Deloitte.

Ciberseguridad
Es su negocio

Ciberseguridad
Preparar. Conocer. Responder

Es la guerra...

Si su empresa utiliza Internet, es vulnerable ante los ciberataques. ¿Está preparada su organización para enfrentarse a las ciberamenazas? ¿Ha considerado qué activos pueden ser vulnerables? ¿Sabe cuál puede ser el coste de un ataque que tenga éxito? ¿Ha planificado cuál sería la respuesta de su empresa a un ataque?

La revolución digital ha aportado inmensos beneficios en innovación y crecimiento, pero la gran dependencia que muchos modelos de negocio tienen con respecto a Internet los expone a nuevas amenazas. Los activos que antes estaban físicamente protegidos, ahora están disponibles en la red; los canales de clientes son vulnerables a interrupciones de funcionamiento y los delincuentes tienen nuevas oportunidades para robar y cometer fraude. Las barreras que protegen de los delitos informáticos son débiles, los métodos son cada vez más sofisticados y los riesgos de ser detectados o capturados se consideran mínimos.

La protección frente a los delitos informáticos debe ser una prioridad para las empresas. Esta cuestión debería tratarse como un riesgo estratégico de negocio, en vez de simplemente como una cuestión tecnológica o de seguridad. ¿Está involucrado el consejo de administración el seguimiento de estos temas? ¿Cómo puede asegurarse de que su empresa está protegiendo sus operaciones de forma adecuada?

¿Cómo pueden afectarle las ciberamenazas?

Las ciberamenazas pueden proceder de delincuentes bien organizados, de hackers o de un sistema de espionaje promovido por los poderes públicos. Los costes directos e indirectos provocados por los ciberincidentes a nivel mundial se han estimado recientemente en unos 388.000 millones de dólares*; esto incluye, entre otro, los costes por robo, fraude, extorsión y pérdida de propiedad intelectual. Además del impacto financiero directo, incidentes recientes han puesto de manifiesto las graves implicaciones empresariales que suponen las ciberamenazas, desde el desplome del precio de las acciones y la pérdida del valor para los accionistas, hasta la perdida de confianza por parte de los mercados y de los consumidores.

Hay muchas formas en las que un ciberataque puede ejercer un impacto negativo en una organización. En el grafico de la derecha se pueden ver cuatro posibles amenazas, los activos que ponen en riesgo y el impacto y las consecuencias de un ataque con éxito. Es fundamental recordar que un ataque materializado puede tener efectos que van más allá de la violación inmediata de los accesos.

Da igual de qué tipo sea su negocio, ahora es fundamental desde un punto de vista económico y estratégico estar preparado para un ciberataque.

* Informe realizado por Cabinet Office y Detica (2011): El coste de los delitos informáticos (publicado el 17/02/2011)

Se avecinan tiempos difíciles

Enfrentarse a las ciberamenazas ya no es solamente una cuestión del departamento de informática, sino que requiere la intervención del conjunto de la empresa, desde el consejo de administración hasta los empleados.

Deloitte ha detectado una serie de barreras que impiden que las organizaciones estén adecuadamente preparadas para responder ante el cibercrimen:

- Miembros del consejo de administración y de la dirección que son reacios a la hora de tomar decisiones debido al lenguaje técnico utilizado para describir las amenazas. No se les está ayudando a comprender el riesgo que suponen estas amenazas para la empresa.

- Empresas y empleados que comparten información, a través de las redes sociales, y que no siempre son conscientes de los riesgos que puede suponer para la empresa.

- La escasa capacidad y preparación de los equipos técnicos para gestionar ciberamenazas cada vez más complejas.

- El coste y la dificultad que suponen desarrollar y mantener la capacidad de supervisión de la seguridad 24 horas al día pueden resultar prohibitivos, y suelen provocar una actitud más reactiva de "responder cuando se ha producido el ataque".

- La inmensa cantidad de información acerca de amenazas informáticas hace que sea difícil que las empresas identifiquen y prioricen donde se requiere.

- La falta de coordinación entre los distintos departamentos involucrados puede impedir que se compartan los conocimientos sobre los riesgos existentes y, por tanto, imposibilitar dar una respuesta efectiva a un ciberataque.

Los ciberataques son en la actualidad prácticamente inevitables. Las organizaciones deben apostar por desarrollar la capacidad para enfrentarse a esta creciente amenaza de forma que puedan atender a clientes, consumidores, accionistas y organismos reguladores. Deloitte opina que los riesgos de negocio relacionados con las ciberamenazas debe considerarse un elemento prioritario en la estrategia de cualquier empresa que utilice Internet.

¿Qué se debe hacer?

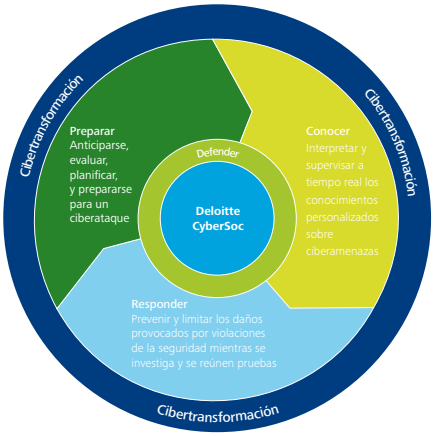
Este tipo de amenaza tan diferente requiere una respuesta muy distinta. Las defensas tradicionales se centran en los controles de seguridad para bloquear las amenazas, pero ni siquiera los mejores sistemas pueden detectar o evitar todos los ataques, y lo único que pueden conseguir es ayudarle a manejar las consecuencias. Para que la empresa aborde un tema tan difuso y complejo, Deloitte identifica tres puntos clave:

Preparar: Comprender -desde los miembros del consejo de administración hasta los empleados- cuáles son los riegos y cuales podrían ser las consecuencias para la empresa de un ciberataque. Asignar recursos para preparar la respuesta de la organización frente a un posible ataque.

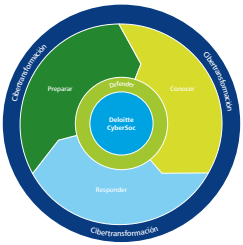
Conocer: Identificar y comprender los objetivos y los mecanismos de un ciberataque. Para ello se necesitan conocimientos generales sobre la evolución de las amenazas, junto con conocimientos específicos de su sector y su organización. Los empleados son también activos fundamentales en la defensa contra los delitos informáticos, por tanto es importante lograr su implicación al tiempo que se toman las medidas técnicas pertinentes.

Responder: Estos conocimientos son útiles solamente si se es capaz de actuar en consecuencia. Una organización debe estar preparada para responder a una amenaza o ataque, tanto a nivel técnico como empresarial. Debe estar preparada para refrenar el impacto de un incidente, comprender su origen, ocuparse rápidamente de las consecuencias que puede tener para la actividad y poner en práctica lo aprendido de modo que se puedan evitar incidentes en el futuro.

El desafío es grande, pero no insuperable. El enfoque que recomendamos hará que evolucione desde una postura tradicional reactiva y adquiera un conocimiento sobre las ciberamenazas que le permita anticiparse a los ataques y responder ágilmente para reducir así su impacto.



Deloitte.



Que el ruido no le distraiga
Conocer

Conocimiento de la situación — la percepción de los elementos del entorno en relación con el espacio/tiempo, la comprensión de su significado y la proyección de su estado tras un cambio en alguna variable".
Definición de Endsley, 1995b

El reto

Explicado de forma sencilla, el conocimiento de la situación consiste en "saber qué es lo que está pasando, de tal modo que pueda averiguar qué hacer". El reto consiste en saber qué ciberamenazas son relevantes para su organización, y prever cuales serán las próximas y de dónde vendrán.

Parte de la dificultad a la hora de responder a este reto reside en la capacidad técnica. La información obtenida a partir de la actividad previa, los datos de auditoría y los registros de seguridad sólo pueden proporcionarnos una imagen estática del pasado, pero debido a la complejidad y a la rapidez de los cambios en el panorama actual con respecto a las cibeamenazas , no es suficiente una perspectiva de lo que ha ocurrido en el pasado.

Las organizaciones necesitan obtener una visión dinámica y a tiempo real de sus posibles amenazas, lo que les permitirá gestionar con los futuros casos.

La otra cara de la respuesta son las personas. La consumerización, la expansión de la tecnología móvil y el uso generalizado de las redes sociales en el trabajo y en el día a día hacen cada vez más difícil distinguir el límite entre red corporativa y dominio público. Le recomendamos que informe a sus empleados sobre las ciberamenazas y el papal que deben desempeñar a la hora de defenderse de ellas.

¿Por qué ahora?

Cuando las amenazas evolucionaban lentamente, las organizaciones podían defenderse de forma eficaz basándose en los principios clásicos de seguridad: "detección y respuesta".

Pero la rapidez con que se desarrollan ahora los nuevos ataques y la complejidad del entorno de Internet hacen que esta forma de actuar ya no sea la adecuada.

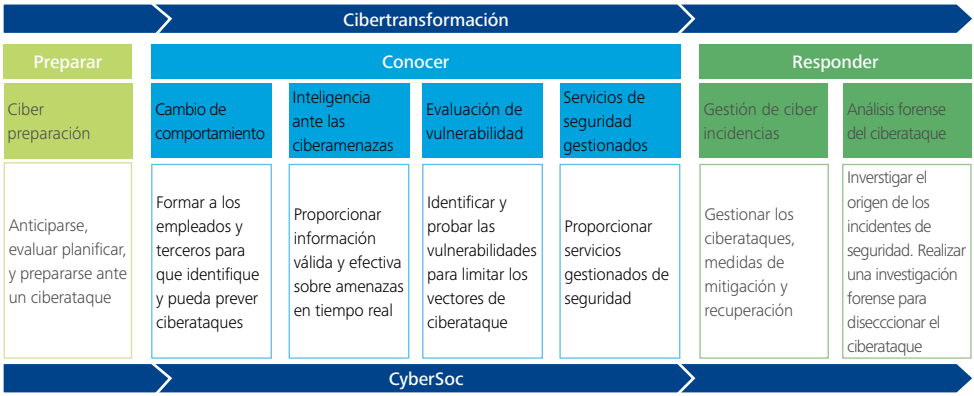
¿Qué puede hacer al respecto?

A medida que los proveedores de soluciones de seguridad adaptan y mejoran sus servicios, las organizaciones tienen cada vez más herramientas y técnicas a su disposición para abordar las amenazas informáticas. El conocimiento eficaz de estas amenazas debe basarse en los siguientes elementos clave:

- Formar a sus empleados para que puedan frustrar posibles intentos de manipulación que les lleven a actuar de forma que puedan exponer a la organización a un ciberataque.
- Proporcionar información válida y efectiva sobre amenazas en tiempo real.
- Identificar y verificar los vulnerabilidades.
- Realizar de forma continua controles de seguridad en áreas de alto riesgo.

Llevar a cabo un examen de la situación proporciona a las organizaciones la información necesaria para adaptar sus defensas y planes a las grandes amenazas, mitigando así los mayores riesgos.

¿Cómo puede ayudar Deloitte?



La capacidad que posee Deloitte proporciona a nuestros clientes servicios a medida: inteligencia aplicada a la ciberseguridad, evaluación de vulnerabilidades, mejora en la madurez del SOC (Security Operations Center) interno y proporcionar servicios gestionado de seguridad en formato externalizado, 24x7 desde el CyberSOC de Deloitte.

Cambio de comportamiento: un programa que aumente el conocimiento de la organización sobre los riesgos informáticos y, específicamente, que forme a los empleados para que puedan identificar y frustrar los intentos de "ingeniería social".

Información relativa a las amenazas informáticas: obtenida de múltiples fuentes de dominio propio y público, y proporcionada a través de un servicio del CyberSOC que permite que nuestros clientes puedan acceder a la información relativa a las amenazas de su organización, sector y zona geográfica, o recibir un resumen ejecutivo e informes detallados.

Evaluación de vulnerabilidad: evaluación y comprobación de las infraestructuras, de las aplicaciones y de los dispositivos móviles para proporcionar a nuestros clientes una visión en profundidad de las vulnerabilidades técnicas que existen en su entorno, pudiendo así remediarlas y eliminar los posibles vectores de ataque informático.

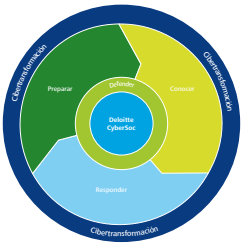
Servicios de seguridad gestionados: proporcionada a través del CyberSoc de forma externalizada, en formato 24x7 y según las necesidades específicas de nuestros clientes.

¿Por qué Deloitte?

Nuestra especial relación con distintos fabricantes de seguridad, combinada con nuestra especialización técnica y los servicios proporcionados por el CyberSOC, nos permiten ofrecer información completa y personalizada de las amenazas que aplican a cada organización. Somos capaces de superar la visión estática convencional sobre riesgos y proporcionar una perspectiva dinámica e inteligente del escenario de ciberamenazas.

Nuestra experiencia

Nuestro equipo especializado en la gestión de la vulnerabilidades cuenta con una amplia experiencia en la evaluación de sistemas, identificando debilidades y frentes de ataque, y aplicando las mejoras prácticas de configuración segura para reducir la exposición a las ciberamenazas.



Planificar y practicar
Preparar

"... Nunca he conocido a un experto en seguridad que diga 'siempre y cuando sigas estos tres pasos no te ocurrirá nada, porque los hackers no te atacarán...' la cuestión es cómo organizarse para poder sobrellevar estas cosas…"
Tim Schaaff, Presidente de Sony Network Entertainment

El reto

¿Qué riesgos suponen para su negocio las ciberamenazas? ¿En qué medida es capaz su organización de gestionar las consecuencias de un ataque? ¿Cuántos ataques ha sufrido en el último mes? ¿Quién gestiona estos ataques?

La preparación ante un ciberataque debe realizarse en el conjunto de la empresa: los ataques que tienen éxito ejercen un impacto directo en el valor para el accionista. Aunque el departamento de informática debe establecer defensas técnicas, una brecha puede tener consecuencias de gran envergadura para el negocio. Identificar los riesgos para la empresa y decidir cómo y cuándo deben elevarse a un nivel jerárquico superior los ciberataques son los puntos de partida para desarrollar una respuesta efectiva y coordinada.

¿Por qué ahora?

Muchas organizaciones de todos los sectores están siendo victimas de ataques.

Algunos ataques han tenido más éxito que otros, pero la mayoría de las organizaciones es objetivo de delincuentes informáticos, y los ataques son persistentes. No hay garantía de que la defensa tenga éxito, así que es imprescindible comprender los riesgos para su negocio y tener la capacidad de responder para proteger al personal, los activos, los clientes y el valor de la organización.

Una visión clara de los riesgos que le amenazan es el comienzo. Después, para estar preparado para hacer frente a las amenazas se requiere una capacidad de respuesta probada y coordinada. Previamente es crucial haber preparado planes, procedimientos y personas, además de disponer de los activos necesarios. Esta capacidad sólo puede obtenerse a través de la práctica. No se puede considerar que los planes sean eficaces hasta que hayan sido probados periódicamente.

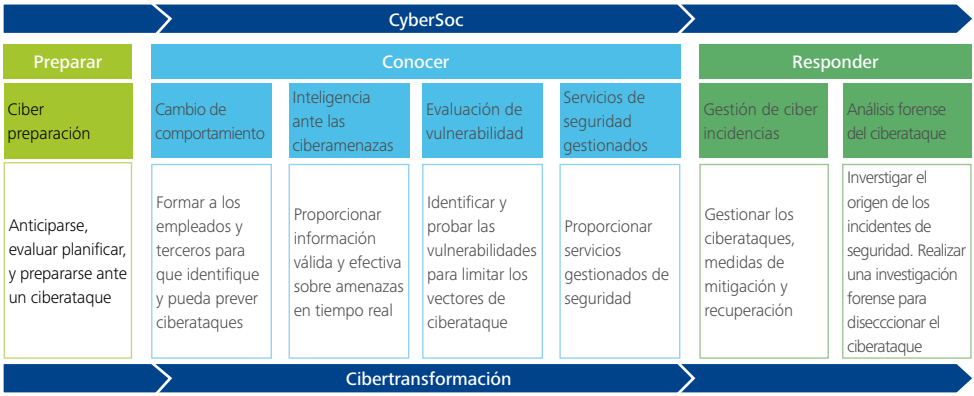
¿Qué puede hacer al respecto?

Para una preparación eficaz es muy importante:

- Comprender bien los riesgos para el negocio y los planes para mitigarlos.
- Definir funciones, responsabilidades y procedimientos de toma de decisiones.
- Delegar autoridad a la hora de responder y definir vías para elevar las cuestiones a los niveles jerárquicos superiores.
- Examinar al personal y probar los planes mediante ejercicios pautados y simulaciones.

Desarrollar y practicar su capacidad de respuesta para reaccionar ante ciberincidentes de forma coordinada, informando oportunamente a dirección para que las tengan en cuenta y les den respuesta, ayudará a anticiparse a las amenazas y a resolverlas rápidamente. Ésta es la clave para minimizar el impacto en su negocio.

¿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.

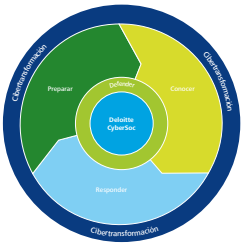
¿Por qué Deloitte?

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.

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.



Con rapidez, decisión y contundencia
Responder

"No hay secretos para el éxito. Se alcanza preparándose, trabajando duro y aprendiendo de los errores".
Colin Powell, 2005

El reto

Cuando se produce una violación de la seguridad, la respuesta debe ser rápida, contundente y decisiva. Es necesaria una acción inmediata en varios frentes. Se deberá establecer la naturaleza de la violación y comprender la magnitud del daño y las pérdidas. Se deberán prevenir los futuros ataques a través de medidas urgentes, hasta que se encuentre una solución a largo plazo. Habrá que tratar con los medios de comunicación y con los agentes externos. Puede que sea necesario adoptar medidas legales y evaluar las responsabilidades.

Una respuesta inadecuada a una violación de la seguridad puede provocar un gran daño a la reputación de la empresa y al valor que ésta tiene para los accionistas. También puede aumentar el riesgo de nuevos ataques.

¿Por qué ahora?

La evolución de las amenazas en el ciberespacio es tal que las organizaciones deben asumir ya que serán atacadas en algún momento y, quizás, de forma reiterada.

Al mismo tiempo, el interés creciente que los medios y las redes sociales dedican a este tema provoca que la noticia de cualquier ataque se extienda con rapidez.

Esta combinación de circunstancias ejerce una presión sin precedentes en los sistemas de respuesta.

Muchas organizaciones están atravesando una fase de reducción de costes, ahorro y restricciones de plantilla. Por ello, será esencial disponer de planes bien elaborados y operativos que permitan utilizar los recursos pertinentes para lograr el máximo efecto inmediatamente después de un ataque.

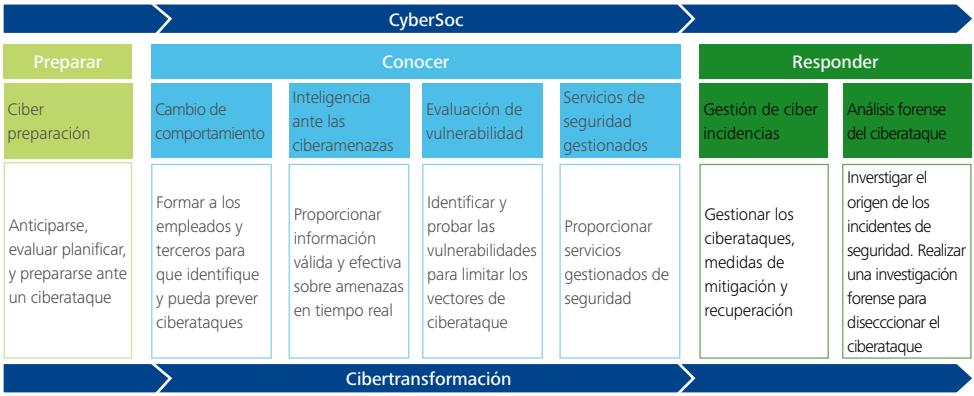
Esta tarea puede complicarse significativamente debido a la intensa atención que despierta cualquier ataque, presionando a la organización para que proteja los intereses de sus accionistas, satisfaga las expectativas de los organismos reguladores y vuelva a operar con normalidad tan pronto como sea posible – a menudo bajo el foco de los medios de comunicación.

¿Qué puede hacer al respecto?

Las violaciones de la seguridad informática son inevitables, así que para minimizar el riesgo que puedan conllevar y su impacto potencial, las organizaciones deben tener una actitud proactiva a la hora de definir, planificar, evaluar y posibilitar estrategias y capacidades de respuesta. Esto debería incluir:

- Definir los procesos y planes necesarios para poder priorizar las acciones de respuesta y mitigación, considerando la continuidad del negocio en su conjunto, las operaciones y las relaciones públicas, además de las operaciones informáticas.
- Disponer de las aptitudes técnicas y las herramientas necesarias para evaluar el origen de la violación, llevar a cabo una investigación forense y probar la validez de la solución técnica.
- Revisar de forma continua, mejorar y adaptar la capacidad de respuesta, además de modificar los perfiles de riesgo organizacional y las ciberamenazas.

¿Cómo puede ayudar Deloitte?



Los servicios de respuesta ante ciberataques de Deloitte han sido diseñados para proporcionar a nuestros clientes acceso a los conocimientos y procedimientos necesarios para gestionar una crisis. Esto incluye:

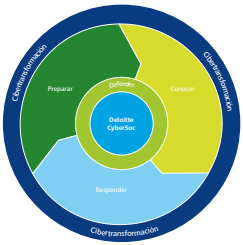
- **Gestión de los ciberincidentes:** nuestros expertos en gestión de crisis pueden ofrecer soporte en la respuesta ante incidentes y en las actividades de gestión, y en la identificación de las brechas de seguridad, en la obtención de lecciones aprendidas a partir de los ciberincidentes y en la planificación de la continuidad de los procesos de negocio que dependen de la red.

- **Investigación forense informática:** nuestros equipos están especializados en la evaluación del origen de los ataques, en el análisis de las violaciones de seguridad y en la investigación forense.

¿Por qué Deloitte?

Una respuesta eficaz frente a los ciberincidentes requiere de la flexibilidad y de la habilidad para tomar decisiones proactivas, a menudo con información limitada. El potencial de Deloitte, al contar con toda una serie de profesionales experimentados, permite proporcionar servicios de gestión y respuesta ante incidentes de seguridad que ayudan a las organizaciones a gestionar los ciberincidentes.

Nuestra experiencia
Trabajamos con numerosas organizaciones afectadas por violaciones en su seguridad informática, ayudándolas a responder e investigar los incidentes, identificar el origen y poner en marcha los planes de mitigación y recuperación.



Un modelo eficiente de operación CyberSOC

"Forrester anticipates that the SOC will become virtualized in the future, in a next-generation transformation that we call SOC 2.0".
Forrester Group, 2010

El reto

Todos los elementos que conforman la infraestructura tecnológica de una organización están sometidos a riesgos de diferente naturaleza que deben ser adecuadamente gestionados, en ocasiones mediante la incorporación de tecnología y servicios destinados a preservar un nivel de seguridad aceptable en los procesos de negocio soportados por dicha infraestructura.

Sin embargo, la operación de sistemas de seguridad o la prestación de servicios especializados requiere personal altamente cualificado y la realización de fuertes inversiones por parte del cliente para garantizar que en ambos casos se materializan los beneficios derivados de su adquisición.

Las organizaciones deben ser capaces de conjugar las necesidades existentes en materia de operaciones de seguridad con la disponibilidad limitada de recursos económicos y humanos.

A este respecto, la externalización de dichas operaciones presenta multitud de ventajas que, convenientemente gestionadas, proporcionan el necesario grado de excelencia en materia de seguridad bajo un modelo extremadamente eficiente en costes, dadas las sinergias y economías de escala que un proveedor especializado puede alcanzar.

¿Por qué ahora?

La popularización de los entornos de computación en la nube (cloud computing) ha propiciado la disponibilidad de un nuevo paradigma para la prestación de servicios de operaciones de seguridad, denominado SOC 2.0, que proporciona un grado de sofisticación tecnológica y una eficiencia en coste sin precedentes.

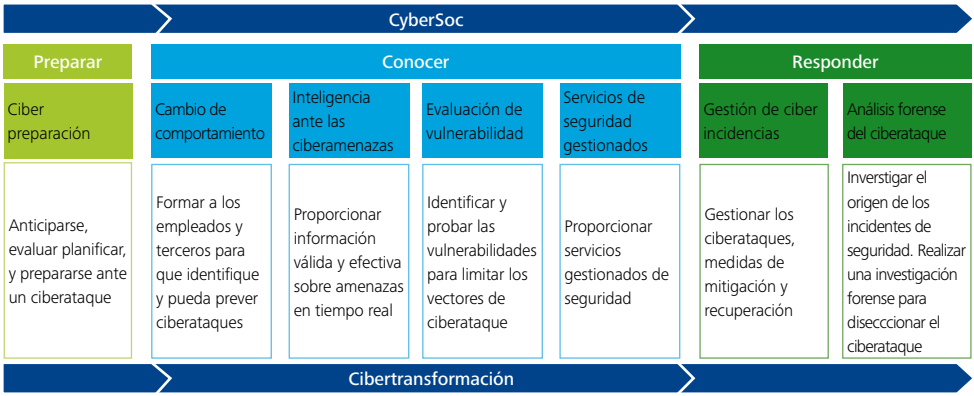
Las organizaciones pueden beneficiarse ahora de la existencia de potentes plataformas de seguridad que cubren un amplio espectro de riesgos tecnológicos comunes en Sistemas de Información corporativos, conjugando la experiencia de un equipo profesional altamente cualificado con la disponibilidad de tecnología eficaz, orientada a resultados y accesible desde un entorno seguro, sin necesidad de realizar una inversión previa.

¿Qué puede hacer al respecto?

Las organizaciones deben determinar cuáles de sus necesidades de seguridad deberían alcanzar umbrales de excelencia superiores a los actuales, o bien identificar aquellos cuya externalización puede derivar en un modelo más eficiente en coste.

- Incorporación de la seguridad en el Ciclo de Vida del Desarrollo de Software.
- Detección y gestión proactiva de vulnerabilidades en los sistemas críticos de la organización.
- Identificación de amenazas relevantes que puedan impactar en los procesos de negocio de la organización.
- Operación eficaz, en modalidad 24x7, de los sistemas de seguridad desplegados.
- Monitorización permanente de alertas de seguridad, y correlación de las mismas para la identificación de escenarios reales de intrusión.

¿Cómo puede ayudar Deloitte?



El CyberSOC ha sido diseñado conforme a los principios de funcionamiento del denominado SOC 2.0, con objeto de proporcionar a las organizaciones una respuesta global, integral y eficaz a sus necesidades de operación de seguridad. La estructura del portfolio de servicios vinculado al CyberSOC establece una correspondencia directa entre dichas necesidades y las capacidades de la plataforma:

- Revisión automatizada de código fuente
- Alerta temprana
- Protección de marca
- Hacking ético gestionado
- Gestión de vulnerabilidades
- Análisis de malware
- Inteligencia en la Red
- Protección frente a phishing
- Protección frente a DDoS
- Tráfico Limpio
- Navegación segura

¿Por qué Deloitte?

El conocimiento en materia de gestión del riesgo tecnológico corporativo, así como la experiencia acumulada por los profesionales de la Firma en grandes organizaciones, resultan claves para materializar los beneficios de un SOC 2.0.

Por otro lado, la plataforma de seguridad que Deloitte emplea en su CyberSOC está constituida por las tecnologías más sofisticadas, cuyo valor ha sido constatado por empresas e instituciones con fuertes requerimientos de seguridad en todo el mundo.

Nuestra experiencia

La experiencia acumulada por Deloitte en la gestión del riesgo tecnológico para las organizaciones más exitosas de los principales sectores de actividad posiciona a la Firma como un excelente aliado en lo que respecta a la prestación de los servicios de un SOC 2.0, bajo un modelo de prestación atractivo, eficiente y orientado al negocio.

Las capacidades de Deloitte

Ayudamos a las organizaciones a **prepararse**, **conocer** y **responder** a las amenazas informáticas.

El potencial de Deloitte de contar con toda una serie de profesionales experimentados, la percepción de nuestra red global y las relaciones estratégicas con proveedores líderes del mercado, nos permite ofrecer una capacidad completa a las organizaciones en materia de ciberseguridad.

Si desea más información, consulte nuestros recursos online:
www.deloitte.com/cyber

Para contactar con nosotros:

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.