiten analizar la estrategia de gestión de ciberincidentes, de tal forma que salgan a la luz y puedan ser eliminados los errores ocultos, las hipótesis falsas, las lagunas en los planes y las expectativas irreales con antelación a que los planes tengan que ser aplicados en la realidad.

Hemos coordinado y evaluado CYBEX2012, el primer ejercicio de ciberseguridad del sector privado en España.

Para más información:
www.deloitte.com/cyber

Nuestra experiencia

El equipo de Deloitte cuenta con experiencia en simulaciones de ciberpreparación ante miembros de consejos de administración, ofreciendo sesiones a medida con resultados prácticos.

Servicios de Seguridad extremo a extremo de Deloitte

Nuestros servicios de Seguridad y Privacidad abarcan desde la capa estratégica hasta la operación de sistemas de seguridad 24x7, persiguiendo la protección integral de los activos críticos de la organización: personas, información, procesos e infraestructuras.

Estrategia y valor de la seguridad corporativa

Definir, diseñar y mejorar el marco de gobierno de la seguridad para asegurar la eficacia, eficiencia y sostenibilidad de la función de seguridad garantizando el cumplimiento de las estrategias de negocio, tecnológicas y los requisitos regulatorios actuales.

Ciberseguridad
Defender contra ciberataques y limitar su impacto actuales.

Protección de la Información y Privacidad
Proteger la información sensible y asegurar el cumplimiento.

Gestión de Identidades y Accesos
Controlar el acceso a la información en un entorno sin frontera.

Preparación y Resilencia
Preparar, planificar y anticipar la respuesta ante los peores escenarios posibles.

Seguridad Patrimonial
Proteger personas e infraestructuras.

Necesidades Emergentes

- Smart Metering
- Cloud Computing
- Social Media Risk
- Movilidad
- Protección Infraestructuras Críticas

CyberSOC

- Optimizar el coste asociado a la operación de la infraestructura de seguridad,
- Incrementar las capacidades de detección de vulnerabilidades tecnológicas y garantizar su adecuada gestión
- Reducir el riesgo asociado a prácticas inadecuadas de desarrollo de software
- Dotar de inteligencia en la Red para identificar amenazas a la marca o los procesos de negocios de nuestros clientes,
- Multiplicar el Retorno de Inversión en Seguridad con un portfolio de servicios prestados a través de una plataforma cloud de alto rendimiento.

Los ciberejercicios son una herramienta excelente para mejorar la protección frente a ciberataques y aumentar la concienciación en ciberseguridad

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

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