Ciberseguridad para empleados de todos los niveles

Kaspersky Security Awareness

kaspersky bring on the future

Más información en kaspersky.es/awareness

Kaspersky Security Awareness

Crea una cultura de ciberseguridad en toda tu organización

Más del 80 % de los incidentes de ciberseguridad se deben a errores humanos. Al crear una cultura de comportamiento seguro en el ámbito de la seguridad, junto con conocimientos y concienciación fundamentales sobre ciberseguridad, en toda tu organización, puedes reducir la superficie de ataque, así como el número de incidentes a los que tienes que hacer frente. La mejor manera de lograr los cambios de comportamiento que resuelven el problema del "factor humano" en la ciberseguridad es mediante una formación que utilice las últimas técnicas y tecnologías en educación de adultos y ofrezca los contenidos más pertinentes y actualizados.

El factor humano: el elemento más vulnerable de la ciberseguridad

Las soluciones de ciberseguridad se desarrollan rápidamente y se adaptan a las complejas amenazas. Esto dificulta la vida de los ciberdelincuentes, que recurren al elemento más vulnerable de la ciberseguridad: el factor humano.

El 55 % de las empresas denuncia infracciones de las políticas de seguridad informática por parte de sus propios empleados*

El 43 % de las pequeñas empresas afirma que las infracciones de las políticas de seguridad de TI por parte de los empleados provocan incidentes de seguridad **

Las fugas de datos son el problema de seguridad más común, **provocadas mayormente por empleados** (22 %) y atacantes (23 %)*.

El 30 % de los empleados admite que comparte los datos de inicio de sesión y contraseña de la PC de su trabajo con los compañeros ***

El 23 % de las organizaciones no cuenta con ninguna política ni regla de ciberseguridad para el almacenamiento de datos empresariales***

Kaspersky Security Awareness: un nuevo enfoque para dominar las habilidades de seguridad de TI

Kaspersky Security Awareness es una solución de eficiencia y eficacia comprobadas, con una larga trayectoria internacional de éxitos. Utilizada por empresas de todos los tamaños para formar a más de un millón de empleados en más de 75 países, la solución abarca más de 25 años de conocimientos en ciberseguridad de Kaspersky con una amplia experiencia en formación de adultos.

Las soluciones de capacitación interesantes y eficaces aumentan la concienciación de ciberseguridad de tu personal para que todos desempeñen su labor en la ciberseguridad general de tu organización. Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo con múltiples componentes.

Ciclo de aprendizaje continuo

Participación/ motivación
- ¿Por qué necesito esto?
- Proceso de conocimiento

Punto de partida
- ¿Soy consciente?
- ¿Qué es lo que sé y dónde están las deficiencias?

Aprendizaje
- Microaprendizaje
- Aprendizaje continuo
- Adaptabilidad

Consolidación
- ¿Lo hice bien?
- ¿Recuerdo esto?
- ¿Actúo en consecuencia?

Factores diferenciadores clave

Gran experiencia en ciberseguridad

Más de 25 años de experiencia en ciberseguridad transformados en un conjunto de habilidades de ciberseguridad que se encuentran en el núcleo de nuestros productos

Capacitación que cambia el comportamiento de los empleados en todos los niveles de su organización

Nuestra capacitación lúdica proporciona compromiso y motivación a través del entretenimiento educativo, mientras que las plataformas de aprendizaje ayudan a internalizar el conjunto de habilidades de ciberseguridad para garantizar que las habilidades aprendidas no se pierdan en el camino.

* IT Security Economics 2022 de Kaspersky

** Informe "IT Security Economics 2021", Kaspersky.

*** "Sorting out a Digital Clutter". Kaspersky, 2019.

Motivación para una concienciación eficaz en materia de seguridad

Los empleados cometen errores. Pero las organizaciones pierden dinero...

52.887 $
por organización empresarial
El costo promedio de un ciberataque provocado por un uso inadecuado de los recursos de TI por parte de los empleados*

30 %
de las filtraciones de malware
se produce a través de correos electrónicos con vínculos y archivos adjuntos falsos**

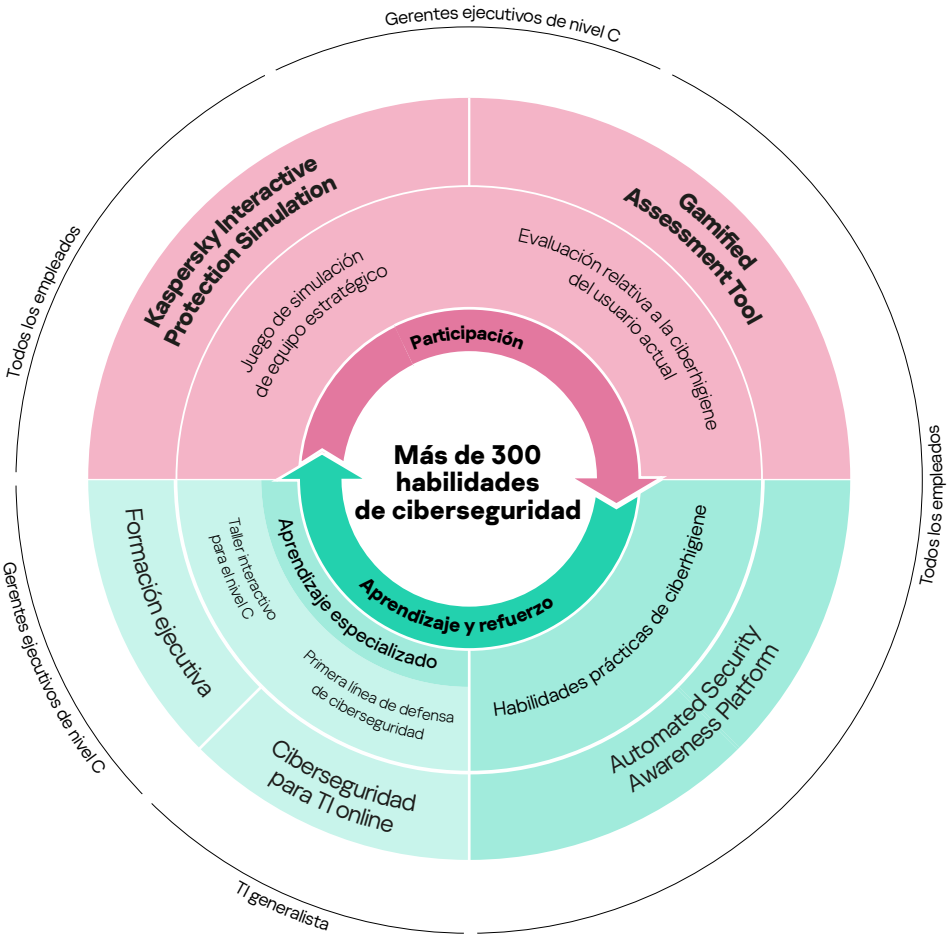
79 %
de empleados
admite haber participado en al menos una actividad de riesgo durante el año anterior a pesar de ser conscientes de los riesgos***

164 $
por registro
El costo promedio global de las filtraciones que afectan a entre 2200 y 102 000 registros****

El 42 % de los encuestados
que trabaja en empresas con más de 1000 empleados
dice que la mayoría de los programas de capacitación a los que asiste son inútiles y poco interesantes*****

Cambiar el comportamiento de los empleados es su mayor desafío en materia de ciberseguridad. En general, las personas no están motivadas para adquirir habilidades y cambiar sus hábitos, por lo que muchos esfuerzos educativos se convierten en poco más que una formalidad vacía. Una capacitación eficaz consta de diferentes componentes, tiene en cuenta las especificidades de la naturaleza humana y la capacidad de asimilar los conocimientos adquiridos. Como expertos en ciberseguridad, Kaspersky sabe cómo es el comportamiento del usuario seguro en el ámbito de la ciberseguridad. Gracias a nuestros conocimientos y experiencia, hemos agregado técnicas y métodos de aprendizaje para inmunizar a los empleados de nuestros clientes contra los ataques, dándoles al mismo tiempo la libertad de actuar sin limitaciones.

Diferentes formatos de formación para diferentes niveles organizativos



* IT Security Economics 2022 de Kaspersky

** Data Breach Investigation Report (Informe de investigación de filtraciones de datos), 2022.

*** "Balancing Risk, Productivity, and Security". Delinea, 2021

**** Cost of a Data Breach Report, 2022. IBM

*****Capgemini "The digital talent gap"

Soluciones de Kaspersky Security Awareness

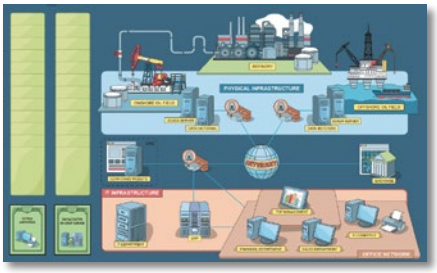
Participación/motivación

Los empleados no siempre están dispuestos a recibir formación obligatoria, y cuando se trata de ciberseguridad, muchos la consideran demasiado complicada o aburrida, o creen que no tiene nada que ver con ellos. Sin la motivación para aprender, es poco probable que el resultado del aprendizaje sea muy positivo. Otro desafío para los encargados de la educación es involucrar a los ejecutivos de las empresas en la capacitación, a pesar de que sus errores pueden costar a la empresa tanto como los de los demás. Aquí es donde entran en juego las técnicas del aprendizaje: al ser tan interesantes, es la forma más eficaz de animar a su personal a superar la resistencia inicial a la capacitación.

El 76 % de los directores ejecutivos admiten haberse saltado los protocolos de seguridad para completar una tarea más rápido, primando la velocidad sobre la seguridad*.

El 62 % de los gerentes admiten que la falta de comunicación en materia de seguridad de TI dentro de su organización provocó al menos un incidente de ciberseguridad**

La capacitación de KIPS está dirigida a altos directivos, expertos en sistemas empresariales y profesionales de TI, con el fin de aumentar su concienciación sobre los riesgos y desafíos asociados al uso de todo tipo de sistemas y procesos de TI.



Juego estratégico de Simulación de protección interactiva de Kaspersky (KIPS): la ciberseguridad desde una perspectiva empresarial

KIPS es un juego en equipo interactivo de dos horas de duración que establece un entendimiento entre los encargados de la toma de decisiones (directores y responsables de TI y ciberseguridad), y cambia sus percepciones de ciberseguridad. Presenta una simulación de software del impacto real que el malware y otros ataques tienen sobre el rendimiento y los ingresos de la empresa. Obliga a los jugadores a pensar estratégicamente, a anticipar las consecuencias de un ataque y a responder en consecuencia con las limitaciones de tiempo y dinero. Cada decisión afecta a todos los procesos empresariales. El objetivo principal es que todo funcione bien. Gana el equipo que termine la partida con más ingresos, después de haber encontrado y analizado todas las trampas del sistema de ciberseguridad y haber respondido adecuadamente.

Trece situaciones relacionadas con la industria (y se agregan más constantemente)

Cada situación demuestra el rol de la ciberseguridad en términos de continuidad y rentabilidad del negocio, lo que pone de manifiesto los desafíos y las amenazas emergentes y los errores típicos que las organizaciones cometen al construir su ciberseguridad. También promueve la cooperación entre los equipos comerciales y de seguridad, lo que ayuda a mantener la estabilidad de las operaciones y la sostenibilidad frente a las ciberamenazas.

KIPS está disponible en dos versiones

La opción KIPS Live más popular crea una atmósfera indescriptible de emoción y entusiasmo gracias a la competitividad cara a cara in situ. Es una gran herramienta para involucrar y crear una cultura de ciberseguridad dentro de una organización.

En la versión KIPS Online, los usuarios pueden interactuar con un gran número de participantes desde cualquier lugar. Ideal para organizaciones globales o actividades públicas, KIPS Online se puede combinar con KIPS Live para añadir equipos remotos al evento en las instalaciones.

- Permite la participación de hasta 300 equipos (1000 participantes) de manera simultánea, desde cualquier ubicación.
- Los distintos equipos pueden escoger interfaces de juego en diferentes idiomas.
- Los clientes pueden personalizar las situaciones preinstaladas si determinan el número y los tipos de ataques del juego de la biblioteca.
- Otra ventaja de la versión online es que permite obtener estadísticas sobre las decisiones de los jugadores, datos sobre las acciones de los equipos en determinadas situaciones y una evaluación comparativa de las acciones de los jugadores en relación con el juego anterior.

KIPS para empresas

Los clientes que tengan una licencia para jugar a KIPS cuando quieran durante el período de vigencia de la licencia pueden jugar con la configuración predefinida o personalizar la situación del juego cada vez que jueguen y escoger y combinar los diferentes ataques de la biblioteca. Esta funcionalidad cambia el juego en todo momento, lo que lo hace aún más interesante.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

Punto de partida

Las personas no suelen ser conscientes de su nivel de incompetencia, lo que las hace especialmente vulnerables. Es necesario que se les ponga a prueba y que reciban información detallada y clara sobre su nivel de competencia en ciberseguridad para que la capacitación posterior sea eficaz. Esto también garantiza que no se pierda tiempo en material que ya es conocido.

Gamified Assessment Tool: una forma rápida y emocionante de evaluar las habilidades de ciberseguridad de los empleados

Kaspersky Gamified Assessment Tool (GAT) le permite estimar rápidamente los niveles de conocimiento de ciberseguridad de sus empleados. Este interesante enfoque interactivo elimina el aburrimiento que suelen tener las herramientas de evaluación clásicas. Solo lleva 15 minutos que los empleados repasen 12 situaciones cotidianas relacionadas con la ciberseguridad. Aquí se evalúa si las acciones del personaje son arriesgadas o no y se expresa el nivel de confianza en la respuesta.

Una vez completado, los usuarios reciben un certificado con una puntuación que refleja su nivel de concienciación en materia de ciberseguridad. También reciben información sobre cada zona, con explicaciones y consejos útiles.

El enfoque lúdico de GAT motiva a los empleados y, al mismo tiempo, les demuestra que, al resolver determinadas situaciones de ciberseguridad, puede haber deficiencias en sus conocimientos. Esto también es útil para que los departamentos de TI y RR. HH. conozcan mejor los niveles de concienciación en materia de ciberseguridad de su organización, y puede servir como paso previo a una campaña educativa más amplia.

Aprendizaje

Nuestra plataforma de aprendizaje online es el núcleo del programa de concienciación. Contiene **más de 300 habilidades en ciberseguridad** cubriendo todos los temas principales de seguridad de TI.
Cada lección incluye casos y ejemplos de la vida real para que los empleados puedan sentir la conexión con lo que tienen que tratar en su trabajo diario. Y pueden utilizar estas habilidades inmediatamente después de la primera lección.

Kaspersky Automated Security Awareness Platform: eficiencia y facilidad de gestión de la formación para organizaciones de cualquier tamaño

Kaspersky ASAP es una herramienta online eficaz y fácil de usar que forma las habilidades de ciberseguridad de los empleados y los motiva a comportarse de manera correcta.

Aunque la formación satisface las necesidades de concienciación en materia de seguridad de todas las empresas, la gestión automatizada atraerá especialmente a quienes no tengan recursos de gestión de formación específicos.

Ventajas clave:

- **Simplicidad a través de la completa automatización:** el programa es muy fácil de iniciar, configurar y supervisar, y la gestión continua está totalmente automatizada, sin necesidad de intervención administrativa. La propia plataforma elabora un calendario educativo para cada grupo de empleados, proporcionando un aprendizaje por intervalos ofrecido automáticamente a través de una mezcla de formatos de capacitación.

- **Facilidad de uso para los administradores……:** Gestión automatizada de plataformas, sincronización con AD (Active Directory), SSO (Single Sign-On), Open API (posibilidad de interactuar con soluciones de terceros), incorporación online durante la primera visita, una sección de preguntas frecuentes y consejos hacen que la gestión de la plataforma sea cómoda y eficaz.

- **……y alumnos:** una estructura clara de las lecciones, lecciones cortas, ejemplos de la vida real, una interfaz fácil de usar, recordatorios por correo electrónico, la posibilidad de volver y repetir las lecciones si es necesario, una interfaz adaptada al PC o al móvil: todo ello hace que el proceso de aprendizaje sea ameno, interesante y eficaz.

Kaspersky ASAP: una herramienta online fácil de gestionar que desarrolla las habilidades de ciberseguridad de los empleados nivel por nivel:

Temas que se cubren en ASAP:

- Contraseñas y cuentas
- Correo electrónico
- Sitios web e Internet
- Redes sociales y servicios de mensajería
- Seguridad para PC
- Dispositivos móviles
- Protección de datos confidenciales
- RGPD
- Industrial Cybersecurity
- Datos personales
- Seguridad de las tarjetas bancarias y PCI DSS
- Doxing
- Seguridad de las criptomonedas
- Seguridad de la información en el trabajo a distancia
- Ley federal rusa 152-FZ

Curso exprés ASAP

Una versión abreviada de la capacitación, en formato de audio y video.

- Teoría interactiva
- Vídeos
- Exámenes

Kaspersky ASAP es una solución multilingüe.

ASAP es ideal para MSP y xSP – Los servicios de formación para múltiples empresas se pueden administrar a través de una sola cuenta y hay disponibles suscripciones de licencias mensuales.

Prueba una versión completamente funcional de Kaspersky ASAP en k-asap.com/es – ¡comprueba personalmente lo fácil que es configurar y administrar tu propio programa de formación en consciencia sobre seguridad corporate!

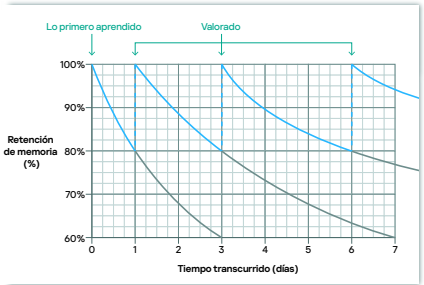
Consolidación

El refuerzo es una parte esencial del programa de aprendizaje, y es necesario para consolidar los conocimientos y las habilidades adquiridas durante el aprendizaje.

La mejor manera de convertir las habilidades aprendidas en hábitos es ponerlas en práctica. Al mismo tiempo, las personas a veces se equivocan y aprenden de la experiencia personal. Pero cuando se trata de ciberseguridad, aprender de los propios errores puede ser muy costoso.

Gracias a la capacitación lúdica, puede "vivir" una situación y experimentar sus consecuencias sin causarse ningún daño a sí mismo o a su empresa.

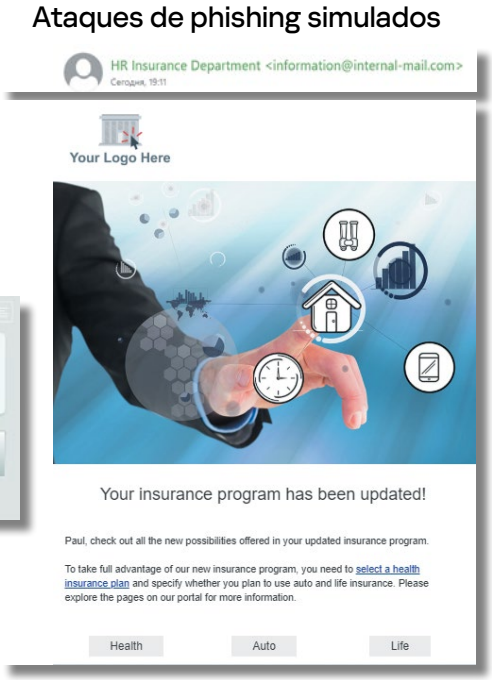
En la capacitación tradicional, el 70 % de lo que se aprende se olvida en el día.



- **Eficiencia de aprendizaje predefinida:** el contenido del programa está estructurado para facilitar el aprendizaje periódico y progresivo con un refuerzo constante. La metodología se basa en las particularidades de la memoria humana para garantizar la retención de los conocimientos y su posterior aplicación práctica.
- **Personalización:** es fácil cambiar la apariencia del programa de capacitación: sustituye el logotipo de Kaspersky por el logotipo de tu empresa en el portal del administrador y del alumno y en los correos electrónicos de la plataforma, personaliza los certificados y agrega contenido personal a cualquier lección.
- **Aprendizaje flexible:** elige la opción de formación de empleados que más te convenga, ya sea para asignar a los empleados un curso rápido básico que te ayudará a cumplir rápidamente los requisitos reglamentarios sobre formación en ciberseguridad o actualizar sus conocimientos, o para elegir un curso principal desglosado en niveles de complejidad para obtener información más detallada y desarrollar en profundidad las habilidades en ciberseguridad.
- **Licencias flexibles** (para los proveedores de servicios administrados): el modelo de licencias por usuario puede empezar con tan solo cinco licencias.

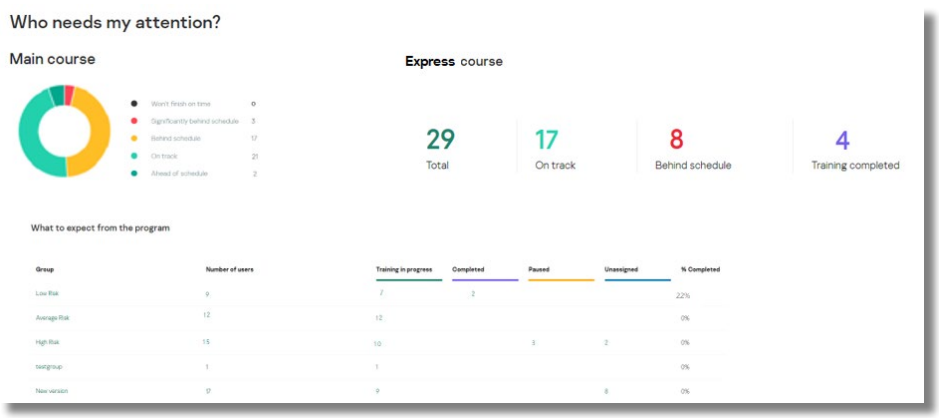
Campañas de phishing simuladas

Los ataques de phishing simulados se pueden usar antes, durante y después de la formación con el objetivo de probar la capacidad de los empleados para resistir los ciberataques y ayudarles, tanto a ellos como a la administración de la empresa, a ver los beneficios de la formación.



Resultados del seguimiento

Puedes seguir la progresión de los empleados desde el panel y evaluar el progreso de toda la empresa, y de todos los grupos, de un solo vistazo. También puedes profundizar para obtener más detalles a nivel individual.



Aprendizaje especializado

Especialistas generales en TI: los servicios de asistencia técnica y otro personal con conocimientos técnicos a menudo se quedan sin formación porque los programas de concienciación estándar no son suficientes para ellos, pero las empresas tampoco necesitan convertirlos en expertos en ciberseguridad: es demasiado costoso, requiere mucho tiempo y es innecesario.

Nos complace anunciar la formación que llena ese vacío, no tan profunda como la formación de expertos, pero más avanzada que la formación para empleados comunes.

Módulos de formación de CITO:

- Software malicioso
- Programas y archivos potencialmente no deseados
- Conceptos básicos de investigación
- Respuesta ante incidentes de phishing
- Seguridad del servidor
- Seguridad de Active Directory

Método de distribución de CITO:

Formato SCORM o en la nube

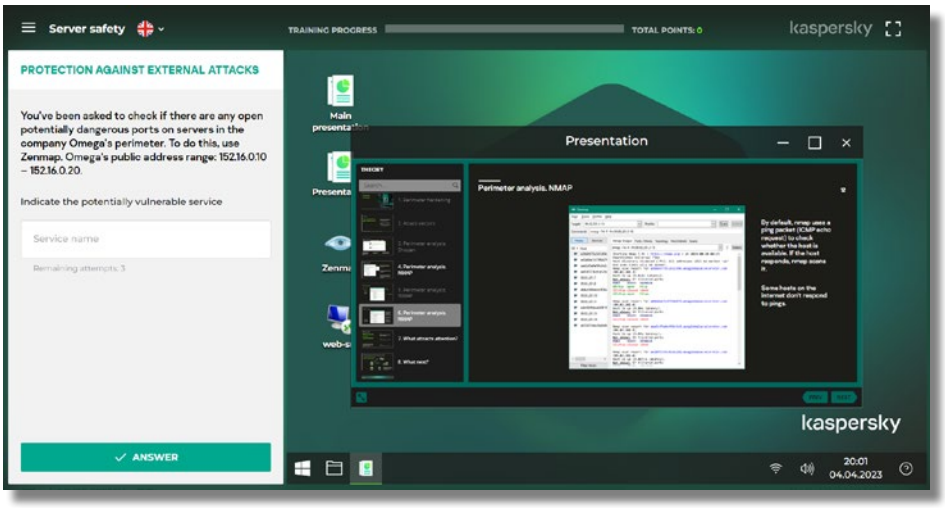
Ciberseguridad para TI online: la primera línea de defensa contra incidentes

Ciberseguridad para TI online es una capacitación interactiva para todos los involucrados en TI. Desarrolla sólidas habilidades de ciberseguridad y de respuesta ante incidentes de primer nivel.

El programa equipa a los profesionales de TI con habilidades prácticas para reconocer un posible escenario de ataque en un incidente de PC aparentemente benigno. Además, fomenta la búsqueda de síntomas maliciosos, y consolidar así el papel de todos los miembros del equipo de TI como primera línea de defensa y seguridad.

CITO también enseña nociones básicas de investigación y enseña a utilizar herramientas y software de seguridad de IT, además de capacitar a los profesionales de IT con habilidades teóricas, prácticas y basadas en ejercicios que les permiten recopilar datos sobre incidentes para el departamento de seguridad de IT.

Esta capacitación está recomendada para todos los especialistas en TI de su organización, pero principalmente para los servicios de asistencia y los administradores de sistemas. La mayoría de los miembros del equipo de seguridad de TI no expertos también se beneficiarán de este curso.



Conseguir la participación de los ejecutivos

Los altos directivos se encuentran entre los objetivos más deseables para los ciberdelincuentes, pero a menudo son un verdadero desafío para los educadores. Sin embargo, sin su participación y apoyo para diversas iniciativas y defensa de la seguridad online, es imposible crear una cultura de ciberseguridad en la organización.

La ciberseguridad es un aspecto importante de la generación de ingresos junto con la gestión de proyectos, los instrumentos financieros y la eficiencia operativa empresarial. Este es el enfoque de nuestro curso para ejecutivos.

Formación ejecutiva:

En nuestro programa de formación para directivos, los líderes empresariales y altos cargos aprenden los fundamentos de la ciberseguridad a través de un taller interactivo dirigido por un tutor o un curso en línea que les permite comprender mejor las ciberamenazas y cómo protegerse contra ellas.

Se presta especial atención a los aspectos financieros de la ciberseguridad y a la viabilidad de invertir en ella, lo que permite a los ejecutivos de alto nivel comprender mejor la conexión entre la ciberseguridad y la eficiencia empresarial. Descubrirán qué significa el panorama actual de amenazas para tu empresa, qué medidas tomar en caso de ciberataque, además de mucha más información interesante, relevante y útil.

Para sacar aún más partido a este curso, lo ideal es combinarlo con la formación KIPS. La formación para directivos puede realizarse antes o después de KIPS, en función de tu enfoque de la concienciación en materia de seguridad.

* La lista actual de módulos está disponible en cito-training.com

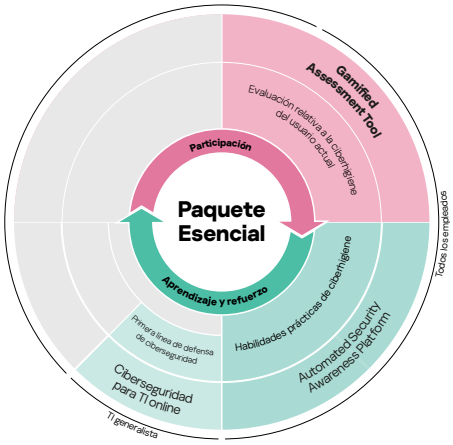
Kaspersky Security Awareness: métodos de formación flexibles

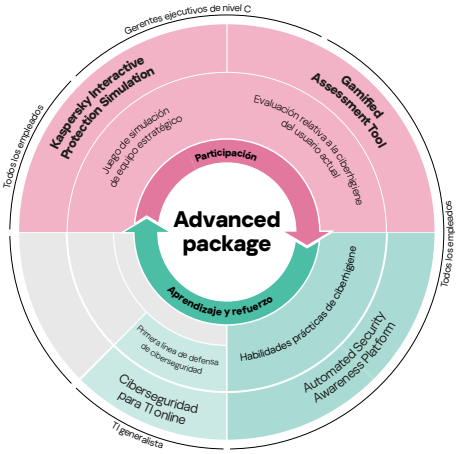
Las soluciones de formación de Kaspersky abordan todos los niveles de tu empresa y se pueden usar por su cuenta o de forma colectiva. También facilitamos la puesta en marcha con paquetes adaptados a tus necesidades.

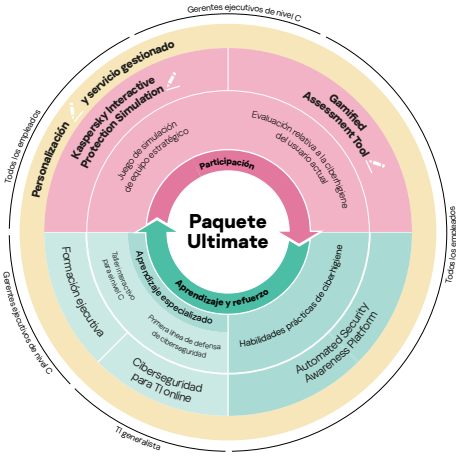
La opción sin complicaciones para concienciar a los empleados en torno a la ciberseguridad, que además es fácil de configurar y gestionar. Ofrece un nivel básico de formación en seguridad para ayudarte a operar con éxito y cumplir con los requisitos normativos o de terceros sobre formación en ciberseguridad general.

Ayuda a las organizaciones más grandes a mantener la continuidad empresarial mediante una solución de formación sencilla y de uso rápido. Apoya a cada nivel de la organización y cambia las conductas abordando todas las etapas del ciclo de aprendizaje.

Maximiza la concienciación en lo que respecta a la ciberseguridad mediante opciones de personalización y servicios gestionados para que los directivos conozcan bien los escenarios de amenaza, los empleados tengan habilidades automáticas de ciberseguridad y el personal general de IT ejerza como primera línea de defensa.







La formación de Kaspersky Security Awareness utiliza los últimos métodos de formación y técnicas avanzadas para garantizar el éxito. Las nuevas soluciones integradas flexibles se pueden adaptar a tus necesidades, por lo que hay una solución para todos. Más información en https://www.kaspersky.es/enterprise-security/security-awareness

Kaspersky Security Awareness: kaspersky.es/awareness
Noticias de seguridad de IT: business.kaspersky.com/

kaspersky.es

kaspersky