Kaspersky Interactive Protection Simulation

Una manera eficaz de generar concienciación sobre ciberseguridad entre los gerentes de niveles superiores y las personas a cargo de la toma de decisiones

kaspersky BRING ON THE FUTURE

Obtenga más información en kaspersky.es/awareness

Kaspersky Interactive Protection Simulation

El "problema de trabajar con personas"

Uno de los mayores desafíos de seguridad es que las diferentes personas en funciones de gerencia de alto nivelperciben la ciberseguridad desde distintas perspectivas, y tienen diferentes prioridades. Esto puede causar una suerte de "Triángulo de las Bermudas de la seguridad" en la toma de decisiones:

- El área comercial ve las medidas de seguridad como una contradicción para sus metas comerciales (menos costoso/más rápido/mejor).
- Es posible que los gerentes de seguridad de TI consideren que la ciberseguridad, al ser un asunto de infraestructura e inversión, queda fuera de su ámbito laboral.
- Es posible que los gerentes a cargo del control de costos no vean cómo los gastos en ciberseguridad se relacionan con los ingresos y ahorros, en lugar de generar costos.

Para tener éxito en materia de ciberseguridad, resulta fundamental que exista un entendimiento mutuo y trabajo conjunto entre las 3 áreas mencionadas. Sin embargo, los formatos de concienciación tradicionales, como las charlas y los ejercicios de tipo equipo rojo contra equipo 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" desde el punto de vista del sentido común.

¿Qué significa KIPS?

Kaspersky Interactive Protection Simulation (KIPS) es parte de la cartera de productos Security Awareness, que ofrece una selección de soluciones de capacitación muy interesantes y eficaces que aumentan la conciencia de ciberseguridad de su personal, para que todos desempeñen su labor en la ciberseguridad general de la organización.

Si bien hoy en día más y más ejecutivos reconocen la importancia de la ciberseguridad, sigue siendo un desafío para aquellos encargados de la educación involucrar a los empleados en la capacitación y convertirlos en verdaderos partidarios de las iniciativas de ciberseguridad.

Ciclo de aprendizaje continuo

KIPS es una simulación comercial estratégica, un juego de equipos, que demuestra la conexión entre la eficacia comercial y la ciberseguridad. El aprendizaje basado en un juego permite que las personas a cargo de la toma de decisiones se involucren en temas de ciberseguridad y los motiva a dar otros pasos en la generación de un entorno corporativo ciberseguro.

KIPS es un ejercicio que hace que las personas a cargo de la toma de decisiones comerciales formen parte de equipos de seguridad de TI, dentro de un entorno comercial simulado, y enfrenten una serie de ciberamenazas inesperadas, en las que el objetivo principal es mantener la empresa en funcionamiento y seguir obteniendo ganancias.
La idea es construir una estrategia de ciberdefensa, al elegir entre los mejores controles proactivos y reactivos disponibles. Cada reacción de los equipos ante los eventos que van ocurriendo cambia el modo en que se desarrolla la situación y, en definitiva, cuántas ganancias obtiene la empresa o cuántas pierde.

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 suena realista, está justificado, porque cada una de las situaciones se basa en casos de la vida real.

¿Por qué KIPS constituye un ejercicio eficaz?

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 que se presentan al ejecutar sistemas informáticos modernos.

Cada uno de los equipos que compiten, de 4 a 6 personas, tiene la tarea de dirigir una empresa, que cuenta con instalaciones de producción y equipos que las controlan. Durante las rondas del juego, las instalaciones de producción generan ganancias, bienestar público oresultados comerciales. No obstante, los equipos también deben enfrentarse a ciberataques que posiblemente afecten el rendimiento del emprendimiento.

A fin de defender su emprendimiento, cada equipo debe tomar decisiones estratégicas, gerenciales y técnicas y, a la vez, considerar las restricciones operativas y mantener un alto nivel de ganancias.

El juego de KIPS es un programa de concienciación dinámico que se basa en "aprender haciendo":

- Divertido, participativo y rápido (dura 2 horas).
- El trabajo en equipo promueve la cooperación.
- La competencia fomenta la toma de iniciativa y las habilidades de análisis.
- El juego desarrolla una mejor comprensión de las medidas de ciberseguridad.

Después del juego de KIPS, los jugadores llegan a conclusiones importantes y accionables que pueden implementar en su trabajo diario:

- Los ciberataques tienen un impacto negativo sobre las ganancias, y se deben enfrentar desde el nivel superior de la gerencia.
- La cooperación entre los empleados de las áreas de TI y comerciales resulta esencial para que la ciberseguridad sea exitosa.
- Un presupuesto de seguridad eficaz es mucho menor que las ganancias que se corre el riesgo de perder, y no es necesario disponer de millones de dólares.
- Las personas se acostumbran a controles de seguridad particulares y a su importancia (capacitación en materia de auditorías, protección antivirus, etc).

La capacitación de KIPS les enseña a los participantes lo siguiente:

- La función real que desempeña la ciberseguridad en la continuidad y la rentabilidad de la empresa.
- Los elementos más destacados de los desafíos y las amenazas emergentes que se presentan en la actualidad.
- Los errores típicos que cometen las empresas al tomar medidas de ciberseguridad.
- El tipo de cooperación entre equipos comerciales y de seguridad que puede ayudar a mantener estables las operaciones, y la sostenibilidad de la empresa ante las ciberamenazas.

Ante el caso de que la empresa sufra 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 para ganar más dinero.

Cada una de las situaciones se enfoca en los respectivos vectores de amenazas, permite descubrir y analizar los errores típicos que se cometen al implementar medidas de ciberseguridad y procedimientos de respuesta ante incidentes en la industria correspondiente.

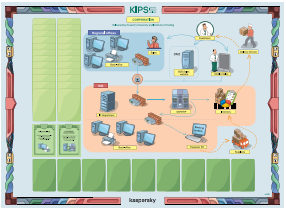
En 2019, se desarrolló una nueva situación, con un enfoque especial sobre la protección de los datos personales para las administraciones públicas locales (Local Public Administrations, LPA). Junto con la serie de ejercicios y unidades de capacitación, KIPS para LPA les permite a los empleados de las administraciones públicas no solo entender los desafíos que se presentan en materia de ciberseguridad, sino también transformar ese conocimiento en modelos de comportamiento positivo. La capacitación también pone énfasis en la importancia que puede tener el trabajo en equipo y la responsabilidad compartida, y cómo estos pueden ayudar a las LPA a tomar mejores decisiones relacionadas con la seguridad física y material de los ciudadanos.

A lo largo de los últimos años, agregamos tres situaciones más que tenían mucha demanda: aeropuertos, industria petroquímica y explotación de petróleo.

De acuerdo con las situaciones, cada equipo es responsable de la seguridad de TI de la empresa ocupada en el área respectiva. La tarea de los equipos es garantizar que la empresa tenga un funcionamiento normal y trabajo estable y seguro, mantenga buenas relaciones con los clientes y proveedores, y detecte y neutralice las ciberamenazas.

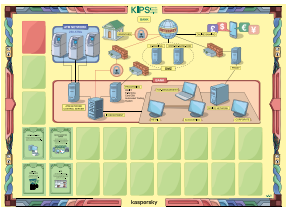
Situaciones de KIPS para empresas de todos los sectores verticales

Sociedad



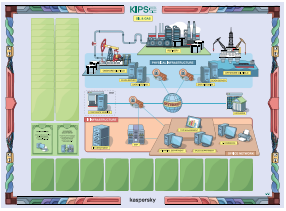
Proteger la empresa contra **ransomware, amenazas persistentes avanzadas (Advanced Persistent Threat, APT), fallas de seguridad en sistemas automatizados.**

Banco



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

Petróleo y gas

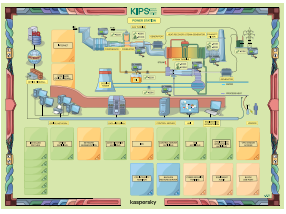


Explorar la influencia de una variedad de amenazas: desde **la desfiguración de sitios web hasta ransomware altamente real y una APT sofisticada.**

Administraciones públicas locales

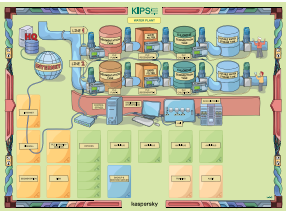
Proteger los servidores web públicos contra la explotación y los ataques.

Central eléctrica



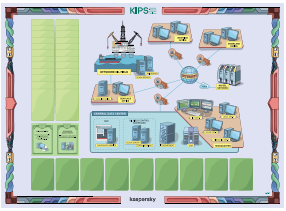
Proteger los sistemas de control industrial y la infraestructura crítica de ciberataques de estilo **Stuxnet.**

Planta de tratamiento de agua



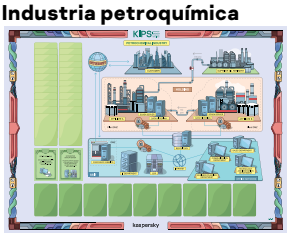
Proteger la infraestructura de TI de la planta de purificación de agua que asegura **el trabajo estable de 2 líneas de producción.**

Explotación de petróleo



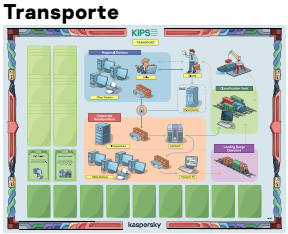
Mantener la ciberseguridad para proteger las ganancias de una empresa global de la industria del petróleo y la energía, con oficinas en todo el mundo.

Industria petroquímica



Garantizar el funcionamiento normal de la nueva sucursal de una gran sociedad tenedora de acciones petroquímica, cuya actividad principal es la producción de etileno.

Transporte



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

Aeropuerto

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

Citas y referencias sobre el juego de KIPS

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

Recomendaciones sobre cómo prepararse para la sesión de KIPS

Programación: se recomienda planificar 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 rol o función,
- los equipos pueden estar integrados por personas de diferentes empresas o departamentos, o de los mismos sectores,
- las personas se pueden conocer 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: se recomienda que tenga alrededor de 3 m2/persona, sin columnas, de forma regular; equipo audiovisual: proyector (6 a 8 lúmenes), pantalla, sistema de sonido (altavoces, mando a distancia, micrófonos).

Wi-Fi con acceso a Internet (para el acceso al servidor del juego de KIPS), desde un iPad de 4 Mbps para cadaxequipo (4 personas) con Wi-Fi u otro tipo de tableta.

Muebles: mesas para los participantes, con espacio para 4 personas (rectangulares, de no menos de 75x180 cm, o redondas, con no más de 1,5 m de diámetro), los participantes deben sentarse en grupos de 4 en las mesas. Mesas para el otro anfitrión y la cantidad de sillas necesaria para los participantes que se ubicarán en las mesas.

Referencias y casos de estudio

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

- KIPS se tradujo a los siguientes idiomas: inglés, ruso, alemán, francés, japonés, español de la UE, español latinoamericano, portugués, turco, italiano.
- KIPS se utilizó en entidades gubernamentales, como CyberSecurity
- Malasia, la NSA de República Checa y el Centro de ciberseguridad de los Países Bajos, para mejorar la concienciación sobre infraestructuras críticas, y para capacitar a cientos de expertos de empresas nacionales de infraestructura crítica.
- KIPS se usa en empresas como BASF (la empresa líder mundial en fabricación de productos químicos), CERN (donde se encuentra el Gran colisionador de hadrones), Mitsubishi, Yokogawa, RusHydro, Panasonic, International Society of Automation (ISA), para capacitar a sus propios ingenieros, desarrolladores y personal de atención al cliente, a fines de que se tome conocimiento y se implementen medidas de ciberseguridad en los entornos de automatización industrial.
- Las licencias de KIPS son otorgadas por autoridades educativas líderes, como el Instituto SANS, y se usan en los programas de capacitación de ciberseguridad que SANS brinda a sus estudiantes en todo el mundo.
- KIPS se otorga con licencia de proveedores y distribuidores de servicios de seguridad, como Mitsubishi-Hitachi Power Systems, para usar como curso de capacitación a clientes finales de sectores de infraestructuras críticas.

Dos tipos de capacitación de KIPS

KIPS Live (versión en vivo)

Tiene más limitaciones, pero genera una mayor participación debido a la presencia en el sitio y la competencia cara a cara. Puede funcionar como un evento de formación de equipos.

- Permite hasta 80 participantes en la misma sala.
- Todos los participantes usan el mismo idioma.
- Hay un capacitador y un asistente en el sitio.
- Los materiales impresos resultan esenciales.

KIPS Online (versión en línea)

Es una herramienta perfecta para organizaciones globales o actividades públicas. Puede combinarse con la versión de KIPS en vivo para agregar equipos remotos al evento en el sitio.

- 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.
- Un capacitador lidera la sesión por WebEx.

Opción para capacitar al capacitador disponible

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 la licencia de la capacitación de KIPS, entrenar a los participantes internos, y llevar a cabo sesiones de KIPS según el ritmo y lo que resulte conveniente al cliente.

Kaspersky ofrece dicha licencia, la cual incluye lo siguiente:

- El derecho a usar el programa de capacitación de KIPS, a nivel interno.
- El conjunto de materiales de capacitación y el derecho a usarlos y reproducirlos.
- Datos de inicio de sesión y contraseñas para el servidor del software de KIPS.
- Guías, materiales educativos y capacitación para el capacitador, disponibles para los líderes de los programas, sobre cómo llevar a cabo la capacitación de KIPS.
- Mantenimiento y soporte (actualizaciones y asistencia técnica para el software y el contenido de capacitación de KIPS).
- Personalización opcional de la situación de KIPS (se aplican cargos adicionales).

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 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.

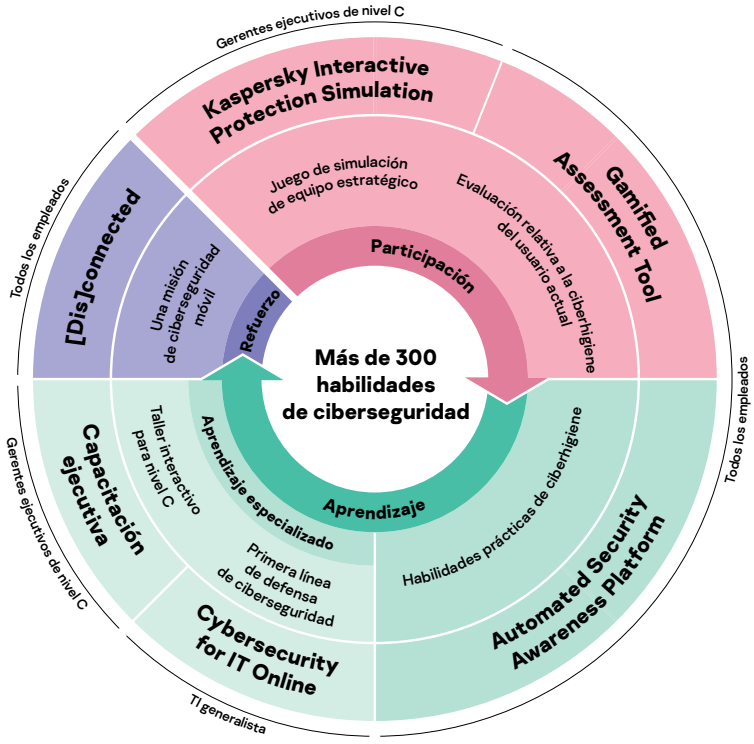
Kaspersky Security Awareness: un nuevo enfoque para dominar las habilidades de seguridad de TI

Kaspersky Security Awareness ofrece una selección de soluciones de capacitación muy interesantes y eficaces que aumentan la conciencia de ciberseguridad de su personal para que todos desempeñen su labor en la ciberseguridad general de su organización. Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo que incluye múltiples componentes.

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 capacitación para diferentes niveles organizativos



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

latam.kaspersky.com

kaspersky