knowbe4

Guía para CISO:

Seis aspectos que debe tener en cuenta para la gestión de riesgos relacionados con el factor humano

WWW.KNOWBE4.COM

KnowBe4 Brazil | R. Gomes de Carvalho, 911 | Sala 208 - Vila Olímpia | CEP: 04547-003 | São Paulo-SP
Tel.: +55 (0800) 761 2668 | Correo electrónico: Sales@KnowBe4.com

CR-0481226

Introducción

Al mismo tiempo que los ciberataques se aprovechan cada vez más de la confianza humana en lugar de las fallas técnicas, los equipos directivos de seguridad de la información (CISO, por sus siglas en inglés) se ven bajo la presión de replantear cómo se gestiona el riesgo impulsado por las personas. La Gestión de riesgos relacionados con el factor humano (HRM, por sus siglas en inglés) representa un cambio de la capacitación de concientización basada en el cumplimiento a una disciplina centrada en el riesgo que se pueda medir y que se enfoque en el comportamiento, la visibilidad y la integración. Para los CISO, la exitosa evaluación e implementación de la HRM implica una alineación con los marcos de riesgos empresariales, las operaciones de seguridad y la cultura de la organización. En este documento se esbozan los aspectos clave que el liderazgo de seguridad debe abordar para garantizar que la HRM genere una reducción real de los riesgos defendibles, no solo métricas de capacitación.

Copyright © 2026 KnowBe4 Todos los derechos reservados.

1 La diferencia entre SAT y HRM

La Capacitación en concientización sobre seguridad (SAT, por sus siglas en inglés) es un enfoque muy utilizado que se centra en la formación del personal con respecto a las ciberamenazas, las políticas de la organización y las prácticas recomendadas. Los programas de SAT tienen la finalidad de generar concientización sobre los riesgos, como el phishing, el malware y los ataques de ingeniería social. Estas iniciativas suelen incluir módulos de video, cuestionarios y correos electrónicos de phishing simulado con el objetivo de evaluar la aptitud del personal.

La HRM representa un enfoque de última generación para gestionar los riesgos de ciberseguridad relacionados con las personas. En lugar de solo educar al personal, la HRM tiene como fin la identificación, cuantificación y mitigación de aquellos riesgos mediante una perspectiva holística impulsada por los datos.

→ De la concientización a la reducción medible de riesgos

La SAT se enfoca en la transferencia de conocimientos. La HRM se enfoca en la reducción del riesgo. La meta de la HRM no es simplemente informar, sino impulsar cambios en el comportamiento a través de la participación continua, la capacitación personalizada y los datos prácticos. No alcanza con que los usuarios sepan qué es el phishing. Se trata de comprender, medir y mitigar los riesgos asociados con el comportamiento humano mediante la modificación del comportamiento.

→ Del aprendizaje universal al aprendizaje personalizado

Muchas de las plataformas de SAT tratan a los usuarios de la misma manera, independientemente de sus perfiles únicos de riesgo. En cambio, la HRM utiliza la IA para generar experiencias personalizadas. El contenido de la capacitación se adapta en función del comportamiento y el rol de un miembro del personal, las amenazas reales y las interacciones previas.

→ De la capacitación estática a la defensa dinámica

Las plataformas de HRM se integran íntimamente con el conjunto de seguridad de una organización y aprovechan los datos en tiempo real que brindan herramientas como las simulaciones de phishing, la protección de terminales y los sistemas de respuesta ante incidentes. Esto permite que los equipos de seguridad cuantifiquen el riesgo a nivel individual y prioricen las intervenciones en consecuencia.

En lugar de brindar una capacitación anual estática, la HRM desarrolla un ciclo de retroalimentación dinámico que analiza los comportamientos, adapta la capacitación y cierra brechas antes de que se exploten las vulnerabilidades.

→ Del enfoque en el cumplimiento al enfoque en el comportamiento

La SAT a menudo se utiliza para satisfacer los requisitos de cumplimiento. Si bien esto es importante, la HRM cambia el enfoque de cumplir requisitos de manera superficial a realmente comprender el comportamiento humano e influir en él. Ayuda a las organizaciones a pasar de preguntarse “¿Nuestro personal conoce las reglas?” a “¿Están tomando decisiones seguras en tiempo real?”.

Copyright © 2026 KnowBe4 Todos los derechos reservados.

2 Métricas clave y ROI para un programa de HRM

La mayoría de las métricas de SAT miden la participación y la retención de conocimientos, no los cambios en el comportamiento real. Si bien la SAT es más fácil de rastrear que la HRM, la facilidad de medición no es lo mismo que el impacto real en la seguridad. Para los CISO que se enfocan en la reducción de riesgos alineada con el negocio, el desafío es tener un modo simple y defendible de justificar la inversión.

Métricas tradicionales de SAT	Métricas de HRM (de comportamiento y basadas en riesgos)
Índice de finalización de la capacitación Porcentaje del personal que completó la capacitación obligatoria.	**Puntaje de riesgo humano** Puntaje de riesgos impulsado por IA en función de comportamientos individuales del personal, como la susceptibilidad ante el phishing, las anomalías en el inicio de sesión y el manejo de datos delicados.
Índice de clics en la simulación de phishing Mide cuántos miembros del personal cayeron ante los ataques de phishing simulado.	**Índice de resiliencia ante el phishing** Rastrea no solo la cantidad de clics, sino también cuántos miembros del personal reportan los intentos de phishing en comparación con quienes los ignoraron.
Cuestionario/Puntajes de evaluación Puntajes promedio en las pruebas de conocimientos sobre ciberseguridad luego de la capacitación.	**Índice de denuncia de amenazas reales** Porcentaje de miembros del personal que reportaron correctamente los incidentes de seguridad y los intentos de phishing reales.
Tiempo dedicado a la capacitación Mide cuánto tiempo participa el personal con el contenido de la capacitación sobre seguridad.	**Reducción de comportamientos riesgosos** Mide la disminución de comportamientos como compartir credenciales, descargar software no autorizado o ignorar advertencias de seguridad.
Participación en la capacitación anual sobre seguridad Garantiza el cumplimiento, pero no mide el comportamiento de seguridad.	**Eficacia de la intervención de seguridad justo a tiempo** Rastrea con qué frecuencia cambia el personal sus comportamientos riesgosos tras recibir alertas de seguridad en tiempo real.
	Índice de detección de amenazas internas Usa análisis de comportamiento para indicar las posibles amenazas internas o el comportamiento negligente antes de que ocurran incidentes.

Copyright © 2026 KnowBe4 Todos los derechos reservados.

3 ¿Por qué conviene adoptar la HRM ahora?

El momento para pasar de SAT a HRM y la aceptación de este cambio son inquietudes comunes. El liderazgo de la organización espera que los CISO tomen decisiones estratégicas de ciberseguridad que tengan un efecto dominó en todo el negocio y que sepan que el momento de realizar los cambios es tan importante como los cambios en sí.

El momento de adoptar la HRM es ahora, debido a cuatro impulsores principales:

1. La ingeniería social y los ataques de phishing representan el mayor riesgo cibernético

Según las investigaciones, entre el 70 % y el 90 % de todos los ciberataques exitosos involucran ingeniería social y phishing.[1] Quienes perpetran estos ataques son personas astutas que comprenden que nuestras defensas han mejorado de forma significativa. Por eso el enfoque cambió y ahora atacan al usuario final.

2. La IA seguirá agravando el problema

Más del 95 % de profesionales de ciberseguridad cree que el contenido generado con IA dificulta la detección del phishing.[2] La IA impulsa el nacimiento de nuevos tipos de ataques de ingeniería social muy convincentes. El personal debe formarse continuamente sobre cómo detectarlos y denunciarlos.

3. La formación tradicional del personal ya no es suficiente

La SAT tradicional por sí sola no es una defensa adecuada el día de hoy, a pesar de ser una capa crucial. Al igual que se han fortalecido la detección reactiva y la respuesta para incluir el rastreo proactivo de amenazas, la gestión de riesgos relacionados con el factor humano en medio del panorama de amenazas actual exige formación y compromiso en otro nivel a fin de mejorar los comportamientos reales de los usuarios.

4. Los mandatos normativos están creciendo

Las organizaciones se enfrentan a requisitos crecientes que se relacionan con la generación de informes y la divulgación de la postura de ciberseguridad. Los gobiernos, las entidades normativas y hasta las aseguradoras reconocen oficialmente que el eslabón más débil de la seguridad suele ser el elemento humano.

1 KnowBe4, If Social Engineering Account for up to 90% of Attacks, Why Is It Ignored? (Si la ingeniería social representa hasta el 90 % de los ataques, ¿por qué se la ignora?)
2 LastPass, Social engineering: Combatting an evolving threat (Ingeniería social: el combate contra una amenaza en evolución), 2024

Copyright © 2026 KnowBe4 Todos los derechos reservados.

4 Alinear la HRM con los marcos de negocios y de riesgo cibernético

Para los CISO, la HRM debe alinearse directamente con los marcos establecidos de negocios y de riesgo cibernético para poder ser fiables y eficaces. La HRM debería generar datos medibles sobre el riesgo relacionado con el factor humano para la gestión de riesgos empresarial, lo que garantiza que las amenazas impulsadas por las personas se evalúen junto con las vulnerabilidades técnicas. Cuando está correctamente alineada, la HRM respalda el cumplimiento normativo, mejora la preparación para las auditorías y ayuda al liderazgo a comprender cómo influye el comportamiento humano en los riesgos materiales. En lugar de operar de forma aislada, la HRM debería integrarse con las estructuras de generación de informes y gobernanza existentes, entre las que se incluyen las siguientes:

- Marcos regulatorios y de Gobierno, Riesgo y Cumplimiento (GRC, por sus siglas en inglés) (p. ej., Comisión de Bolsa y Valores de EE. UU. [SEC, por sus siglas en inglés], Directiva sobre la seguridad de las redes y sistemas de información [NIS2, por sus siglas en inglés], Reglamento de Resiliencia Operativa Digital [DORA, por sus siglas en inglés]).
- Respuesta ante incidentes y procesos de manejo de crisis.
- Gobernanza de acceso e identidad e iniciativas de confianza cero.

Esta alineación les permite a los CISO convertir el riesgo humano en un impacto de negocios.

5 La cultura y la integración organizacional

La HRM es una iniciativa cultural y una capacidad de seguridad en partes iguales. La reducción sostenible del riesgo requiere comportamientos de seguridad que se deben reforzar en toda la organización; no debe limitarse a eventos de capacitación anual. Los CISO deben asegurarse de que la HRM se integre con el liderazgo de RR. HH., del departamento legal, de comunicaciones y de negocios para integrar las expectativas de seguridad en la incorporación de personal, la ejecución de políticas y la gestión del rendimiento. Cuando se reconoce y refuerza un comportamiento seguro, el personal se vuelve una parte activa en la defensa, en lugar de un ente receptor de capacitaciones.

Copyright © 2026 KnowBe4 Todos los derechos reservados.

6 La integración con las herramientas de seguridad y los flujos de trabajo

Para que la HRM genere resultados medibles de seguridad, se debe integrar por completo con las herramientas existentes de seguridad y los flujos de trabajo operativos. La HRM no debe actuar como una plataforma independiente de concientización, sino como una fuente de inteligencia sobre riesgos centrada en los humanos que enriquezca el ecosistema general de seguridad. Esto permite una detección más rápida de los ataques que se basan en la confianza y una priorización más precisa de los riesgos e intervenciones dirigidas, como la capacitación justo a tiempo o los controles de acceso.

Las integraciones clave deberían incluir lo siguiente:

- Plataformas de identidad (Gestión de Identidades y Accesos [IAM, por sus siglas en inglés]/Autenticación Multifactor [MFA, por sus siglas en inglés])
- Portales de correo electrónico (reporte de intentos de phishing)
- Tableros de Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés)/Gestión de Información y Eventos de Seguridad (SIEM, por sus siglas en inglés)
- Tableros de riesgos para personal ejecutivo

Obtenga más información sobre **KnowBe4 HRM+**

Copyright © 2026 KnowBe4 Todos los derechos reservados.

Prueba de seguridad contra el phishing (PST) gratuita

Descubra qué porcentaje de sus empleados tienen predisposición para ser víctimas de phishing (phish-prone) con la prueba de seguridad contra el phishing (PST) gratuita.

Automated Security Awareness Program gratuito

Cree un programa en concientización sobre seguridad personalizado para su organización.

Phish Alert Button gratuito

Ahora sus empleados tienen una forma segura de denunciar los ataques de phishing con un solo clic.

Comprobación de exposición del correo electrónico gratuita

Descubra antes que los malhechores cuál de las direcciones de correo electrónico de sus usuarios está expuesta.

Domain Spoof Test gratuita

Descubra si hackers pueden falsificar una dirección de correo electrónico de su propio dominio.

Acerca de KnowBe4

KnowBe4 capacita al personal para que todos los días puedan tomar decisiones de seguridad más acertadas. KnowBe4, que es elegida por más de 70 000 organizaciones de todo el mundo, ayuda a fortalecer la cultura de la seguridad y a gestionar el riesgo humano. KnowBe4 ofrece una plataforma integral impulsada por IA para la gestión del riesgo humano que crea una capa defensiva adaptable capaz de fortificar el comportamiento de los usuarios ante las últimas amenazas para la ciberseguridad. La plataforma HRM+ contiene módulos de capacitación para la concientización y el cumplimiento, seguridad del correo electrónico en la nube, asesoramiento en tiempo real, protección antiphishing colaborativa, AI Defense Agents (agentes de defensa con IA) y mucho más. KnowBe4 es la única plataforma de seguridad global de su estilo, y usa contenido, herramientas y técnicas de protección de la ciberseguridad personalizados y pertinentes para incentivar al personal a pasar de ser la mayor posible víctima de ataques a ser el activo más importante de la organización. Para obtener más información, visite www.KnowBe4.com.

knowbe4

KnowBe4 Brazil | R. Gomes de Carvalho, 911 | Sala 208 - Vila Olímpia | CEP: 04547-003 | São Paulo-SP
Tel.: +55 (0800) 761 2668 | www.KnowBe4.com | Sales@KnowBe4.com

Los nombres de otros productos y empresas aquí mencionados pueden ser marcas comerciales o marcas comerciales registradas de sus respectivas empresas.