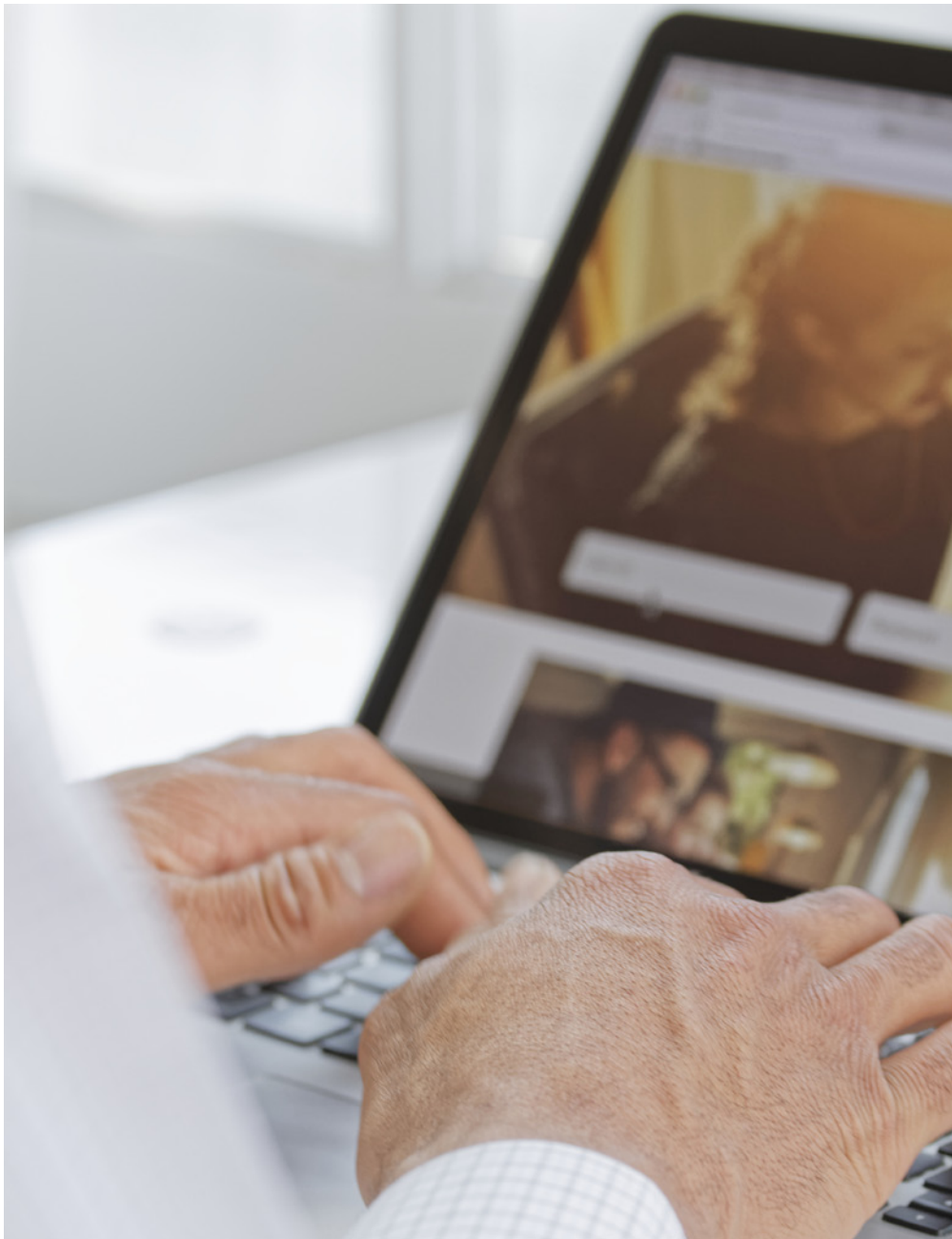
Ciberseguridad colaborativa:
Nuestros servicios



pwc

Ciberseguridad colaborativa

Diagnósticos y Roadmaps

La correcta comprensión del estado actual de la situación de ciberseguridad de la organización en las dimensiones humana, normativa, organizacional y tecnológica; permiten identificar las iniciativas requeridas para elevar el nivel de madurez de la ciberseguridad.

Diagnósticos

Permiten a los responsables de la organización tomar conciencia de las deficiencias así como de los riesgos y vulnerabilidades a los que se encuentra expuesta y el impacto que puede llegar a tener un incidente. Además, permite priorizar las iniciativas necesarias para elevar el nivel de ciberseguridad.
Una de nuestras principales herramientas de diagnóstico es el Cyber&Information Security Fast Assessment (CISFAST), el cual tiene por propósito identificar el nivel de riesgo inherente de su organización, el nivel de madurez de ciberseguridad actual y las medidas más urgentes que debería adoptar para elevar su seguridad a un nivel aceptable.

Roadmaps

Corresponde a la identificación, priorización y valorización del conjunto de iniciativas necesarias para reducir los riesgos y vulnerabilidades detectados en la fase de diagnóstico.

Cultura organizacional y concienciación

Las personas no tienen porque ser el eslabón más débil, al contrario, deben ser su mejor línea de defensa. Por medio de una fuerte cultura organizacional de ciberseguridad, esta formará parte de los hábitos y rutina diaria de la organización.

Educación y capacitación

Programas de formación continua en ciberseguridad destinados a fortalecer las competencias de los miembros de la organización, así como para mantenerlos actualizados en las materias de sus respectivas áreas de desempeño. Se incluyen charlas, cursos de capacitación, conferencias, programas en línea, etc.

Entrenamiento y Ejercicio

Planes anuales de pruebas de distinta complejidad para fortalecer la efectividad de los procedimientos de ciberseguridad de la organización. Se ponen a prueba los sistemas de seguridad establecidos, la disciplina de seguridad de las personas y la capacidad de reacción de la empresa. Sus resultados constituyen una valiosa retroalimentación para la mejora continua y la evaluación sistemática de los programas de evaluación.

Evaluación de planes, controles y sistemas

Se revisan en los planes, controles o sistemas el grado de cumplimiento que tienen respecto de las exigencias establecidas en regulaciones, mejores prácticas, estándares, configuraciones recomendadas o normas internas; de manera de asegurar una correcta interpretación y aplicación de estas últimas.

Liderazgo y gobernanza: Estrategia, políticas y planes

Liderazgo evidente y responsabilidades definidas son claves para una ciberseguridad bien conducida, lo cual se refleja en una estructura normativa sólida y una seguridad ágil y efectiva.

Desarrollo de estrategia, políticas, normas y procedimientos

Desarrollo o actualización de la estructura normativa de la organización, para alinearla a objetivos o estándares empresariales, así como a regulaciones legales. Además, se proponen mejoras al gobierno corporativo.

Servicios gestionados de ciberseguridad

La seguridad efectiva requiere personas en permanente perfeccionamiento, es una actividad de 24 hrs. y necesita especialistas difíciles de obtener. Además, estos últimos al estar insertos en las dinámicas propias de la organización, pueden perder objetividad, rigurosidad o distraerse en tareas ajenas. Estos y otros inconvenientes pueden resolverse con servicios expertos externos.

Asesoría especializada a directorios y comités

Acompañamiento experto en directorios o comités donde se traten temas de ciberseguridad. Figura similar a un director externo independiente, disponible permanentemente para asesorar a los miembros de Directorios y Comités.

CISO externo

Grupo de expertos que cumplen la función de un CISO para empresas que no disponen de este rol, de manera de evaluar, proponer y monitorear la implementación y eficacia de sus medidas de ciberseguridad. También pueden apoyar la función de un CISO corporativo o evaluar independientemente las iniciativas de ciberseguridad de la empresa

Gestión del conocimiento

Con el propósito de aquilatar y aprovechar el conocimiento adquirido en la organización en relación a la ciberseguridad, se proponen los procedimientos y plataformas necesarias para su gestión.

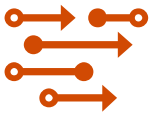
Servicios avanzados

Las organizaciones que han elevado su ciberseguridad a un estado superior de eficacia, consideran actividades que van más allá de la prevención, adoptando iniciativas proactivas que le permiten aventajar a los atacantes.

Ciberinteligencia

Nuestros servicios de inteligencia ayudan a generar una ciberseguridad ágil y consciente de los riesgos relevantes para sus operaciones.
Reportes oportunos respecto de amenazas reales, en base al análisis de la situación estratégica de sectores, regiones o industrias específicas, con el respaldo de una sólida base de conocimientos técnicos y visión de primera línea de carácter global.

Detección patrones anómalos (Inteligencia artificial)



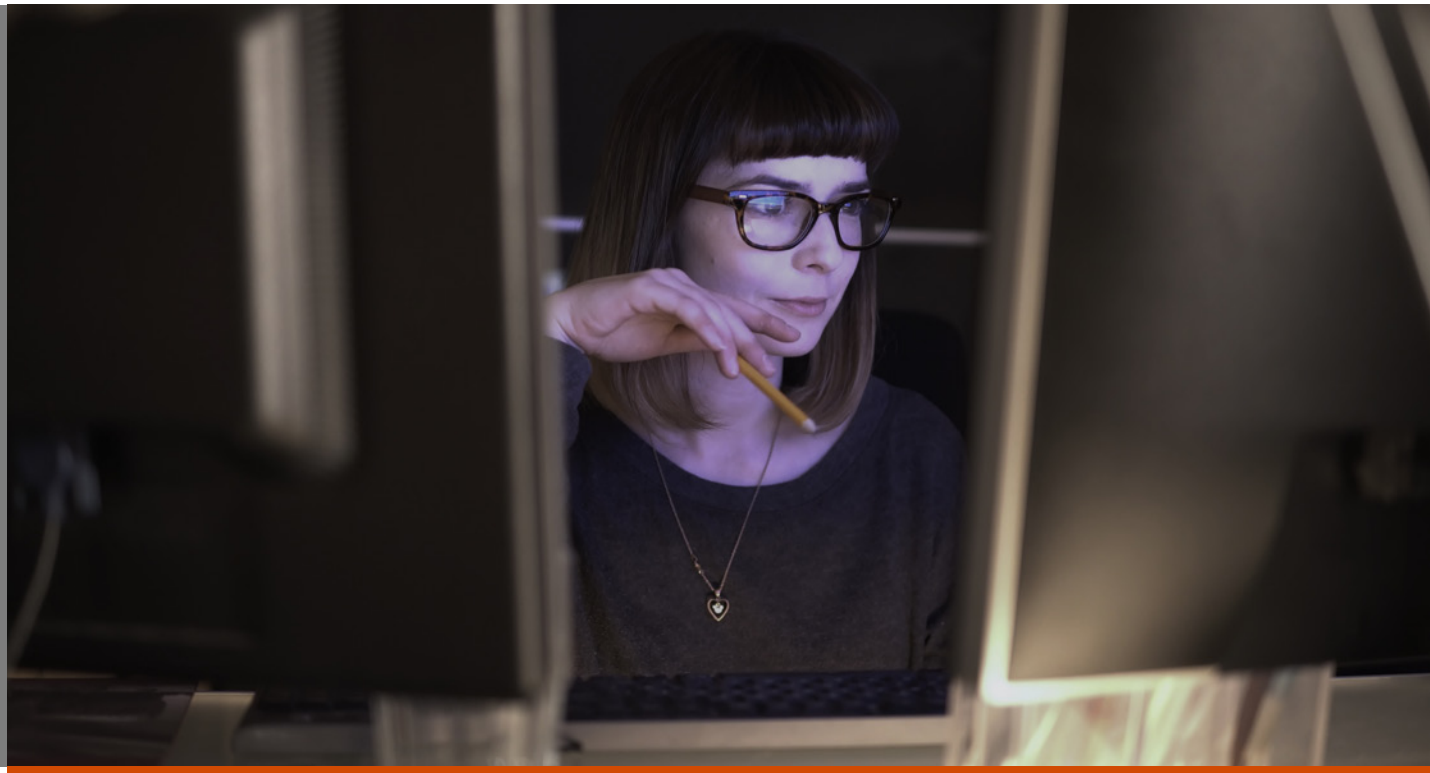
Los ataques más graves están precedidos de la penetración de las redes y sistemas, con el propósito de obtener la información necesaria para explotarlas. Esta actividad es persistente, sigilosa, profunda y, la mayor de las veces, muy difícil de detectar por analistas humanos o sistemas tradicionales. Contamos con la inteligencia artificial para identificar en el tráfico de las redes corporativas, los patrones anómalos que dan indicios de esta actividad, lo que permite adelantarse y neutralizar este tipo de ataques.

Informática forense

En cualquier tipo de caso en los que se necesite recolección de evidencia digital; se requiere la aplicación de procedimientos forenses que no afecten su aceptabilidad como prueba. Sin embargo, estos procedimientos también pueden emplearse preventivamente ante situaciones indeseables dentro de la empresa como fraudes, mal uso de equipos o conductas prohibidas.

Defensa activa

Los atacantes pueden ser engañados y de este modo se pueden mejorar los procesos de detección, ganar tiempo para la defensa, aprender de sus técnicas e, incluso, contribuir a su identificación.



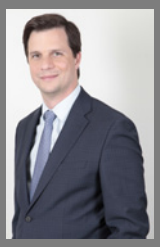
Otros servicios

Las tecnologías de ciberseguridad evolucionan y mantenerse al día en ellas es fundamental para la ciberseguridad corporativa.

Soluciones tecnológicas de ciberseguridad

Junto a empresas líderes en la industria de tecnologías de ciberseguridad así como avalados por la experiencia de PwC global; estamos en condiciones de acompañar a las organizaciones en sus procesos de implementación o modernización de tecnologías de ciberseguridad.

Contactos:



Federico Morello
Socio Líder de Consultoría y Asesoría Empresarial
PwC Chile
federico.morello@cl.pwc.com
(56) 2 2940 0181
www.pwc.cl

Héctor Gómez
Cybersecurity Senior Manager
PwC Chile
hector.gomez@cl.pwc.com
(56) 2 2940 0181
www.pwc.cl