Programas de capacitación por computadora para todos los niveles organizativos

Kaspersky Security Awareness

kaspersky PREPARADOS PARA EL FUTURO

Obtenga más información en latam.kaspersky.com/awareness

Kaspersky Security Awareness

La forma más eficaz de diseñar un sistema de ciberseguridad en su organización

Más del 80 % de los incidentes de ciberseguridad se deben a errores humanos. Una cultura de comportamiento seguro en el ámbito de la ciberseguridad, junto con la concienciación y las habilidades fundamentales en toda la organización, son la clave para reducir la superficie de ataque y el número de incidentes a los que hay que hacer frente. Las organizaciones a menudo se esfuerzan por encontrar las herramientas y los métodos adecuados para una capacitación eficaz de los empleados que cambie el comportamiento para mejor. La clave para conseguirlo es implementar una capacitación que emplee las últimas técnicas y tecnologías en la educación de adultos y ofrezca los contenidos más relevantes 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 52 % de los ejecutivos afirma que los empleados representan la mayor amenaza a la seguridad operativa*

El 43 % de las pequeñas empresas sufrió un incidente de seguridad a causa de infracciones de las políticas de seguridad de TI por parte de los empleados**

El 60 % de los empleados tiene datos confidenciales en su dispositivo corporativo (datos económicos, base de datos de correo electrónico, etc.)***

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 ofrece una selección de soluciones de capacitación muy interesantes y eficaces que aumentan la conciencia de ciberseguridad de su personal para que todos desempeñen su labor en 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

Participación/ motivación	Punto de partida	Aprendizaje	Refuerzo
– ¿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 20 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.

* Informe "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure" de 2020.

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

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

Motivación para una concienciación 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...

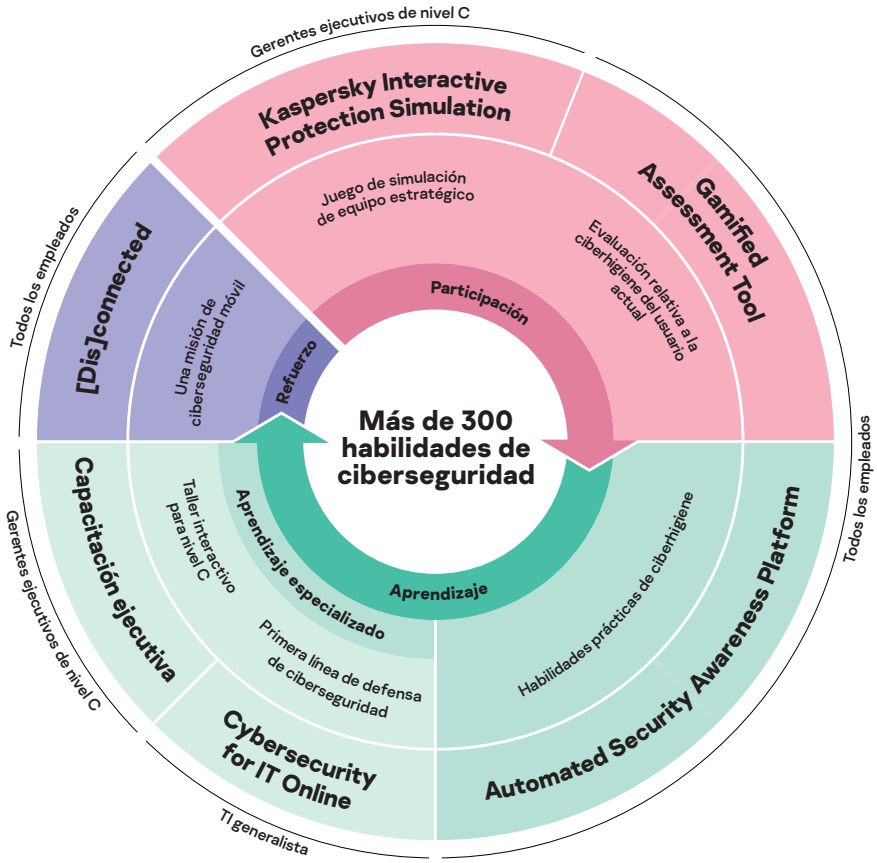
$1 315 000
por organización empresarial
El impacto económico promedio de una filtración de datos provocada por el uso inapropiado que los empleados hacen de los recursos de TI*

El 50 %
de las empresas
informa haber experimentado amenazas causadas directamente por comportamientos indebidos del personal, lo cual las convierte en las amenazas más comunes para la seguridad de la TI*

El 86 %
de las empresas
afirma que al menos una persona hizo clic en un enlace de phishing**

$5 010 000
es el costo promedio de cada filtración
debido a ataques BEC (Correo electrónico empresarial en peligro). Se trata de un tipo de phishing en el que los atacantes secuestran cuentas de correo electrónico empresariales reales o las falsifican

Diferentes formatos de formación para diferentes niveles organizativos



* Informe "IT Security Economics 2021" de Kaspersky
** Tendencias de amenazas a la ciberseguridad en 2021, CISCO
*** Informe "Cost of a Data Breach 2021" IBM

Soluciones de Kaspersky Security Awareness

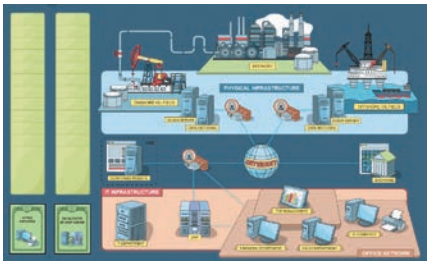
Motivación

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.

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

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**

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.

Escenarios personalizados

Desde el tercer trimestre de 2022, en el caso de ámbitos industriales seleccionados, las empresas podrán crear sus escenarios de juego con diferentes ataques. Al usar diferentes combinaciones de ataques, las organizaciones con una licencia empresarial de KIPS pueden jugar en el mismo escenario industrial en múltiples oportunidades.

Realidad virtual de KIPS

KIPS Power Station VR es una nueva experiencia inmersiva en un entorno realista tan parecido como sea posible a la operación real de una central eléctrica. La tecnología les permite a los gerentes visualmente "desempeñarse" como especialistas en seguridad de la información y demostrar el rol de la ciberseguridad y su impacto empresarial, para que puedan observar las consecuencias de sus decisiones informáticas en un gráfico en 3D muy realista, en lugar de solo contar con una idea abstracta.

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.

Aprendizaje

Nuestra plataforma de aprendizaje en línea es el núcleo del programa de concientización. 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 ASA: 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 de la computadora
- Dispositivos móviles
- Protección de datos confidenciales
- RGPD
- Industrial Cybersecurity

Curso rápido de ASAP

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

- Teoría interactiva
- Vídeos
- Pruebas

Kaspersky ASAP es una solución de múltiples lenguajes de clientes o sistemas.

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 toma 15 minutos para 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.

Kaspersky Automated Security Awareness Platform: eficaz y sencilla administración de capacitaciones para las 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 concientización en 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 plataforma crea un programa educativo para cada grupo de empleados y proporciona un aprendizaje periódico que se ofrece automáticamente a través de una gran variedad de formatos de capacitación, como módulos de aprendizaje, refuerzo por correo electrónico, pruebas y ataques de phishing simulados.
- **Eficacia:** 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.
- **Aprendizaje flexible:** elija la opción de capacitación para empleados adecuada para usted. Puede elegir entre asignar a los empleados un curso básico y rápido que le permitirá 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.
- **Licencias flexibles** (para los proveedores de servicios administrados): el modelo de licencias por usuario puede empezar con tan solo cinco licencias.

ASAP 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.com. Vea lo fácil que es configurar y administrar su programa de capacitación sobre concientización en seguridad corporativa.

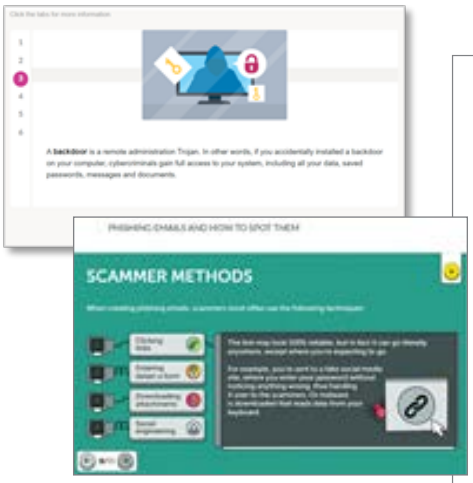
Campañas de phishing simuladas

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

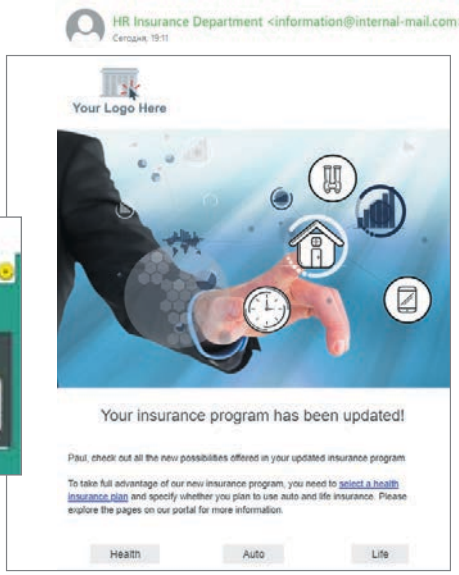
Lecciones interactivas

Curso principal

Curso rápido



Ataques de phishing simulados



Haga un seguimiento de los resultados

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.

Refuerzo

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.

[Des]conectado: una búsqueda móvil de ciberseguridad

[Des]conectado es un juego para dispositivos móviles de ciberseguridad altamente inmersivo y rico en historias, en el que los usuarios se enfrentan al reto de mantener un equilibrio saludable entre el trabajo y la vida privada, y tener éxito tanto personal como profesional.

Los elementos de la ciberseguridad se entretejen en la trama del juego, y este revela cómo nuestras decisiones en torno a la ciberseguridad pueden ayudar a conseguir, o estropear, estos objetivos. Hay 24 casos para resolver, que incluyen temas sobre contraseñas y cuentas, correo electrónico, navegación web, redes sociales y servicios de mensajería, seguridad informática y dispositivos móviles.
Las aplicaciones emuladas integradas, como los servicios de mensajería instantánea, las aplicaciones bancarias, etc., garantizan una experiencia de inmersión completa.

Al final del juego, los jugadores reciben un resumen del éxito con el que han afrontado el proyecto y descubren si sus habilidades de seguridad son suficientes para hoy y para el futuro.

El juego funciona en teléfonos móviles. Podrá encontrar una **demostración gratis** en Google Play y en App Store: https://kas.pr/mobilestores

Aprendizaje avanzado

Especialistas generales de TI: Los empleados del servicio de asistencia y todo otro personal con conocimientos técnicos suelen excluirse de las capacitaciones porque los programas estándar de concientización no son suficientes para ellos y, además, las empresas no tienen la necesidad de volverlos 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 una más avanzada que para los empleados comunes.

Módulos de capacitación en CITO:

- Software malicioso
- Archivos y programas 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

Pruebe uno de los módulos de CITO de gratis: cito-training.com

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.

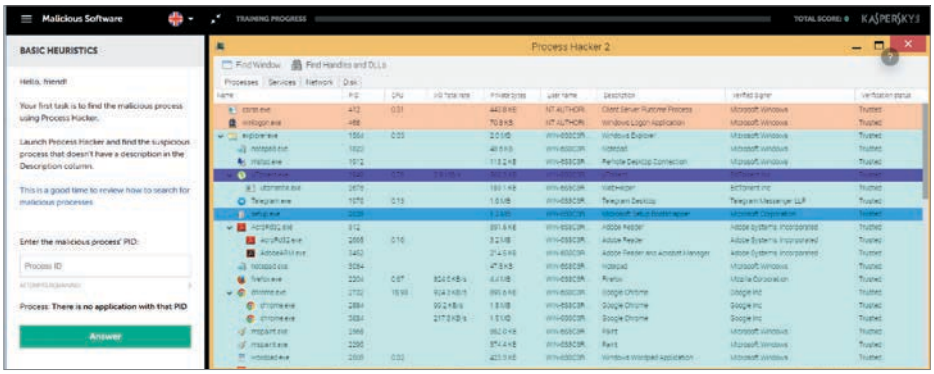
Ciberseguridad para TI en línea: la primera línea de defensa contra incidentes

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.



Capacitación ejecutiva: aumente la resiliencia del negocio para una transformación digital

Los líderes empresariales y los administradores de nivel superior aprenderán los conocimientos básicos de la ciberseguridad mediante un curso con tutores que les brinda un mejor entendimiento de las ciberamenazas y en el que aprenderán a protegerse de estas.

Las investigaciones muestran que existe una relación directa entre la velocidad y eficacia de la respuesta a un incidente y el nivel de daño que este puede causar. En el curso, se prestará especial atención a los aspectos financieros de la ciberseguridad y la viabilidad de invertir en ella, lo que les brinda a los ejecutivos un mejor entendimiento de la relación entre la ciberseguridad y un negocio eficiente.

La simulación de protección interactiva de Kaspersky (KIPS) puede usarse junto con esta capacitación para consolidar aún más el material mediante ejercicios prácticos.

Objetivos del curso

- Dar cuenta respecto de la información más reciente en ciberamenazas modernas y el riesgo que suponen para las empresas
- Actualizar a los líderes respecto del panorama de las ciberamenazas
- Brindar una oportunidad para practicar las reglas básicas de una cultura de ciberseguridad corporativa y personal
- Garantizar que se comprenda el impacto en el negocio de los principales problemas de regulación en el área de la seguridad de la información
- Aclarar los conceptos básicos de ciberseguridad y los métodos de protección frente a ataques dirigidos
- Brindar recomendaciones prácticas para redactar una política corporativa
- Aconsejar respecto de las comunicaciones al momento de responder a incidentes e investigarlos

Kaspersky Security Awareness: formas flexibles de capacitar

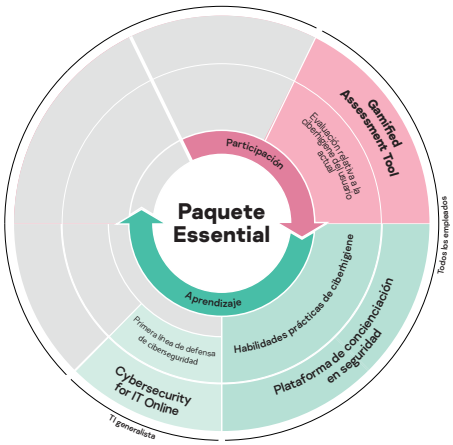
Las soluciones de capacitación de Kaspersky abordan cada nivel de su empresa y se pueden usar por su cuenta o de forma colectiva. También ayudamos a que comenzar sea más sencillo con paquetes personalizados según sus necesidades.

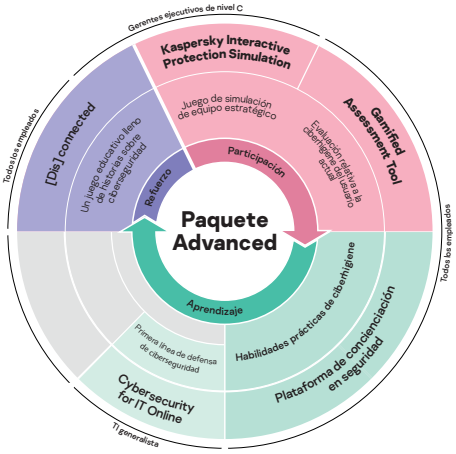
La opción sin contratiempos que aumenta la concientización de los empleados en torno a la ciberseguridad es fácil de configurar y administrar.

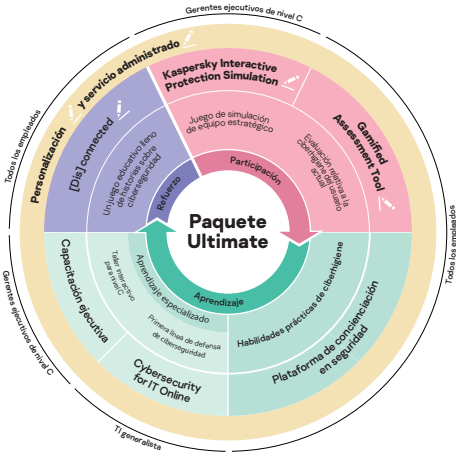
Brinda un nivel básico de capacitación en seguridad para permitirle operar de forma exitosa y satisfacer los requisitos normativos o de terceros en cuanto a la capacitación general en ciberseguridad.

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 toda etapa del ciclo de aprendizaje.

Garantiza el máximo de concientización 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 le sirva 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: kaspersky.com/awareness
Noticias de seguridad de IT: business.kaspersky.com

kaspersky.com

kaspersky PREPARADOS PARA EL FUTURO