Capacitación efectiva para los empleados. Facilidad de uso para los gerentes.

k-asap.com/es

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky PREPARADOS PARA EL FUTURO

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 constituyen el mayor riesgo de ciberseguridad

1 315 000 $
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*

132 000 $
por pyme
El impacto económico promedio de una filtración de datos provocada por la pérdida física de dispositivos móviles de propiedad de la empresa, que exponen a la organización a riesgos*

El 50 %
de las empresas
informa haber experimentado amenazas causadas directamente por comportamientos indebidos del personal, lo cual las convierte en las amenazas más comunes para la seguridad de la TI*

El 43 %
de las pequeñas empresas
sufrió un incidente de seguridad a causa de infracciones de las políticas de seguridad de TI por parte de los empleados*

El 26 %
de los empleados
afirmó que su cuenta de correo electrónico personal tiene la misma contraseña que su cuenta del trabajo**

Barreras para el lanzamiento del programa de concienciación de seguridad eficiente

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.

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

Los conocimientos no se retienen

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

Una carga administrativa

¿Cómo crear un programa y establecer objetivos?

¿Cómo gestionar las asignaciones de formación?

¿Cómo controlar el progreso?

¿Cómo implicar plenamente a las personas en la formación?

* Informe: Informe "IT security economics 2021", de Kaspersky

** https://www.beyondidentity.com/blog/password-sharing-work

Gestión de la concienciación sencilla y eficiente 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.

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 más de 300 habilidades de ciberseguridad prácticas y esenciales que todos los empleados deben poseer.

Si educa a sus empleados acerca de los problemas relacionados con la ciberseguridad (si cambia sus actitudes y comportamientos) estará protegiendo su negocio y sus sistemas de IT.

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 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.

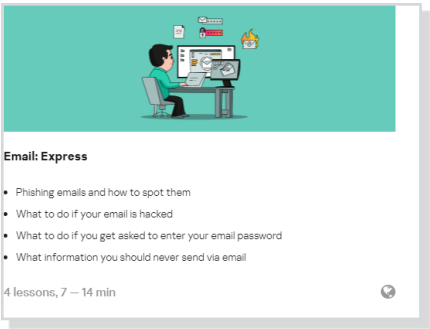
Gestión de ASAP: sencillez mediante una automatización completa

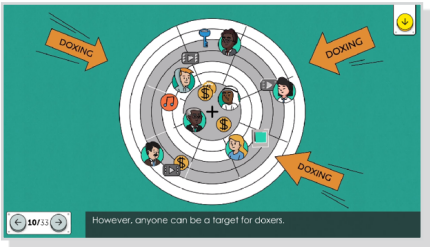
Inicie su programa en 4 sencillos pasos

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





Mejores principios de aprendizaje

Kaspersky ASAP está cambiando la forma de proporcionar contenido de aprendizaje de ciberseguridad. Ahora, puede elegir asignarles a los empleados un curso básico rápido, el cual lo ayudará a cumplir de inmediato con los requisitos reglamentarios de capacitación en ciberseguridad, o reforzar sus conocimientos, además de la opción de un curso completo, dividido en distintos niveles de complejidad

Curso rápido

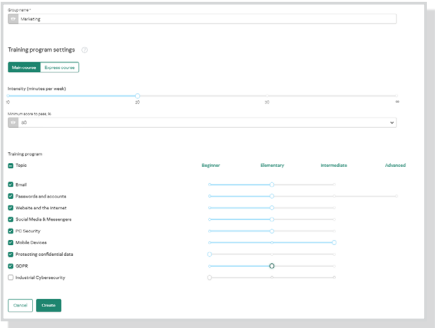
Una versión abreviada de la capacitación, en formato de audio y video. Cada uno de los 6 temas principales de ciberseguridad contiene varias lecciones cortas, para ayudar al usuario a dominar habilidades básicas de ciberseguridad.
- Teoría interactiva
- Vídeos
- Pruebas

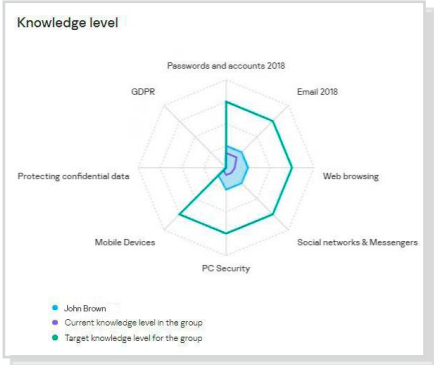
Los simulacros de ataques de phishing no se incluyen en la ruta de aprendizaje, pero el administrator puede asignarlos de forma adicional, como una campaña de phishing

Rutas de aprendizaje específicas 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





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:
  - Curso principal o rápido, o una combinación de ambos
  - Temas de capacitación incluidos en el curso principal o en el curso rápido, los cuales sean necesarios para los estudiantes del grupo
  - El nivel objetivo que desea que alcancen los estudiantes, para cada tema elegido del curso principal.

Informes procesables en cualquier momento

- Disfrute de tableros con toda la información necesaria para controlar y administrar resúmenes de estadísticas sobre los usuarios de la empresa, los puestos de capacitación y las capacitaciones en grupo, con la opción de elegir el nivel individual de un menú desplegable
- Obtenga sugerencias sobre cómo mejorar los resultados
- Descargue informes desde la página principal con un solo clic y configure la frecuencia con la que los recibe por correo electrónico

Libertad de acción

Los empleados pueden estudiar en el momento que les resulte conveniente, y desde cualquier dispositivo. El diseño adaptado para teléfonos móviles facilita aun más el aprendizaje. Los usuarios pueden acceder al portal de capacitación mediante enlaces personalizados, desde la invitación a la capacitación, o usar el mismo enlace para todos los usuarios, mediante la tecnología de Inicio de sesión único (Single Sign-On, SSO)

Metodología del curso principal mediante 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

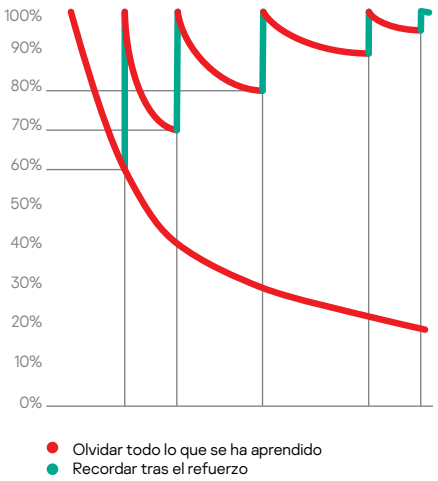
- Cada nivel incluye: una evaluación de refuerzo de lecciones interactivas (prueba y ataque de phishing simulado, si procede)
- Todos los elementos de formación respaldan la habilidad concreta que se enseña en cada unidad, de forma que las habilidades se dominen verdaderamente y pasen a formar parte del nuevo comportamiento deseado

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

La curva del olvido (Ebbinghaus)

El refuerzo reiterado ayuda a desarrollar unas habilidades sólidas.



Cada tema consta de varios niveles que detallan las habilidades específicas de seguridad. Los niveles se definen de acuerdo con el grado de riesgo que ayudan a eliminar: el Nivel 1, por lo general, es suficiente para protegerse de los ataques más sencillos y los ataques masivos. Para protegerse de ataques más sofisticados y dirigidos, es necesario estudiar los niveles más altos.

Temas de formación

- Contraseñas y cuentas
- Correo electrónico
- Sitios web e Internet
- Redes sociales y servicios de mensajería
- Seguridad para PC
- Dispositivos móviles
- Protección de datos confidenciales
- RGPD
- Industrial Cybersecurity

Ejemplo: habilidades practicadas en el tema "Websites and the Internet" (Sitios web e Internet)

Principiante Para evitar ataques en masa (baratos y fáciles)	**Elemental** Para evitar ataques en masa en un perfil específico	**Intermedio** Para evitar ataques dirigidos bien preparados	**Protección*** Para evitar ataques dirigidos
23 habilidades, que incluyen: – Reconocer ventanas emergentes falsas – Prestar atención a acciones de redirección – Distinguir entre enlaces de descarga genuinos y falsos. – Reconocer archivos ejecutables que se encuentren en la web – Ser capaz de determinar la autenticidad de una extensión del navegador.	**34 habilidades, que incluyen:** – Únicamente ingresar datos en sitios con un certificado válido de Capa de sockets seguros (SSL) – Usar diferentes contraseñas para diferentes registros – Reconocer sitios falsos mediante varios signos - Evitar los enlaces numéricos – Reconocer direcciones de enlaces de red inválidos de subdominios falsos	**12 habilidades, que incluyen:** – Comprobar los enlaces compartidos antes de enviarlos – Usar software solo de fabricantes de confianza de torrents – Descargar solo contenido legal de torrents – Borrar las cookies del navegador regularmente	**13 habilidades, que incluyen:** - Reconocer los enlaces falsos sofisticados (incluidos los enlaces con un aspecto similar al de la empresa, enlaces con redirecciones) – Comprobar sitios mediante utilidades especiales – Reconocer si el navegador está minando – Evitar los sitios de black SEO
	+ 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

* Se añadirá durante 2022

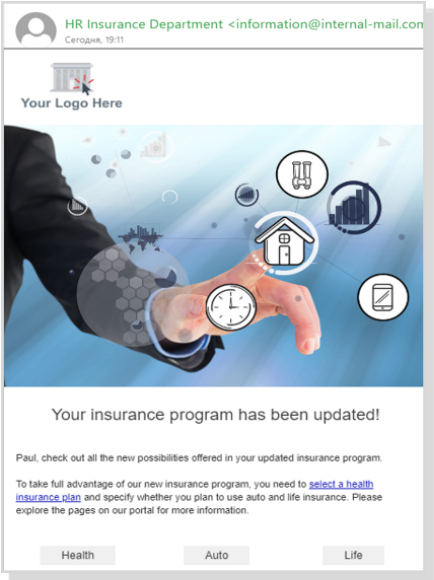
Idiomas

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
- Checo
- Kazajo
- Polaco
- Esloveno
- Rumano
- Turco
- Húngaro
- Danés
- Sueco
- Griego*
- Serbio
- Brasil (Portugués)*
- Portugués
- Rumano
- Serbio
- Esloveno
- Sueco
- Turco
- Griego
- Japonés
- Chino (mandarín)*

* disponibles en 2022

Ejemplo de plantilla de phishing simulado editable y comentarios



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 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.

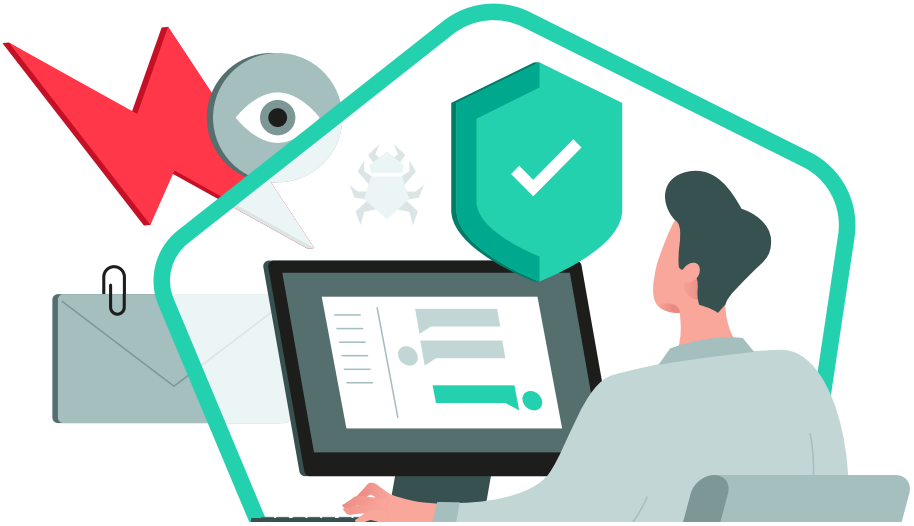
El estilo visual y los textos no solo se traducen a diferentes idiomas, sino que se ajustan para reflejar las distintas culturas y actitudes locales.

Campañas de phishing simuladas

Las campañas de phishing son un elemento agregado al proceso de capacitación principal, el cual evalúa las habilidades prácticas de los empleados para evitar ataques de phishing. Esto ayudará a la persona encargada de administrar la capacitación a identificar las deficiencias en los conocimientos de los usuarios, y a fomentar que estudien temas con los que tengan dificultades.

La plataforma viene con plantillas de correo electrónico preparadas que contienen ejemplos de phishing que se pueden enviar a los usuarios de la plataforma en todos los idiomas disponibles. El set de plantillas disponibles se actualiza regularmente con nuevas incorporaciones. También puede crear correos electrónicos personalizados basados en plantillas predefinidas.

Pruebe un ataque de phishing simulado antes de iniciar la formación: ¡pruebe la resistencia de sus empleados! Esto ayudará a que los empleados y los gerentes puedan observar los beneficios de la capacitación.



Kaspersky Security Awareness: un nuevo enfoque para dominar las habilidades de seguridad de TI

Factores diferenciadores clave del programa

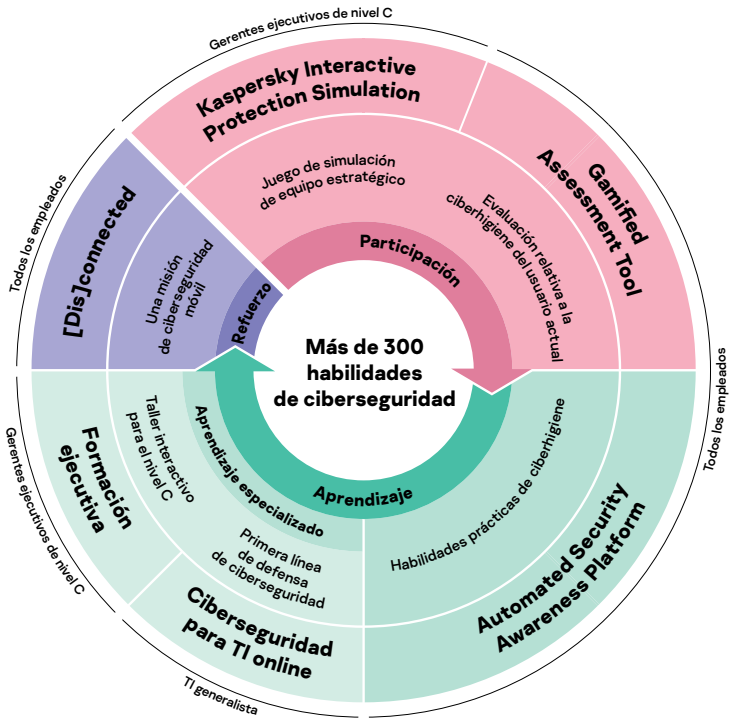
Gran experiencia en ciberseguridad
Más de 20 años de experiencia en ciberseguridad transformados en un conjunto de habilidades de ciberseguridad que se encuentran en el núcleo de nuestros productos

Capacitación que cambia el comportamiento de los empleados en todos los niveles de su organización
Nuestra capacitación lúdica proporciona compromiso y motivación a través del entretenimiento educativo, mientras que las plataformas de aprendizaje ayudan a internalizar el conjunto de habilidades de ciberseguridad para garantizar que las habilidades aprendidas no se pierdan en el camino.

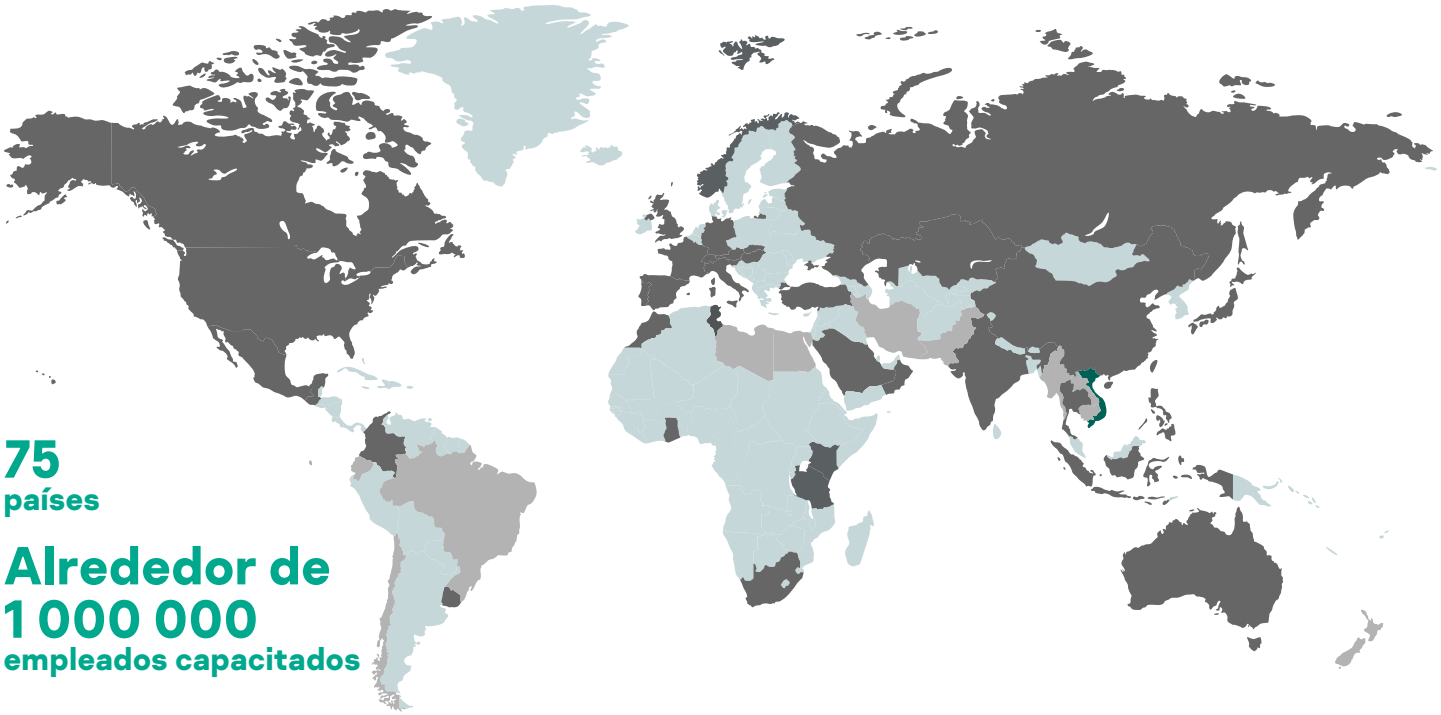
Kaspersky Security Awareness ofrece una amplia gama de soluciones que cubre todas las necesidades de ciberseguridad de las empresas y facilita la adquisición de habilidades que todo empleado debería tener gracias a las últimas técnicas y tecnologías de aprendizaje.

Una solución formativa flexible para todo el mundo

Elija una única solución centrada en una necesidad de seguridad concreta, o bien deje que le proporcionemos paquetes que le ayuden a iniciar y dirigir iniciativas de formación en función de todas sus necesidades y prioridades. Puede encontrar más información sobre los paquetes aquí: kaspersky.es/awareness



Kaspersky Security Awareness a nivel global



75
países

Alrededor de 1 000 000
empleados capacitados

Prueba gratuita de Kaspersky ASAP: k-asap.com/es
Ciberseguridad de empresa: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.es/awareness
Noticias de seguridad de TI: business.kaspersky.com

www.kaspersky.es

kaspersky **PREPARADOS PARA EL FUTURO**

2022 AO KASPERSKY LAB. LAS MARCAS REGISTRADAS Y LOGOS SON PROPIEDAD DE SUS RESPECTIVOS DUEÑOS.