Kaspersky Security Awareness

# Creamos una cultura de ciberseguridad que protege tu empresa

kaspersky preparados para el futuro

### Error humano

Es una de las amenazas principales: en promedio, entre el 64 % y el 86 % de las filtraciones se deben a acciones humanas no maliciosas[1]

### 4,4 millones USD

Es el coste promedio de una filtración de datos por organización[2]

### Los reglamentos exigen concienciación sobre la seguridad

Forma parte del cumplimiento: normativas como PCI DSS, ISO/IEC 27001, RGPD, NIS 2, entre otras, exigen o recomiendan con énfasis realizar programas de concienciación sobre la seguridad para proteger los datos confidenciales

### Crear una cultura con conciencia sobre la seguridad vale la pena

Un estudio de Kaspersky revela que más del 85 % de los empleados que completan la formación de concienciación afirman haber mejorado su nivel de alerta y precaución, un cambio de actitud que ayuda a prevenir incidentes.

**92 %**

de los usuarios recomendarían Kaspersky Security Awareness a otras personas

**3 millones**

Empleados que han completado nuestro programa de formación con éxito

**+ 160**

países en los que las organizaciones protegen a sus empleados con nuestras soluciones de formación

# Un enfoque eficaz para reducir el riesgo cibernético humano

Desarrolla una cultura de comportamiento cibernético seguro en toda la organización, basada en una fuerte conciencia sobre la ciberseguridad y habilidades prácticas. De este modo, se reduce la cantidad de incidentes producto del error humano. La mejor manera de abordar el factor humano es a través de un programa de formación estructurado que combine contenidos actualizados y pertinentes con los métodos y las tecnologías de aprendizaje más recientes.

## Soluciones de Kaspersky Security Awareness

Kaspersky Security Awareness fortalece a las empresas sin importar su tamaño en todo el mundo para incrementar los conocimientos cibernéticos entre los empleados y fomentar una cultura en la que la seguridad es responsabilidad de todos. Debido a que los cambios sostenibles en el comportamiento llevan tiempo, nuestro enfoque consiste en crear un ciclo de aprendizaje continuo con diversas herramientas y materiales de refuerzo: Kaspersky Interactive Protection Simulation, la formación ejecutiva, Automated Security Awareness Platform y el curso Ciberseguridad para TI online.


# Por qué nuestros clientes escogen Kaspersky Security Awareness

### Habilidades y confianza para detectar amenazas reales y responder ante ellas

Aprovechando los casi 30 años de experiencia de Kaspersky en ciberseguridad y nuestra inteligencia frente a amenazas en tiempo real, creamos contenidos de formación en ciberseguridad de gran relevancia. A medida que surgen nuevas amenazas, nuestros contenidos evolucionan, lo que contribuye a garantizar que tus empleados estén siempre preparados.

### Aprendizaje accesible e interactivo

Nuestra formación se basa en un aprendizaje interactivo con una estructura clara y lógica que ayuda a los empleados a relacionar las clases con sus tareas diarias. De esta manera, se mejora la comprensión, la retención y la aplicación práctica.

### Cambio duradero en el comportamiento

Nuestra metodología refuerza las habilidades nuevas, proporciona una motivación constante y ayuda a integrar el aprendizaje en las rutinas de la organización. El resultado es un cambio sostenido en el comportamiento, en el que las prácticas seguras se convierten en un hábito.

### Participación de todos los niveles

Desde los ejecutivos, que necesitan información de alto nivel y útil para la toma de decisiones, hasta el personal de primera línea, que requiere orientación práctica, ofrecemos el material adecuado, en el formato adecuado, para cada público.

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures, Verizon Data Breach Reports

2 Cost of a Data Breach Report 2025, IBM

# Kaspersky Automated Security Awareness Platform: cómo crear un firewall humano

Kaspersky Automated Security Awareness Platform (ASAP) es una herramienta en línea que ofrece formación continua y les proporciona a los empleados las habilidades y los conocimientos necesarios para identificar y detener vectores de ataque reales.

Creado por expertos de primer nivel, Kaspersky ASAP potencia las capacidades de tu personal y fortalece tu empresa:

**Reduce la cantidad de incidentes provocados por errores humanos,** además de sus consiguientes perjuicios financieros y en la reputación

**Reduce al mínimo el riesgo de multas por incumplimiento,** ya que se corresponde con los requisitos normativos

**Reduce el tiempo y el esfuerzo** necesarios para administrar la formación en materia de concienciación y alivia la carga de trabajo de los equipos de TI

Kaspersky ASAP es mucho más que una herramienta antiphishing. La formación se basa en las técnicas de MITRE ATT&CK y muestra qué vectores de ataque provocados por humanos pueden ayudar a prevenir los empleados. A continuación se incluyen algunos ejemplos:

| Técnica MITRE | Contra amenazas | Habilidades y resultados del comportamiento |
|---|---|---|
| T1566: Phishing | Correos electrónicos maliciosos | Reconocimiento e informe de intentos de phishing |
| T1585: Establecimiento de cuentas | Cuentas o perfiles falsos | Verificación de autenticidad antes de compartir información |
| T1199: Relación de confianza | Aprovechamiento de la confianza de los partners | Capacidad para cuestionar solicitudes inusuales |
| T1091: Replicación en soportes extraíbles | Soportes extraíbles | Conocimiento del peligro de malware en dispositivos USB |
| T1078: Cuentas válidas | Robo de credenciales | Prohibición de acceso mediante ingeniería social |

**95 %**

de los empleados formados ahora pueden detectar ataques de phishing

**20x**

veces menos de filtraciones de datos cuando los empleados reciben formación constante [1]

Entre los temas principales que trata ASAP se incluyen, entre otros, los siguientes:

- Correo electrónico
- Contraseñas y cuentas
- Sitios web e Internet
- Seguridad para PC
- Datos confidenciales
- Datos personales
- Seguridad física de los datos
- GDPR
- Inteligencia artificial y redes neuronales
- Ataques a los principales administradores
- Dispositivos móviles
- Redes sociales y servicios de mensajería instantánea
- Ataques a la cadena de suministro
- Industrial cybersecurity
- Seguridad de las tarjetas bancarias y PCI DSS
- Cómo responder ante incidentes
- Vishing

Capacita a tus empleados para que se conviertan en una capa adicional de protección, junto con las herramientas técnicas.

Comenzar prueba

1 Investigación de Kaspersky Automated Security Awareness Platform, 2025

# Contenidos y metodología que se graban en la memoria, para asimilar los conocimientos y poner en práctica las habilidades

### Elaborado por expertos

Contenido basado en casi 30 años de experiencia en ciberseguridad y en un modelo de competencias que abarca habilidades prácticas y esenciales en materia de ciberseguridad sobre diversos temas.

### Una amplia variedad de opciones de personalización

Añade tu logotipo y los certificados de tu marca, enriquece las clases con diapositivas internas, documentos o directivas, añade módulos SCORM/PDF personalizados y ajusta las estructuras de las pruebas.

### Diversidad de contenidos

Favorece la retención de conocimientos mediante módulos y ejercicios interactivos, casos reales, pruebas, vídeos y simulaciones de phishing en diversos escenarios.

### Centrada en el ser humano

Con un diseño pensado en función de cómo las personas asimilan, retienen y aplican la información

## Cómo funciona

Todos los miembros de tu organización deben tener conocimientos sobre ciberseguridad, pero el nivel de profundidad de esos conocimientos varía según la función y el perfil de riesgo. Ahí es donde fracasan los programas de formación universales. Nuestra plataforma ayuda a tu equipo a desarrollar más de 500 habilidades prácticas, agrupar al personal sin esfuerzo y asignar la formación adecuada a cada participante con solo unos clics, utilizando los componentes que se indican a continuación.

### Curso principal

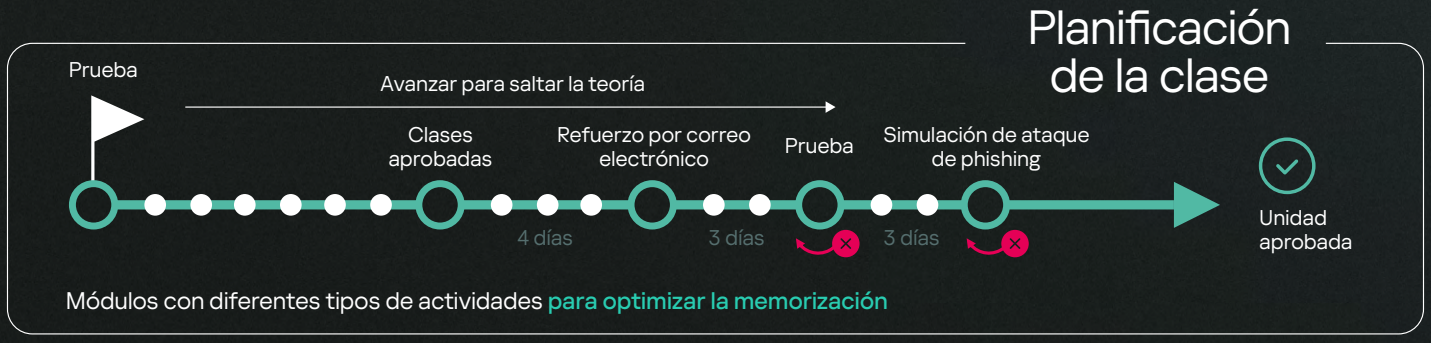
Obtén conocimientos en profundidad a través de microclases organizadas según el nivel de complejidad.

### Curso express

Cumple de forma rápida con los requisitos de formación en ciberseguridad o actualiza tus conocimientos con cursos de formación breves y muy interesantes en formato audiovisual.

### Simulador de phishing

Ejecuta simulacros de ataques de phishing antes, durante y después de la formación, para poner a prueba la capacidad de los empleados en la defensa de los ciberataques.




Módulos con diferentes tipos de actividades para optimizar la memorización

## Una solución fácil de administrar para organizaciones de cualquier tamaño

### Incorporación sencilla

Regístrate en línea y obtén acceso a la versión de prueba para hasta cinco usuarios durante dos meses. Incluye una guía de inicio y asistencia en línea

### Gestión proactiva de riesgos humanos

La integración perfecta con Kaspersky SIEM y XDR, junto con las API para la integración con aplicaciones de terceros, ofrece una visión completa del comportamiento de los empleados y permite asignar las formaciones según incidentes de seguridad reales directamente desde la consola

### Agrupación automatizada de usuarios según la personalización de las reglas predefinidas

Organiza según la función, el departamento o el perfil de riesgo

### Opciones de implementación flexibles

Disponible como plataforma de SaaS o instalación local

### Automatización completa

Los módulos de formación, las pruebas y las simulaciones de phishing se asignan automáticamente, alineados con la configuración del grupo de formación

### Asistencia de varios usuarios y funciones de administrador flexibles

Ideal para organizaciones con filiales y equipos distribuidos, ya que permite una supervisión centralizada al mismo tiempo que se delega la gestión a los administradores locales.

### Informes claros

Los paneles de control proporcionan datos esenciales con vistas detalladas del progreso, las demoras o el bajo rendimiento de cada empleado, además de un informe en PDF listo para enviar a la administración con solo un clic

### Inscripción sin complicaciones

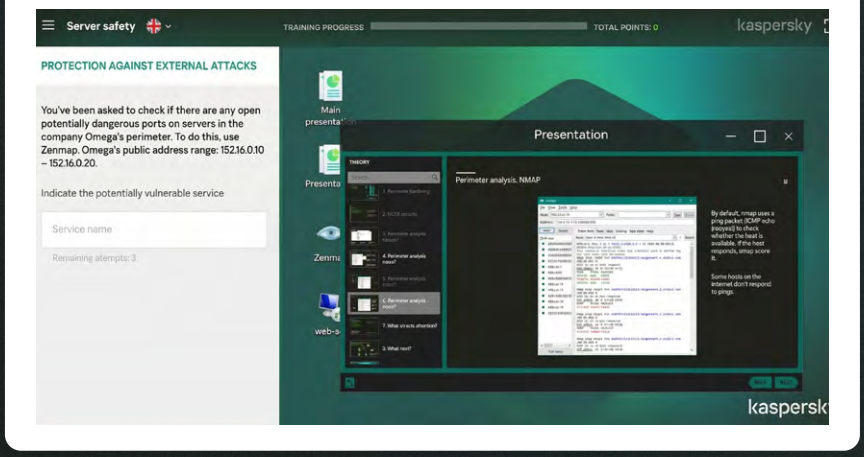
Se integra con Active Directory y SSO

# Ciberseguridad para TI online

Ciberseguridad para TI online (CITO) es un programa de formación interactivo que les ofrece las habilidades prácticas necesarias a los especialistas de servicio de asistencia técnica, a los administradores de sistemas y a los miembros no especializados de los equipos de seguridad de TI. El objetivo es detectar ciberataques ocultos en incidentes de PC cotidianos, recopilar datos pertinentes y actuar como primera línea de defensa en materia de ciberseguridad.

## Habilidades prácticas para la respuesta ante incidentes de primer nivel:

- Aprende a detectar, analizar y responder ante la presencia de malware, programas potencialmente no deseados, exploits y ataques de phishing
- Aplica herramientas y técnicas reales para fortalecer la seguridad de la infraestructura de TI e investigar los incidentes de manera eficaz
- Desarrolla habilidades para el análisis de registros, la recolección de evidencia digital y la investigación de amenazas
- Aprende a proteger los servidores y Active Directory mediante el refuerzo de la seguridad, la configuración de directivas y la supervisión




Los participantes completan seis módulos que combinan teoría concisa, consejos prácticos y entre 4 y 13 ejercicios por módulo, con un enfoque en herramientas de TI reales y tareas cotidianas.

- Software malicioso
- Programas y exploits potencialmente no deseados
- Seguridad de servidores
- Conceptos básicos de investigación
- Phishing e inteligencia de código abierto
- Seguridad de Active Directory

# Formación de Kaspersky para ejecutivos

Promueve una cultura de seguridad de arriba abajo y demuestra cómo las decisiones de la dirección influyen directamente en la exposición frente a los riesgos, el cumplimiento normativo y la resiliencia organizativa a largo plazo.

La formación de Kaspersky para ejecutivos es un taller presencial dirigido a los líderes empresariales y a los gerentes principales en el que se explica qué implica el panorama actual de amenazas para tu empresa, qué medidas hay que tomar en caso de ciberataques y mucho más. Además de los principios básicos de ciberseguridad, los participantes obtienen información clave sobre la viabilidad financiera de las inversiones en seguridad, lo que les permite a los líderes de alto nivel vincular la protección con el rendimiento de la empresa. Lo ideal es combinar esta formación con KIPS.

## Explicación de los aspectos fundamentales de la ciberseguridad relacionados con las empresas en un lenguaje claro, accesible y sin tecnicismos:

- Comprende mejor a la ciberseguridad como parte de un sistema global
- Descubre cómo los riesgos cibernéticos afectan las operaciones empresariales y cómo se pueden gestionar
- Conoce la función del personal de dirección en la gobernanza de la ciberseguridad

# Kaspersky Interactive Protection Simulation (KIPS): la ciberseguridad desde una perspectiva empresarial

KIPS aumenta la toma de conciencia sobre los riesgos y retos asociados al uso de todo tipo de sistemas de TI y los procesos empresariales. Se trata de un juego interactivo en equipo de dos horas de duración que está dirigido a altos directivos, expertos en sistemas empresariales y profesionales de TI. Los escenarios específicos del sector exponen a los participantes a técnicas de ataque modernas que los expertos de Kaspersky observan en campañas activas, incluyendo ataques a la cadena de suministro, el aprovechamiento del acceso de terceros, la ingeniería social o el malware. Debido a que trabajan con limitaciones de tiempo y presupuesto, los equipos deben elaborar estrategias, anticipar el impacto de los incidentes de seguridad y responder de forma eficaz para proteger el rendimiento y los ingresos de la empresa.

- Fomenta el entendimiento entre los responsables de la toma de decisiones
- Ayuda a visualizar los riesgos de ciberseguridad y a relacionarlos directamente con los ingresos y las operaciones
- Involucra a los equipos en cuestiones de ciberseguridad y fomenta una cultura que da prioridad a la seguridad

**14 casos prácticos específicos para cada sector,** a los que se añaden otros constantemente

- Aeropuerto
- Empresa
- Banco
- Petróleo y gas
- Transporte
- Central eléctrica
- Planta de tratamiento de agua
- Administración pública local
- Industria petroquímica
- Holding de petróleo
- Pequeñas y medianas empresas
- Telecomunicaciones
- Atribución técnica
- IT

## KIPS en vivo

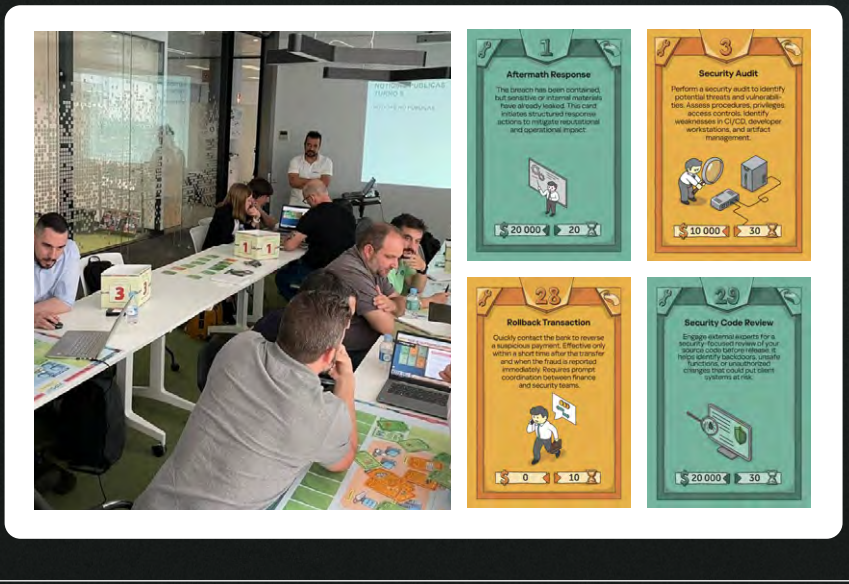
Se trata de una actividad entretenida que puede llevarse a cabo como un evento independiente o como una sesión dentro de una conferencia, seminario o evento corporativo ya programado.

- Hasta 100 participantes, entre 4 y 5 personas en cada equipo
- Con un moderador presencial y un asistente de formación

## KIPS online

La versión online es perfecta para las organizaciones globales o las actividades públicas. También se puede combinar con KIPS Live para incluir equipos remotos a un evento on-site.

- Hasta 300 equipos (1000 participantes) desde cualquier ubicación




## Opciones de personalización de KIPS

- Pizarras, tarjetas y números de mesa con marca compartida o con la marca del cliente
- Un escenario único, creado en colaboración con Kaspersky, que puede reproducir tu red, los incidentes pasados o las amenazas específicas de tu sector

# Creamos una cultura de ciberseguridad

La verdadera resiliencia cibernética no se reduce solo a directivas y tecnologías, sino que es una cuestión de cultura. Y la cultura viene determinada por cómo actúan las personas, cómo lideran los responsables, cómo se diseñan los procesos y cómo la tecnología lo hace todo posible:

- El personal y su comportamiento
- El liderazgo y la cooperación
- La integración operativa
- Preparación y habilitación en materia de seguridad

Una cultura de ciberseguridad sostenible se logra cuando hay un compromiso constante. Por eso hemos desarrollado un enfoque sistemático basado en cinco pasos fundamentales en los que puedes utilizar las soluciones de Kaspersky Security Awareness.


## ¿Cuál es el nivel actual de madurez en la cultura de ciberseguridad de tu organización?

**0 Fragmentada**
Riesgo: la ausencia de prácticas y estructuras básicas genera un alto nivel de vulnerabilidad. Incluso un incidente menor puede provocar graves consecuencias.

**1 Consciente y reactiva**
Riesgo: solo se siguen las normas establecidas explícitamente. En situaciones no previstas, los empleados actúan según su propio criterio.

**2 Administrado**
Riesgo: la cantidad de incidentes está disminuyendo, pero el sistema sigue siendo vulnerable ante situaciones más complejas.

**3 Integrada**
Riesgo: los procesos parecen funcionar correctamente, pero si la cultura cibernética no actúa como un sistema que se autorregula, sigue existiendo un "riesgo de retraso".

**4 Resiliente**
Resultado: la cantidad y la gravedad de los incidentes sigue disminuyendo. La organización es capaz de adaptarse rápidamente a la evolución del panorama de amenazas.

> Cuando la seguridad deja de ser una campaña y se convierte en una cultura, el riesgo disminuye, y los resultados hablan por sí solos.
>
> CISO
>
> Servicios de atención al cliente

Con Kaspersky ASAP, alinea a las personas, los procesos y las tecnologías para comenzar a crear una cultura de resiliencia cibernética.

Probar ahora

# Kaspersky Security Awareness

Ten cuidado.
Mantente a salvo.

www.kaspersky.es



#kaspersky
#cybersecuritytruetobusiness