



Kaspersky
Security
Awareness

Creamos una
cultura de
ciberseguridad
que protege su
empresa

kaspersky cybersecurity
true to business



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 maliciosas¹



\$4,4 millones

Es el costo promedio de una filtración de datos por organización²



Los reglamentos exigen una toma de conciencia sobre la seguridad

Esto forma parte del cumplimiento: normativas como PCI DSS, ISO/IEC 27001, RGPD, NIS 2, entre otras, exigen o recomiendan con énfasis realizar programas de toma de conciencia 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 capacitación de toma de conciencia 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

de empleados completaron nuestros programas de capacitación con éxito

Más de 160

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

Un enfoque eficaz para reducir el riesgo cibernético humano

Desarrolle 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 capacitación 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 las empresas sin importar su tamaño en todo el mundo para ampliar 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, Capacitación ejecutiva, Automated Security Awareness Platform y el curso Ciberseguridad para TI en línea.



Por qué nuestros clientes eligen 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 capacitación en ciberseguridad de gran relevancia. A medida que surgen nuevas amenazas, nuestros contenidos evolucionan, lo que contribuye a garantizar que sus empleados estén siempre preparados.

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.

Aprendizaje accesible e interactivo

Nuestra capacitación 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.

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 capacitación 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 del personal y fortalece su 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 capacitación en la toma de conciencia y alivia la carga de trabajo de los equipos de TI

Kaspersky ASAP es mucho más que una herramienta antiphishing. La capacitación 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	Amenaza	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 socios	Capacidad para cuestionar solicitudes inusuales
T1091: replicación en medios extraíbles	Medios 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 capacitados ahora pueden detectar ataques de phishing

20 veces

menos filtraciones de datos cuando los empleados reciben capacitación 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 del equipo
- Datos confidenciales
- Datos personales
- Seguridad física de datos
- RGPD
- Inteligencia artificial y redes neuronales
- Ataques a los principales administradores
- Dispositivos móviles
- Redes sociales y servicios de mensajería
- Ataques a la cadena de suministro
- Ciberseguridad industrial
- Seguridad de tarjetas bancarias y PCI DSS
- Cómo responder ante incidentes
- Vishing

Capacite a sus empleados para que se conviertan en una capa adicional de protección, junto con las herramientas técnicas. Comience hoy con acceso instantáneo a una demostración.

[Comenzar prueba](#)

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.



Diversidad de contenidos

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



Una amplia variedad de opciones de personalización

Agregue su logotipo y los certificados de su marca, enriquezca las clases con diapositivas internas, documentos o directivas, agregue módulos SCORM/PDF personalizados y ajuste las estructuras de las pruebas.



Enfoque centrado 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 la organización deben tener conocimientos sobre ciberseguridad, pero el nivel de profundidad de esos conocimientos varía según la función y el perfil de riesgo. Aquí es donde fallan las capacitaciones con enfoque generalizado. Nuestra plataforma ayuda a su equipo a desarrollar más de 500 habilidades prácticas, agrupar al personal sin esfuerzo y asignar la capacitación adecuada a cada participante con solo unos clics, utilizando los componentes que se indican a continuación.

Curso principal

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

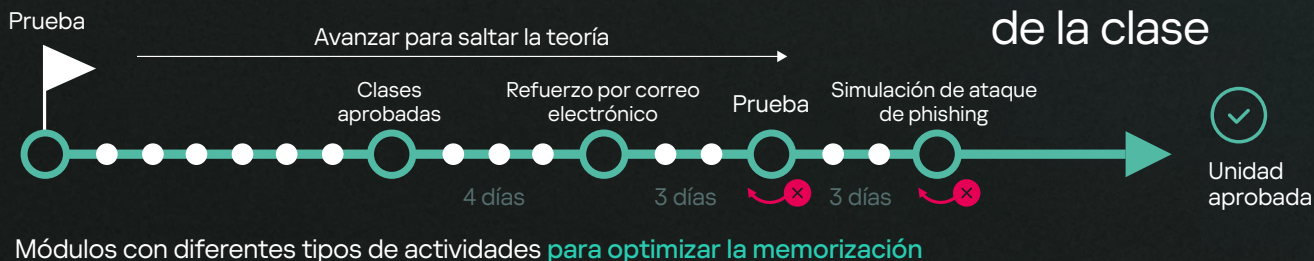
Curso rápido

Cumpla de forma rápida con los requisitos de capacitación en ciberseguridad o actualice sus conocimientos con cursos de capacitación breves y muy interesantes en formato audiovisual.

Simulador de phishing

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

Planificación de la clase



Una solución fácil de administrar para organizaciones de cualquier tamaño



Incorporación simple

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



Automatización completa

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



Gestión proactiva de riesgos humanos

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



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.



Agrupación automatizada de usuarios según la personalización de las reglas predefinidas

Organice según la función, el departamento o el perfil de riesgo.



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.



Implementación flexible

Disponible como plataforma de SaaS o instalación local.



Inscripción sin complicaciones

Se integra con Active Directory y SSO.



Ciberseguridad para TI en línea

Ciberseguridad para TI en línea (CITO) es un programa de capacitación 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:



Aprenda a detectar, analizar y responder ante la presencia de malware, programas potencialmente no deseados, exploits y ataques de phishing



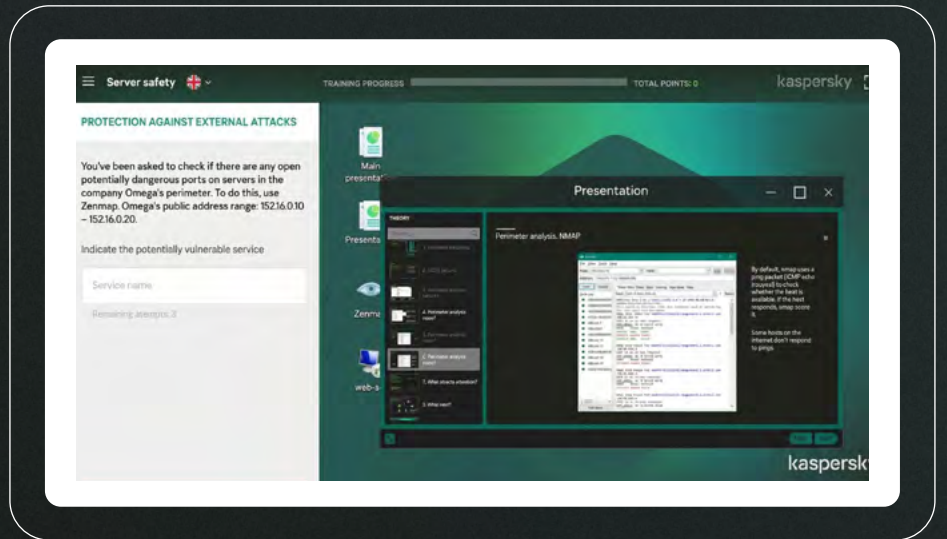
Aplique herramientas y técnicas reales para fortalecer la seguridad de la infraestructura de TI e investigar los incidentes de manera eficaz



Desarrolle habilidades para el análisis de registros, la recopilación de evidencia digital y la investigación de amenazas



Aprenda 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 para servidores

Conceptos básicos de investigación

Phishing e inteligencia de código abierto

Seguridad de Active Directory



Kaspersky Executive Training

Promueva una cultura de seguridad de arriba hacia abajo y demuestre 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.

Kaspersky Executive Training 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 su 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 permite a los líderes de alto nivel vincular la protección con el rendimiento de la empresa. Lo ideal es combinar esta capacitación con KIPS.

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



Comprenda mejor la ciberseguridad como parte de un sistema global



Descubra cómo los riesgos cibernéticos afectan las operaciones empresariales y cómo se pueden gestionar



Conozca 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 desafíos 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, como 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

Catorce casos prácticos específicos para cada sector, a los que se agregan otros constantemente



Aeropuerto



Empresa



Banco



Petróleo y gas



Transporte



Central eléctrica



Planta de tratamiento de agua



Administración pública local



Industria petroquímica



Explotación de petróleo



Pequeñas y medianas empresas



Operador



Atribución técnica



TI

KIPS Live (versión en vivo)

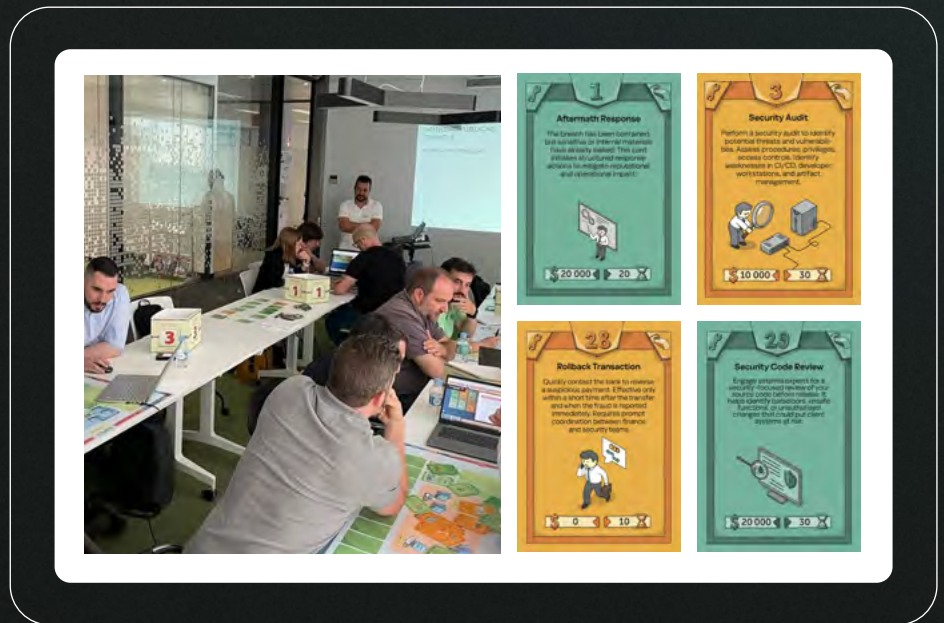
Se trata de una actividad entretenida que puede llevarse a cabo como un evento independiente o como una sesión dentro de una conferencia, seminario o evento corporativo ya programado.

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

KIPS Online (versión en línea)

La versión en línea es perfecta para las organizaciones globales o las actividades públicas. También se puede combinar con KIPS Live para incluir equipos remotos a un evento presencial.

- 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 su red, los incidentes pasados o las amenazas específicas de su 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:

• Personal y comportamiento

• Liderazgo y cooperación

• Integración operativa

• Preparación y habilitación en materia de seguridad

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



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



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

Cuando la seguridad deja de ser una campaña y se vuelve una cultura, el riesgo cae y los resultados se vuelven visibles.

[Pruébalo ya mismo](#)

CISO

Servicios de interacción con el cliente



Kaspersky Security Awareness

Tenga cuidado.
Manténgase a salvo.