

Gestión sencilla  
y eficaz para  
organizaciones  
de cualquier  
tamaño

# Kaspersky ASAP: Automated Security Awareness Platform

kaspersky

BRING ON  
THE FUTURE



Kaspersky  
Automated Security  
Awareness Platform

# Kaspersky ASAP: Automated Security Awareness Platform

Más del 80 % de los ciberincidentes se debe a errores humanos, y las empresas pierden millones en la recuperación tras incidentes relacionados con los empleados. Sin embargo, la eficacia de los programas de formación tradicionales destinados a evitar estos problemas es limitada, además de que no suele inspirar ni estimular el comportamiento necesario.

Los errores humanos suponen el mayor riesgo cibernético actual

**1 057 000 \$**

**por organización empresarial**

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

**98 000 \$**

**por pyme**

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

**52 %**

**de las empresas**

considera a los empleados la mayor amenaza para la ciberseguridad empresarial\*\*

**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\*\*\*

## Barreras para el lanzamiento de un programa de concienciación sobre seguridad eficaz

Aunque las empresas están dispuestas a implementar programas de concienciación sobre la seguridad, muchas no están satisfechas ni con el proceso ni con los resultados. Este aspecto supone un desafío especialmente para las pequeñas y medianas empresas, que normalmente no cuentan ni con la experiencia ni con los recursos necesarios.

**No es eficaz para los estudiantes:**



Se considera un trabajo pesado, difícil, aburrido e irrelevante

**Una carga administrativa:**



¿Cómo crear un programa y establecer objetivos?



Se dicta qué no hacer en lugar de explicar las buenas pautas



¿Cómo gestionar las asignaciones de formación?



Los conocimientos no se retienen



¿Cómo controlar el progreso?



La lectura y la escucha no son tan eficaces como la práctica



¿Cómo implicar plenamente a las personas en la formación?

\* Informe: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky, 2019

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

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

# Gestión de la concienciación sencilla y eficaz para organizaciones de cualquier tamaño

Presentamos Automated Security Awareness Platform, la base del portfolio de formación de Kaspersky Security Awareness.

La plataforma es una herramienta online con la que los empleados pueden adquirir unas sólidas habilidades prácticas relativas al mundo cibernético a lo largo del año. No se requieren ni recursos especiales 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 ciberseguridad en el entorno corporativo.

## Cómo evaluar un programa de concienciación

Uno de los criterios más importantes a la hora de elegir un programa de concienciación es su eficacia. Con ASAP, la eficacia está integrada en el contenido y la gestión de la formación. El contenido de la plataforma se basa en un modelo de competencias que consta de 350 habilidades de ciberseguridad prácticas y esenciales que todos los empleados deben poseer. Si no cuentan con estas habilidades, ya sea por ignorancia o negligencia, los empleados pueden dañar la empresa.

## Formación eficaz

### Coherente

- Contenido estructurado y bien diseñado.
- Lecciones interactivas, refuerzo constante, pruebas, ataques de phishing simulados para garantizar la aplicación práctica de los conocimientos.

Los materiales de formación y su estructura se organizan de acuerdo con las particularidades de la memoria humana, nuestra capacidad para absorber y retener información.

### Práctica y atractiva

- Es relevante para la vida laboral diaria de los empleados.
- Conocimientos que se pueden poner en práctica de inmediato.

Dar ejemplos de situaciones reales en las que los empleados se pueden reconocer a sí mismos contribuye a la que estos se impliquen en el aprendizaje y a que retengan la información.

### Positiva

- Le da un matiz proactivo al comportamiento seguro.
- Explica "por qué" y "cómo" en lugar de los tabús.

Un exceso de reglas y restricciones puede provocar descontento, mientras que unas explicaciones y convicciones en consonancia con lo que piensan las personas contribuyen de forma natural a que se apliquen los nuevos métodos y a que cambie el comportamiento.

## Gestión sencilla

### Administración sencilla

La gestión del aprendizaje totalmente automatizada aporta a todos los empleados el nivel de conocimientos de seguridad adecuado para su perfil de riesgo, sin la necesidad de que el administrador de la plataforma tenga que intervenir.

### Control sencillo

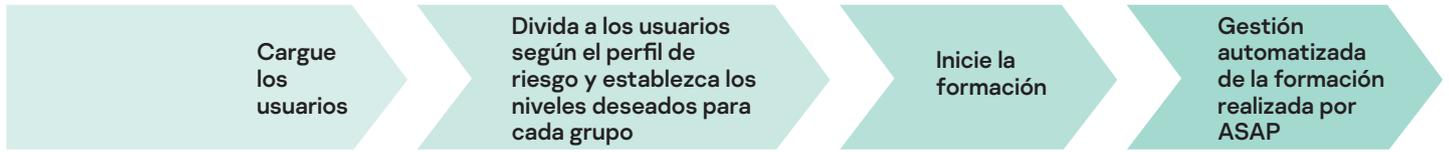
Panel "todo en uno" e informes procesables.

### Participación sencilla

La plataforma envía automáticamente invitaciones y correos electrónicos motivadores, así como informes semanales de estudiantes y administradores.

# Gestión de ASAP: sencillez mediante una automatización completa

## Inicie su programa en 4 sencillos pasos



Cargue los usuarios

Divida a los usuarios según el perfil de riesgo y establezca los niveles deseados para cada grupo

Inicie la formación

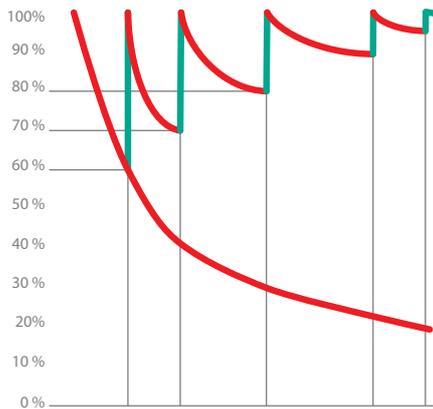
Gestión automatizada de la formación realizada por ASAP

Este es el único paso en el que el administrador debe pensar y tomar decisiones.

La plataforma crea un programa educativo para cada grupo, en función del ritmo y el nivel deseado, y proporciona recomendaciones e informes procesables.

### La curva del olvido (Ebbinghaus)

El refuerzo reiterado ayuda a desarrollar unas habilidades sólidas.



- Olvidar todo lo que se ha aprendido
- Recordar tras el refuerzo

### Se adapta al ritmo y la capacidad de aprendizaje de cada empleado

- La plataforma garantiza automáticamente que los usuarios aprendan los conceptos básicos y superen las pruebas sobre estos antes de avanzar al siguiente nivel.
- La dirección no necesita dedicar tiempo al análisis del progreso individual ni a los ajustes manuales.

### Beneficiarse de los planes de formación específicos para cada perfil de riesgo

Utilice las reglas automatizadas para asignar a los empleados a un determinado grupo según el nivel formativo deseado. Este nivel formativo deseado 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.

### Aprendizaje flexible

- El alcance de la formación es completamente flexible, al tiempo que se mantienen las ventajas de la gestión del aprendizaje secuencial y automatizada.
- Para cada grupo de formación, puede seleccionar:
  - Los temas que los estudiantes del grupo necesitan aprender (y omitir los que no desea enseñar en ese momento).
  - El nivel deseado que desea que alcancen los estudiantes para cada tema concreto. Los empleados no dedicarán su tiempo de trabajo a aprender temas irrelevantes.

### Obtenga informes procesables en cualquier momento

- Disfrute de paneles con toda la información necesaria para realizar un control.
- Obtenga sugerencias sobre cómo mejorar los resultados.
- Descargue informes desde la página principal con un solo clic y configure la frecuencia de con la que los recibe por correo electrónico.

# Metodología ASAP

## Aprendizaje progresivo y continuo

- De lo sencillo a lo más complejo, tema a tema y nivel a nivel para que la adquisición de conocimientos sea mayor.
- Ampliación y aplicación de los conocimientos adquiridos previamente en nuevos contextos.

## Contenido multimodal

- Cada nivel incluye una evaluación de refuerzo de lecciones interactivas (prueba y ataque de phishing simulado, si procede).
- Todos los elementos de formación respaldan la habilidad concreta que se enseña en cada unidad, de forma que las habilidades se dominen verdaderamente y pasen a formar parte del nuevo comportamiento deseado.
- La "curva del olvido" de Ebbinghaus: metodologías de aprendizaje basadas en las particularidades de la memoria humana.
- La repetición ayuda a afianzar hábitos seguros y evita el olvido.
- Refuerzo en cada módulo.

## Aprendizaje periódico

- La "curva del olvido" de Ebbinghaus: metodologías de aprendizaje basadas en las particularidades de la memoria humana.
- La repetición ayuda a afianzar hábitos seguros y evita el olvido.
- Refuerzo en cada módulo.

## Temas de formación

Cada tema consta de varios niveles que detallan las habilidades específicas de seguridad.

Los niveles se definen según los grados de riesgo que 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.

- Contraseñas y cuentas
- Correo electrónico
- Navegación web
- Redes sociales y programas de mensajería
- Seguridad para PC
- Dispositivos móviles
- Datos confidenciales\*
- GDPR\*

\* Se añadirá en el primer trimestre de 2020

## Ejemplo: Habilidades de formación en el tema "Navegación web"

<b>Principiante</b> Para evitar ataques en masa (baratos y fáciles)	<b>Elemental</b> Para evitar ataques en masa en un perfil específico	<b>Intermedio</b> Para evitar ataques dirigidos bien preparados	<b>Avanzada</b> Para evitar ataques dirigidos
<b>13 habilidades, que incluyen:</b> <ul style="list-style-type: none"><li>- Configurar su PC (actualizaciones, antivirus)</li><li>- Ignorar sitios web obviamente maliciosos (aquellos que piden actualizar el software, optimizar el rendimiento del PC, enviar SMS, instalar reproductores, etc.)</li><li>- No abrir nunca archivos ejecutables desde sitios web</li></ul>	<b>20 habilidades, que incluyen:</b> <ul style="list-style-type: none"><li>- Suscribirse e iniciar sesión sólo en sitios de confianza</li><li>- Evitar los enlaces numéricos</li><li>- Introducir la información confidencial sólo en sitios de confianza</li><li>- Reconocer las señales de que un sitio web es malicioso</li></ul>	<b>14 habilidades, que incluyen:</b> <ul style="list-style-type: none"><li>- Reconocer enlaces falsos</li><li>- Reconocer los archivos y las descargas maliciosas</li><li>- Reconocer software malicioso</li></ul>	<b>13 habilidades, que incluyen:</b> <ul style="list-style-type: none"><li>- Reconocer los enlaces falsos sofisticados (incluidos los enlaces con un aspecto similar al de la empresa, enlaces con redirecciones)</li><li>- Evitar los sitios de black SEO</li><li>- Cerrar la sesión una vez se ha terminado</li><li>- Configuración avanzada de PC (desactivar Java, adblock, noscript, etc.)</li></ul>
	+ refuerzo de 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

## Idiomas

Desde julio de 2019, la plataforma (tanto la interfaz de estudiante como la de administrador) está disponible en los siguientes idiomas:

- Árabe
- Neerlandés
- Inglés
- Francés
- Alemán
- Italiano
- Portugués
- Ruso
- Español

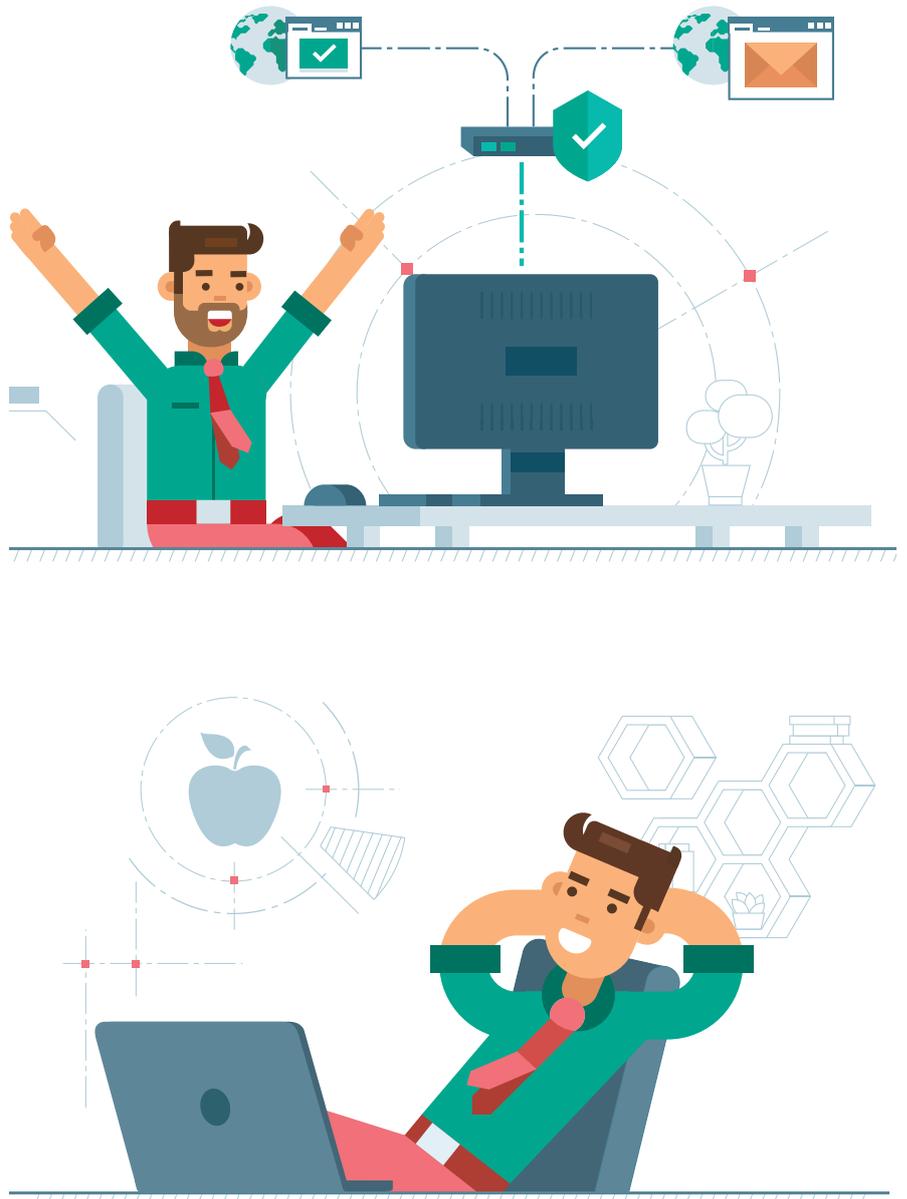
# El contenido estructurado y bien equilibrado y la relevancia en la vida real garantizan la eficacia

Los principios de aprendizaje utilizados en ASAP se basan en la metodología que tiene en cuenta las particularidades de la naturaleza humana, nuestra capacidad para percibir y absorber información. El contenido está lleno de ejemplos y casos reales que resaltan la importancia personal de la ciberseguridad para los empleados. La plataforma se centra en la adquisición de habilidades, y no solo en proporcionar información, por lo que los ejercicios prácticos y las tareas relacionadas con los empleados 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 distintas culturas y actitudes locales.

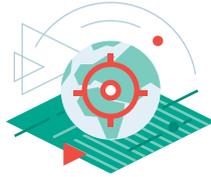
## Tareas basadas en la simulación y ejercicios para desarrollar habilidades prácticas y mantener a los usuarios entretenidos y motivados





# Kaspersky Security Awareness

## 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

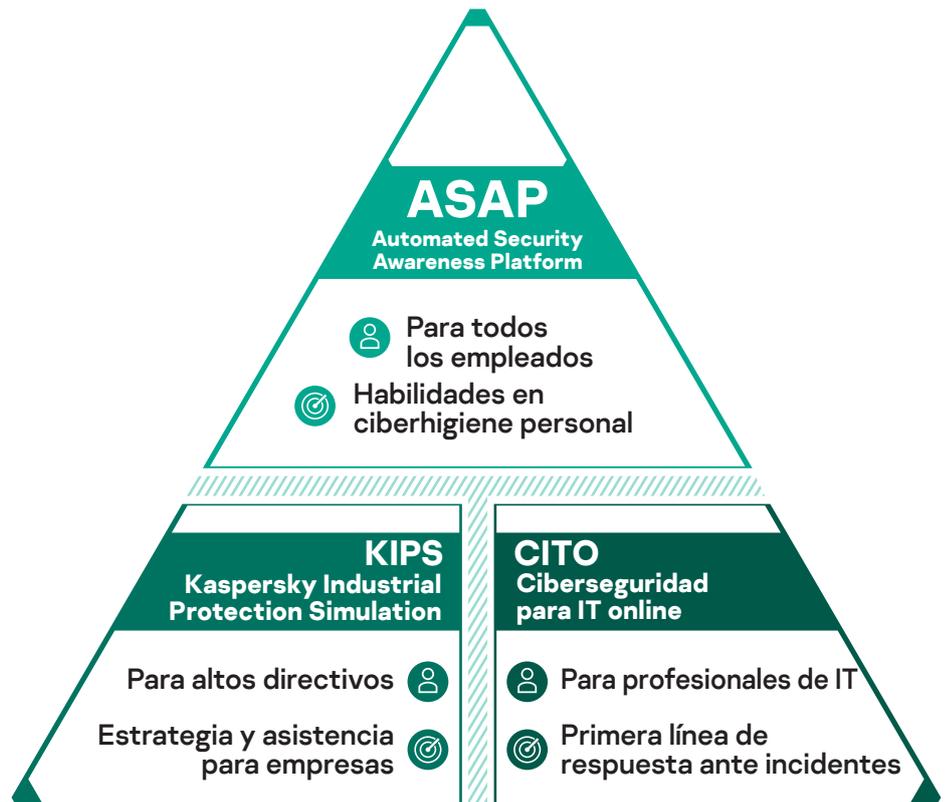
- De lo sencillo a lo más complejo.
- Ampliación y aplicación de conocimientos adquiridos previamente en nuevos contextos.



### Gestión y control sencillos

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

## Diferentes formatos de formación para diferentes niveles organizativos



---

Prueba gratuita de Kaspersky ASAP: [k-asap.com](https://k-asap.com)  
Ciberseguridad de empresa: [www.kaspersky.com/enterprise](https://www.kaspersky.com/enterprise)  
Kaspersky Security Awareness: [www.kaspersky.es/awareness](https://www.kaspersky.es/awareness)  
Noticias de seguridad de IT: [business.kaspersky.com](https://business.kaspersky.com)

[www.kaspersky.es](https://www.kaspersky.es)

**kaspersky** BRING ON  
THE FUTURE