

Le presentamos  
AIDA: la gestión de  
riesgos humanos a la  
manera de KnowBe4



# Le presentamos AIDA: la gestión de riesgos humanos a la manera de KnowBe4

## Índice

|                                               |   |
|-----------------------------------------------|---|
| <b>Introducción</b>                           | 3 |
| Hablemos de AIDA                              | 3 |
| La conexión con la gestión de riesgos humanos | 4 |
| <b>Los primeros cuatro agentes de AIDA</b>    | 4 |
| Agente de capacitación automatizado           | 5 |
| Agente de generación de plantillas            | 6 |
| Agente de actualización de conocimientos      | 7 |
| Agente de cuestionarios sobre políticas       | 8 |
| <b>De aquí en adelante</b>                    | 9 |
| <b>El resultado</b>                           | 9 |

# Introducción

El aumento de los ciberataques impulsados con IA está captando la atención de todos los profesionales de seguridad de la información. Según estudios de la industria, más del 95 % de los profesionales de ciberseguridad cree que el contenido generado con IA dificulta la detección del phishing.

Este avance tecnológico en manos de malhechores generó un nuevo tipo de ataques de ingeniería social muy convincentes que son difíciles de combatir con capacitación en concientización sobre seguridad (SAT, por sus siglas en inglés) de carácter genérico.

Es hora de combatir la IA con IA. Para eso, llega KnowBe4 AIDA: agentes de defensa con inteligencia artificial. AIDA es un paquete de agentes impulsados con IA que optimiza su enfoque a la gestión de riesgos humanos (HRM, por sus siglas en inglés) mediante varias tecnologías de IA a fin de preparar capacitaciones para usuarios personalizadas, adaptables y muy eficaces que cambien de verdad los comportamientos.

En este informe técnico, veremos la manera en que los cuatro primeros agentes de AIDA pueden ayudar a optimizar su estrategia de HRM y exploraremos casos de uso.

## Hablemos de AIDA

AIDA es un paquete integral de agentes que ya incluye IA y que revoluciona los métodos de SAT de las organizaciones. AIDA emplea la IA para ofrecer capacitaciones hiperpersonalizadas, eficientes y adaptables que reducen los riesgos de las organizaciones y fomentan cambios duraderos de comportamiento.

A diferencia de otros productos clásicos de SAT, KnowBe4 AIDA continuamente aprende y se adapta a las necesidades particulares de su organización para garantizar el máximo impacto y retorno de la inversión de sus iniciativas de concientización sobre seguridad. Por ejemplo, al reducir de un promedio de siete días a apenas unos segundos el tiempo que les lleva a sus administradores crear contenido de capacitación, AIDA le ahorra tiempo drásticamente a su equipo de seguridad.

Más adelante en este informe técnico, veremos en mayor detalle cada uno de los primeros cuatro recursos de AIDA, pero aquí le presentamos un resumen:



**Agente de capacitación automatizado:** utiliza IA con 316 indicadores que influyen en 37 factores de las siete áreas de conocimiento para analizar el historial de aprendizaje, la función, el puntaje de riesgo, los patrones de comportamiento y hasta los idiomas de sus usuarios a fin de poder asignar automáticamente el contenido más relevante y atractivo. Esto garantiza que cada uno de sus usuarios, independientemente de su cargo o ubicación, reciba capacitación personalizada según sus necesidades y su estilo de aprendizaje específicos. Este recurso permite optimizar la retención y la aplicación real de sus prácticas recomendadas de seguridad.



**Agente de generación de plantillas:** AIDA aprovecha la IA generativa para crear plantillas de phishing muy realistas que pueden reflejar los vectores de ataque actuales. Los indicadores de ingeniería social (SEI), o señales de alarma, se basan en el [marco Phish Scale del Instituto Estadounidense de Estándares y Tecnología \(NIST, por sus siglas en inglés\)](#).



**Agente de actualización de conocimientos:** AIDA proporciona actualizaciones de conocimientos breves en intervalos óptimos y garantiza que sus usuarios realmente apliquen los conceptos de seguridad críticos.



**Agente de cuestionarios sobre políticas:** AIDA genera cuestionarios inteligentes basados en las políticas de seguridad y cumplimiento específicas de su organización. Esto garantiza que sus usuarios no solo reconozcan, sino que verdaderamente comprendan las pautas que se espera que sigan.

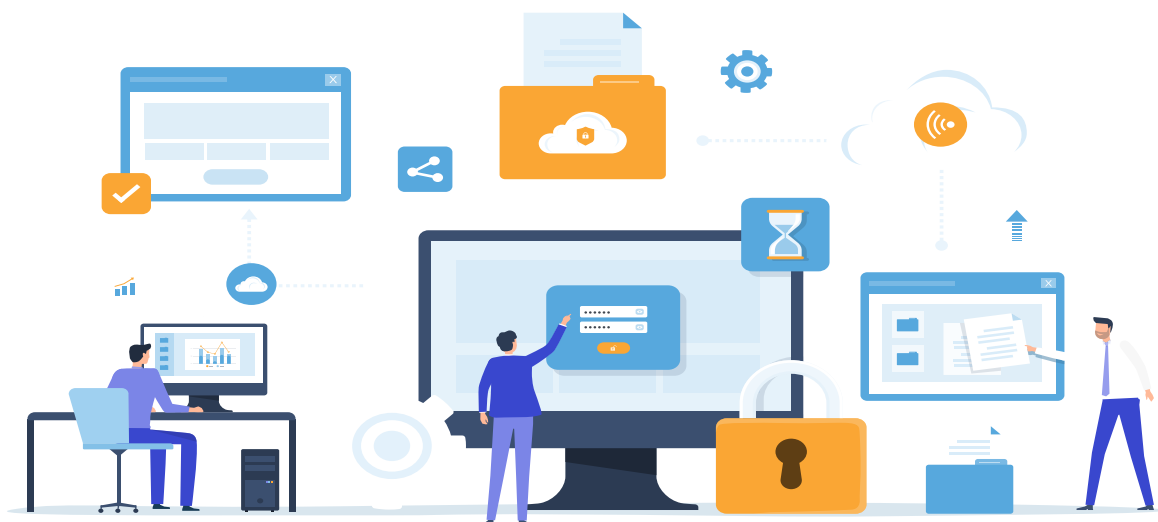
## La conexión con la gestión de riesgos humanos

La HRM ahora es la manera principal de atender la necesidad permanente de sólidas culturas de seguridad en las organizaciones de todos los tamaños. El concepto no se enfoca solo en ofrecer SAT con una frecuencia determinada. La meta es crear una cultura de la seguridad positiva a través de tres tácticas principales:

- 1 Cuantificar el riesgo humano mediante la detección y la medición del comportamiento humano
- 2 Utilizar esas mediciones para implementar contenido de capacitación pertinente y personalizado
- 3 Definir actualizaciones de conocimientos recurrentes para garantizar que los usuarios sepan cómo protegerse de los riesgos cibernéticos de mayor prevalencia e impacto

La SAT genérica que se encuentra en el mercado ya no es eficaz en su complejo entorno de trabajo. Un evento de capacitación por año no es suficiente. Además, los usuarios tienen agendas cada vez más cargadas, por lo cual, en las capacitaciones, debe aprovecharse bien el tiempo. Una estrategia de HRM le permite ofrecer contenido pertinente y atractivo que cambie el comportamiento del usuario y tenga eco en diferentes roles, departamentos e incluso idiomas. AIDA es el pilar de esta iniciativa.

Ahora profundizaremos en los primeros cuatro recursos de AIDA que hacen posible todo esto y hablaremos de lo que se viene.



## Los primeros cuatro agentes de AIDA

Antes de hablar de estos cuatro agentes, exploremos un recurso de KnowBe4 clave para todos ellos: SmartRisk Agent™ de KnowBe4. Esta función ofrece información y parámetros procesables, llamados "puntaje de riesgo", para que pueda comprender las fortalezas y las debilidades de la seguridad de su organización.

[SmartRisk Agent](#) utiliza los datos de comportamiento de los usuarios finales de todos los productos de KnowBe4 para medir el riesgo cibernético de los seres humanos. Los puntajes de riesgo multidimensionales de este agente están diseñados para simplificarle la detección de posibles problemas en los niveles del usuario, el grupo y la organización. Cuantos más productos KnowBe4 use, obtendrá mejores datos.

Esto es lo que puede hacer cada uno de los primeros cuatro agentes:



## Agente de capacitación automatizado

### Lo que hace

El agente de capacitación automatizado analiza varios puntos de datos, incluidos los [puntajes de riesgo](#), los resultados de pruebas de phishing y las preferencias de aprendizaje individuales, para crear una experiencia de capacitación personalizada para cada usuario. Se luce a la hora de identificar los conocimientos faltantes y ocuparse de aportarlos a través de módulos de aprendizaje dirigidos obtenidos en la [enorme biblioteca de contenido de ModStore de KnowBe4](#).

### Cómo usarlo

Configure el agente para alinearlos con las necesidades específicas de su organización. Por ejemplo, defina los criterios para la inscripción, los plazos para la finalización y las preferencias para las notificaciones. Todo eso puede hacerlo desde la consola de KnowBe4. El modo de prueba del agente le permite hacer una vista previa de las recomendaciones de la capacitación antes de implementarla para que se asegure de estar cómodo con las tareas automatizadas.

¿Necesita un seguimiento del rendimiento de las capacitaciones? Acceda a métricas de seguimiento, como las tasas de finalización de tareas y los resultados de las encuestas, a fin de medir la eficacia de su programa de capacitación.

### Casos de uso

**Fortalecimiento de puntos débiles en cuanto al phishing:** a partir de las respuestas de los usuarios o los malos resultados de pruebas de phishing simulado específicas, asigne automáticamente capacitaciones que les enseñen a los usuarios las estrategias y las tácticas de phishing específicas antes de que las vean en la vida real.

**Integración de nuevos miembros del personal:** evalúe el puntaje de riesgo de los nuevos miembros del personal y sugiera SAT pertinente para los conocimientos que ya poseen mediante grupos inteligentes especiales.



## Agente de generación de plantillas

### Lo que hace

El generador de plantillas de phishing produce correos electrónicos de phishing muy convincentes personalizados para las necesidades y el perfil de riesgo de su organización mediante el poder de la IA generativa integrada. El agente puede diseñar diversos escenarios de phishing en varios idiomas y con diferentes niveles de dificultad, tonos y vectores de ataque a fin de garantizar que sus usuarios estén preparados para todo el abanico de amenazas que podrían encontrar en la vida real.

### Cómo usarlo

Usted puede configurar fácilmente diferentes variables, como el idioma, el lugar y el vector de ataque. Configure la dificultad de los correos electrónicos de phishing simulado seleccionando [indicadores de ingeniería social \(SEI\)](#) específicos o eligiendo un nivel de dificultad predefinido. Las plantillas, una vez generadas, se pueden consultar, editar y guardar para el futuro, lo cual le ahorra tiempo valioso a la hora de crear y gestionar un buen programa de simulación de phishing.

### Casos de uso

***Simulación de correos electrónicos corporativos comprometidos (BEC, por sus siglas en inglés):*** tómese una semana por mes o por trimestre para diseñar BEC que parezcan provenir de su director ejecutivo (CEO) u otros miembros ejecutivos de rango elevado. Use los recursos de IA generativa del agente para imitar el estilo de redacción del ejecutivo y solicitar una transferencia bancaria o alguna otra acción urgente.

***Pruebas de phishing en varios idiomas:*** prepare e implemente rápidamente correos electrónicos de phishing en varios idiomas para una fuerza de trabajo global. El generador de plantillas hasta puede adaptar el texto de los correos electrónicos a una región específica con las expresiones, los matices y los estilos culturales locales.

***Respuesta rápida ante las amenazas emergentes:*** ¿Halló un ataque totalmente nuevo en la vida real? Solo necesita unos minutos con el generador de plantillas para diseñar un ataque de phishing simulado similar que prepare a su fuerza de trabajo para lo que se viene.





## Agente de actualización de conocimientos

### Lo que hace

El agente de actualización de conocimientos ayuda a los usuarios a perfeccionar sus habilidades de ciberseguridad y ganar insignias con cuestionarios breves generados con IA basados en escenarios: una forma rápida y divertida de repasar los puntos clave de su capacitación reciente.

### Cómo usarlo

Habilite y configure el recurso en la pestaña Capacitación con AIDA o cuando cree una nueva campaña de capacitación. Aquí, puede definir parámetros como el plazo entre la finalización de una capacitación y la disponibilidad de la actualización de conocimientos. Una vez activado el recurso, los usuarios pueden acceder a sus actualizaciones de conocimientos en su Experiencia de aprendizaje, lo que simplifica la interacción con este elemento continuo de su proceso de aprendizaje.

### Casos de uso

**Refuerzo de la concientización sobre phishing:** las actualizaciones de conocimientos generadas con IA basadas en escenarios se pueden usar en una capacitación sobre medidas correctivas ofrecida luego de que el usuario haya hecho clic en un correo electrónico de phishing simulado, a fin de complementar la capacitación inicial. Este refuerzo sostenido ayuda a mantenerse alerta a las cambiantes tácticas de phishing.

**Retención de las capacitaciones de cumplimiento:** las actualizaciones periódicas y enfocadas en temas clave del cumplimiento permiten que las organizaciones sometidas a requisitos regulatorios específicos demuestren la diligencia debida continua para mantener una cultura de cumplimiento, y así reducir los riesgos y mejorar los resultados de las auditorías.



## Agente de cuestionarios sobre políticas

### Lo que hace

Este agente de cuestionarios sobre políticas impulsado con IA genera automáticamente cuestionarios basados en las políticas específicas de su organización, lo que garantiza que los empleados no solo lean, sino también comprendan y retengan la información clave.

### Cómo usarlo

En su consola de KnowBe4, puede agregar la política de su organización en formato PDF. Tras agregar la política, puede editar y administrar preguntas de cuestionarios relacionadas con la política y, luego, crear una campaña de capacitación para asignar la política a sus usuarios. Una vez que haya asignado la política a una campaña, puede realizar un seguimiento del progreso y los reconocimientos de sus usuarios.

### Casos de uso

***Incorporación de empleados nuevos:*** a través de cuestionarios sobre políticas personalizados, puede asegurarse de que los empleados nuevos no solo consulten las políticas, sino también demuestren haberlas entendido. Esto puede proporcionar un punto de referencia mensurable de la eficacia de la capacitación inicial sobre cumplimiento y reducir el riesgo de incumplimiento de las políticas debido a interpretaciones erróneas.

***Revisión anual de las políticas:*** simplifique su proceso anual de revisión de las políticas usando el agente de cuestionarios sobre políticas para generar rápidamente cuestionarios actualizados que reflejen los cambios en las pautas y las reglas de la empresa. Las campañas de capacitación basadas en políticas ayudan a garantizar la retención de los conocimientos y ofrecen a los administradores métricas claras del nivel de comprensión de las políticas en toda la empresa, lo que permite identificar áreas donde se necesita más capacitación o aclaraciones.



## De aquí en adelante

Las capacidades de estos cuatro agentes se verán considerablemente optimizadas al trabajar al unísono con un modelo de orquestación impulsada con IA, que tiene un enfoque de actividad continua basado en metas para lograr el riesgo humano más bajo en su organización.

Pero esto es apenas el comienzo. Se planea agregar lo siguiente en el futuro:

- **Agente de orquestación:** este agente impulsado con IA asumirá el rol de administrador de SAT y gestionará las simulaciones de phishing, la distribución y los informes.
- **Agente impulsado por metas:** este agente optimizará la definición de objetivos, los vectores de ataque y la frecuencia de las capacitaciones para reducir en la máxima medida el riesgo humano en su organización.
- **Agente de defensa adaptable:** este agente, al considerar los horarios de trabajo y las amenazas actuales, programará las capacitaciones en los horarios menos molestos y adaptará el contenido para atender los riesgos emergentes.
- **Agente de evaluación de la SAT:** este agente creará evaluaciones de SAT personalizadas en función de las políticas y los procedimientos específicos de su organización.

## El resultado

AIDA no es solo el próximo paso de la HRM a la manera de KnowBe4. Es un gran salto para ofrecer un paquete de agentes impulsados con IA que transforma la manera de ocuparse de la HRM. AIDA capacita a su organización para que se mantenga a la vanguardia usando la IA para vencer a las amenazas de la IA.

Esto es lo que AIDA les aporta a usted y su organización:

- La alineación de AIDA con el [marco Phish Scale del NIST](#) garantiza que su SAT sea coherente con las iniciativas de seguridad más amplias de su organización.
- Al reducir de un promedio de 7 días a apenas unos segundos el tiempo que les lleva a sus administradores crear contenido de capacitación, AIDA le ahorra tiempo drásticamente a su equipo de seguridad.
- Mejore las relaciones entre su equipo de seguridad y otros departamentos garantizando que los usuarios estén alineados con los objetivos de seguridad, lo cual fomenta la cultura de la seguridad de su organización.
- Al gestionar activamente el riesgo humano de manera eficiente, tendrá flexibilidad en su presupuesto de seguridad para invertir en otras iniciativas clave.
- Maximice el valor de su conjunto tecnológico de seguridad existente con la integración perfecta de AIDA.

KnowBe4 es el único proveedor que abarca en su totalidad la concientización, el comportamiento y la cultura de la seguridad para que las organizaciones puedan abordar el elemento humano de la ciberseguridad. KnowBe4 se enfoca en ayudar a las organizaciones a crear una buena cultura de la seguridad gestionando el riesgo humano con base en los datos.

Ver a AIDA en acción →

## Recursos adicionales



### **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.



### **Programa en concientización sobre seguridad automatizado 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 los hackers pueden falsificar una dirección de correo electrónico de su propio dominio.



## Acerca de KnowBe4

KnowBe4 capacita a sus empleados para que todos los días puedan tomar decisiones de seguridad más acertadas. Decenas de miles de organizaciones en todo el mundo confían en la plataforma KnowBe4 para fortalecer su cultura de seguridad y reducir el riesgo humano. KnowBe4 desarrolla una capa humana de defensa para que las organizaciones puedan reforzar el comportamiento de los usuarios a través de capacitaciones de vanguardia sobre cumplimiento y concientización sobre seguridad.

La implementación de KnowBe4 se traduce en usuarios que están alerta y se preocupan por el daño que causan el phishing, el ransomware y otras amenazas de ingeniería social. La plataforma incluye un paquete completo de capacitaciones sobre concientización y cumplimiento, asesoramiento en tiempo real para los usuarios, ingeniería social simulada por IA y defensa colectiva contra el phishing.

Con contenido en más de 35 idiomas, KnowBe4 ofrece la biblioteca más grande del mundo con contenido interesante que siempre está actualizado con el fin de reforzar su firewall humano.

**Para obtener más información, visite [www.KnowBe4.com](http://www.KnowBe4.com).**

# KnowBe4

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200, São Paulo-SP  
Tel: +55 (0800) 761 2668 | [www.KnowBe4.com](http://www.KnowBe4.com) | [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)

© 2025 KnowBe4, Inc. Todos los derechos reservados. Otros nombres de productos y empresas aquí mencionados pueden ser marcas comerciales y/o marcas comerciales registradas de sus respectivas empresas.

07F01K01