KASPERSKY lab

# Kaspersky Security Awareness

Programas de formación online para todos los niveles organizativos

www.kaspersky.com/awareness
#truecybersecurity

# La forma más eficaz de diseñar una cultura cibersegura en su organización

Más del 80 % de los ciberincidentes se deben a errores humanos. Las empresas gastan millones para recuperarse de incidentes relacionados con su 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 el objetivo deseado.

**Los errores de los empleados son los responsables de la mayoría de los incidentes de ciberseguridad que se dan en las organizaciones de hoy en día.**

Los errores humanos pueden suponer un ciberriesgo importante para una organización, aun cuando se realicen programas de concienciación tradicionales:

**1 155 000 USD por empresa**: impacto económico medio de los ataques causados por descuidos de los empleados*

**101 000 USD por PYME**: impacto económico de los ataques causados por phishing o ingeniería social **(1,3 millones de dólares por empresa)***

**Hasta 400 USD por empleado al año**: coste medio de los ataques de phishing**

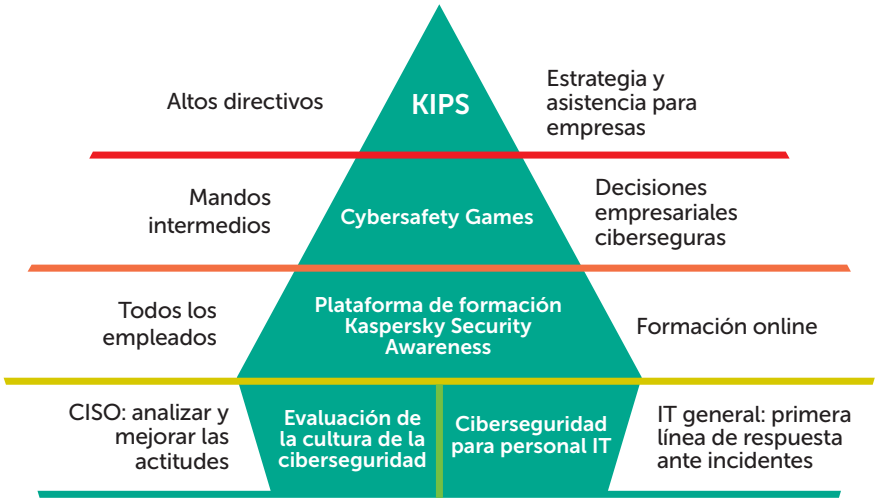
* Informe "Human factor in IT security: How Employees are Making Businesses Vulnerable from Within", International, junio de 2017

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

## La solución: la formación de Kaspersky Security Awareness

Kaspersky Lab ha lanzado una familia de productos de formación gamificada online que utilizan las técnicas más 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.

### Diferentes formatos de formación para diferentes niveles organizativos




## Un enfoque que ofrece resultados demostrados

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

Al menos un
**50 %**
de reducción en el impacto económico de los incidentes

Un alentador
**86 %**
de participantes recomendaría el programa

# Los empleados son un objetivo clave de los cibercriminales

A medida que las empresas son más conscientes de las amenazas de los ciberataques, las defensas técnicas se van fortaleciendo. Ahora es mucho más difícil acceder ilegalmente a las redes corporativas, y los hackers responden a esto creando nuevos métodos de acceso a datos protegidos. Sus esfuerzos apuntan al nuevo eslabón más débil de la seguridad cibernética corporativa: los empleados.[1]

**Plataforma de formación de habilidades para empleados: formación gamificada interactiva dirigida a los empleados con diferentes niveles de habilidades de ciberseguridad.**

La plataforma está disponible en 281 idiomas.

Gracias al uso de la plataforma, y a la Guía de prácticas recomendadas de Kaspersky Lab, las empresas pueden establecer e implementar un plan educativo potente, continuo y evaluable en materia de ciberseguridad. En él, se anima a los empleados a pasar de los conceptos de seguridad sencillos a los más complejos, en función de su labor y responsabilidad, y del panorama de amenazas predominante.

Vea nuestra demostración interactiva en www.kaspersky.com/demo-sa


## Una plataforma de formación de habilidades para empleados que desarrolla el comportamiento ideal ante la ciberseguridad

La plataforma consigue, a través de típicos escenarios y situaciones, simulaciones de ciberataques y diferentes explicaciones, hacer entender las amenazas potenciales. Además, proporciona las habilidades necesarias para tratarlas. El aprendizaje online permite a los empleados practicar y estudiar a través de un portal interactivo.

### Módulos de formación interactivos

- Amenos y cortos • Basados en ejercicios correlacionados • Inscripción automática que refuerza habilidades específicas • 29[2] módulos que cubren todas las áreas de la seguridad

### Evaluación de conocimientos

- Incluye evaluaciones aleatorias o predefinidas, preguntas definidas por el cliente y opciones de dificultad personalizables • Abarca una amplia gama de escenarios de seguridad • La amplia biblioteca de preguntas al azar elimina la posibilidad de hacer trampas

### Ataques de phishing simulados

- Tres tipos de ataques de phishing con una amplia gama de plantillas y niveles de dificultad
- "Momentos de formación" que aparecen cada vez que los empleados abren correos electrónicos de phishing
- Plantillas personalizables
- Asignación automática de módulos de formación que cubren las lagunas de conocimiento identificadas a través de casos de ataques simulados

### Informes y análisis

- Proporciona estadísticas de la organización en conjunto o por departamento, ubicación y puesto, así como a nivel individual
- Supervisa la dinámica y los niveles de habilidades de los empleados
- Admite la exportación de datos en un número de formatos para el sistema de gestión de aprendizaje (LMS) del cliente

### Principales ventajas para el cliente:

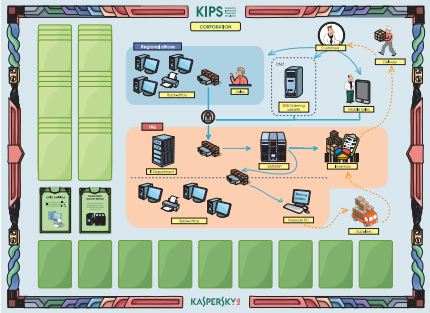
- **Ahorro de tiempo:** se pueden asignar módulos de formación específicos a los trabajadores en función de su departamento y nivel de experiencia; todo el mundo puede aprender a su propio ritmo.
- **Gamificación e interactividad:** sin explicaciones aburridas, es un aprendizaje interactivo y práctico.
- **Proporciona habilidades concretas, no solo conocimiento:** combina materiales educativos y pruebas con situaciones reales simuladas.
- **Proporciona datos comparativos:** compare el rendimiento de su empresa con el del sector en general.
- **No se necesitan recursos adicionales:** la formación se puede realizar en el lugar de trabajo del cliente, sin que se requieran habilidades, formación o recursos adicionales.

1 Mustard IT, 19 de agosto de 2017
2 A octubre de 2017

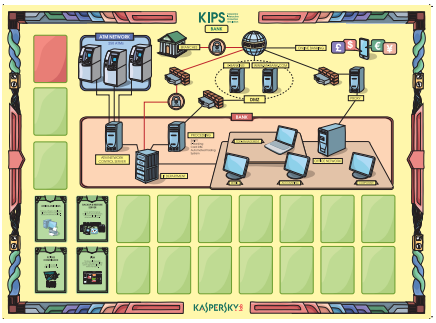
**La formación en KIPS está dirigida** a altos directivos, expertos en sistemas empresariales y profesionales de IT, con el fin de aumentar su concienciación sobre los riesgos y problemas de seguridad que sufren los sistemas informatizados modernos

### Algunos escenarios de KIPS:

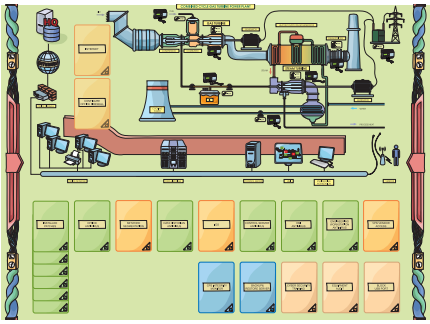
**Empresarial**



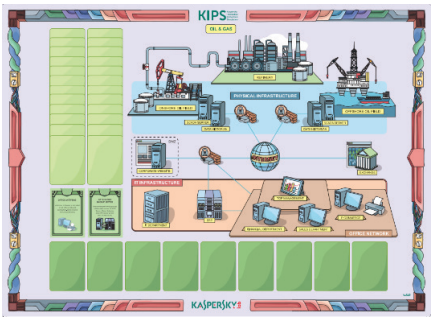
**Bancario**



**Central eléctrica**



**Petróleo y gas**



**KIPS online:**

- Idóneo para empresas globales
- Hasta 300 equipos a la vez
- Los distintos equipos pueden elegir interfaces de juego en diferentes idiomas

# La formación en Kaspersky Interactive Protection Simulation (KIPS) fomenta la comprensión y el apoyo a la ciberseguridad

## Qué es KIPS

KIPS es un juego de rol en equipos que simula un entorno empresarial donde los participantes deben tratar una serie de ciberamenazas inesperadas sin olvidarse de maximizar sus beneficios y mantener la confianza del mercado.

La idea consiste en crear una estrategia de ciberdefensa seleccionando los mejores controles proactivos y reactivos disponibles.

## KIPS resulta extraordinariamente eficaz porque:

- Ofrece un nuevo enfoque viable a la ciberseguridad
- Es divertido, atractivo y rápido (2 horas)
- La cooperación se basa en el trabajo en equipo
- Fomenta las habilidades de iniciativa y análisis en un entorno competitivo
- Permite realizar descubrimientos y cometer errores a la hora de desarrollar un programa de ciberseguridad y un comportamiento ciberseguro, y analizarlo todo de forma segura a través del juego.

## La experiencia KIPS:

- Muéstrese preparado para las amenazas emergentes: aprenda cómo operan técnicamente los criminales (inteligencia frente a amenazas) y entienda sus metas.
- Descubra cómo combinar la respuesta ante incidentes con la prevención de incidentes.
- Vea qué pasa cuando se olvida de configurar los controles de seguridad correctamente.
- Preste atención a las alertas desde un punto de vista global que lo tenga en cuenta todo: la seguridad, los recursos de IT y su empresa.

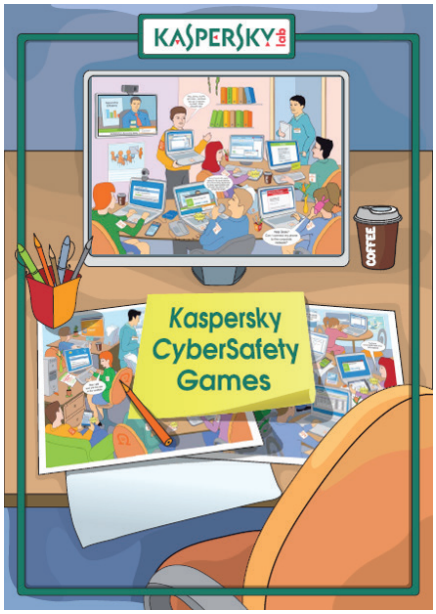
## Hay disponibles escenarios relacionados con el sector (todos como KIPS Live y KIPS Online, con 10 idiomas admitidos)

- **Empresarial:** protección de la empresa frente a ransomware, amenazas avanzadas persistentes (APT), errores de seguridad de automatización, etc.
- **Bancario:** protección de entidades financieras frente a las APT de alto nivel que atacan los cajeros automáticos, servidores de gestión y sistemas empresariales.
- **Administración pública:** protección de servidores web públicos frente a ataques y exploits.
- **Central eléctrica o planta de tratamiento de aguas:** protección de sistemas de control industrial e infraestructura crítica.
- **Empresas de transporte:** protección de pasajeros y transporte de mercancías frente a Heartbleed, ransomware y APT.
- **Petróleo y gas:** análisis de la influencia de una amplia gama de amenazas, desde la destrucción de sitios web hasta ransomware actual y APT sofisticadas.

Cada escenario muestra a los participantes el verdadero papel de la ciberseguridad en lo referente a la continuidad y rentabilidad de la empresa, destacando los retos y amenazas emergentes, así como los típicos errores empresariales al desarrollar su ciberseguridad. Al mismo tiempo, fomenta la cooperación entre los equipos de seguridad y los comerciales, lo que ayuda a mantener la estabilidad de las operaciones y la sostenibilidad contra las ciberamenazas.

**Juegos de gestión de la ciberseguridad:** educación y motivación para los mandos intermedios

- Combina los juegos con una completa cobertura de los temas de seguridad, con ejemplos, explicaciones y ejercicios.
- Se basa en el software específico de juegos de gestión de la ciberseguridad, con un proceso de distribución de la formación fácil de gestionar.
- Se divide en módulos cortos, con un total de 4 horas.




# Cybersafety games garantía de decisiones empresariales ciberseguras

Este taller altamente interactivo (que combina formación impartida por instructor y formación online) permite a los mandos intermedios centrarse en la importancia de la ciberseguridad en sus trabajos y proporciona las competencias, los conocimientos y la visión esenciales para mantener unas prácticas de trabajo seguras en sus divisiones.

El mayor desafío del equipo de seguridad casi siempre reside en involucrar al equipo de gestión, es decir, a las personas que interactúan con los empleados diariamente y toman decisiones para la empresa.

Por este motivo, Kaspersky Lab ha desarrollado un **programa de formación que tiene el objetivo específico de convertir a los mandos intermedios en defensores y embajadores de la ciberseguridad.**

**Kaspersky CyberSafety Management Games proporciona a los responsables:**

- **Comprensión:** adopción interna de medidas de ciberseguridad como un conjunto de acciones importantes pero sencillas.
- **Supervisión:** visualización del proceso de trabajo diario desde el punto de vista de la ciberseguridad.
- **Toma de decisiones para la ciberseguridad:** consideraciones sobre ciberseguridad como parte integral de los procesos de negocio.
- **Refuerzo e inspiración:** los equipos departamentales reciben liderazgo y orientación influyentes.

Se puede calificar como una "formación de formadores" para los centros de formación de empresas que proporciona ventajas de implantación clave:

- Facilidad de distribución: los responsables de la formación sobre concienciación no tienen que ser expertos en seguridad.
- Facilidad de programación: se organizan sesiones cortas de formación modular dentro del horario de trabajo del empleado.

**La formación en ciberseguridad para personal IT está dirigida a los especialistas del servicio técnico, así como a los administradores de servicio local y de seguridad de IT general.**

**Formato de la formación**

La formación es totalmente online: los participantes solo necesitan tener conexión a Internet con el LMS y un navegador Chrome.

Cada uno de los 5 módulos comprende una breve introducción teórica, consejos prácticos, y entre 4 y 10 ejercicios (en cada uno de ellos se practica una habilidad específica y se muestra cómo utilizar las herramientas y software de seguridad de IT en el trabajo diario).

El estudio está ideado para realizarse a lo largo de un año. La tasa recomendada de progreso es de 1 módulo por semana. Cada módulo lleva unos 45 minutos.

La evaluación se realiza a través de una encuesta, en la nube, que los empleados completan en unos 15 minutos. Se tarda una media de 2 semanas en realizar la encuesta a todos los empleados.

El cliente recibe un informe consolidado de los resultados de la encuesta.

# Ciberseguridad para IT online

Formación interactiva para quienes forman parte de los departamentos de IT internos, que permite desarrolllar una ciberseguridad fuerte, así como habilidades de respuesta ante incidentes de primer nivel

Resulta imposible mantener una postura de ciberseguridad corporativa sólida, sin que todos los empleados relevantes hayan recibido la formación sistemática necesaria. La mayoría de las empresas proporcionan educación y formación en ciberseguridad en dos niveles: formación especializada para equipos de seguridad de IT, y concienciación general sobre la seguridad para los empleados que no pertenecen a IT. Ninguno de estos métodos funciona para la gran cantidad de personal de IT que no está directamente relacionado con la seguridad, pero cuyo puesto le ofrece una posición ideal para realizar importantes contribuciones específicas a la ciberseguridad corporativa.

## Respuesta ante incidentes de primer recurso

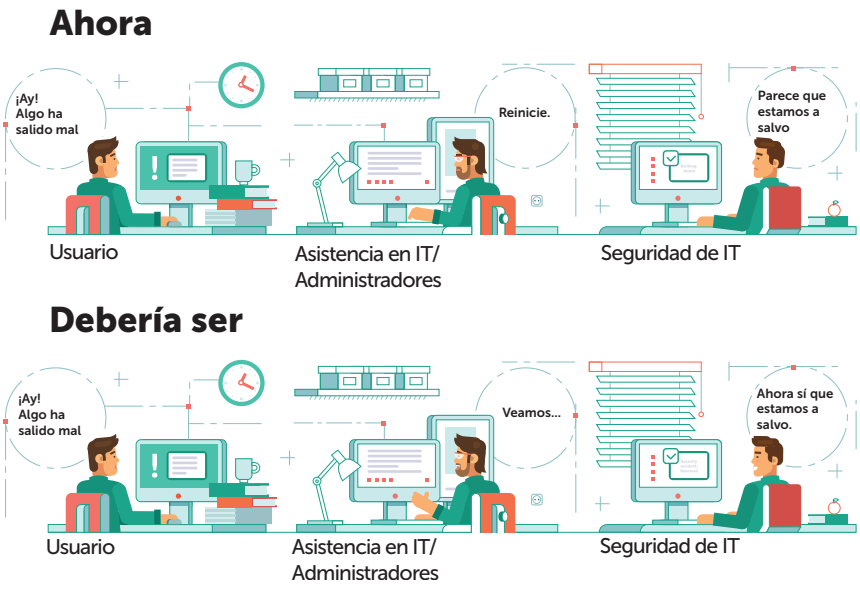
Kaspersky Lab ofrece la primera formación online del mercado para profesionales generales de IT empresarial.

El curso consta de 5 módulos:

- Software malicioso
- Programas y archivos potencialmente no deseados
- Conceptos básicos de investigación
- Respuesta ante incidentes de phishing
- Seguridad empresarial

## Este curso dota a los profesionales de IT con conocimientos prácticos que incluyen:

- Cómo reconocer un posible escenario de ataque en un incidente de equipo aparentemente benigno.
- Cómo recopilar datos de los incidentes para remitírselos a los equipos de seguridad de IT.
- Cómo detectar síntomas malintencionados, y consolidar así el papel de todos los miembros del equipo de IT como primera línea de defensa y seguridad.

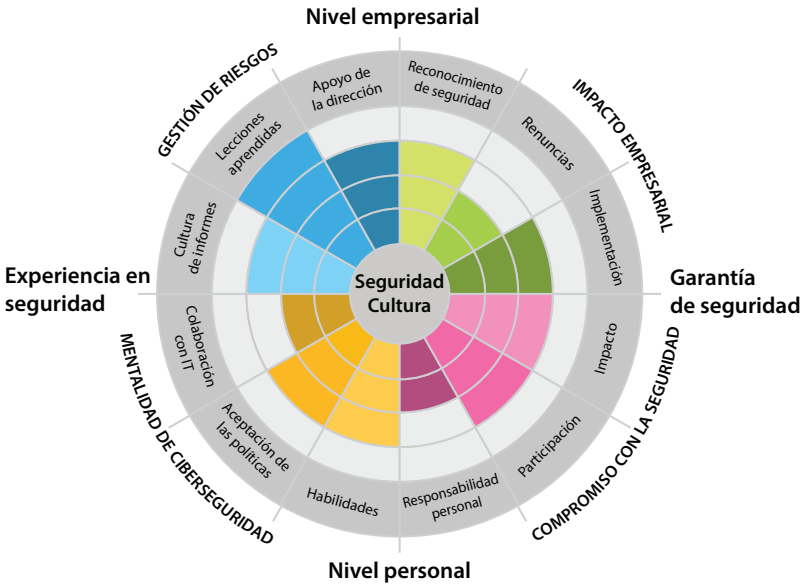


# Evaluación de la cultura de la ciberseguridad

La evaluación se ocupa de la cultura de la seguridad desde diferentes perspectivas:

- Nivel empresarial (dirección)
- Nivel individual (empleado)
- Disponibilidad de conocimientos especializados
- Garantía de seguridad como proceso

La evaluación de la cultura de la ciberseguridad analiza el comportamiento diario actual y la actitud hacia la ciberseguridad en todos los niveles de la empresa, mostrando cómo perciben los empleados sus diferentes aspectos.




Los resultados del informe pueden emplearse para reconocer las áreas en las que existe un desequilibrio y a las que debe prestarse atención, para justificar y alinear las prioridades en las actividades internas y externas del departamento de seguridad, como la concienciación y la formación, las comunicaciones internas, el intercambio de información y la colaboración en la empresa.

La cultura de la ciberseguridad incluye áreas de conocimiento, que serán evaluadas y medidas en conjunto en toda la organización. Los resultados de la evaluación dan pie a un debate sobre la función de la ciberseguridad para fomentar la eficiencia de la empresa:

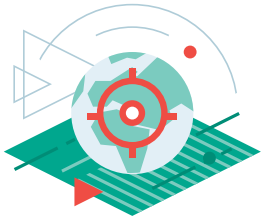
- Mentalidad de ciberseguridad (percepción de la seguridad y las políticas)
- Gestión de riesgos (orientación, comentarios, mejoras)
- Compromiso (actitud y comportamiento en relación con la seguridad)
- Impacto en el negocio (el equilibrio entre la seguridad y la eficiencia empresarial)

Tenga en cuenta que el informe sobre la cultura de la ciberseguridad no constituye una evaluación del nivel de madurez en cuanto a seguridad técnica de la empresa, ni tampoco una medida de la eficacia del departamento de seguridad.

Este informe revela cómo los empleados perciben la ciberseguridad, su forma de ver la cultura, las costumbres, los rituales y la práctica diaria de ciberseguridad, así como su percepción personal de diferentes aspectos de la seguridad corporativa. Esta percepción procede de diferentes prácticas y unidades de la empresa, y no simplemente de la actividad del departamento encargado de la gestión de riesgos o de seguridad.

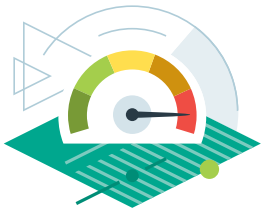
# Kaspersky Security Awareness: un nuevo enfoque del aprendizaje

## Factores diferenciadores clave



### Definición de objetivos y elección de un programa

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

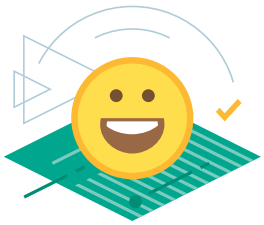


### Gestión del aprendizaje

- Aprendizaje automático
- Rutas de aprendizaje personalizables
- 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

- Formación gamificada
- Competencia y retos
- Prevención de sobrecarga

# Nuevo enfoque de eficacia demostrada

Retorno de la inversión más de

**30 veces**

superior gracias a la concienciación sobre la seguridad

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 %**

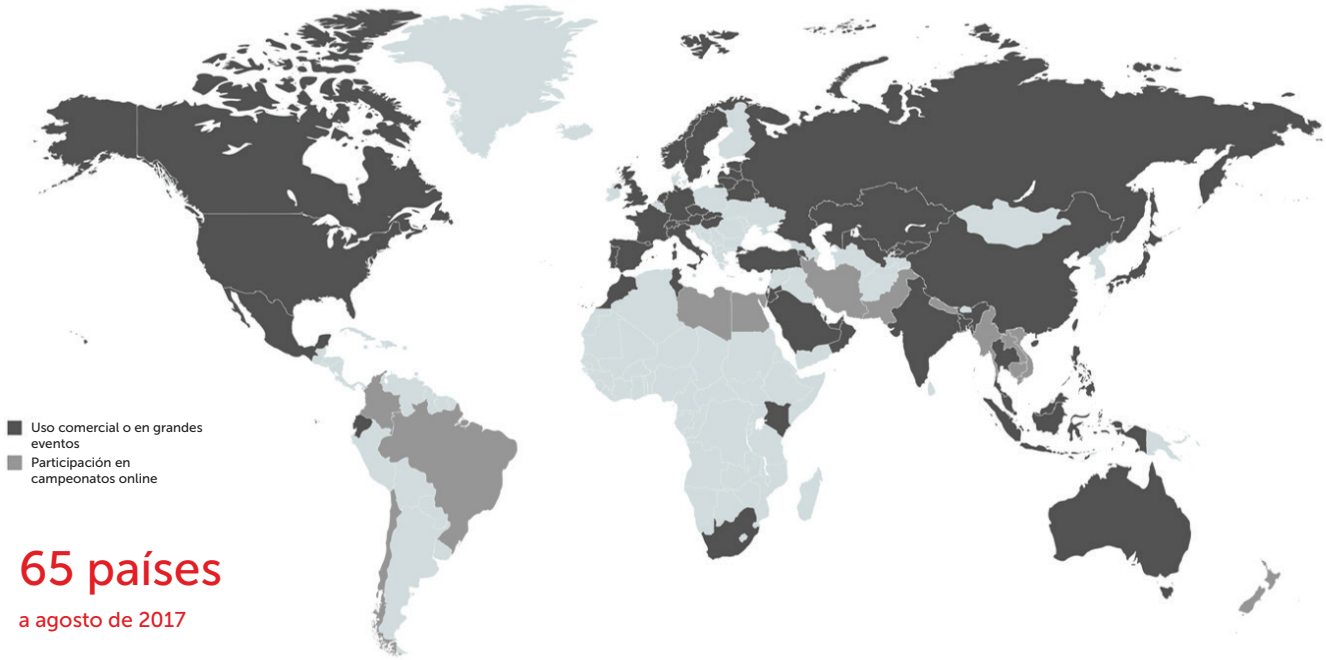
de probabilidad de que el conocimiento se aplique en el trabajo diario

La friolera del

**86 %**

de participantes dispuestos a recomendar la experiencia

# Kaspersky Security Awareness a nivel global




**65 países**

a agosto de 2017

Creado con mapchart.net

**www.kaspersky.es**



Kaspersky Lab Iberia
Ciberseguridad de empresa: **www.kaspersky.com/enterprise**
Kaspersky Security Awareness:
**www.kaspersky.com/awareness**
Demostración del producto: **www.kaspersky.com/demo-sa**