Programas de capacitación por computadora para todos los niveles organizativos

Kaspersky Security Awareness

kaspersky PREPARADOS PARA EL FUTURO

Obtenga más información en 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 complejas amenazas. Esto dificulta la vida de los ciberdelincuentes, que recurren al elemento más vulnerable de la ciberseguridad: el factor humano.

El 52 % de los ejecutivos de nivel C dicen que los empleados son la mayor amenaza para 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", 2020

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

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

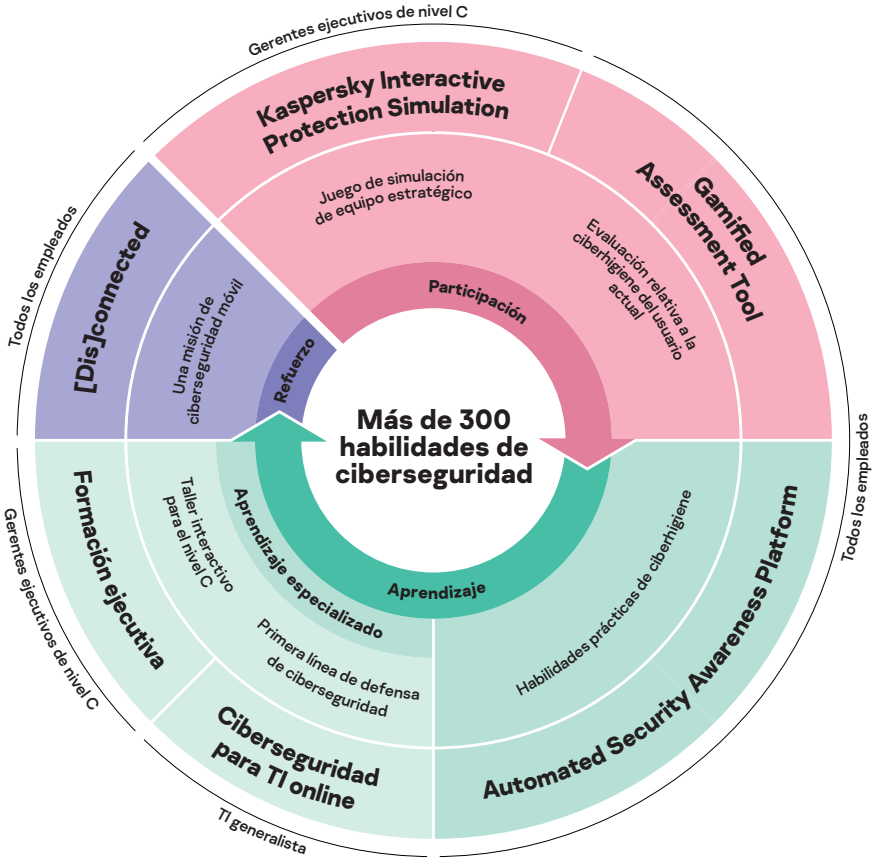
1 315 000 $
por organización empresarial
El impacto económico promedio de una filtración de datos provocada por el uso inapropiado que los empleados hacen de los recursos de TI*

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 ha hecho clic en un enlace de phishing**

5,01 millones $
el coste medio por filtración
de ataques BEC (BEC - Business Email Compromise - es un tipo de phishing en el que los atacantes secuestran o suplantan cuentas de correo electrónico corporativas legítimas)

Diferentes formatos de formación para diferentes niveles organizativos



* Informe "IT Security Economics 2021", Kaspersky
** Cybersecurity threats trends 2021, CISCO
*** "2018 Cost of a Data Breach Study, 2021". IBM

Soluciones de Kaspersky Security Awareness

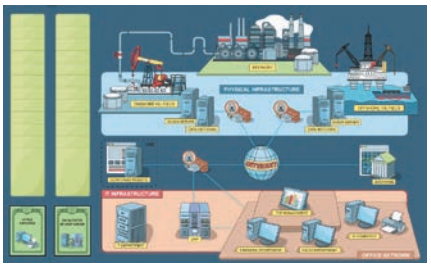
Motivación

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.

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.



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.

Diez 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.

Personalización de escenarios

A partir del tercer trimestre de 2022, en algunos escenarios industriales, las empresas podrán crear sus propios escenarios de juego con diferentes ataques. Usando diferentes combinaciones de ataques, las empresas con una licencia empresarial de KIPS pueden jugar en el mismo escenario industrial varias veces.

La realidad virtual de KIPS

KIPS Power Station VR es una nueva experiencia inmersiva en un entorno realista lo más cercano posible a las operaciones reales de una central eléctrica. La tecnología permite a los administradores "trabajar" como especialistas en seguridad de la información, demostrando visualmente el papel de la ciberseguridad y su impacto comercial para que puedan ver las consecuencias de sus decisiones de TI en gráficos 3D altamente realistas en lugar de hacerse una idea abstracta de ellas.

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 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 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

Curso rápido de ASAP

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

- Teoría interactiva
- Vídeos
- Exámenes

Kaspersky ASAP es una solución multiidioma o de 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 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.

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 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 formación de empleados que más le convenga, ya sea para asignar a los empleados un curso rápido básico que le 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.

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.

Pruebe una versión completamente funcional de Kaspersky ASAP en asap.kaspersky.com — ¡compruebe personalmente lo fácil que es configurar y administrar su propio programa de formación en consciencia sobre seguridad corporate!

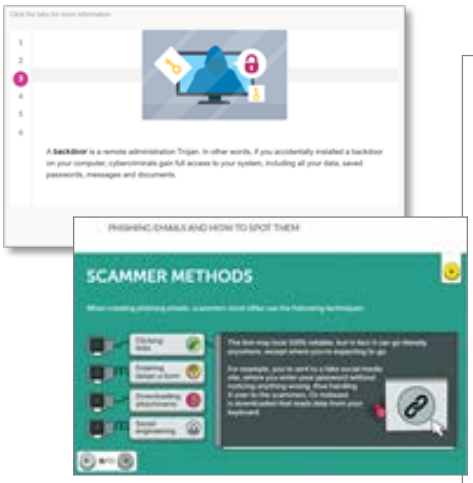
Campañas de phishing simuladas

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.

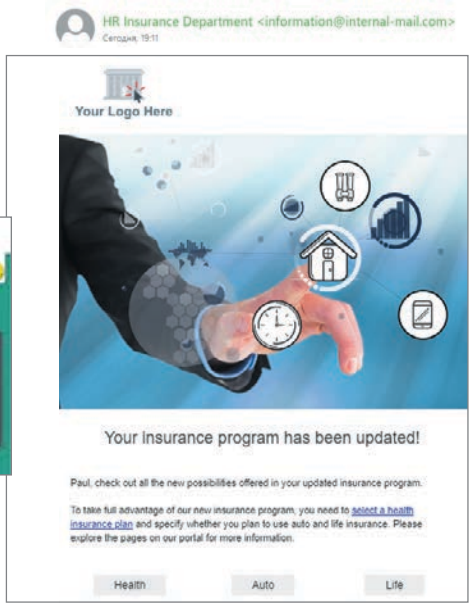
Lecciones interactivas

Curso principal

Curso rápido



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 profundizar para obtener más detalles a nivel individual.

Refuerzo

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.

[Dis]connected: una búsqueda de ciberseguridad móvil

[Dis]connected es un juego 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 en lo personal como en lo profesional.

Los elementos de la ciberseguridad se entretejen en la trama del juego, y el juego revela cómo nuestras decisiones en torno a la ciberseguridad pueden ayudar a conseguir, o estropear, los objetivos. Hay 18 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, las aplicaciones bancarias, etc., garantizan una experiencia de inmersión aún más 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 se ejecuta en teléfonos móviles. Hay disponible una **demostración gratuita** en Google Play y AppStore: https://kas.pr/mobilestores

Aprendizaje avanzado

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
- 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 CITO gratis:
cito-training.com

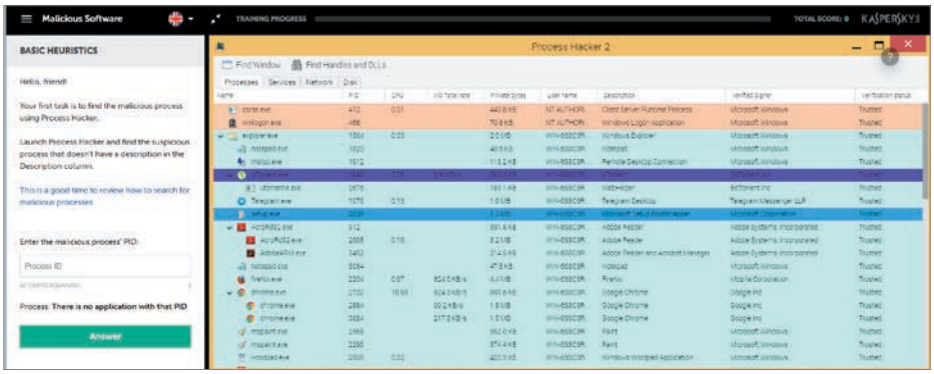
Ciberseguridad para TI en línea: la primera línea de defensa contra incidentes

Ciberseguridad para TI en línea 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.



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 cibernética, 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 para ejecutivos: aumento de la resiliencia empresarial para la transformación digital

Los líderes empresariales y los altos directivos aprenden los conceptos básicos de la ciberseguridad a través de un curso dirigido por un tutor que les brinda una mejor comprensión de las ciberamenazas y cómo protegerse contra ellas.

Las investigaciones muestran que existe un vínculo directo entre la velocidad y la eficiencia de la respuesta a incidentes y el grado de daño que puede causar un incidente. El curso presta especial atención a los aspectos económicos de la ciberseguridad y a la viabilidad de invertir en ella, lo que brinda a sus ejecutivos de nivel C una mejor comprensión de la relación entre la ciberseguridad y la eficiencia empresarial.

Kaspersky Interactive Protection simulation (KIPS) se puede utilizar además de esta formación para consolidar aún más el material mediante ejercicios prácticos.

Objetivos del curso

- Compartir la información más reciente sobre las ciberamenazas modernas y sus riesgos para las empresas
- Poner al día a los alumnos sobre el panorama moderno de las ciberamenazas
- Brindar la oportunidad de practicar las reglas básicas de la cultura de ciberseguridad corporativa y personal
- Asegurar que se comprende el impacto para las empresas de los principales aspectos regulatorios en el campo de la seguridad de la información
- Aclarar los conceptos básicos de ciberseguridad y los métodos de protección contra ataques dirigidos.
- Dar recomendaciones prácticas para la política corporativa
- Asesorar sobre comunicaciones para responder e investigar incidentes

Kaspersky Security Awareness: métodos de formación flexibles

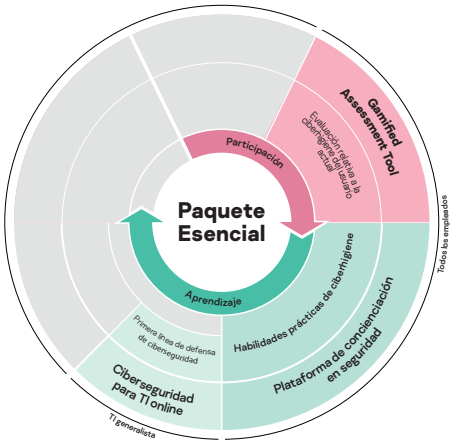
Las soluciones de formación de Kaspersky abordan todos los niveles de su empresa y se pueden usar por su cuenta o de forma colectiva. También facilitamos el inicio del uso de paquetes adaptados a sus necesidades.

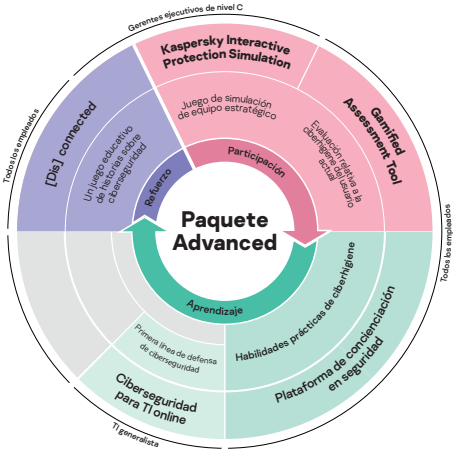
La opción sin complicaciones para concienciar a los empleados en torno a la ciberseguridad, que además es fácil de configurar y gestionar.

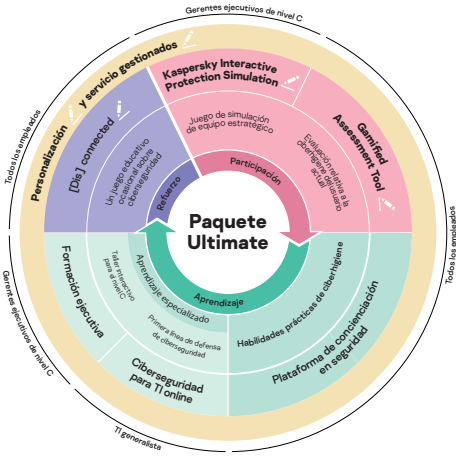
Ofrece un nivel básico de formación en seguridad para ayudarle a operar con éxito y cumplir con los requisitos normativos o de terceros sobre formación en ciberseguridad general

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 sus necesidades, por lo que hay una solución para todos. Más información en www.kaspersky.es/enterprise-security/security-awareness

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

kaspersky.es

kaspersky PREPARADOS PARA EL FUTURO