



Kaspersky
Security
Awareness

Creamos una cultura
de ciberseguridad que
protege tu empresa



Por qué es importante una cultura centrada en la seguridad



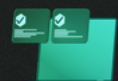
Error humano

Entre el 62 % y el 80 % de las infracciones se deben a acciones humanas, entre las que se incluyen errores, uso indebido de privilegios e ingeniería social^{1,2}



4,99 millones de dólares

es el coste promedio de una filtración de datos por organización³



Las normativas exigen la concienciación sobre seguridad como parte del cumplimiento: **PCI DSS, ISO/IEC 27001, RGPD, NIS 2** y otras normativas exigen o recomiendan firmemente implementar programas de concientización sobre seguridad para proteger los datos confidenciales



Más del 85 %

de los empleados que completan la formación en concienciación informan de una mayor atención y precaución, un cambio de comportamiento que ayuda a prevenir incidentes⁴

90 %

de los usuarios recomendaría Kaspersky Security Awareness a otras personas⁴

3 millones

empleados que han completado nuestro programa de formación con éxito

Más de 160

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

Reduce el riesgo cibernético humano con Kaspersky Security Awareness

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.

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 escoger Kaspersky Security Awareness

Casi 30 años de experiencia en ciberseguridad

Sobre la base de la experiencia global de Kaspersky, creamos contenido de formación en ciberseguridad altamente relevante. A medida que surgen nuevas amenazas, nuestros contenidos evolucionan, lo que contribuye a garantizar que tus 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.

Aprendizaje accesible e interactivo

Nuestra formación utiliza un aprendizaje interactivo que ayuda a los empleados a relacionar lo aprendido con sus tareas diarias, lo que mejora la retención y la aplicación de los conocimientos en situaciones reales.

Participación de todos los niveles

Desde los ejecutivos hasta el personal de primera línea, ofrecemos el contenido adecuado, en el formato adecuado para cada audiencia.

1 2026 Data Breach Investigations Report, Verizon

2 2026 Cyber risk Survey, Kaspersky

3 2026 Cost of a Data Breach Report, IBM

4 2024 Security Awareness & Training Data Quadrant, Info-Tech Research Group



Kaspersky Automated Security Awareness Platform

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

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



Reduce el número de incidentes relacionados con el factor humano

y el perjuicio financiero y de reputación que ello conlleva



Reduce al mínimo el riesgo de multas por incumplimiento

al cumplir con los requisitos normativos



Reduce el tiempo y el esfuerzo

necesarios para administrar la formación en concienciación y alivia la carga de trabajo de los equipos de TI

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

**MITRE
ATT&CK**

Técnica MITRE

Contra amenazas

Competencias y resultados conductuales

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 software malicioso 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 filtraciones de datos cuando los empleados reciben formación constante¹

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

Email

Contraseñas y cuentas

Sitios web e Internet

Seguridad para PC

Datos confidenciales

Datos personales

Seguridad física de los datos

RGPD

Inteligencia artificial y redes neuronales

Ataques a los principales administradores

Redes sociales y servicios de mensajería

Ataques a la cadena de suministro

Industrial cybersecurity

Seguridad de las tarjetas bancarias y PCI DSS

Cómo responder ante incidentes

Vishing

Dispositivos móviles

¹ Investigación de Kaspersky Automated Security Awareness Platform, 2025

Forma, evalúa y refuerza la concienciación de los empleados en materia de seguridad gracias a nuestra experiencia internacional y nuestra flexibilidad

Kaspersky ASAP ofrece tres planes adaptados a organizaciones de cualquier tamaño y nivel de cultura de seguridad.

		Essential	Proactive	Advanced
		Ideal para equipos pequeños	Ideal para empresas en crecimiento	Ideal para empresas con requisitos específicos y una cultura de seguridad consolidada
		Formación en concienciación sobre seguridad adaptada a los requisitos normativos	Formación y evaluación proactivas en concienciación sobre seguridad	Formación personalizada y de gran impacto en concienciación sobre seguridad
Phishing	Evalúa la preparación de los empleados frente a los ciberataques mediante simulaciones de phishing realistas y personalizables	●	●	●
Curso rápido	Lecciones interactivas que desarrollan habilidades prácticas para hacer frente a las amenazas relacionadas con el factor humano y garantizan que tu organización cumpla con la normativa	●	●	●
Curso principal	Formación en concienciación sobre seguridad totalmente automatizada y adaptada a los niveles de riesgo, con microaprendizaje y refuerzo de habilidades		●	●
Personalización de contenido	Módulos personalizables, pruebas, páginas y dominios de phishing, y mucho más			●
Despliegue local	Opción de implementar la solución en tu propia infraestructura para mantener un control total sobre los datos confidenciales, las integraciones y el cumplimiento normativo			●

Una solución fácil de administrar para organizaciones de cualquier tamaño



Incorporación sencilla

Inscripción rápida en línea y acceso a la versión de prueba para un máximo de cinco usuarios durante dos meses. Incluye una guía de inicio y asistencia en línea



Automatización completa

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



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



Soporte multiinquilino y funciones de administración 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

Organización por función, departamento o perfil de riesgo



Informes claros y adaptados a las necesidades de los ejecutivos

Los paneles 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



Opciones de implementación flexibles

Disponible como plataforma de SaaS o instalación local



Inscripción sin complicaciones

Se integra con Active Directory y SSO



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 escenarios específicos de cada sector con incorporaciones continuas



IT



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

Kaspersky Interactive Protection Simulation

KIPS aumenta la concienciación sobre los riesgos y desafíos asociados al uso de todo tipo de sistemas de TI y 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 de cada sector exponen a los participantes a las técnicas de ataque modernas observadas por los expertos de Kaspersky en campañas activas, entre las que se incluyen los ataques a la cadena de suministro, el aprovechamiento del acceso de terceros, la ingeniería social y el software malicioso. 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.

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 en vivo para incluir a equipos remotos en 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 tu red, los incidentes pasados o las amenazas específicas de tu sector



Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online (CITO) es un programa de formación interactivo dirigido a especialistas en servicios de asistencia técnica, administradores de sistemas y miembros no especializados de equipos de seguridad de TI. Permite desarrollar habilidades prácticas para detectar ciberataques ocultos en incidentes cotidianos relacionados con el ordenador, recopilar datos relevantes y actuar como primera línea de ciberdefensa.

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

Habilidades prácticas de respuesta ante incidentes y de refuerzo de la seguridad:



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



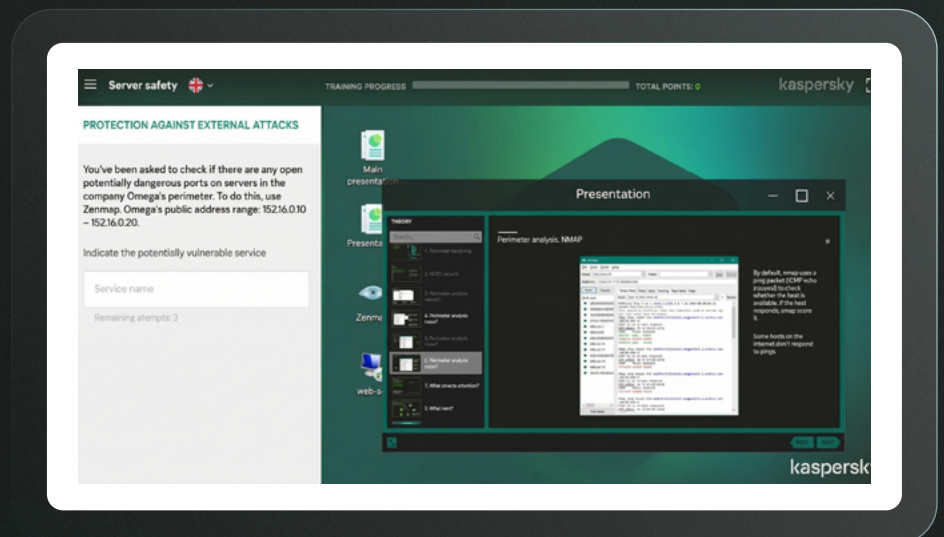
Aplica herramientas y técnicas reales para fortalecer la seguridad de la infraestructura de TI e investigar los incidentes de manera eficaz



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



Formación de Kaspersky para ejecutivos

Impulsa una cultura de seguridad desde la dirección al mostrar cómo las decisiones de los ejecutivos influyen directamente en la postura de seguridad, el cumplimiento normativo y la resiliencia de la organización 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. 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

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 dirigen los líderes, cómo se diseñan los procesos y cómo la tecnología lo hace todo posible.



El personal y su comportamiento



El liderazgo y la cooperación

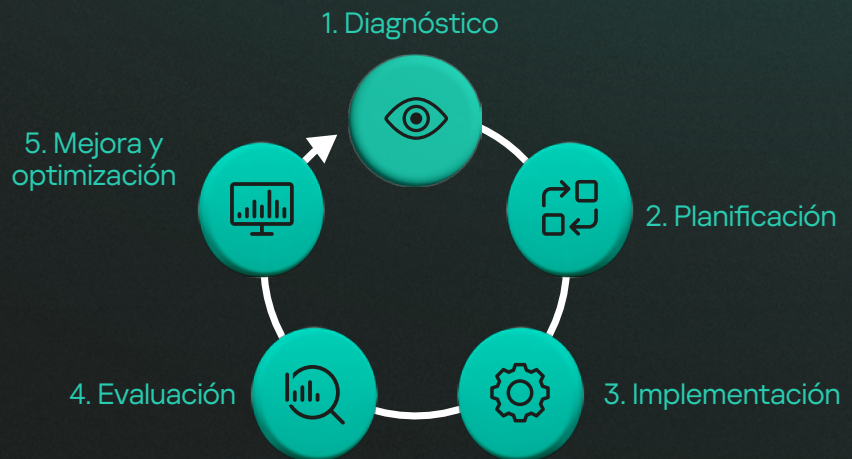


La integración operativa



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 siguen 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

Empieza tu prueba gratuita y evalúa ahora mismo tu nivel de cultura de seguridad



Kaspersky Security Awareness

Ten cuidado.
Mantente a salvo.

www.kaspersky.es

© 2026 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas
pertenecen a sus respectivos propietarios.

#kaspersky
#truetobusiness