Kaspersky ASAP: Kaspersky Automated Security Awareness Platform

Gestión sencilla y eficiente para organizaciones de cualquier tamaño

www.kaspersky.es/awareness
asap.kaspersky.com
#truecybersecurity

Kaspersky ASAP: Kaspersky Automated Security Awareness Platform

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.

Los errores humanos suponen el mayor riesgo cibernético actual

72 000 € por pyme
Impacto financiero medio de los ataques causados por empleados descuidados o desinformados[1]

87 500 € por pyme
Impacto financiero de los ataques causados por phishing/ingeniería social[1]

350 € por empleado al año
Coste promedio de los ataques de phishing (los otros tipos de ciberamenazas están excluidos de este total)[2]

El 52 % de todas las organizaciones
señalaron las acciones descuidadas de empleados/usuarios como el mayor problema en su estrategia de seguridad de IT[1]

Barreras para el lanzamiento del programa de concienciación de seguridad eficiente

Si bien las empresas están empezando a aplicar programas de concienciación sobre ciberseguridad, muchas de ellas no están satisfechas con el proceso y los resultados. Todo esto supone un desafío para las pequeñas y medianas empresas que generalmente no tienen ni experiencia ni recursos formados.

No saben cómo establecer objetivos y planificar la formación

Se tarda demasiado tiempo en gestionar la formación

Los informes no ayudan en el control de objetivos

Los empleados no valoran el programa → no desarrollan las habilidades

Incluso las organizaciones con equipos formados tienen a menudo dificultades para lograr una verdadera mejora en el comportamiento de los usuarios como resultado de las formaciones en concienciación en materia de seguridad.

Muchas empresas eligen aplicar un único esfuerzo educativo ("todo sobre ciberseguridad en 1 hora") o bien programas de formación profesional después de los cuales, sin embargo, solo utilizan algunas funciones e instrumentos básicos. Este programa normalmente consiste en una serie de campañas al año de ataques simulados de phishing y algunas lecciones de introducción, ya que los demás elementos del programa son demasiado difíciles de ejecutar y gestionar. De cualquier manera, los empleados no obtienen las habilidades sólidas necesarias para crear una cultura cibersegura para su organización.

[1] "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab y B2B International, junio de 2017

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

Gestión de la concienciación sencilla y eficiente para organizaciones de cualquier tamaño

Kaspersky Lab presenta Automated Security Awareness Platform, la base de la pirámide de formación de Kaspersky Security Awareness.

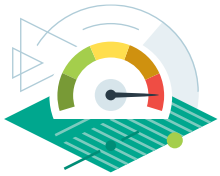
La plataforma es una herramienta online para que los empleados adquieran unas sólidas habilidades prácticas relativas al mundo cibernético a lo largo del año. No se requieren ni recursos específicos ni ningún tipo de logística para el lanzamiento y la gestión de la plataforma; además, aporta ayuda incorporada a la organización en todas las etapas del camino hacia la seguridad cibernética en el entorno corporativo:

Paso 1:

Establecimiento de objetivos formativos y justificación de un programa

- Fije objetivos en comparación con otras empresas del mercado
- Defina el equilibrio entre el nivel de competencia en ciberseguridad deseado para cada grupo de empleados y el tiempo de aprendizaje total necesario para alcanzarlo

Paso 2:



Garantía de que todos los empleados están formados de la mejor forma posible

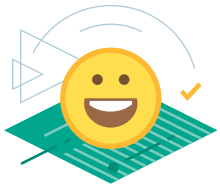
- Utilice la gestión automática del aprendizaje, que permite formar a cada empleado para que alcance el nivel de aptitudes en seguridad adecuado para su perfil de riesgo
- Asegúrese de reforzar las habilidades adquiridas para evitar que se olviden
- Forme a los empleados de manera individual y adaptada a su ritmo para evitar el exceso de formación y el desinterés

Paso 3:

Seguimiento del progreso con análisis e informes prácticos

- Realice un seguimiento directo de datos, tendencias y previsiones
- Utilice previsiones en tiempo real de la evolución y la distancia hasta el objetivo anual de formación
- Aborde aspectos conflictivos antes de que se conviertan en problemas (por ejemplo, puede aprovechar la información sobre las unidades organizativas que necesitan más atención para conseguir los resultados esperados)
- Compare resultados provisionales con los datos globales de Kaspersky Lab

Paso 4:



Garantía de la valoración de la formación y consecuentemente su eficiencia

- Fomente la participación de los empleados con ejercicios prácticos e interactivos
- Ofrezca situaciones de aprendizaje que se correspondan con las tareas cotidianas de los participantes
- Evite la sobrecarga por exceso de información y formación

Gestión del programa: sencillez mediante una automatización completa

Iniciar el programa en 10 minutos

- Establecer objetivos basados en estándares del sector
- Empezar la formación
- Pague sólo por los usuarios activos (aquellos que están aprendiendo)

La plataforma se adapta al ritmo y la capacidad de aprendizaje de cada empleado

- La plataforma se asegura automáticamente que el usuario aprende y supera las pruebas sobre los fundamentos antes de avanzar más en el estudio
- La dirección no necesita dedicar tiempo al análisis del progreso individual y a los ajustes manuales

Benefíciese de los planes de formación específicos para cada perfil de riesgo

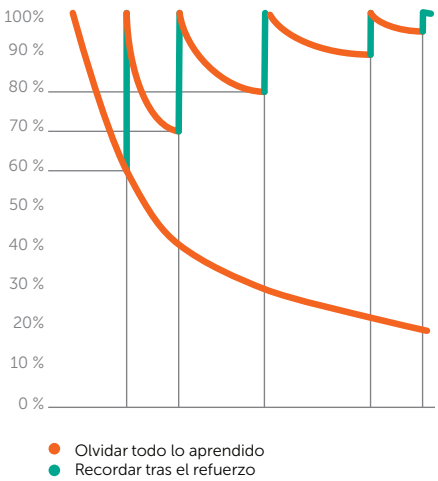
- Utilice las reglas automatizadas para asignar los empleados a un determinado grupo según el nivel formativo deseado. El nivel formativo esperado depende del riesgo que pueda entrañar el puesto de un empleado concreto para la empresa. A mayor riesgo, mayor debe ser el nivel formativo. Por ejemplo, los puestos de IT o de contabilidad suelen conllevar más riesgos que otros trabajadores.
- Cada grupo de usuarios estudia el material únicamente hasta el nivel que verdaderamente necesita, sin dedicar tiempo excesivo a la formación.

Obtenga informes procesables en cualquier momento

- Aproveche los paneles con toda la información necesaria para calcular el progreso
- Obtenga sugerencias sobre qué hacer para mejorar los resultados
- Compare los resultados con referentes mundiales/de la industria

La curva del olvido (Ebbinghaus)

El refuerzo reiterado ayuda a desarrollar unas habilidades sólidas.



Eficacia formativa: microaprendizaje continuo

Las habilidades aumentan por niveles, desde el más sencillo hasta el más avanzado. La plataforma reasigna automáticamente más tareas a quienes no completaron un nivel anterior. De este modo, se garantiza una gran capacidad de retención y se evita que se olvide todo lo que se ha aprendido.

Microaprendizaje

- El contenido está especialmente concebido para el microaprendizaje (de 2 a 10 minutos), para evitar clases largas y aburridas.

Conjunto completo de herramientas para cada tema de seguridad

- Cada nivel incluye: Lección interactiva y vídeo → refuerzo → evaluación (prueba o ataque de phishing simulado)

Cada tema consta de varios niveles que detallan las habilidades específicas de seguridad. Los niveles se definen según los grados de riesgo que se ayudan a eliminar: Normalmente, el nivel 1 es suficiente para proteger de ataques sencillos y masivos, mientras que, para la protección ante ataques más sofisticados y dirigidos, se necesita alcanzar niveles posteriores.

Temas de formación*

- Correo electrónico
- Navegación web
- Contraseñas
- Redes sociales y programas de mensajería
- Seguridad para PC
- Dispositivos móviles
- Datos confidenciales
- Datos personales o GDPR
- Ingeniería social
- Seguridad en el hogar y en desplazamientos

Ejemplo: Habilidades de formación en el tema de "navegación web"

Principiante para evitar ataques (baratos y fáciles) en masa	Elemental para evitar ataques en masa en un perfil específico	Intermedio para evitar ataques dirigidos bien preparados	Avanzado para evitar ataques dirigidos
13 habilidades, que incluyen: - Configurar su PC (actualizaciones, antivirus) - Ignorar sitios web obviamente maliciosos (aquellos que piden actualizar el software, optimizar el rendimiento del PC, enviar SMS, instalar reproductores, etc.) - No abrir nunca archivos ejecutables desde sitios web	**20 habilidades, que incluyen:** - Suscribirse e iniciar sesión sólo en sitios de confianza - Evitar los enlaces numéricos - Introducir la información confidencial sólo en sitios de confianza - Reconocer los signos de un sitio web malicioso	**14 habilidades, que incluyen:** - Reconocer enlaces falsos - Reconocer los archivos y las descargas maliciosas - Reconocer software malicioso	**13 habilidades, que incluyen:** - Reconocer los enlaces falsos sofisticados (incluidos los enlaces con un aspecto similar al de la empresa, enlaces con redirección) - Evitar los sitios de black SEO - Cerrar la sesión una vez se ha terminado - Configuración avanzada de PC (desactivar Java, adblock, noscript, etc.)
	+ refuerzo de las habilidades elementales	+ refuerzo de las habilidades anteriores	+ refuerzo de las habilidades anteriores

Puntos clave del tema: enlaces, descargas, instalaciones de software, suscripción e inicio de sesión, pagos, SSL

* La lista definitiva de los temas formativos está sujeta a cambios.

Idiomas

A otoño de 2018, la plataforma está disponible en los siguientes idiomas*:
- Inglés
- Alemán
- Italiano
- Ruso

Los siguientes serán:
- Árabe
- Francés
- Español

Además, se añaden nuevos idiomas regularmente para garantizar la formación completa y eficiente en todas las regiones.

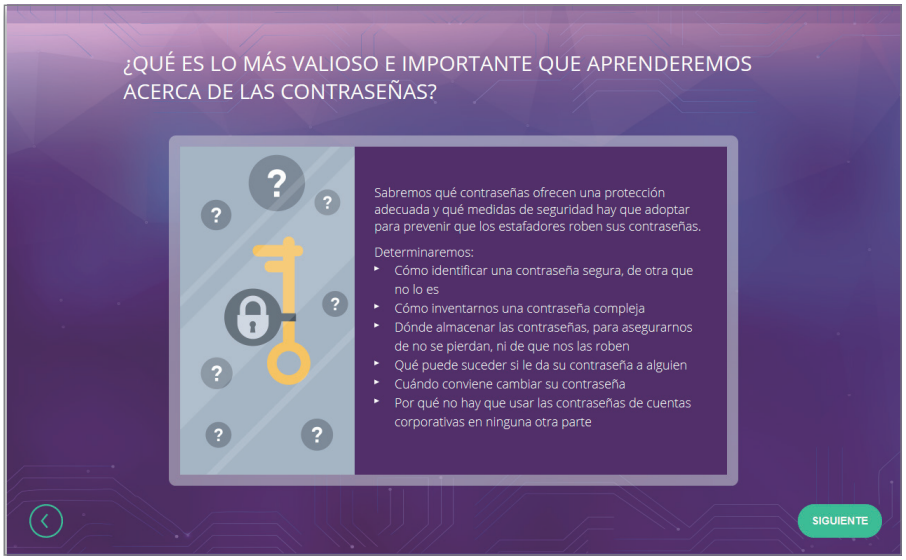
Gamificación y relevancia en la vida real para garantizar la eficiencia

El contenido de la plataforma se basa en principios de simulación que muestran eventos de la vida real y resaltan la importancia personal de ciberseguridad para los empleados. La plataforma se centra en la formación de habilidades, y no solo en proporcionar conocimientos, por lo que los ejercicios prácticos y las tareas relacionadas con el empleado son la base de cada módulo.

Los módulos combinan diferentes tipos de ejercicios para mantener a los usuarios interesados y atentos, y para motivarlos a aprender y adquirir una conducta segura.

El estilo visual y los textos no solo se traducen a diferentes idiomas, sino que se ajustan para reflejar las culturas y las actitudes locales.

Tareas basadas en la simulación y ejercicios para desarrollar habilidades prácticas y mantener a los usuarios entretenidos y motivados



* El orden y los tiempos finales de las variantes locales pueden variar

Kaspersky® Security Awareness

Kaspersky Lab ha lanzado una familia de productos de formación gamificada por ordenador que utilizan las técnicas modernas de aprendizaje y abordan todos los niveles de la estructura empresarial. Este enfoque ayuda a crear una cultura de ciberseguridad colaborativa que genera un nivel autosuficiente de ciberseguridad en toda la organización.

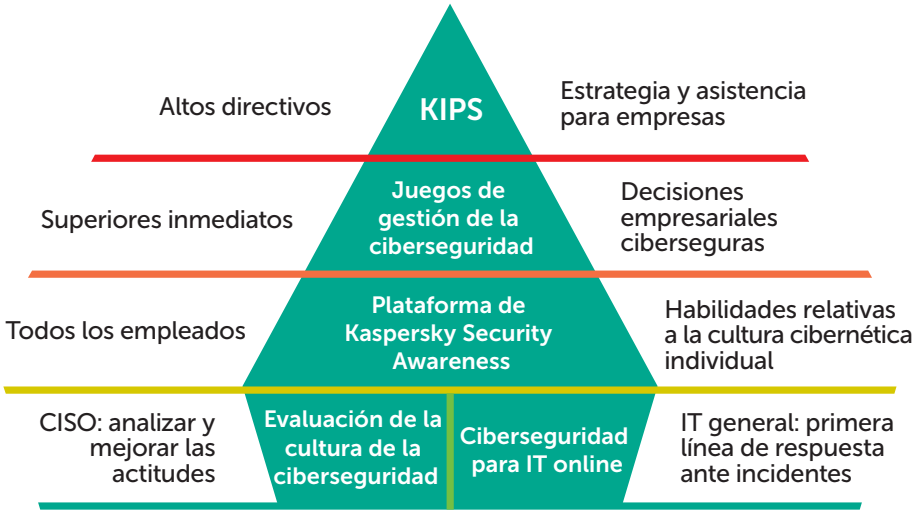
Hasta un
90 %
de reducción en el número total de incidentes

Un mínimo del
50 %
de reducción del impacto económico de los incidentes

Hasta un
93 %
de probabilidad de que el conocimiento se aplique en el trabajo diario

Más de
30 veces
de retorno de la inversión en seguridad

La friolera del
86 %
de participantes dispuestos a recomendar la experiencia



Definición de objetivos y elección de un programa

- Establecimiento de objetivos basado en los datos globales
- Datos comparativos frente al resto del mundo/los promedios del sector

Gestión del aprendizaje

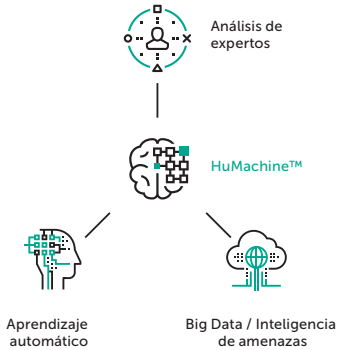
- Automatización del aprendizaje
- Rutas de aprendizaje autoajustables
- Cálculo de tiempo invertido

Informes y análisis

- Informes procesables en cualquier momento
- Análisis de la capacidad de mejora efectuados sobre la marcha

Reconocimiento y eficiencia del programa

- Ejercicios prácticos
- Prevención del cansancio y la sobrecarga por exceso de información
- Transmisión de un nivel alto de conocimiento y retención de capacidades



Kaspersky Lab
Concienciación sobre seguridad: **www.kaspersky.es/awareness**
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.lat/**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.es