Ciberseguridad para empleados de todos los niveles

Kaspersky Security Awareness

kaspersky bring on the future

Obtenga más información en
latam.kaspersky.com/awareness

Kaspersky Security Awareness

Cree una cultura de ciberseguridad en toda su 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 su organización, puede reducir la superficie de ataque, así como el número de incidentes a los que tiene 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 amenazas complejas. 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 capacitar a más de un millón de empleados en más de 75 países, la solución reúne más de 25 años de experiencia en ciberseguridad de Kaspersky con una amplia experiencia en educación de adultos.

Las soluciones de capacitación muy interesantes y eficaces aumentan la concienciación de su personal en materia de ciberseguridad para que todos contribuyan a la ciberseguridad general de su 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

1	2	3	4
Participación/ motivación	**Punto de partida**	**Aprendizaje**	**Consolidación**
– ¿Por qué necesito esto? – Proceso de conocimiento	– ¿Soy consciente? – ¿Qué es lo que sé y dónde están las deficiencias?	– Microaprendizaje – Aprendizaje continuo – Adaptabilidad	– ¿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", Kaspersky

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

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

Motivación para una concientización eficaz en materia de seguridad

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.

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*

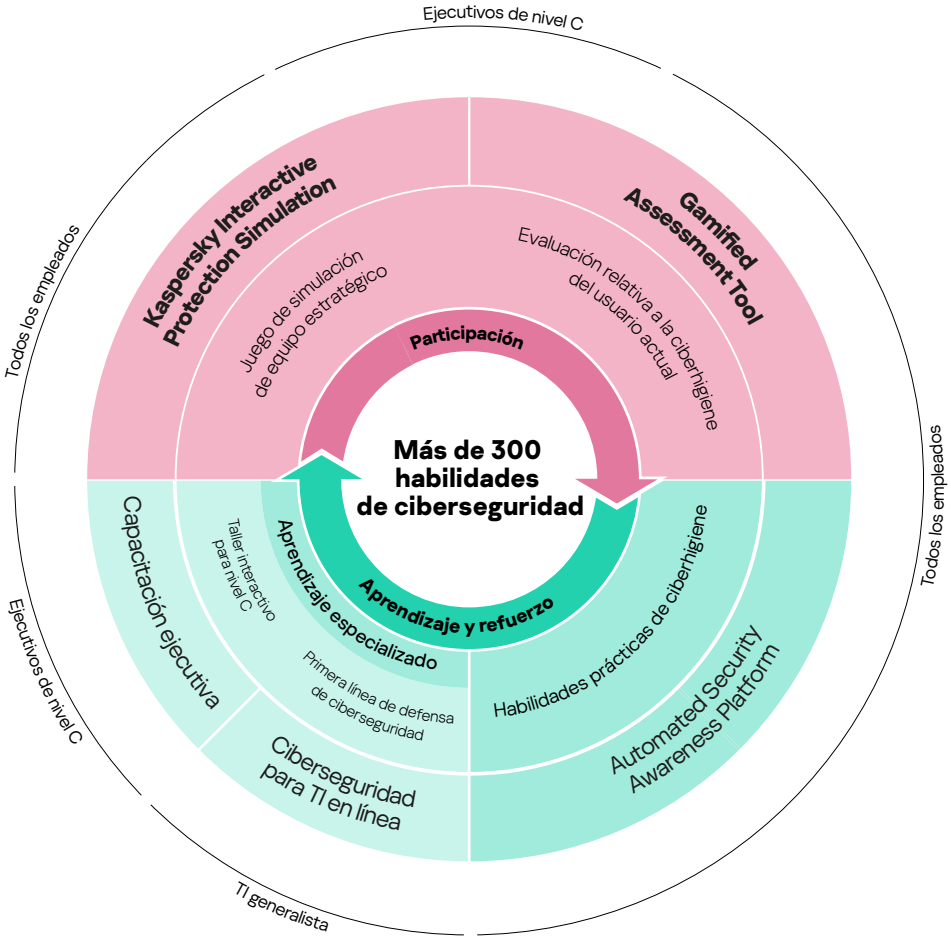
El 30 %
de las filtraciones de malware
se produce a través de correos electrónicos con vínculos y archivos adjuntos falsos**

El 79 %
de los 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*****

Diferentes formatos de formación para diferentes niveles organizativos



* "IT Security Economics 2022", Kaspersky
** Data Breach Investigation Report, 2022
*** "Balancing Risk, Productivity, and Security", Delinea 2021
**** Cost of a Data Breach, 2022. IBM
*****Capgemini "The digital talent gap"

Soluciones de Kaspersky Security Awareness

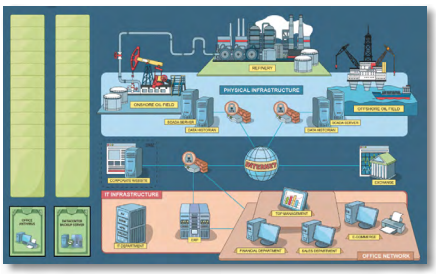
Participación y motivación

Los empleados no siempre están dispuestos a recibir una capacitación 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 admite haberse saltado protocolos de seguridad para acelerar los procesos, sacrificando la seguridad en aras de la velocidad*.

El 62 % de los gerentes admite que los malentendidos relacionados con la seguridad de TI dentro de su organización produjeron 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.



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 todo el tiempo)

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 agregar equipos remotos a eventos en los predios del cliente.

- Permite la participación de hasta 300 equipos (1000 participantes) de manera simultánea, desde cualquier ubicación.
- Los diferentes equipos pueden elegir interfaces de juego en distintos idiomas.
- Los clientes pueden personalizar escenarios preinstalados determinando en la biblioteca el número y los tipos de ataques del juego.
- Otro beneficio de la versión en línea es que permite obtener estadísticas sobre las elecciones de los jugadores, datos sobre las acciones de los equipos en ciertas situaciones y un parámetro de las acciones de los jugadores respecto del juego anterior.

KIPS para empresas

Los clientes que tengan una licencia que les permita jugar a KIPS con la frecuencia que deseen durante el período de la licencia pueden jugar con la configuración predefinida o personalizar el escenario cada vez que juegan, eligiendo y combinando diferentes ataques de la biblioteca. Esta funcionalidad permite cambiar el juego cada vez y hacerlo 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. Los empleados solo demorarán 15 minutos en repasar 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 en línea es el núcleo del programa de concienciación. Contiene **más de 300 habilidades en ciberseguridad** que cubren los principales temas de seguridad informática.
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: eficaz y sencilla administración de capacitaciones para organizaciones de cualquier tamaño

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

A pesar de que la capacitación satisface las necesidades de concienciación en materia de seguridad de todas las empresas, la administración automatizada será atractiva en particular para aquellas que no cuentan con recursos específicos de administración de capacitaciones.

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, lo que resulta en una oferta automática de aprendizaje por intervalos 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), un panel intuitivo, incorporación en línea 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 intuitiva, recordatorios por correo electrónico, la posibilidad de volver y repetir las lecciones si es necesario, una interfaz adaptada a PC o dispositivos móviles: todo ello hace que el proceso de aprendizaje sea ameno, interesante y eficaz.

Kaspersky ASAP: una herramienta en línea fácil de administrar 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 mensajería
- Seguridad para PC
- Dispositivos móviles
- Protección de datos confidenciales
- RGPD
- Ciberseguridad industrial
- 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 acelerado de ASAP

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

- Teoría interactiva
- Vídeos
- Pruebas

Kaspersky ASAP es una solución disponible en varios idiomas.

P es ideal para MSP y xSP: los servicios de capacitación para diversas empresas pueden administrarse mediante una única cuenta y existen suscripciones a licencias mensuales disponibles.

Pruebe una versión completamente funcional de Kaspersky ASAP en asap.kaspersky.es. Vea lo fácil que es configurar y administrar su programa de capacitación sobre concienciación en seguridad corporativa.

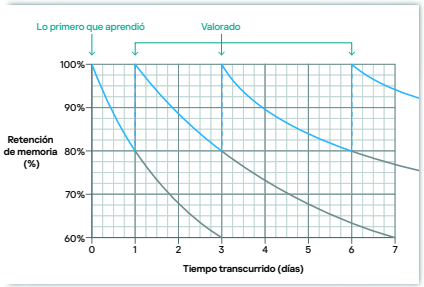
Consolidación

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

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



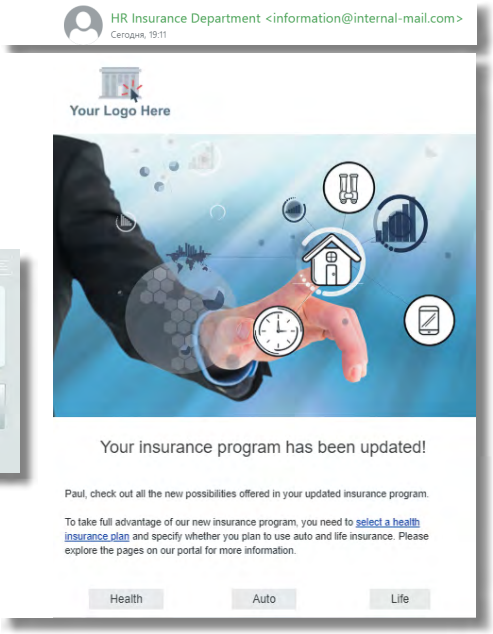
- **Eficiencia de aprendizaje predefinida:** el contenido del programa está estructurado para facilitar el aprendizaje periódico y progresivo con un refuerzo constante. La metodología se basa en las particularidades de la memoria humana para garantizar la retención de los conocimientos y su posterior aplicación práctica.
- **Personalización:** es fácil cambiar la apariencia del programa de capacitación: sustituya el logotipo de Kaspersky por el logotipo de su empresa en el portal del administrador y del alumno, así como en los correos electrónicos de la plataforma, personalice los certificados y agregue contenido personal a cualquier lección.
- **Aprendizaje flexible:** elija la opción de capacitación para empleados adecuada para usted. Puede elegir asignarles a los empleados un curso rápido básico que les permita alcanzar los requisitos de seguridad con rapidez respecto de la capacitación en ciberseguridad o actualizar su conocimiento, o asignar un curso principal con diversos niveles de dificultad para desarrollar habilidades más complejas en ciberseguridad.
- **Flexibilidad de las licencias** (para proveedores de servicios gestionados): el modelo de licencias por usuario puede empezar a partir de apenas 5 licencias, y se pueden gestionar varias empresas desde una única cuenta.

Campañas de phishing simulado

Los ataques de phishing simulados pueden utilizarse antes o después de la capacitación, o incluso durante ella, para evaluar las habilidades de resistencia a los ciberataques de los empleados y para permitirles a ellos, y a la administración de la empresa, percibir las ventajas de la capacitación.

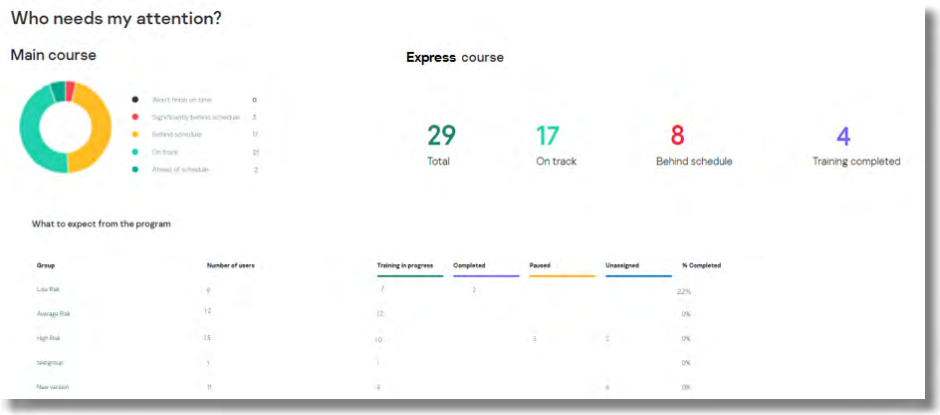
Lecciones interactivas

Ataques de phishing simulados



Resultados del seguimiento

Puede 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 puede obtener más detalles de cada persona.



Aprendizaje especializado

Especialistas generales de TI: Los empleados del servicio de asistencia y todo el personal con conocimientos técnicos suelen excluirse de las capacitaciones porque los programas estándar de concienciación no son suficientes para ellos y, además, las empresas no tienen la necesidad de convertirlos en expertos en seguridad; es demasiado costoso, insume mucho tiempo y no se justifica.

Nos complace anunciar que esta capacitación sí los satisface. No se trata de una formación en profundidad para expertos, pero sí es una formación más avanzada que para los empleados comunes.

Módulos de capacitación en CITO:

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

Método de distribución de CITO:

Formato SCORM o en la nube

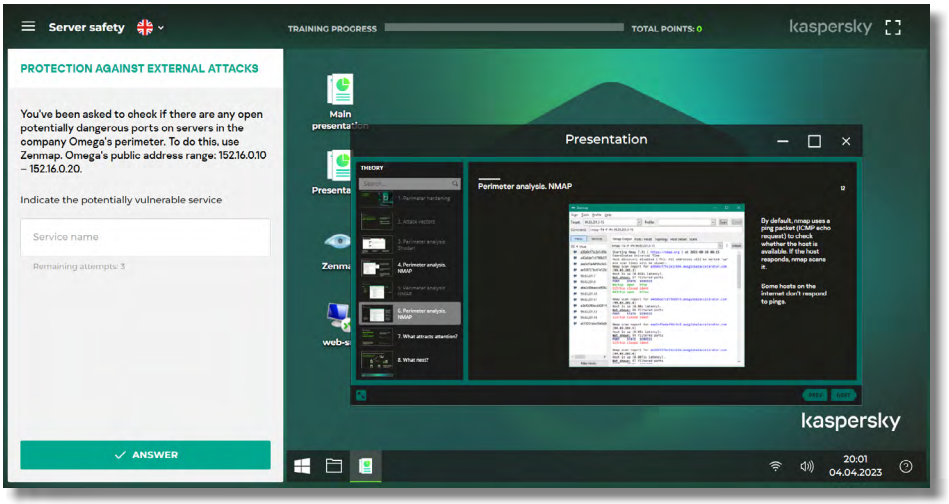
Ciberseguridad para TI en línea: la primera línea de defensa contra incidentes

Ciberseguridad para TI en línea es una capacitación interactiva para aquellas personas involucradas en TI. Desarrolla sólidas habilidades de ciberseguridad y de respuesta ante incidentes de primer nivel.

El programa dota a los profesionales informáticos con habilidades prácticas para reconocer un posible escenario de ataques en un incidente del equipo que parece 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 aspectos básicos de investigación y cómo usar herramientas y software de seguridad de TI, y brindará a sus profesionales de TI habilidades teóricas, prácticas y basadas en ejercicios para permitirles recopilar datos de incidentes que pueden entregar al equipo de seguridad de TI.

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 administradores de nivel superior son los objetivos más tentadores de los ciberdelincuentes. Sin embargo, suelen plantear un verdadero desafío para los educadores. De todos modos, sin su participación ni respaldo en diversas iniciativas y programas de defensa de ciberseguridad, es imposible crear una cultura de seguridad informática en la organización.

La ciberseguridad es un aspecto importante en la generación de ingresos, la administración de proyectos, los instrumentos de financiación y las operaciones eficaces empresariales. Este es el objetivo del curso para ejecutivos.

Capacitación ejecutiva:

En nuestro programa de capacitación para ejecutivos, los líderes empresariales y altos directivos 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 su empresa, qué medidas tomar en caso de un ciberataque, además de mucha información interesante, relevante y útil.

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

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

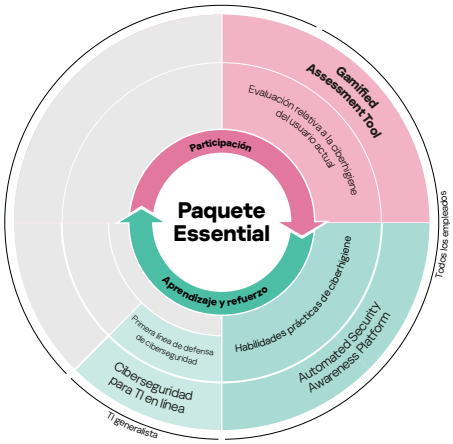
Kaspersky Security Awareness: formas flexibles de capacitar

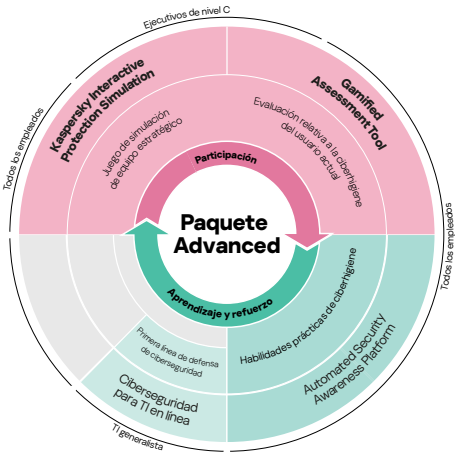
Las soluciones de capacitación de Kaspersky abordan cada nivel de su empresa y se pueden usar por su cuenta o de forma colectiva. También ayudamos a que comenzar sea más sencillo con paquetes personalizados según sus necesidades.

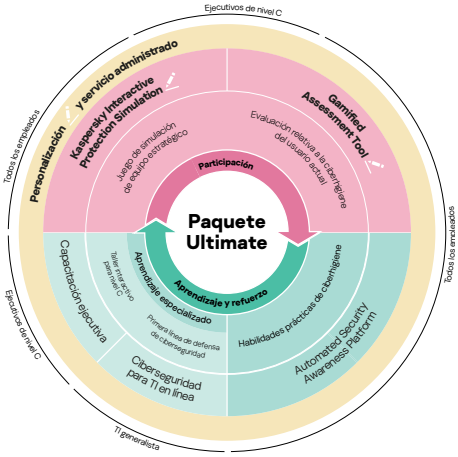
La opción sin contratiempos que aumenta la concienciación de los empleados en torno a la ciberseguridad es fácil de configurar y administrar.
Brinda un nivel básico de capacitación en seguridad para permitirle operar con éxito y satisfacer los requisitos normativos o de terceros en cuanto a la capacitación general en ciberseguridad.

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

Garantiza el máximo nivel de concienciación en ciberseguridad, con servicios administrados y personalizados, para que los ejecutivos conozcan bien los escenarios de amenaza, los empleados tengan habilidades automáticas de ciberseguridad y el personal general de TI se desempeñe como primera línea de defensa.







La capacitación de Kaspersky Security Awareness emplea los métodos de formación más recientes y técnicas avanzadas para garantizar el éxito. Los nuevos paquetes de soluciones flexibles pueden personalizarse de acuerdo con sus necesidades. De modo que sí: existe una solución para todos. Obtenga más información en latam.kaspersky.com/awareness

Kaspersky Security Awareness: latam.kaspersky.com/enterprise-security/security-awareness
Noticias de seguridad de IT: business.kaspersky.com/

latam.kaspersky.com

kaspersky