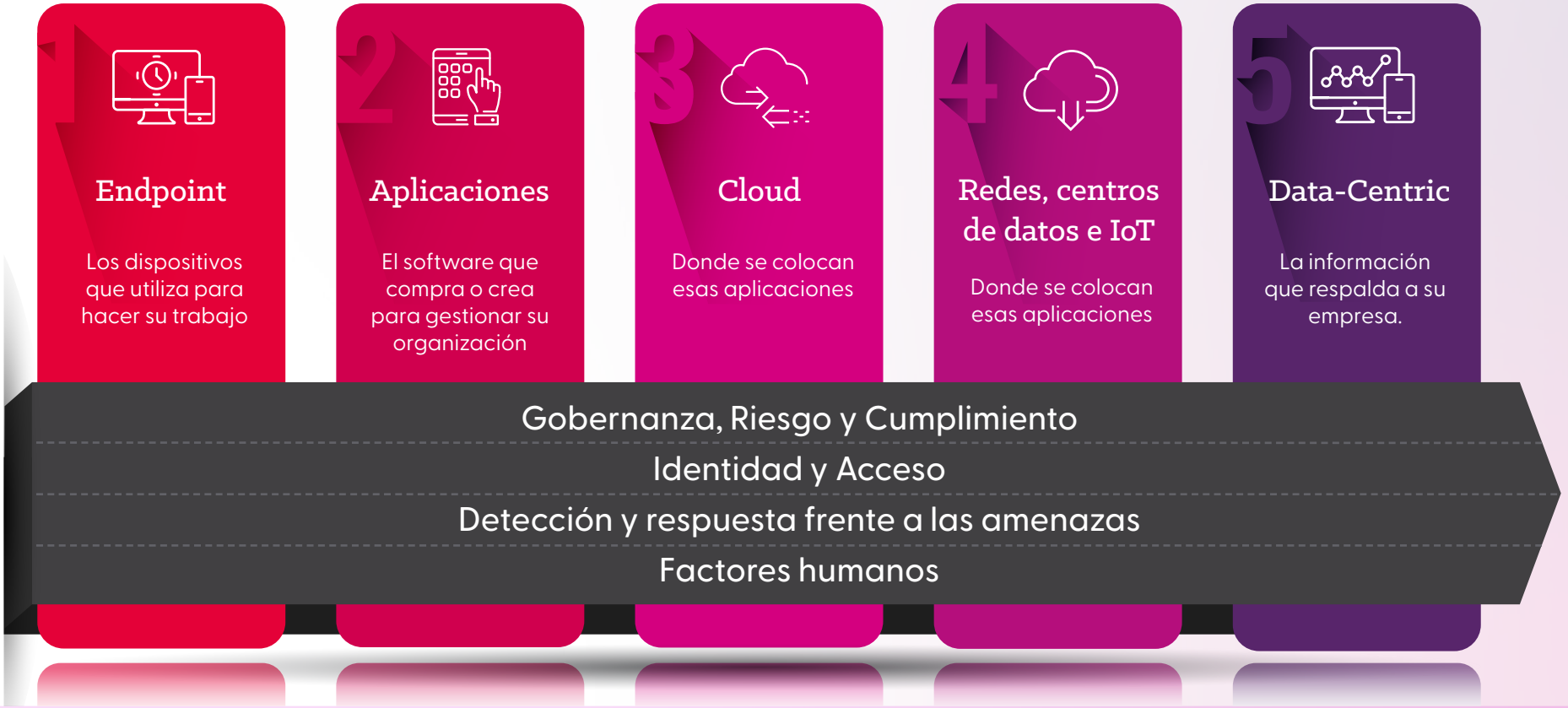
# Guía Insight sobre factores humanos en la seguridad

Insight

# Introducción

En Insight, sabemos lo importante que es un enfoque holístico de seguridad. Los atacantes buscarán su área más débil, no la más fuerte. Contamos con experiencia técnica en las cinco áreas de dominio tecnológico (Endpoints, Aplicaciones, Nube, Red, Datacentre e IOT) - pero como integrador de soluciones líder, creemos que también se debe prestar mucha atención a las interacciones entre estos dominios tecnológicos (Gobernanza, Riesgo y Cumplimiento, Identidad y Acceso, Detección y Respuesta a Amenazas, y Factores Humanos). Las brechas donde se conectan los dominios tecnológicos son a menudo donde se puede conseguir un valor adicional, ayudando a mejorar su postura general de seguridad de una forma rentable.

## Modelo de seguridad integral de Insight



# ¿Qué son los factores humanos y por qué son importantes?

Aunque la infraestructura de seguridad y las herramientas y controles se mejoran e investigan continuamente, las brechas siguen produciéndose, y no son fáciles de identificar y resolver. Existen muchos controles de seguridad especializados para diferentes tipos de amenazas, desde ataques a endpoints hasta ataques a cadenas de suministro, pero cuando se examina cómo ocurrieron realmente estos ataques, las tres razones principales son:

- **Contraseñas** – se ha descifrado una contraseña poco segura, no se modificó una contraseña predeterminada o se utilizó la misma contraseña en varios sitios.
- **Phishing** – un usuario fue engañado para que facilitara sus credenciales, visitara un sitio web comprometido o abriera un archivo adjunto hostil.
- **Patching** – una vulnerabilidad conocida se dejó sin parchear durante demasiado tiempo y fue explotada por malware, o un usuario instaló algún software de riesgo que quedó comprometido.

Los equipos de TI pueden utilizar la tecnología para ayudar a reducir las posibilidades de que se produzcan infracciones, pero los usuarios finales siempre tendrán un papel que desempeñar en el apoyo a la seguridad de una organización. Equipos de TI: a menudo se concentran en la tecnología, a veces en el proceso, y descuidan el factor humano, que puede determinar el fracaso o el éxito de un proyecto.

Proceso: las políticas escritas que explican lo que los usuarios deben y no deben hacer adoptan muchas formas, como políticas de seguridad de la información, contratos de trabajo, manuales del staff, políticas de uso aceptable o planes de respuesta a incidentes.

Tecnología: las herramientas, los sistemas y los controles que proporcionan directrices y restricciones sobre lo que pueden hacer los usuarios deben ser lo suficientemente estrictos como para restringir las actividades de riesgo obvias, pero lo suficientemente permisivos como para ofrecer cierta flexibilidad y no romper los procesos empresariales.

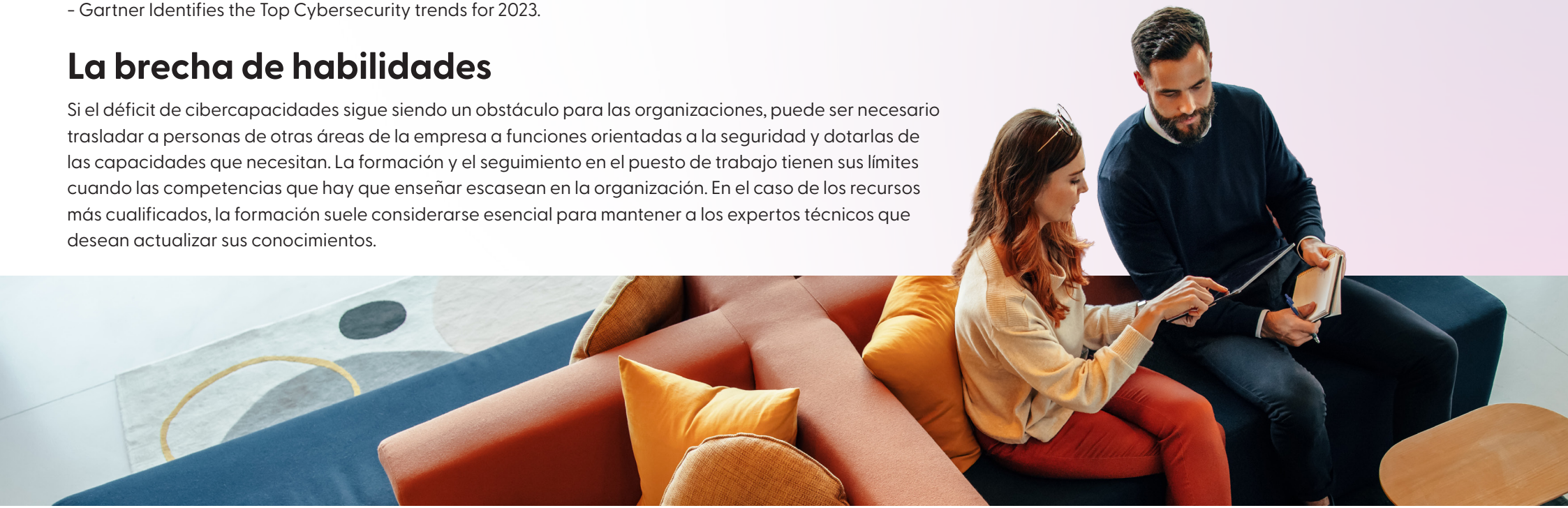
Personas: cuando no hay ningún proceso documentado o las personas no lo conocen, tienen que usar su propio criterio. O cuando una tecnología falla a la hora de prevenir una nueva amenaza, las personas son a menudo la primera y última línea de defensa, confiando únicamente en sus habilidades y formación actuales.

En 2027, el 50% de los directores de seguridad de la información (CISO) de las grandes empresas habrán adoptado prácticas de diseño de seguridad centradas en el ser humano para minimizar los riesgos de ciberseguridad y maximizar la adopción de controles.

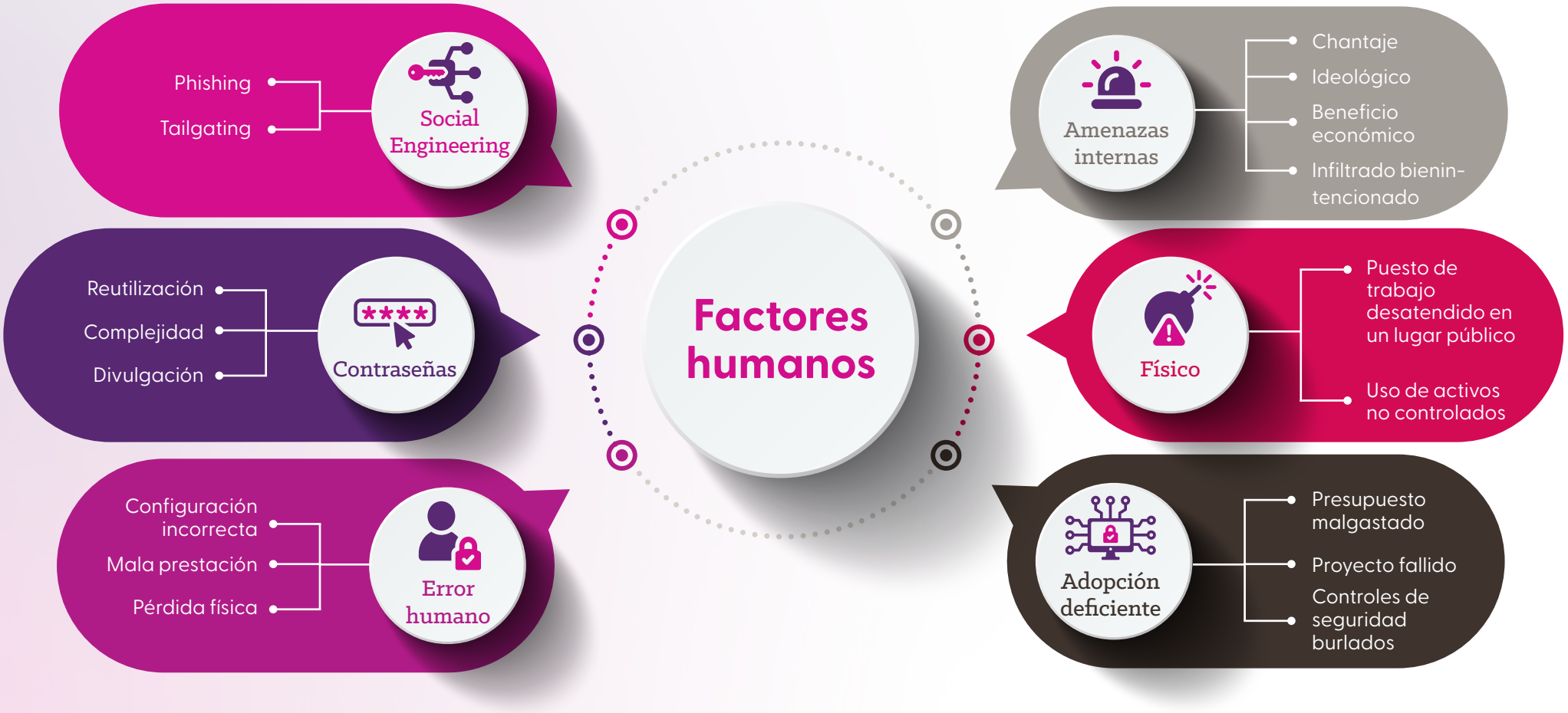
- Gartner Identifies the Top Cybersecurity trends for 2023.

## La brecha de habilidades

Si el déficit de cibercapacidades sigue siendo un obstáculo para las organizaciones, puede ser necesario trasladar a personas de otras áreas de la empresa a funciones orientadas a la seguridad y dotarlas de las capacidades que necesitan. La formación y el seguimiento en el puesto de trabajo tienen sus límites cuando las competencias que hay que enseñar escasean en la organización. En el caso de los recursos más cualificados, la formación suele considerarse esencial para mantener a los expertos técnicos que desean actualizar sus conocimientos.



# Los factores humanos pueden afectar a casi todos los aspectos de su estrategia de seguridad.



# La importancia de las personas

Debe adaptar sus factores humanos en la estrategia de seguridad a los diferentes tipos de usuarios, o personas de su organización. Un enfoque genérico no será muy eficaz: las personas deben estar capacitadas en relación con su función actual y comprender cómo pueden ayudar personalmente a la seguridad de la organización.

A continuación se muestra un ejemplo de cómo se podrían clasificar los tipos de usuarios en una empresa típica. No obstante, cada organización es diferente.

### Usuario final

- Diferentes niveles de competencias informáticas, algunos sólo tienen conocimientos muy básicos.
- Es probable que el uso de varios idiomas sea un requisito en las organizaciones globales
- Los temas pueden estar relacionados con phishing, GDPR, seguridad física, etc.

### Desarrollador

- Por lo general, tendrá conocimientos técnicos avanzados, pero es posible que desconozca las técnicas de codificación segura.
- Es probable que requiera una formación muy específica, utilizando el mismo lenguaje de programación que el desarrollador
- Es probable que la gamificación y el aprendizaje práctico tengan un mejor impacto que el aprendizaje no interactivo

### Administrador de TI

- Los usuarios técnicamente avanzados quieren poder desarrollar aún más sus conocimientos y enfrentarse a retos
- La gamificación y la competición pueden ayudar a impulsar la adopción
- Al igual que en el caso de los pilotos, la experiencia práctica en un entorno de simulación seguro y utilizado con regularidad puede ayudar a responder a situaciones reales de seguridad de alto estrés.

### Líder empresarial

- Se centra en actividades de aprendizaje en grupo basadas en el trabajo en equipo para poner a prueba los procesos de toma de decisiones y las definiciones de funciones y responsabilidades.
- Centrado en el negocio
- Puede implicar muchas funciones diferentes para poner a prueba la dinámica del equipo

# Cómo puede ayudar Insight

## Concienciación sobre seguridad gestionada para usuarios finales

En el actual entorno digital, en el que la mayoría de las operaciones comerciales se realizan en línea, es vital que los usuarios finales sean conscientes de la seguridad. Las organizaciones deben asegurarse de que sus empleados conocen los posibles peligros de los ciberataques y cómo pueden reducirlos. Esto implica enseñar a los empleados seguir buenas prácticas de gestión de contraseñas, hábitos de navegación seguros y cómo detectar e informar de Emails dudosos.

Los ataques de phishing son uno de los mayores riesgos para la ciberseguridad de una organización. Estos ataques intentan engañar a las personas para que revelen información personal como nombres de usuario, contraseñas o información financiera. Los simulacros de phishing son una forma útil de enseñar a los empleados a protegerse de estos ataques. Mediante la creación de falsos correos electrónicos de phishing que parezcan reales, los empleados pueden aprender a detectar y denunciar los mensajes dudosos.

Trabajamos con KnowBe4, experto en formación de concienciación sobre seguridad para usuarios finales, que proporciona una plataforma completa con módulos de formación, simulaciones de phishing y otras herramientas que enseñan a los empleados las amenazas más recientes y cómo evitarlas. La plataforma utiliza métodos atractivos, como vídeos, cuestionarios y juegos interactivos, para implicar a los empleados y hacer más divertida la experiencia de formación.


Su metodología se basa en un ciclo de formación y pruebas- no una vez al año, sino regularmente en pequeños tramos para reforzar la formación y poder medir las mejoras. De este modo, la formación puede impartirse en la cantidad adecuada y a las personas adecuadas.

Ofrecemos una solución completa de principio a fin que aprovecha la plataforma KnowBe4 para impartir a nuestros clientes una formación eficaz sobre concienciación en materia de seguridad. Nuestro servicio gestionado incluye supervisión e informes continuos, lo que nos permite identificar áreas en las que puede ser necesaria formación adicional y proporcionar los comentarios oportunos a nuestros clientes. De este modo, las organizaciones pueden centrarse en sus actividades empresariales principales mientras nosotros nos ocupamos de sus necesidades de formación en materia de concienciación sobre seguridad, ayudándoles a mantenerse a salvo de las ciberamenazas.

# Plataforma de ciberresiliencia del personal

Una plataforma basada en SaaS diseñada para ejercitar, evaluar, actualizar y probar de forma continua la resistencia del personal cibernético de una organización.

## Para particulares:

Un entorno de aprendizaje atractivo y gamificado que cubre todo el espectro de la formación técnica práctica para la empresa.

- Ciberprofesionales ofensivos y defensivos
- Desarrolladores y expertos en seguridad de aplicaciones
- Profesionales de la seguridad de infraestructuras y de la nube

## Para equipos:

Responder a las amenazas de seguridad requiere un esfuerzo de equipo, desde los técnicos hasta los ejecutivos. Involucramos a equipos de toda su organización para mejorar sus capacidades de toma de decisiones en situaciones de crisis y de respuesta técnica para responder de forma adaptable y eficaz a los riesgos cibernéticos.

- Equipo directivo
- Equipo de gestión de crisis
- Equipos técnicos de ciberseguridad

## Para la organización:

Ejercicios de desarrollo de competencias que impulsen un cambio de comportamiento transformador en toda la organización.

- Altos cargos
- Empleados de primera línea
- Objetivos de alto riesgo de ciberataques

Todos estos elementos son accesibles desde cualquier lugar con un simple navegador web, por lo que pueden ser utilizados incluso por personas ajenas a las organizaciones, por ejemplo, como parte de una evaluación previa a la contratación.

Como empresa, podrá:

- Probar continuamente la cibercapacidad
- Mejorar la rapidez y calidad de respuesta.
- Mejorar la contratación y el desarrollo profesional.
- Reducir las vulnerabilidades de la nube y las aplicaciones.
- Reducir los costes de ciberseguridad.

# Adopción y gestión del cambio

La adopción y la gestión del cambio desempeñan un papel crucial en el apoyo a los factores humanos de la ciberseguridad, garantizando que las medidas, políticas y tecnologías de seguridad se adopten e integren efectivamente en la cultura y las prácticas de una organización. Los factores humanos, como el comportamiento, la concienciación y los hábitos de los usuarios, suelen ser los eslabones más débiles de la ciberseguridad, ya que pueden ser explotados por agentes malintencionados.

**He aquí cómo la adopción de Insights y la gestión del cambio pueden resultar beneficiosas a la hora de abordar estos factores humanos:**

**Concienciación y educación de los usuarios:** La adopción y la gestión del cambio implica educar a los usuarios sobre las amenazas de ciberseguridad, las mejores prácticas y la importancia de la seguridad. Gracias a la formación y a una comunicación clara, los usuarios son más conscientes de los riesgos potenciales y pueden tomar decisiones con conocimiento de causa para mejorar la seguridad.

**Cambio de comportamiento:** La gestión del cambio tiene como objetivo modificar el comportamiento de los usuarios en línea con las prácticas de seguridad deseadas. Mediante el establecimiento de nuevas rutinas y hábitos, se puede animar a los usuarios a adoptar comportamientos seguros, como actualizar periódicamente las contraseñas, ser cautelosos con los correos electrónicos de phishing e informar de actividades sospechosas.

**Cambio cultural:** El éxito de las iniciativas de adopción y gestión del cambio fomentan una cultura de la seguridad dentro de la organización. Cuando la ciberseguridad se arraiga en la cultura de la organización, es más probable que los empleados den prioridad a la seguridad en sus actividades diarias, lo que conduce a un entorno general más seguro. Reducción de la resistencia: La gente suele resistirse a los cambios, especialmente cuando alteran sus rutinas familiares. Las estrategias eficaces de gestión del cambio anticipan y abordan esta resistencia, ayudando a mitigar el rechazo a las medidas de seguridad y facilitando una adopción más fluida de las nuevas prácticas.

Diseño centrado en el usuario: Los procesos de adopción y gestión del cambio implican comprender las necesidades de los usuarios y adaptar las soluciones de seguridad a esas necesidades. Este enfoque centrado en el usuario aumenta

Mejora continua: La adopción y la gestión del cambio son procesos continuos que implican recabar opiniones y ajustar las estrategias en función de las experiencias del mundo real. Esto permite a las organizaciones perfeccionar las prácticas de seguridad en respuesta a la evolución de las amenazas y las necesidades de los usuarios.

Canales de comunicación: Una comunicación eficaz es clave para fomentar la confianza y la transparencia en las iniciativas de ciberseguridad. La adopción y la gestión del cambio ofrecen vías para un diálogo abierto entre los equipos de seguridad y los usuarios, garantizando que se abordan las preocupaciones y se resuelven los malentendidos.

Mitigación de amenazas internas: Al fomentar un sentimiento de pertenencia y lealtad entre los empleados, la adopción y la gestión del cambio pueden ayudar a reducir la probabilidad de amenazas internas, en las que los empleados ponen en peligro la seguridad de forma intencionada o involuntaria.

Fomentar la responsabilidad: Los procesos de gestión del cambio hacen hincapié en la responsabilidad individual y colectiva en materia de seguridad. Cuando los usuarios se sienten responsables de sus actos, es más probable que respeten los protocolos de seguridad e informen rápidamente de posibles incidentes.

**Adaptación a las nuevas tecnologías:** Cl panorama de la ciberseguridad evoluciona rápidamente, con la aparición frecuente de nuevas tecnologías. La adopción y gestión del cambio ayudan a los usuarios a adaptarse a estos avances ofreciéndoles formación y apoyo, lo que garantiza que las nuevas tecnologías se utilicen de forma segura desde el principio..

# Conclusión

Pas personas son el mayor riesgo para la seguridad de una organización y necesitan recibir formación periódica y eficaz para convertirse en guardianes activos de la seguridad de su empresa. Una persona bien formada puede ser la última línea de defensa contra una brecha que se haya escapado de sus controles técnicos y basados en procesos.

La formación anual tradicional sobre concienciación en materia de seguridad es algo que nadie espera con impaciencia, y si una organización pone tan poco empeño en la seguridad como preparar un vídeo árido y un puñado de preguntas de tipo test, no es de extrañar que los empleados adopten el mismo enfoque con respecto a la seguridad. Considere algunas de las siguientes mejores prácticas a la hora de definir sus factores humanos en la estrategia de seguridad.

## Métodos y técnicas de formación:

- Recurrir a la gamificación y la competición para aumentar el deseo de participar de los individuos.
- Las sesiones de formación deben ser periódicas y breves: piense en 10 minutos a la semana en lugar de una hora al año para una formación general sobre concienciación en materia de seguridad.
- Aproveche las pruebas para asegurarse a nivel organizativo de que se están cumpliendo sus objetivos de madurez y para proporcionar feedback instantáneo a los participantes de que están aprendiendo el material.
- Considere la posibilidad de una formación individual muy específica, centrada en las competencias técnicas, junto con ejercicios en equipo para poner a prueba los procesos y las capacidades de trabajo en equipo.

## Comunicación y compromiso:

- Expresarse en el idioma local y en el tono adecuado puede ser tan importante como el contenido.

## Gestión de incidentes:

- Un proceso sólido de gestión de incidentes, sometido a pruebas de estrés, puede marcar la diferencia entre un incidente de seguridad banal y un incidente crítico para la empresa..

## Inclusividad en la concienciación sobre seguridad:

- Su estrategia debe tener en cuenta a todas las personas, desde el usuario ocasional de TI hasta el administrador de seguridad más técnico de su organización. Todos tienen su parte en el mantenimiento de la seguridad.

El aspecto humano de la estrategia de seguridad de una organización no es una mera formalidad; es un factor esencial que puede marcar la diferencia entre estar seguro o expuesto. Como hemos demostrado, desde el uso de métodos de formación modernos hasta garantizar la diversidad, es vital crear un enfoque integral que reconozca la importancia del elemento humano. Al centrarnos en el aprendizaje continuo, la comunicación eficaz, una sólida gestión de incidentes y la inclusión de todas las funciones de una organización, sentamos las bases de una postura de seguridad resistente. A medida que la tecnología cambia y las amenazas se vuelven más avanzadas, es la persona bien formada, consciente y comprometida la que se erigirá como una barrera sólida contra posibles violaciones. La adopción y la gestión del cambio garantizan que las medidas, políticas y tecnologías de seguridad se integren sin problemas en la cultura y las prácticas cotidianas de una organización. Cambia la perspectiva de una simple concienciación a un cambio de comportamiento práctico, creando una cultura de seguridad proactiva. Este cambio genera menos oposición, favorece la mejora continua y refuerza la responsabilidad entre los empleados. A medida que cambia el panorama de la ciberseguridad, resulta crucial mantenerse al día de las nuevas tecnologías. La gestión del cambio garantiza que las organizaciones no sólo se adapten, sino que prosperen en medio de estos cambios utilizando las nuevas herramientas con seguridad y eficacia.

# Próximos pasos

Al comprender los riesgos de su organización, elegir las tecnologías y plataformas adecuadas para el aprendizaje e integrarlas en sus procesos empresariales, Insight puede ayudarle a crear y aplicar una estrategia coherente de factores humanos en la ciberseguridad. También podemos hacer un seguimiento y mejorar la adopción a medida que avanza el despliegue. Póngase en contacto con nuestros consultores de seguridad o expertos en adopción y gestión del cambio para obtener más información.

- **es.insight.com**
- **0344 846 3333**