Kaspersky Interactive Protection Simulation

Desarrollar concienciación sobre ciberseguridad entre los gerentes de niveles superiores y las personas a cargo de la toma de decisiones

kaspersky bring on the future

Obtén más información en
www.kaspersky.es/awareness

Kaspersky Interactive Protection Simulation

El "problema de trabajar con personas"

Uno de los mayores retos en seguridad a los que se enfrentan las empresas en la actualidad es que los diferentes directivos ven la ciberseguridad desde perspectivas diferentes y tienen prioridades distintas. Esto puede dar como resultado una especie de "Triángulo de las Bermudas de la seguridad" a la hora de tomar decisiones:

- Las empresas consideran las medidas de seguridad
- como una contradicción a sus objetivos empresariales (menos costoso/más rápido/mejor).
- Los administradores de seguridad de TI pueden percibir que la ciberseguridad como problema de infraestructura e inversión está fuera de sus competencias.
- Los responsables del control de costes pueden no ver la correlación entre los gastos en ciberseguridad y los ingresos y ahorros, pero sí los costes que generan.

Para que la ciberseguridad sea eficaz, es necesario que estos directivos se entiendan y colaboren estrechamente entre sí. Sin embargo, los formatos tradicionales de concienciación, como las conferencias y los ejercicios de tipo equipo rojo contra azul, son deficientes, muy extensos, demasiado técnicos y resultan inconvenientes para los gerentes que viven ocupados, además de que no logran generar un "idioma común".

La ciberinmunidad de una empresa comienza con los ejecutivos superiores

Hoy en día, para muchas empresas es prioridad cuidar la sostenibilidad de su infraestructura de TI. Sin embargo, los problemas de ciberseguridad suelen ser responsabilidad del personal de TI y de seguridad de TI, lo que puede generar una cultura fragmentada de comportamiento en materia de ciberseguridad dentro de la empresa. Los líderes empresariales se centran principalmente en las ventas, la experiencia del cliente, los riesgos y los costes, y a menudo descuidan la ciberseguridad mientras se esfuerzan por alcanzar sus objetivos. Pero sin el apoyo y el ejemplo de la junta directiva, crear una cultura unificada de ciberseguridad puede ser inalcanzable.

El 76 % de los directores ejecutivos admiten haberse saltado los protocolos de seguridad para completar una tarea más rápido, primando la velocidad sobre la seguridad*.

El 62 % de los gerentes admiten que la falta de comunicación en materia de seguridad de TI dentro de su organización provocó al menos un incidente de ciberseguridad**.

El 51 % de los trabajadores del sector de la seguridad de la información consideran que hablar sobre el aumento del presupuesto para la seguridad de TI es lo más difícil, pero están de acuerdo cuando se trata de estrategias de comunicación prácticas.

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

Cómo funciona Kaspersky Security Awareness

Kaspersky Security Awareness es una solución probada, eficiente y eficaz con un largo historial de éxitos a nivel internacional. Esta solución se utiliza en empresas de todos los tamaños para **formar a más de un millón de empleados en más de 75 países** y conjuga los más de 25 años de experiencia de Kaspersky en ciberseguridad con la amplia experiencia de Kaspersky Academy en la formación de adultos.

La cartera se compone de interesantes productos de formación que **aumentan la concienciación sobre ciberseguridad** de sus empleados a todos los niveles, lo que les permite desempeñar su papel en la ciberseguridad general de su organización.

Cada producto de la cartera desempeña una función específica en el ciclo global de aprendizaje y también está disponible de forma independiente.

Un juego estratégico empresarial de ciberseguridad para ejecutivos

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

Los participantes se encuentran en un entorno empresarial simulado como miembros del equipo de seguridad de TI, en el que se enfrentan a una serie de ciberamenazas inesperadas mientras tienen que mantener el buen funcionamiento de la empresa y obtener ingresos.

Para elaborar una estrategia de ciberdefensa, deben escoger entre los mejores controles proactivos y reactivos a su disposición. Cada decisión que toman cambia la forma en que se desarrolla la situación y, en última instancia, afecta a los ingresos que la empresa obtiene o deja de obtener.

Mediante el equilibrio de las prioridades de ingeniería, empresa y seguridad con respecto al coste de un ciberataque realista, los equipos analizan los datos y toman decisiones estratégicas basadas en información incierta y recursos limitados. Si esto suena realista, es porque todas las situaciones se basan en hechos 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, atractivo y rápido (2 horas).
- Trabajo en equipo: cooperación.
- La competitividad potencia la iniciativa y las habilidades de análisis.
- Los juegos desarrollan el conocimiento de las medidas de ciberseguridad.
- Todas las situaciones y ataques se basan en casos reales

Por qué funciona KIPS

La formación KIPS está dirigida a expertos en sistemas empresariales, personal de TI y gerentes inmediatos, con el fin de aumentar su concienciación sobre los riesgos y problemas de seguridad que conlleva el funcionamiento de los sistemas informatizados modernos.

Cada equipo de 4 a 6 personas se encarga de dirigir una empresa que incluye instalaciones de producción y ordenadores que las controlan. Durante el juego, las instalaciones de producción generan ingresos, concienciación pública y resultados empresariales. Al mismo tiempo, los equipos deben hacer frente a los ciberataques que amenazan con afectar al rendimiento de la empresa.

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

- Los ciberataques perjudican los ingresos y los altos directivos deben encargarse de ellos.
- La cooperación entre los responsables de la toma de decisiones de TI y los que no lo son es esencial para garantizar una ciberseguridad eficaz en todas las empresas.
- Un presupuesto de seguridad adecuado no hará saltar la banca, pero la pérdida de ingresos como consecuencia de un ciberataque posiblemente sí lo haga.
- Las personas se familiarizan rápidamente con los controles de seguridad y su importancia (formación en auditoría, antivirus, etc.).

KIPS está disponible en dos versiones:

La opción **KIPS Live**, muy popular, crea una atmósfera de emoción y entusiasmo, y es una gran herramienta para comprometer y crear una cultura de ciberseguridad dentro de la organización.

En la **versión KIPS Online**, los usuarios pueden interactuar con un gran número de participantes desde donde les resulte más cómodo.

Ideal para organizaciones globales o actividades públicas, KIPS Online se puede combinar con KIPS Live para añadir equipos remotos al evento en las instalaciones.

- Permite la participación de hasta 300 equipos (1000 participantes) de manera simultánea, desde cualquier ubicación.
- Los distintos equipos pueden escoger interfaces de juego en diferentes idiomas.
- Los clientes pueden personalizar las situaciones preinstaladas si determinan el número y los tipos de ataques del juego de la biblioteca.
- Los clientes que tengan una licencia para jugar a KIPS cuando quieran durante el período de vigencia de la licencia pueden jugar con la configuración predefinida o personalizar la situación del juego cada vez que jueguen y escoger y combinar los diferentes ataques de la biblioteca. Esta funcionalidad cambia el juego en todo momento, lo que lo hace aún más interesante.
- Otra ventaja de la versión online es que permite obtener estadísticas sobre las decisiones de los jugadores, datos sobre las acciones de los equipos en determinadas situaciones y una evaluación comparativa de las acciones de los jugadores en relación con el juego anterior.

KIPS muestra lo siguiente:

- La función 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 permite mantener las operaciones estables y una protección sostenida contra las ciberamenazas.

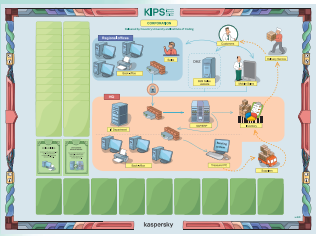
Según la situación, los equipos son responsables de la seguridad de TI de la empresa en esa industria. Su tarea es garantizar el funcionamiento normal y sin interrupciones de la empresa, mantener las relaciones con clientes y proveedores, y encontrar y neutralizar las ciberamenazas.

Cuando la empresa sufre un ciberataque, los participantes experimentan el impacto que tiene en la producción y los ingresos, y aprenden a adoptar distintas estrategias y soluciones de negocios e IT para minimizar los efectos negativos y seguir obteniendo dinero.

El GANADOR es 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.

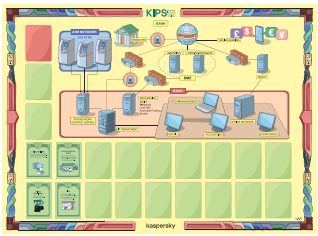
Situaciones de KIPS para empresas de todos los sectores verticales

Sociedad



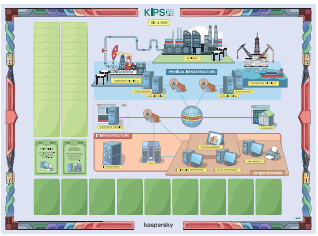
Protege la empresa frente a **ransomware, APT, errores de seguridad de automatización.**

Banco



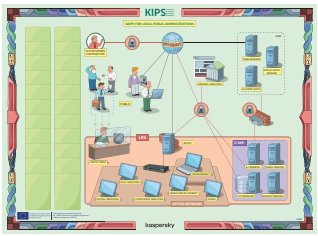
Protege las instituciones financieras contra **APT emergentes de alto nivel, como Tyukpin, Carbanak.**

Petróleo y gas



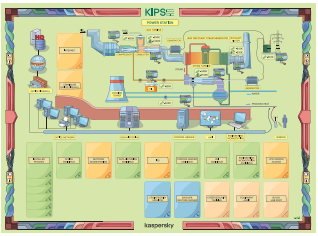
Examina el impacto de diversas amenazas, desde **la desfiguración del sitio web hasta un ransomware real y una sofisticada APT.**

Administraciones públicas locales



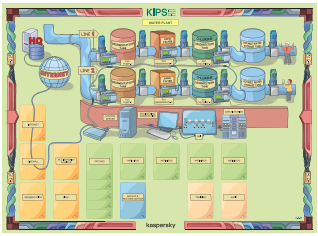
Protege los servidores web públicos frente a ataques y exploits.

Central eléctrica



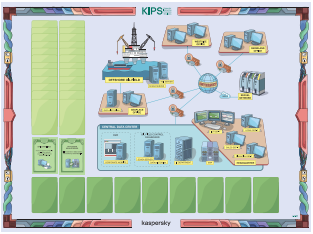
Protege los sistemas de control industrial y las infraestructuras críticas de ciberataques del tipo Stuxnet.

Planta de tratamiento de agua



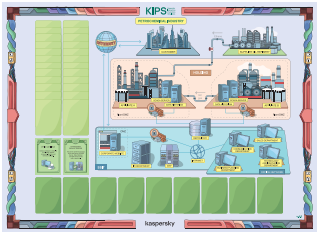
Protege la infraestructura de TI de una planta de purificación de agua y garantice la estabilidad de dos líneas de producción.

Holding de petróleo



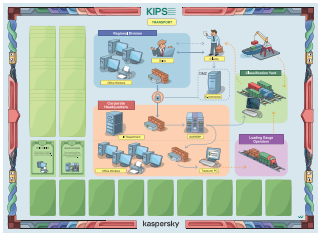
Garantiza la ciberseguridad para proteger los ingresos de una empresa petrolera y de energía internacional con oficinas en todo el mundo.

Industria petroquímica



Garantiza el funcionamiento normal de la nueva sucursal de una gran compañía petroquímica que se centra en la producción de etileno.

Transporte

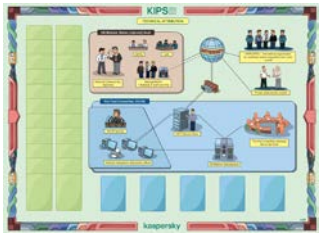


Protege las empresas de logística contra amenazas de tipo **Heartbleed, APT, B2B Ransomware, Insider.**

Aeropuerto

Garantiza la seguridad de los pasajeros y la entrega puntual de productos en el aeropuerto, y protege los activos de numerosos ciberataques y amenazas.

Atribución técnica



Investiga y determina quienes son los responsables de un ataque APT complejo en los servidores de la ONU.

Pequeñas y medianas empresas

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

Telecomunicaciones

Protege los activos de una gran compañía de telecomunicaciones integrada por un proveedor de telecomunicaciones, un proveedor de servicios en la nube, un desarrollador de juegos y la sede central.

¿Quieres aprovechar aún más a KIPS?

¿Por qué no completas tu experiencia KIPS con la **formación para ejecutivos**, que forma parte de la cartera de Kaspersky Security Awareness? Esta formación para directivos se puede realizar antes o después de haber jugado a KIPS, en función de tu enfoque de la concienciación en materia de seguridad. Para mejorar tu experiencia KIPS, descubre lo que significa el panorama actual de amenazas para tu empresa, las medidas que debes tomar en caso de que se produzca un ciberataque, además de mucha otra información interesante, relevante y útil. (La formación para ejecutivos se ofrece en dos formatos: un taller interactivo presencial o un curso online)

Qué opinan los usuarios y clientes de KIPS sobre el juego

Kaspersky Industrial Protection Simulation fue toda una revelación y debería ser obligatoria para todos los profesionales de seguridad.

Warwick Ashford,
Computer Weekly

En CERN tenemos un gran número de sistemas informáticos y de ingeniería en los que trabajan miles de personas. Por eso, desde el punto de vista de la ciberseguridad, aumentar la concienciación y lograr que las personas participen y tomen medidas sobre ciberseguridad resulta tan importante como realizar controles técnicos. La formación de Kaspersky demostró ser interesante, participativa y eficaz.

Stefan Luders,
CERN CISO

Fue realmente revelador y varios de los participantes preguntaron si podían jugarlo en sus empresas.

Joe Weiss PE,
CISM, CRISC, ISA Fellow

Tenemos que construir una red de personas basada en la afiliación y la cooperación, y KIPS es una herramienta perfecta para empezar.

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 combinación 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 2 horas antes del juego para que lleven a cabo los preparativos y la organización.

Sala: planifique aprox. 3 m2 por persona, sin columnas, equipo AV estándar: proyector (de 6 a 8 lúmenes), pantalla, sistema de sonido (parlantes, control remoto, micrófonos).

Wi-Fi con acceso a Internet (para acceder al servidor de juegos KIPS), iPad con Wi-Fi de 4 Mbps por cada equipo (4 personas) con soporte Wi-Fi u otra tableta.

Muebles: mesas para los participantes para 4 personas (de tamaño rectangular no inferior a 75 x 180 cm o tamaño circular con un diámetro no superior a 1,5 m); los participantes se deben sentar en grupos de cuatro en las mesas. Mesas para coanfitriones, sillas para todos los participantes.

Referencias y casos de estudio

Profesionales de seguridad industrial de más de 50 países jugaron a KIPS.

- KIPS está traducido a los siguientes idiomas: inglés, ruso, alemán, francés, japonés, español para la UE, español para Latinoamérica, portugués, turco, italiano, chino, holandés, árabe.
- Numerosas agencias gubernamentales utilizan KIPS, entre ellas CyberSecurity Malaysia, la NSA de la República Checa y Cyber Security Centrum en los Países Bajos, lo que aumenta la concienciación sobre la infraestructura crítica para cientos de expertos dentro de las organizaciones nacionales de infraestructura crítica.
- Las autoridades educativas líderes otorgan las licencias de KIPS, como el Instituto SANS, y se usan en los programas de formación de ciberseguridad que SANS brinda a sus estudiantes en todo el mundo.
- KIPS cuenta con licencias de proveedores de servicios de seguridad y vendedores como Mitsubishi-Hitachi Power Systems, donde se utiliza en la formación de clientes de infraestructuras críticas.
- KIPS forma parte del Proyecto Geiger de la Comisión Europea para formar y proteger a las pequeñas empresas y microempresas frente a las ciberamenazas y mejorar su gestión de la privacidad.

Formación de formadores disponible

Si un cliente desea utilizar KIPS para formar a un público más amplio, un gran número de empleados, directivos y expertos de varios departamentos o centros, puede ser útil adquirir una licencia de formación de KIPS, para formar a los formadores internos y llevar a cabo las sesiones de KIPS al ritmo y conveniencia del cliente.

Este tipo de licencia incluye lo siguiente:

- Los derechos para utilizar de forma interna el programa de formación de KIPS.
- El conjunto de materiales de formación y el derecho a usarlos y reproducirlos.
- Inicio de sesión y contraseña para el servidor de software KIPS mientras la licencia esté vigente.
- Guía del formador, educación y formación para los responsables del programa sobre cómo dirigir y realizar la formación de KIPS.
- Mantenimiento y asistencia técnica (actualizaciones y soporte para el software y el contenido de la formación de KIPS).
- Personalización opcional de las situaciones de KIPS (se aplican cargos adicionales).

KIPS para partners y centros de formación

KIPS es una gran oportunidad para que los partners se beneficien de las soluciones de concienciación de varias maneras. No solo pueden venderlo como producto, sino también a los clientes de sus centros de formación, o incluso llevar a cabo ellos mismos las sesiones. (Los especialistas en formación de Kaspersky pueden preparar a los partners para la formación si escogen esa opción).

Kaspersky Security Awareness

Factores diferenciadores clave del programa

Gran experiencia en ciberseguridad

Más de 25 años de experiencia en ciberseguridad transformados en un conjunto de habilidades que se encuentran en el núcleo de nuestros productos.

Formación que cambia el comportamiento de los empleados en todos los niveles de su organización

Nuestra formación 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.

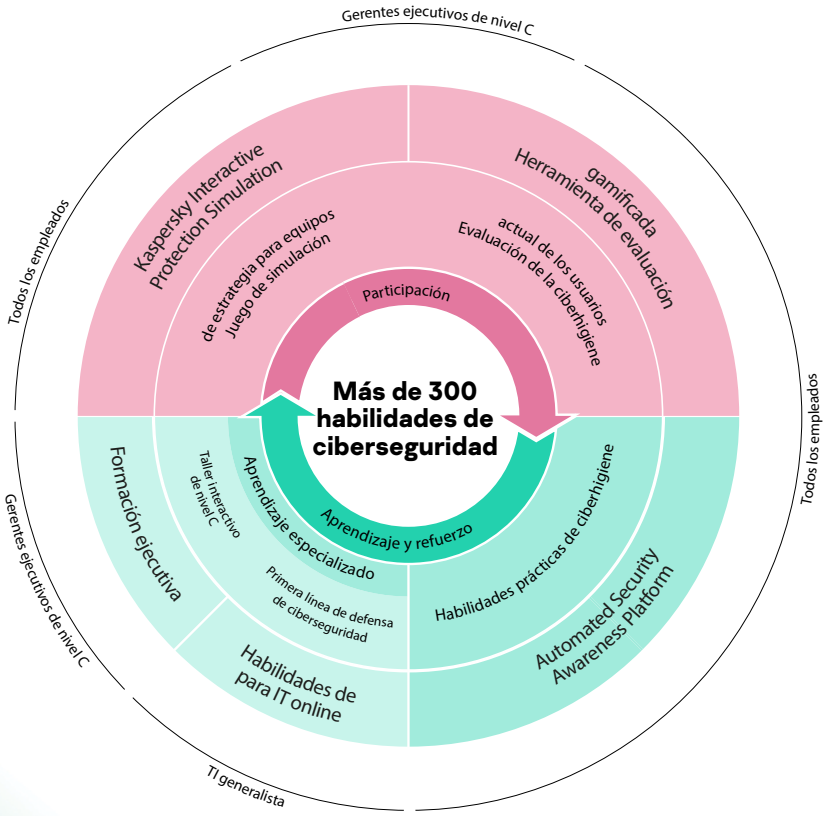
Kaspersky Security Awareness: un nuevo enfoque para dominar las habilidades de seguridad de TI

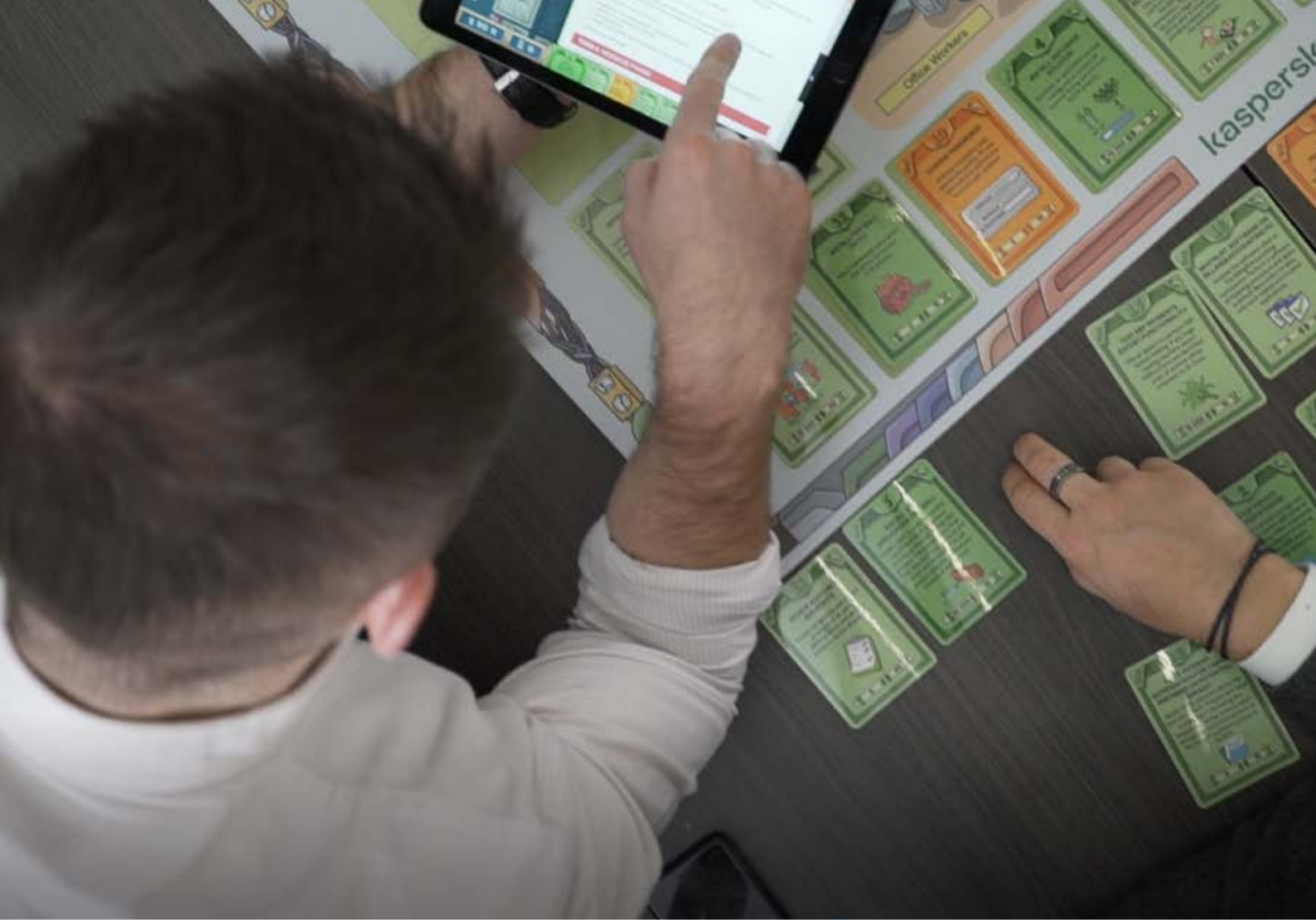
Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo que incluye múltiples componentes. El aprendizaje basado en juegos involucra a los altos directivos, que se convierten en defensores de las iniciativas de ciberseguridad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

Ciclo de aprendizaje continuo

Participación/ motivación	Punto de partida	Aprendizaje	Refuerzo
– ¿Por qué necesito esto? – Proceso de conocimiento	– ¿Soy consciente? – ¿Qué es lo que sé y dónde están las deficiencias?	– Microaprendizaje – Aprendizaje continuo – Adaptabilidad	– ¿Lo hice bien? – ¿Recuerdo esto? – ¿Actúo en consecuencia?

Diferentes formatos de formación para diferentes niveles organizativos





Ciberseguridad de empresa: www.kaspersky.es/enterprise
Kaspersky Security Awareness: www.kaspersky.es/awareness

www.kaspersky.es

kaspersky