
**Programas de
formación por
ordenador para
todos los niveles
organizativos**

2019

Kaspersky Security Awareness

kaspersky

Obtenga más información en
kaspersky.es/awareness

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

Más del 80 % de los ciberincidentes se debe a errores humanos. Las empresas pierden millones para recuperarse de incidentes relacionados con el personal, pero la eficacia de los programas de formación tradicionales ideados para evitar estos problemas es limitada y, por lo general, dichos programas no logran suscitar ni motivar el comportamiento deseado.

Las personas son el eslabón más débil de la cadena de la ciberseguridad:

52 % de las empresas considera a los empleados la mayor amenaza para la ciberseguridad empresarial*

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

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

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

La solución:

Convertir las debilidades humanas en puntos fuertes aprovechando nuestra capacidad de aprender, y hacer de los empleados la nueva primera línea de defensa.

¿Por qué los clientes no están satisfechos con los programas de formación sobre concienciación existentes?

No son eficaces:

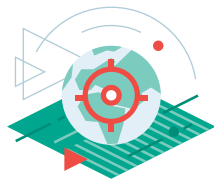
- Los empleados consideran que la formación es aburrida, que dista mucho de la vida laboral real y que se trata de un trabajo pesado e irrelevante
- Se dicta qué no hacer en lugar de explicar las buenas pautas
- La lectura y la escucha no son tan eficaces como la práctica

Una carga administrativa:

- Dificultad para gestionar y controlar el proceso de formación
- Dificultad para encontrar nuevas formas de involucrar y motivar a los empleados para que aprendan

Kaspersky Security Awareness: un nuevo enfoque del aprendizaje

Factores diferenciadores clave



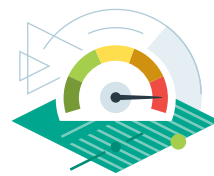
Formación específica basada en funciones

- Aprenda lo que necesita saber, en función de su puesto y perfil de riesgo.
- Ejemplos reales y habilidades que se pueden poner en práctica de inmediato.
- Aprendizaje mediante la práctica.



Centrada en el ser humano

- Formación estructurada de acuerdo con la forma en que las personas piensan de forma natural.
- Da un matiz proactivo y positivo al comportamiento seguro.
- Información y habilidades fáciles de asimilar y retener, gracias a las metodologías basadas en las particularidades de la memoria humana.



Aprendizaje progresivo y continuo

- De lo sencillo a lo más complejo.
- Ampliación y aplicación de conocimientos adquiridos previamente en nuevos contextos.



Gestión y control sencillos

- Online.
- Gestión automatizada del aprendizaje.
- Invitaciones y correos electrónicos motivadores enviados automáticamente con recomendaciones individuales para cada estudiante.

* Investigación: "The cost of a data breach", Kaspersky, primavera de 2018.

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

Concienciación eficaz en materia de seguridad

La formación del personal en todos los niveles es esencial para aumentar la concienciación sobre la seguridad en toda la organización y motivar al conjunto de los empleados a prestar atención a las ciberamenazas y a las tácticas defensivas, incluso si no consideran que forme parte específicamente de sus responsabilidades laborales.

Los errores de los empleados son los responsables de la mayoría de los incidentes de ciberseguridad que se dan en las organizaciones de hoy en día.

Los errores humanos pueden suponer un ciberriesgo importante para una organización, aun cuando se siguen programas de concienciación tradicionales:

1 057 000 \$

por empresa: impacto económico medio de los robos de datos provocados por el uso inapropiado que los empleados hacen de los recursos de IT*

101 000 \$

por pyme: impacto económico de los ataques causados por phishing o ingeniería social (1,3 millones de dólares por empresa)**

Hasta

400 \$

por empleado al año: coste medio de los ataques de phishing***

Formación de Kaspersky Security Awareness

Kaspersky ofrece productos de formación por ordenador que combinan la experiencia en ciberseguridad con técnicas y tecnologías educativas que siguen las prácticas recomendadas. Este enfoque cambia el comportamiento de los usuarios y ayuda a crear un entorno de ciberseguridad en toda la organización.

Diferentes formatos de formación para diferentes niveles organizativos



* Informe: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky, 2018

** Informe "Human factor in IT security: How Employees are Making Businesses Vulnerable from Within", International, junio de 2017

***Cálculos basados en el informe "Cost of Phishing and Value of Employee Training" de Ponemon Institute, agosto de 2015.

Descripción de los productos de Kaspersky Security Awareness

ASAP ofrece objetivos de formación fáciles de establecer, un itinerario de aprendizaje predefinido y bien equilibrado, relevancia para la vida real y elaboración de informes procesables, lo que garantiza que el programa tenga buena acogida y aporte valor tanto a los empleados como a la dirección.

Cada tema consta de diferentes niveles que desarrollan las habilidades específicas de seguridad. Los niveles se definen según los grados de riesgo que ayudan a eliminar. El nivel 1 aborda el comportamiento ante ataques directos y masivos. Los niveles superiores proporcionan formación sobre concienciación para enfrentarse a los ataques más sofisticados y dirigidos.

La plataforma está disponible en nueve idiomas: inglés, alemán, italiano, francés, español, ruso, árabe, portugués y holandés*.

ASAP es ideal para MSP y xSP: los servicios de formación para varias empresas se pueden gestionar a través de una única cuenta y las licencias se pueden adquirir mediante una suscripción mensual.

Pruebe una versión totalmente funcional de Kaspersky ASAP en asap.kaspersky.com y compruebe por sí mismo lo fácil que es configurar y gestionar su propio programa de formación de concienciación sobre seguridad corporativa.



1. Kaspersky Automated Security Awareness Platform (ASAP)

Un nuevo enfoque integral para los programas educativos online, que no solo se basa en la información, sino también en la "percepción de patrones", lo que permite a los empleados comportarse de forma segura, incluso cuando se enfrentan a amenazas completamente nuevas.

Gestión automatizada del aprendizaje

- La plataforma solo tarda 10 minutos en iniciarse: le resultará rápido y sencillo cargar la lista de usuarios, dividir a los usuarios en grupos y establecer un nivel deseado para cada grupo, en función de los niveles de riesgo.
- Después, la propia plataforma crea un programa educativo para cada grupo y proporciona un aprendizaje periódico con un refuerzo constante, que se ofrece automáticamente a través de una gran variedad de formatos de formación, como módulos de aprendizaje, refuerzo por correo electrónico, pruebas y ataques de phishing simulados.

Elaboración de informes procesables disponible en cualquier momento

- Siga el progreso de los estudiantes a través del intuitivo panel, que proporciona un seguimiento directo de datos, tendencias y previsiones.
- Reciba recomendaciones sobre cómo mejorar los resultados.
- Programa de formación universal.
- Se trata una amplia gama de temas clave de ciberseguridad, todos ellos disponibles en diferentes niveles, del principiante absoluto al avanzado.

Ventajas clave:

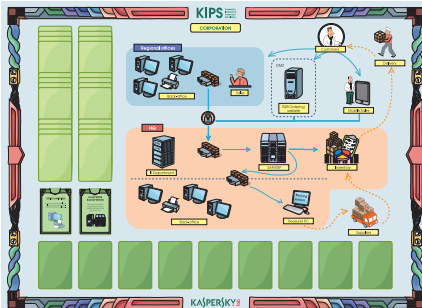
- **Sencillez mediante una automatización completa:** el programa es muy fácil de iniciar, configurar y supervisar, y la gestión continua está totalmente automatizada, sin necesidad de intervención administrativa.
- **Eficacia:** el contenido del programa está estructurado para facilitar el aprendizaje 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.
- **Licencias flexibles:** el modelo de licencias por usuario puede empezar con tan solo 5 licencias.

* Desde julio de 2019

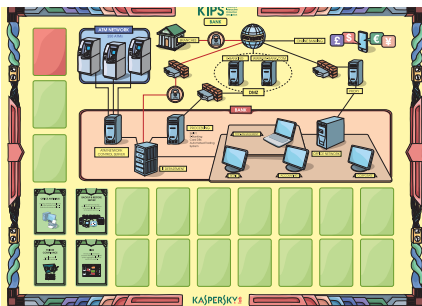
La formación en KIPS está dirigida a altos directivos, expertos en sistemas empresariales y profesionales de IT, con el fin de aumentar su concienciación sobre los riesgos y problemas de seguridad que sufren los sistemas informatizados modernos.

Algunos escenarios de KIPS:

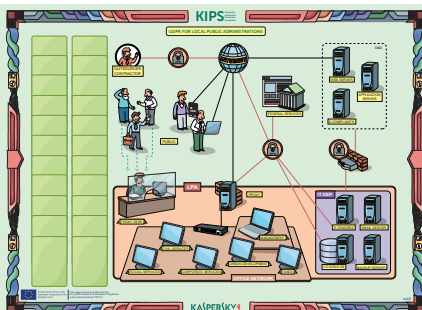
Empresa



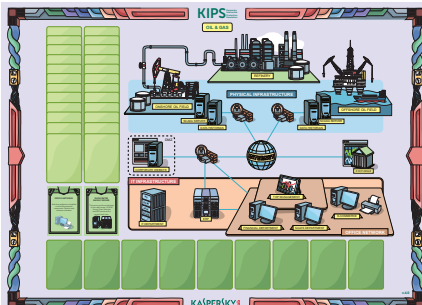
Banco



Administraciones públicas locales ¡NOVEDAD!



Petróleo y gas



KIPS online:

- Idóneo para empresas globales
- Hasta 300 equipos a la vez
- Los distintos equipos pueden elegir interfaces de juego en diferentes idiomas
- Un instructor dirige cada sesión mediante WebEx

2. La formación de Kaspersky Interactive Protection Simulation (KIPS) fomenta la comprensión y el apoyo estratégicos

Qué es KIPS

KIPS es un juego de rol en equipos que simula un entorno empresarial donde los participantes deben enfrentarse a una serie de ciberamenazas inesperadas sin olvidarse de maximizar sus beneficios y mantener la confianza del mercado.

La idea consiste en crear una estrategia de ciberdefensa seleccionando los mejores controles proactivos y reactivos disponibles.

KIPS resulta extraordinariamente eficaz porque:

- Ofrece un nuevo enfoque viable a la ciberseguridad
- Es divertido, atractivo y rápido (2 horas)
- La cooperación se basa en el trabajo en equipo
- Fomenta las habilidades de iniciativa y análisis en un entorno competitivo
- Permite realizar descubrimientos y cometer errores a la hora de desarrollar un programa de ciberseguridad y un comportamiento ciberseguro, y analizarlo todo de forma segura a través del juego.

La experiencia KIPS:

- Muéstrase preparado para las amenazas emergentes: aprenda cómo operan técnicamente los criminales (inteligencia frente a amenazas) y entienda sus metas.
- Descubra cómo combinar la respuesta ante incidentes con la prevención de incidentes.
- Vea qué pasa cuando se olvida de configurar los controles de seguridad correctamente.
- Preste atención a las alertas desde un punto de vista global que lo tenga en cuenta todo: la seguridad, los recursos de IT y su empresa.

Escenarios relacionados con el sector disponibles (todos como KIPS Live y KIPS Online, con 10 idiomas ofrecidos)

- **Empresa:** protección de la empresa frente a ransomware, amenazas avanzadas persistentes (APT), errores de seguridad de automatización, etc.
- **Banca:** protección de entidades financieras frente a las APT de alto nivel que atacan los cajeros automáticos, servidores de gestión y sistemas empresariales.
- **Administración electrónica o administraciones públicas locales:** Protección de servidores web públicos frente a ataques y exploits.
- **Central eléctrica o planta de tratamiento de aguas:** Protección de sistemas de control industrial e infraestructura crítica.
- **Empresas de transporte:** Protección de pasajeros y transporte de mercancías frente a Heartbleed, ransomware y APT.
- **Petróleo y gas:** Análisis de la influencia de una amplia gama de amenazas, desde la destrucción de sitios web hasta ransomware actual y APT sofisticadas.

Cada escenario muestra a los participantes el verdadero papel de la ciberseguridad en lo referente a la continuidad y rentabilidad de la empresa, destacando los retos y amenazas emergentes, así como los típicos errores empresariales al desarrollar su ciberseguridad. Al mismo tiempo, fomenta la cooperación entre los equipos de seguridad y los comerciales, lo que ayuda a mantener la estabilidad de las operaciones y la sostenibilidad contra las ciberamenazas.

La formación en IT de la ciberseguridad está dirigida a los especialistas del servicio técnico, así como a los administradores de servicio local y de seguridad de IT general.

Formato de la formación

La formación es totalmente online: los participantes solo necesitan tener conexión a Internet o acceso al LMS corporativo y un navegador Chrome.

Cada uno de los 4 módulos comprende una breve introducción teórica, consejos prácticos, y entre 4 y 10 ejercicios (en cada uno de ellos se practica una habilidad específica y se muestra cómo utilizar las herramientas y el software de seguridad de IT en el trabajo diario).

El estudio está ideado para realizarse a lo largo de un año. La tasa recomendada de progreso es de 1 ejercicio por semana. Cada ejercicio lleva entre unos 5 y 45 minutos.

3. Ciberseguridad para IT online

Formación interactiva para quienes forman parte de IT, que permite desarrollar una ciberseguridad fuerte, así como habilidades de respuesta ante incidentes de primer nivel.

Resulta imposible mantener una postura de ciberseguridad corporativa sólida si no todos los empleados relevantes han recibido la formación sistemática necesaria. La mayoría de las empresas proporcionan educación y formación en ciberseguridad en dos niveles: formación especializada para equipos de seguridad de IT, y concienciación general sobre la seguridad para los empleados que no pertenecen a IT. Ninguno de estos métodos funciona para la gran cantidad de personal de IT que no está directamente relacionado con la seguridad, pero cuyo puesto le ofrece una posición ideal para realizar importantes contribuciones específicas a la ciberseguridad corporativa.

Respuesta ante incidentes de primer recurso

Kaspersky Lab ofrece una la primera formación online del mercado para profesionales generales de IT empresarial.

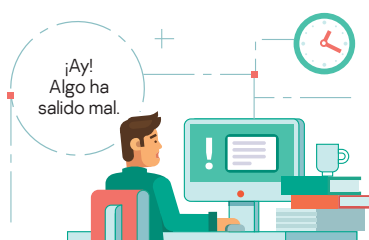
El curso consta de 4 módulos:

- Software malicioso
- Programas y archivos potencialmente no deseados
- Conceptos básicos de investigación
- Respuesta ante incidentes de phishing

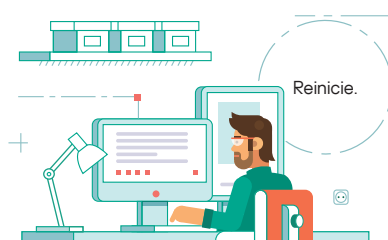
Este curso dota a los profesionales de IT de conocimientos prácticos, que incluyen:

- Cómo reconocer un posible escenario de ataque en un incidente de equipo aparentemente benigno.
- Cómo recopilar datos de los incidentes para remitírselos a los equipos de seguridad de IT.
- Cómo detectar síntomas malintencionados, y consolidar así el papel de todos los miembros del equipo de IT como primera línea de defensa y seguridad.

Ahora



Usuario



Asistencia en IT/Administradores

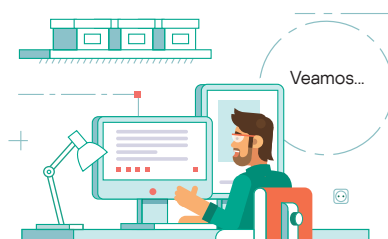


Seguridad de IT

Debería ser



Usuario



Asistencia en IT/Administradores

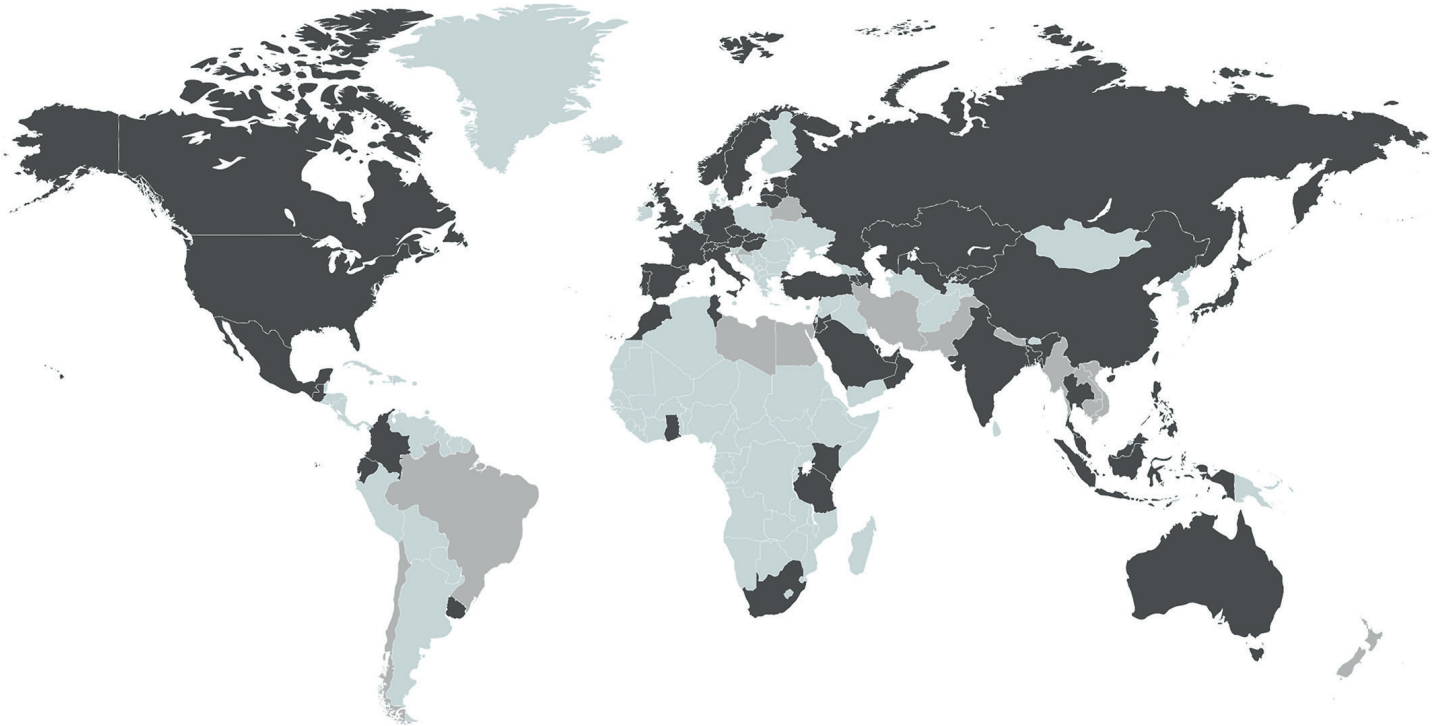


Seguridad de IT

75
países

250 000
empleados formados

Kaspersky Security Awareness a nivel global



A fecha de marzo de 2019

■ Uso comercial o en grandes eventos
■ Participación en campeonatos online

Creado con mapchart.net

Ciberseguridad de empresa: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
Noticias de seguridad de IT: business.kaspersky.com

www.kaspersky.es

kaspersky BRING ON
THE FUTURE