Kaspersky Interactive Protection Simulation

Haga que los altos directivos y los responsables de la toma de decisiones tomen conciencia de la ciberseguridad.

kaspersky bring on the future

Obtenga más información en
latam.kaspersky.com/awareness

Kaspersky Interactive Protection Simulation

El "problema de trabajar con personas"

Uno de los mayores retos de seguridad en las empresas es que los gerentes de alto nivel de diferentes departamentos perciben la ciberseguridad desde distintas perspectivas, porque tienen diferentes prioridades. Esto puede causar una suerte de "Triángulo de las Bermudas de la seguridad" en la toma de decisiones:

- Las empresas consideran que las medidas de seguridad son contrarias a sus objetivos comerciales (más barato / más rápido / mejor).
- Con frecuencia los gerentes de seguridad de TI consideran que la ciberseguridad, al ser un asunto de infraestructura e inversión, está fuera de sus competencias laborales.
- Los responsables de gastos no siempre entienden lo rentable que es invertir en seguridad cibernética. Y que no son gastos vanos, sino una forma de evitarlos.

Para tener éxito en materia de ciberseguridad, resulta fundamental que exista un entendimiento mutuo y trabajo conjunto entre las tres áreas mencionadas. Sin embargo, los formatos de concienciación tradicionales, como las charlas y los ejercicios de equipo contra equipo, son deficientes, muy extensos, demasiado técnicos y resultan inconvenientes para los gerentes que no disponen de tiempo, además de que no logran generar un "idioma común" desde el punto de vista del sentido común.

La ciberinmunidad de una empresa comienza con las gerencias de primera línea

Hoy en día, para muchas empresas es una prioridad cuidar la sostenibilidad de su infraestructura de TI. Sin embargo, los problemas de ciberseguridad suele ser responsabilidad del personal de TI y de seguridad de TI, lo que puede crear fracturas en el comportamiento de ciberseguridad dentro de la empresa. Los líderes empresariales se centran en las ventas, la experiencia del cliente, los riesgos y los costos, y a menudo pasan por alto la ciberseguridad al trabajar para lograr sus objetivos. Pero sin el apoyo y ejemplo del cuerpo directivo, la creación de una cultura coherente de ciberseguridad puede ser inalcanzable.

El 76 % de los directores ejecutivos admiten haberse saltado protocolos de seguridad para hacer algo rápido, sacrificando la seguridad en aras de la velocidad*.

El 62 % de los gerentes admiten que los malentendidos relacionados con la seguridad de TI dentro de su organización condujeron a al menos un incidente de ciberseguridad **.

El 51% de los responsables de seguridad informática encuentran que es difícil discutir el aumento del presupuesto para la seguridad de TI. Pero todos conocen estrategias de comunicación viables.

La mayoría de los altos cargos **(56%) y TI (48%)** están de acuerdo en que proporcionar ejemplos de la vida real es el método más eficaz para facilitar la comunicación sobre problemas relacionados con la seguridad de TI **.

Cómo funciona Kaspersky Security Awareness

Kaspersky Security Awareness es una solución de eficiencia y eficacia comprobadas, con una larga trayectoria internacional de éxitos. Utilizado por empresas de todos los tamaños para **capacitar a más de un millón de empleados en más de 75 países**, la solución reúne los más de 25 años de experiencia de Kaspersky en ciberseguridad con la amplia experiencia de Kaspersky Academy en educación de adultos.

La cartera se compone de atractivos productos de formación destinados a **aumentar la conciencia de la ciberseguridad** de los empleados de todo nivel, para que puedan desempeñar su papel en la ciberseguridad general de su organización.

Cada producto de la cartera desempeña un papel específico en el ciclo de aprendizaje general, y también está disponible de forma independiente.

Un juego estratégico de ciberseguridad para ejecutivos

Kaspersky Interactive Protection Simulation (KIPS) es una simulación estratégica de negocios, un juego de equipos que demuestra la conexión entre la eficacia comercial y la ciberseguridad.

Los participantes se colocan en un entorno empresarial simulado como miembros del equipo de seguridad de TI, donde se enfrentan a una serie de ciberamenazas inesperadas. Al mismo tiempo, tienen que hacer que la empresa siga funcionando y obteniendo ingresos.

Deben construir una estrategia de ciberdefensa eligiendo entre los mejores controles proactivos y reactivos disponibles. Cada elección que hacen cambia la forma en que se desarrolla el escenario y, en última instancia, afecta la cantidad de ingresos que la empresa obtiene o deja de obtener.

Para encontrar el equilibrio entre las prioridades de ingeniería, comerciales y de seguridad, contra los costos de un ciberataque realista, los equipos analizan datos y toman decisiones estratégicas sobre la base de información incierta y recursos limitados. Si esto suena realista, es porque todos los escenarios se basan en eventos de la vida real.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

KIPS es un juego de concienciación dinámica con un enfoque de "aprender haciendo":

- Divertido, participativo y rápido (dura 2 horas).
- El trabajo en equipo genera cooperación
- La competencia fomenta la toma de iniciativas y las habilidades de análisis.
- El juego desarrolla una mejor comprensión de las medidas de ciberseguridad.
- Todos los escenarios y ataques se basan en casos de la vida real

Por qué KIPS funciona

La capacitación de KIPS está orientada a expertos de sistemas comerciales, especialistas en TI y gerentes de línea, y tiene por objeto incrementar su grado de conciencia sobre los riesgos y problemas de seguridad de los sistemas informáticos modernos.

Cada equipo de 4 a 6 personas tiene la tarea de administrar un negocio, con sus instalaciones de producción y las computadoras que las controlan. Durante el juego, las instalaciones de producción generan ingresos, conciencia pública y resultados comerciales. Al mismo tiempo, los equipos deben hacer frente a los ciberataques que amenazan con afectar el rendimiento de la empresa.

Al final del juego, los jugadores habrán adquirido conocimientos importantes y prácticos que pueden aplicar en su trabajo.

- Los ciberataques perjudican los ingresos y deben ser abordados por los altos ejecutivos.
- La cooperación entre los responsables de la toma de decisiones de TI y no TI es esencial para que la ciberseguridad sea efectiva dentro de cada negocio
- Un presupuesto de seguridad adecuado no dejará la caja vacía, pero la pérdida de ingresos como resultado de un ciberataque exitoso podría hacerlo...
- Las personas aprenden rápido a manejar los controles de seguridad y su importancia (capacitación en auditoría, antivirus, etc.).

KIPS está disponible en dos versiones:

La popularísima opción **KIPS Live** crea una atmósfera de emoción y entusiasmo, y es una gran herramienta para involucrar y crear una cultura de ciberseguridad dentro de una organización.

En la versión **KIPS Online** , los usuarios pueden interactuar con un gran número de participantes desde cualquier lugar que les resulte conveniente.

Perfecto para organizaciones globales o actividades públicas, KIPS Online se puede combinar con KIPS Live para agregar equipos remotos a eventos en los predios del cliente.

- Permite la participación de hasta 300 equipos (1000 participantes) de manera simultánea, desde cualquier ubicación.
- Los diferentes equipos pueden elegir una interfaz de juego en distintos idiomas.
- Los clientes pueden personalizar escenarios preinstalados, determinando en la biblioteca el número y los tipos de ataques del juego.
- Los clientes con una licencia que les permita jugar a KIPS con la frecuencia que deseen durante el período de la licencia pueden jugar con la configuración predefinida o personalizar el escenario cada vez que juegan, eligiendo y combinando diferentes ataques de la biblioteca. Esta funcionalidad cambia el juego cada vez, haciéndolo aún más interesante.
- Otro beneficio de la versión en línea es que permite obtener estadísticas sobre las elecciones de los jugadores, datos sobre las acciones de los equipos en ciertas situaciones y las calificaciones de las acciones de los jugadores en el juego anterior.

KIPS muestra:

- El papel que juega la ciberseguridad en la continuidad y rentabilidad del negocio.
- Los desafíos y amenazas emergentes que enfrentan las empresas.
- Los errores típicos que cometen las empresas al construir su ciberseguridad.
- Cómo la cooperación entre los equipos comerciales y de seguridad ayuda a mantener operaciones estables y una protección sostenida contra las ciberamenazas.

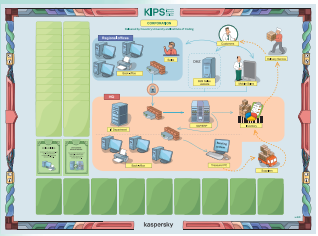
Dependiendo del escenario, los equipos son responsables de la seguridad de TI de la empresa en esa industria. Su tarea es garantizar el funcionamiento normal e ininterrumpido de la empresa, mantener las relaciones con clientes y proveedores, y encontrar y neutralizar las ciberamenazas.

Cuando la empresa sufre un ciberataque, los jugadores experimentan el impacto sobre la producción y las ganancias, y aprenden a adoptar diferentes estrategias y soluciones comerciales y de TI, a fin de minimizar el impacto del ataque y sin perder ganancias.

El equipo que termine la partida con más ingresos, después de haber encontrado y analizado todas las trampas del sistema de ciberseguridad y haber respondido adecuadamente **GANA.**

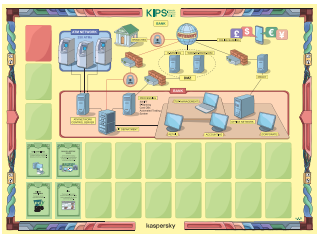
Situaciones de KIPS para empresas de todos los sectores verticales

Sociedad



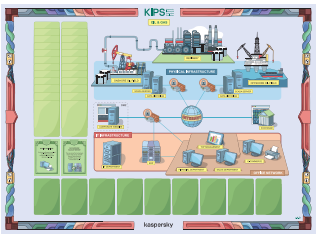
Proteger la empresa contra **ransomware, amenazas persistentes avanzadas (Advanced Persistent Threat, APT), fallas de seguridad en sistemas automatizados.**

Banco



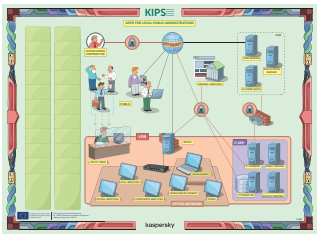
Proteger las instituciones financieras contra **APT emergentes de alto nivel, como Tyukpin y Carbanak.**

Petróleo y gas



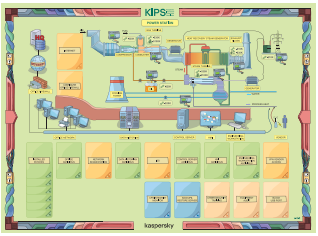
Explorar el impacto de una variedad de amenazas, desde **la desfiguración del sitio web a un ransomware real y una APT sofisticada.**

Administraciones públicas locales



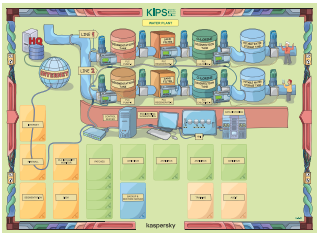
Proteger los servidores web públicos contra ataques y exploits.

Central eléctrica



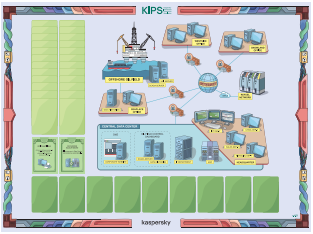
Proteger los sistemas de control industrial y la infraestructura crítica de ciberataques de estilo Stuxnet.

Planta de tratamiento de agua



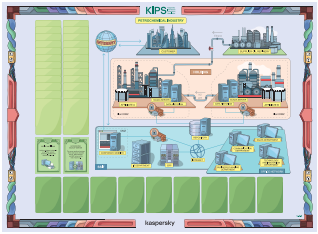
Proteger la infraestructura de TI de una planta de purificación de agua, asegurando la estabilidad de dos líneas de producción.

Explotación de petróleo



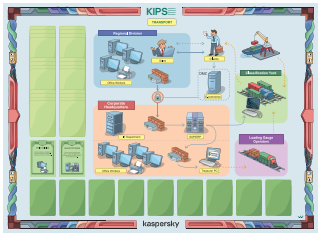
Preservar la ciberseguridad para proteger los ingresos de una empresa global de petróleo y energía con oficinas en todo el mundo.

Industria petroquímica



Garantizar el funcionamiento normal de la nueva sucursal de una gran holding petroquímico, cuya actividad principal es la producción de etileno.

Transporte

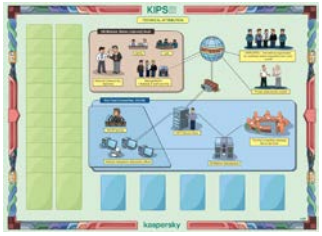


Proteger las empresas de logística contra amenazas de tipo **Heartbleed, APT, B2B Ransomware e Insider.**

Aeropuerto

Garantizar la seguridad de los pasajeros, y la entrega oportuna de bienes en el aeropuerto y, a la vez, proteger sus activos contra una serie de ciberataques y amenazas.

Atribución técnica



Investigar y determinar quienes son los responsables de un ataque APT complejo en servidores de la ONU.

Pequeñas y medianas empresas

Ayudar a las PYME a proteger sus negocios de las amenazas de ciberseguridad relacionadas con DDoS, ransomware, hackeo de aplicaciones móviles y robo de identidad.

Telecomunicaciones

Proteger los activos de un gran holding de telecomunicaciones formado por un proveedor de telecomunicaciones, un proveedor de servicios de nube, un desarrollador de juegos y la sede.

¿Quiere sacarle más partido a KIPS?

¿Por qué no completar su experiencia KIPS con **Formación ejecutiva**, que es parte del portafolio de Kaspersky's Security Awareness? Esta capacitación para gerentes se puede hacer antes o después de jugar KIPS, según cuál sea su enfoque de Conciencia de seguridad. Mejore su experiencia con KIPS descubriendo qué significa el panorama actual de amenazas para su empresa, qué medidas adoptar en caso de un ciberataque, además de una gran cantidad de otra información interesante, relevante y útil. (La capacitación para ejecutivos viene en dos formatos: un taller interactivo fuera de línea o un curso en línea)

Qué opinan los usuarios y clientes de KIPS sobre el juego

La Simulación de protección industrial de Kaspersky (Kaspersky Industrial Protection Simulation, KIPS) realmente me abrió los ojos y debería ser una herramienta obligatoria para todos los profesionales de seguridad.

Warwick Ashford,
Computer Weekly

En CERN, tenemos una gran cantidad de sistemas de TI y de ingeniería, con miles de personas que trabajan en ellos. Por eso, desde el punto de vista de la ciberseguridad, aumentar la conciencia y lograr que las personas participen y tomen medidas sobre ciberseguridad resulta tan importante como los controles técnicos. La capacitación de Kaspersky demostró ser interesante, participativa y eficaz.

Stefan Luders,
CERN CISO

Fue una experiencia muy reveladora, y una gran cantidad de los participantes solicitó usar este juego en sus empresas.

Joe Weiss PE,
CISM, CRISC, socio de ISA

Debemos construir una red de personas que funcione sobre la base de la afiliación y la cooperación, y KIPS es una herramienta perfecta para dar inicio a ese proceso.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, República Checa

¿Cómo prepararse para una sesión de KIPS?

Programación: planifique la sesión de KIPS como un evento separado, o una sesión dentro de un evento, una conferencia o un seminario existente (en este caso, el momento óptimo para la sesión de KIPS es la noche del primer día).

Grupo: de 20 a 100 personas, divididas en equipos de 3 a 4 personas. Es ideal que cada equipo tenga una mezcla de personas de las áreas de Administración, Ingeniería, Seguridad de CISO/TI:

- es mejor contar con, al menos, un miembro de cada papel o función,
- los equipos pueden estar integrados por personas de diferentes empresas o departamentos, o de los mismos sectores,
- no importa si los participantes se conocen o no.

Organización:el juego toma de una hora y media a dos horas, pero la sala debe estar disponible para el equipo facilitador de Kaspersky durante dos horas antes del juego para que lleven a cabo los preparativos y la organización.

Sala: planee ~ 3 m^2 por persona, sin columnas, equipo AV estándar: proyector (6–8 lúmenes), pantalla, sistema de sonido (parlantes, control remoto, micrófonos).

Wi-Fi con acceso a Internet (para acceder al servidor de juegos KIPS), iPad u otro tipo de tablet con Wi-Fi de desde 4Mbps para cada equipo (4 personas).

Muebles:mesas para los participantes, con espacio para 4 personas (rectangulares, de no menos de 75x180 cm, o redondas, de no más de 1,5 m de diámetro), los participantes deben sentarse en grupos de 4. Mesas para coanfitriones, sillas para todos los participantes.

Referencias y casos de estudio

Profesionales de seguridad industrial de más de 50 países han jugado a KIPS.

- KIPS está traducido a los siguientes idiomas: inglés, ruso, alemán, francés, japonés, español de la UE, español latinoamericano, portugués, turco, italiano.
- KIPS es utilizado por numerosas agencias gubernamentales, entre ellas CyberSecurity Malaysia, la NSA de la República Checa y Cyber Security Centrum en los Países Bajos, lo que aumenta la consciencia sobre la infraestructura crítica para cientos de expertos dentro de las organizaciones nacionales de infraestructura crítica.
- KIPS está autorizado por las principales autoridades educativas, como el Instituto SANS, donde se utiliza en la formación de estudiantes de SANS en todo el mundo.
- KIPS tiene licencia de proveedores y proveedores de servicios de seguridad, entre ellos Mitsubishi-Hitachi Power Systems, donde se utiliza en la capacitación para clientes de infraestructura crítica
- KIPS es parte del Proyecto Geiger de la Comisión Europea para capacitar y proteger a las pequeñas y microempresas frente a las ciberamenazas y mejorar su gestión de la privacidad

Opción disponible: capacitar al capacitador

En los casos en que el cliente desee utilizar KIPS para capacitar a una gran cantidad de empleados, gerentes y expertos de múltiples departamentos o sitios, puede resultar útil adquirir una licencia de capacitación en KIPS, entrenar a los participantes internos, y llevar a cabo sesiones de KIPS según el ritmo y lo que resulte más conveniente.

Este tipo de licencia incluye:

- El derecho a usar el programa de capacitación de KIPS dentro de la organización.
- El conjunto de materiales de capacitación y el derecho a usarlos y reproducirlos.
- Inicio de sesión / contraseña para el servidor de software KIPS mientras la licencia esté vigente.
- Guía del capacitador, educación y capacitación para líderes de programas sobre cómo ejecutar y llevar a cabo la capacitación de KIPS.
- Mantenimiento y asistencia (actualizaciones y asistencia técnica para el software y el contenido de capacitación de KIPS).
- Personalización opcional de los escenarios de KIPS (se aplican cargos adicionales).

KIPS para socios y centros de formación

KIPS es una gran oportunidad para que los socios se beneficien de las soluciones de concienciación de varias maneras. No solo pueden venderlo como un producto. También pueden venderlo a sus clientes del centro de capacitación o incluso realizar las sesiones ellos mismos. (Los especialistas en capacitación de Kaspersky pueden mejorar las habilidades de prestar capacitación de los socios, si éstos eligen esa opción).

Kaspersky Security Awareness

Factores diferenciadores clave

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 mediante juegos 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: un nuevo enfoque para dominar las habilidades de seguridad de TI

Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo que incluye múltiples componentes. El aprendizaje basado en juegos involucra a los altos directivos, que se convierten en defensores de las iniciativas de ciberseguridad y en la construcción de una cultura de comportamiento cibernético. El juego permite realizar una evaluación que ayuda a definir las lagunas en los conocimiento de los empleados y los motiva para un mayor aprendizaje, mientras que las plataformas en línea y las simulaciones los dotan de las habilidades adecuadas y las refuerzan.

Ciclo de aprendizaje continuo

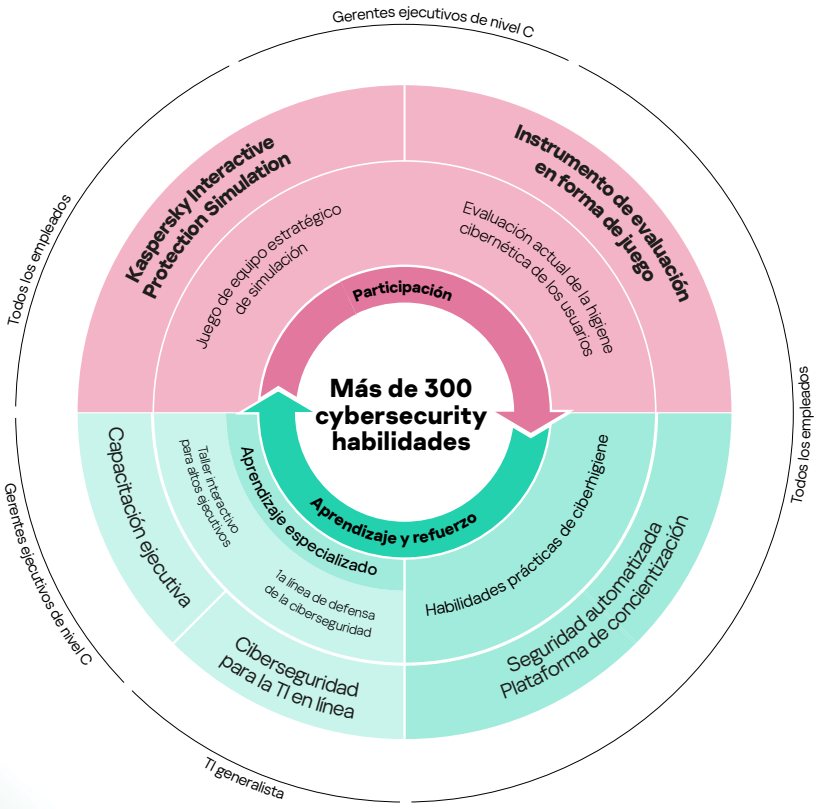
Participación/ motivación
- ¿Por qué necesito esto?
- Proceso de conocimiento

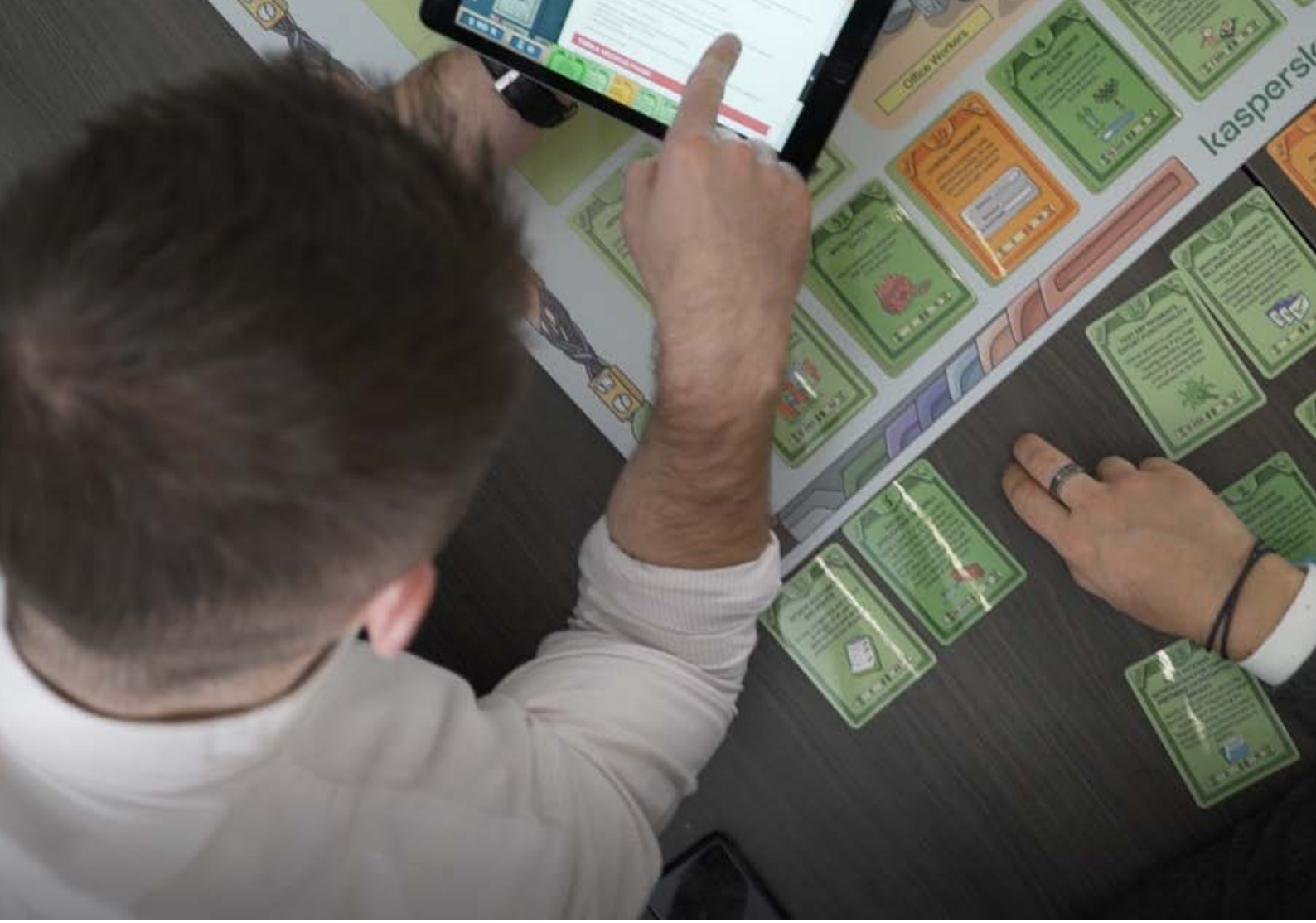
Punto de partida
- ¿Soy consciente?
- ¿Qué es lo que sé y dónde están las deficiencias?

Aprendizaje
- Microaprendizaje
- Aprendizaje continuo
- Adaptabilidad

Refuerzo
- ¿Lo hice bien?
- ¿Recuerdo esto?
- ¿Actúo en consecuencia?

Diferentes formatos de formación para diferentes niveles organizativos





Ciberseguridad empresarial: latam.kaspersky.com/enterprise
Kaspersky Security Awareness: latam.kaspersky.com/awareness

latam.kaspersky.com

kaspersky