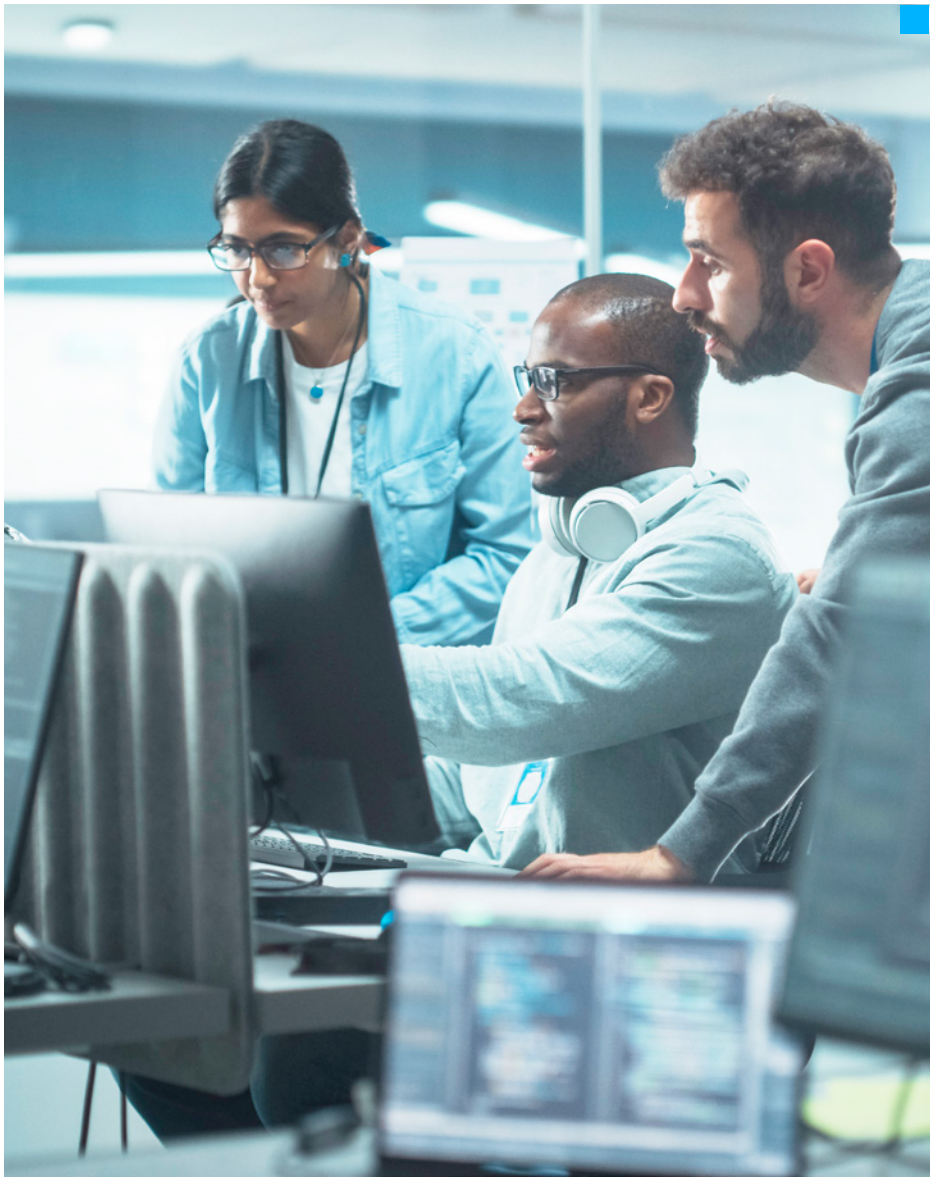
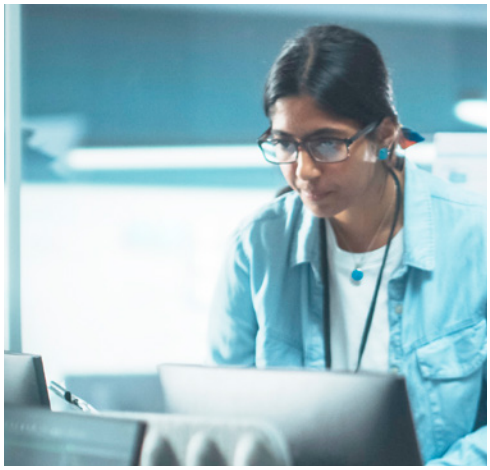


# IA y automatización para la ciberseguridad

*Cómo los líderes alcanzan el éxito combinando la tecnología y el talento*

## Cómo puede ayudar IBM

IBM Security implementa tecnologías de IA, como machine learning y el procesamiento del lenguaje natural, para ayudar a los analistas de las operaciones de seguridad a adelantarse a las amenazas y reducir los costes y el tiempo de respuesta. Para obtener más información, visite: ibm.com/es-es/security/artificial-intelligence.



# Puntos clave

*Al reducir las tareas rutinarias, la IA combinada con la automatización permite a los equipos de ciberseguridad utilizar la escasa experiencia humana donde más se necesita.*

## El ritmo y el volumen de los incidentes de seguridad demandan un nuevo enfoque operativo

La IA combinada con la automatización aumenta la visibilidad y productividad en las operaciones de seguridad. Los líderes en la adopción de la IA están supervisando el 95 % de las comunicaciones de red y reduciendo el tiempo para detectar incidentes en un tercio.

## La IA con fines de seguridad está ganando terreno

Los ejecutivos informan de una amplia adopción de la IA en las operaciones de seguridad: el 93 % ya la utiliza o está considerando implementarla.

## Los líderes en la adopción de la IA con fines de seguridad están mejorando las mediciones de desempeño en los costes clave

Los más destacados aumentaron la rentabilidad de la inversión en seguridad (ROSI, por sus siglas en inglés) en un 40 % o más y redujeron los costes de las vulneraciones de datos en al menos un 18 %, lo que ayudó a liberar fondos que se pueden reinvertir en su plantilla de ciberseguridad.

# El cambio rápido eleva el riesgo cibernético

Las operaciones digitales modernas están generando valor y, a su vez, creando nuevas vulnerabilidades.

En 2021, hubo un aumento de las amenazas de ciberseguridad. Los sistemas de Colonial Pipeline y de varias plantas de procesamiento de agua de los Estados Unidos fueron algunos de los objetivos de los ataques.[1] Según un estudio reciente, el ransomware aumentó un 105 % de 2020 a 2021, y la producción se convirtió en la industria más afectada.[2] En el último año también se han producido algunos de los ataques a las cadenas de suministro de más impacto hasta la fecha. Desde los exploits de SolarWinds y Microsoft Exchange Server hasta las vulnerabilidades de Apache Log4j, los ataques de alto perfil han invadido los portales de noticias, lo que ha aumentado la toma de conciencia y ha generado alarma entre los líderes empresariales y sus clientes.[3]

¿Qué hace que la situación actual se diferencie de manera categórica del pasado?

En resumen, la pandemia aceleró la transformación digital y amplió tanto las oportunidades como los riesgos.[4] Ahora hay muchos más trabajadores remotos. Más usuarios del cloud. Más servicios de cloud. Integraciones de sistemas fundamentales con colaboradores externos. Una increíble cantidad de dispositivos periféricos que transmiten datos de IoT al cloud. Todos están interconectados y son interdependientes, y permiten una conectividad sofisticada y la creación de valor avelocidades y escalas que eran imposibles hace algunos años.

Pero los beneficios de la innovación también tienen un coste: nuevos dispositivos, nuevos colaboradores y nuevas integraciones abren la organización de formas que pueden aumentar de manera radical su superficie general de ataque. Han surgido nuevos vectores de amenaza: desde un proveedor despistado hasta un empleado insatisfecho; desde la exfiltración de datos hasta la denegación del servicio y el ransomware. Y, para seguir complicando la cuestión, las tácticas, las técnicas y los procedimientos de los actores de amenazas evolucionan: utilizan la inteligencia artificial (IA) y la automatización para identificar debilidades y desarrollar ataques más eficaces (consulte la Figura 1).[5]

El resultado neto es el duro descubrimiento de muchos ejecutivos de que las operaciones digitales continuas aportan valor, pero también crean nuevas vulnerabilidades. A pesar de la eficacia que permiten los servicios tecnológicos avanzados, muchas organizaciones se están dando cuenta lentamente de que sus huellas digitales están repletas de complejidades y aspectos desconocidos. A esta dinámica se suma el hecho de que los pequeños grupos de seguridad se ven abrumados por un exceso de datos de fuentes dispares, la abundancia de herramientas y, con frecuencia, la escasez de información. Estas dificultades pueden superar con facilidad las destrezas de los expertos en seguridad con más conocimientos y la capacidad de los equipos de operaciones de ciberseguridad más grandes y mejor preparados.

## La realidad operativa actual demanda un nuevo enfoque

Para posicionar a sus equipos para el éxito, los líderes en ciberseguridad deben adoptar una postura más preventiva y proactiva para proteger las operaciones comerciales básicas. Nuestra investigación señala que más organizaciones están optando por un enfoque orientado hacia el futuro con respecto a la gestión de amenazas y están adoptando la automatización con tecnología de IA para obtener mejor información, productividad y economía de escala.

Las tecnologías de IA pueden transformar la seguridad de cuatro formas clave:

- Las capacidades de machine learning ayudan a identificar patrones, adoptar inventarios de activos y servicios nuevos y perfeccionar el desempeño de los modelos de IA.
- Las capacidades de razonamiento ayudan a documentar el análisis de datos, mejorar el modelado de escenarios y prever nuevos vectores de ataque.
- El procesamiento de lenguaje natural se puede usar para minar fuentes de datos textuales, mejorar la inteligencia en materia de amenazas y enriquecer los recursos de conocimientos.
- La automatización puede ayudar a orquestar las tareas que llevan mucho tiempo, mejorar los tiempos de respuesta y reducir la carga de los analistas humanos.

En conjunto, estas capacidades pueden transformar las operaciones de seguridad.

En este informe, demostramos cómo esta combinación de IA y automatización puede facilitar un desempeño mucho mejor, ya sea en términos de velocidad, información o flexibilidad. Estas mejoras en el desempeño permiten que los equipos de ciberseguridad se concentren en lo que realmente importa: ofrecer protección proactiva contra amenazas, detectar las amenazas, responder a ellas y recuperarse de su impacto, al mismo tiempo que se reducen los costes y la complejidad.

FIGURA 1

**Disruptores de la seguridad**

Los equipos de operaciones de seguridad se están enfrentando a nuevos desafíos

Vectores de ataque nuevos y en expansión

Los atacantes están inclinándose por las amenazas adaptativas y multivariantes

Los atacantes están inclinándose por la automatización

Brechas en las habilidades cibernéticas y capacidad limitada

Falta de visibilidad y coordinación con proveedores externos

Falta de información en los diferentes tipos de datos: metadatos, contextuales y de comportamiento

Exceso de información de distintas fuentes de datos y herramientas

**Capítulo 1**

# La IA con fines de seguridad gana terreno de manera veloz

Para entender cómo se está usando la IA para respaldar las operaciones de seguridad y cuantificar su impacto en el desempeño de la ciberseguridad, el IBM Institute for Business Value (IBV) se asoció con APQC (American Productivity and Quality Center) para encuestar a 1000 ejecutivos responsables de la ciberseguridad de la TI y la tecnología operativa de sus organizaciones. Ellos representan a 16 industrias y 5 regiones globales (consulte Metodología del estudio y la investigación en la página 32).

Les pedimos a los encuestados que proporcionaran información sobre el desempeño de la función de seguridad de sus organizaciones y la medida en que están aplicando la IA y la automatización para gestionar el riesgo cibernético y el cumplimiento. También describieron cómo están usando la IA para respaldar las operaciones de seguridad con fines de protección, prevención y detección, y para los procesos de respuesta. Usamos esta información para evaluar el impacto de la IA en el desempeño de la ciberseguridad, con énfasis en la productividad, la resiliencia y los beneficios comerciales asociados.

En general, descubrimos que la mayoría de las empresas, tanto a nivel global como en las diferentes industrias, está adoptando o considerando adoptar la IA combinada con la automatización en sus funciones de seguridad. El 64 % de los encuestados ha implementado la IA en las funciones de seguridad, en al menos uno de los procesos del ciclo de vida de la seguridad, y el 29 % lo está considerando. En otras palabras, la IA con fines de seguridad podría convertirse pronto en una funcionalidad casi universal (consulte la Figura 2). El 7 % restante que no está considerando el uso de la IA y la automatización con fines de seguridad se pone en una posición precaria, en la que son más propensos a tener dificultades a la hora de seguir el ritmo de aumento de la velocidad y el volumen de los eventos de seguridad.

FIGURA 2

**Amplia adopción**

Solo un pequeño grupo no está considerando utilizar la IA en las operaciones de seguridad

Para referimos al 64 % que actualmente está poniendo a prueba, implementando, operando u optimizando soluciones de seguridad de IA utilizamos la expresión "adoptantes de la IA". Si bien su implementación de la IA con fines de seguridad es incipiente, dado que la mayoría la utiliza hace menos de 2 años en un entorno empresarial habitual, se espera que su aceptación sea rápida. Al considerar los usos específicos de la IA, el porcentaje de adoptantes de la IA que la aprovechan para promover la protección y prevención crecerá, aproximadamente, en un 40 % en los próximos tres años, y se espera el mismo crecimiento en las áreas de detección y respuesta.

Esta adopción acelerada prevista de la IA con fines de seguridad es coherente con las conclusiones de otra investigación. Según un estudio reciente, el gasto en IA relacionado con la ciberseguridad aumentará con una tasa de crecimiento anual compuesta del 24 % hasta 2027, hasta alcanzar un valor de mercado de 46 000 millones de dólares.[6]

## La tecnología combinada con el talento arroja resultados positivos

Los adoptantes de la IA reconocen cómo la información y la automatización controladas por la IA complementan las capacidades avanzadas de identificación y respuesta de sus expertos en seguridad. Observan que, al igual que un analista de seguridad experimentado, los sistemas de IA con fines de seguridad son muy hábiles para identificar comportamientos anómalos, evaluar las vulnerabilidades de forma dinámica y destacar actividades anómalas que pueden ser indicio de nuevas amenazas. El 65 % de los adoptantes informan de que este uso de la IA ha tenido un impacto positivo significativo en sus operaciones de seguridad (consulte la Figura 3 en la página 7). Pero, a diferencia de un analista humano, la IA con fines de seguridad utiliza machine learning y la automatización para ajustarse a la velocidad y escala implacables de las operaciones multicloud híbridas, con un nivel de consistencia y profundidad que va mucho más allá de las capacidades del profesional de seguridad más hábil y cualificado. (Consulte "¿Qué hace que la IA con fines de seguridad sea tan eficaz?").

Por ejemplo, la IA se está utilizando para hacer un seguimiento de los comportamientos normales y automatizar el desarrollo de modelos. Con este fin, las soluciones de seguridad de IA señalan variaciones de los comportamientos previstos y analizan las consecuencias de las amenazas de las rutas de acceso de excepción. El 57 % de los adoptantes menciona que aumentar la respuesta a amenazas para automatizar la contención y optimizar la continuidad comercial tiene un gran impacto. Al entender la actividad anómala en contexto, las soluciones de seguridad de IA pueden determinar qué políticas y controles de seguridad están en riesgo, complementar una alerta con información relevante e iniciar acciones de remediación prescritas.

Esta forma de trabajar como "ciberasistente" para los expertos humanos pone de relieve uno de los beneficios más importantes de la IA con fines de seguridad: alivia la presión sobre los equipos de seguridad que se enfrentan a la escasez continua de habilidades y recursos. El 60 % de los adoptantes de la IA indican que el enriquecimiento de datos automatizado y las capacidades de segundo filtro que ayudan a los analistas a operar con más eficacia han sido extremadamente beneficiosos para sus funciones de seguridad. Dado que los modelos de amenazas de IA identifican muchos más eventos en un plazo más extenso y en una variedad de condiciones operativas, pueden aportar capacidades expertas para soportar las amenazas que pueden esquivar a los analistas humanos.

Gracias a la información generada por la IA, las capacidades de automatización controladas por la IA pueden aislar las amenazas por usuario, dispositivo o ubicación e iniciar medidas apropiadas de notificación y escalado mientras los expertos humanos determinan cuál es la mejor manera de investigar y remediar la situación. En las organizaciones que han desarrollado estas capacidades, los analistas de ciberseguridad pueden concentrarse en lo que realmente importa: desarrollar las destrezas y la experiencia para resolver los problemas más complejos que requieren el criterio humano.

**Perspectiva**

# ¿Qué hace que la IA sea tan eficaz?

La IA con fines de seguridad y la automatización se están volviendo rápidamente esenciales para defender una superficie de ataque en expansión y responder al enorme aumento de los eventos de seguridad. ¿Qué hace que la IA sea tan eficaz? En resumen, la respuesta es la combinación del machine learning iterativo y el ajuste del modelo analítico.

El ajuste consiste en el proceso de optimizar el desempeño de un modelo analítico sin hacer que dependa demasiado de variables propensas a cambiar de una situación a la siguiente. Entre bambalinas, los algoritmos de machine learning usan innumerables ejemplos para identificar patrones y aprender cómo responder de mejor manera a diferentes variables. Este proceso de entrenamiento es fundamental para mejorar el desempeño del modelo de IA.

Las soluciones de seguridad de IA, que mejoran la precisión del modelo y la recuperación por medio de machine learning, pueden ayudar a reducir la fatiga de los analistas causada por alertas, distinguiendo las verdaderas amenazas de seguridad (es decir, los positivos reales) de los eventos ordinarios, como los falsos positivos y los verdaderos negativos (consulte la figura). Estas soluciones ayudan a clasificar la mayoría de los eventos de seguridad, a enriquecer esos eventos con datos contextuales y a respaldar la inspección y las actividades de investigación de los analistas. Al usar la IA para mejorar la relación señal/ruido, los analistas pueden dedicar su tiempo a concentrarse en las verdaderas amenazas que plantean el mayor riesgo.


*Fuente: adaptación de https://en.wikipedia.org/wiki/F-score*

La IA y la automatización crean entornos de trabajo más enriquecedores, lo que permite a los analistas volver a concentrarse en problemas complejos que requieren criterio humano.

Dado que la IA puede analizar fuentes de datos estructurados y desestructurados sintetizando datos internos y externos con servicios de inteligencia en materia de amenazas e inteligencia de código abierto (OSINT, por sus siglas en inglés), puede ofrecer una imagen integral de las variables situacionales y las amenazas en contexto. Para los analistas de ciberseguridad, esto reduce el tiempo que se requiere para detectar incidentes, responder a ellos y recuperarse una vez que suceden.

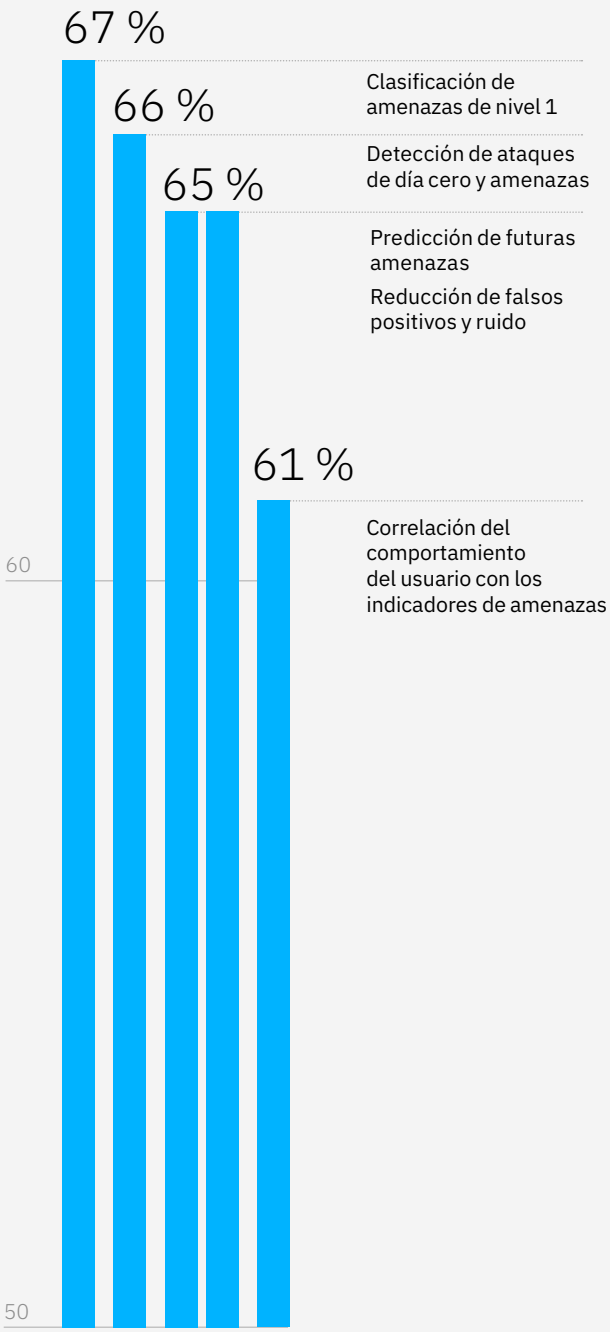
Al facilitar procedimientos de escalamiento, revisión y remediación más eficientes, la IA mejora el gobierno y el cumplimiento de la seguridad. Al automatizar las tareas repetibles y que llevan tiempo, la IA puede mitigar la fatiga y ayudar a mejorar la capacidad del analista para tomar decisiones mejores y más informadas, con más velocidad y menos errores. Y al encauzar el gran volumen de eventos por medio de la IA con fines de seguridad y las soluciones de automatización, los líderes aprovechan al máximo a los analistas humanos capacitados y sus habilidades difíciles de encontrar. El resultado final es un entorno laboral más enriquecedor y satisfactorio, algo que puede marcar una diferencia real a la hora de atraer y retener el talento en ciberseguridad, que es difícil de hallar.

Los adoptantes de la IA que han combinado con éxito la información y la automatización de IA con la experiencia de sus empleados mencionan los beneficios adicionales del uso de la IA en sus resultados en materia de seguridad (consulte la Figura 3). El 67 % informa que la habilidad de clasificar las amenazas de nivel 1 con más eficacia está ayudando a eliminar los costes y el tiempo asociados con la detección básica. Otro 65 % sostiene que la reducción de los falsos positivos y el ruido ha disminuido la necesidad de la inspección por parte de analistas humanos. Y el 65 % afirma que el uso del análisis del comportamiento está facilitando la predicción de futuras amenazas, un paso importante para volverse más proactivo.

FIGURA 3

**Ventaja de la IA**

Los adoptantes de la IA mejoran el desempeño utilizando soluciones de IA para funciones críticas




*P: ¿Cuál de los siguientes usos de la IA ha tenido el mayor impacto en sus operaciones de seguridad (seleccione los 5 principales)?*

## Las inversiones en IA rinden

Una fuente estima que, para 2025, los ciberdelitos le costarán a la economía mundial un promedio de 10,5 billones de dólares por año.[7] En 2021, según el informe anual del coste de una vulneración de datos de Ponemon Institute e IBM, el coste promedio de la vulneración de datos alcanzó un récord absoluto, mientras que la cantidad de vulneraciones de datos alcanzó un porcentaje alarmante del 68 %, lo que magnifica esos costes.[8]

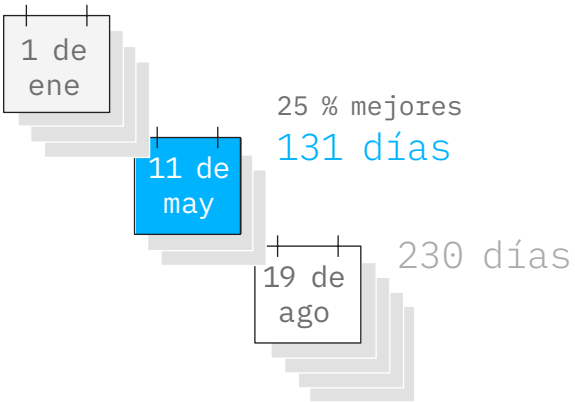
Los resultados de nuestra investigación revelan que una inversión inicial en IA a lo largo del ciclo de vida de la seguridad está ayudando a las organizaciones a combatir de forma más eficiente los ciberdelitos, lo que se refleja en las mediciones de desempeño del coste de la seguridad. De hecho, el 25 % de los adoptantes con mejor desempeño, aquellos con un percentil de 75 o 25 en cada métrica, sostienen que la IA más la automatización permitieron mejoras significativas en tres métricas de desempeño clave, lo que dio como resultado una mejora fundamental en el desempeño y la eficacia de sus funciones de seguridad. (Para obtener más información sobre las mediciones de quienes tienen un mejor desempeño, consulte Metodología del estudio y la investigación en la página 32). Esto es lo que han logrado:

- Reducir el coste total de ciberseguridad al menos en un 15 %, lo que señala beneficios en términos de eficacia y productividad en los procesos del ciclo de vida de la seguridad para la protección y prevención, y para la detección y respuesta.
- Reducir los costes de la vulneración de datos en un 18 % como mínimo, lo que señala una mejora en la eficacia de los procesos de detección y respuesta. Esto se refleja en una reducción o elusión de los costes operativos y para la reputación asociados, incluidos los posibles negocios (clientes y proveedores), inversiones y futuras oportunidades comerciales que se han perdido.
- Mejorar el retorno de la inversión en seguridad (ROSI) en un 40 % o más, lo que indica una reducción y evasión del riesgo cibernético y los costes operativos y para la reputación asociados.

Nuestra investigación es compatible con otros estudios que han concluido que la IA ofrece beneficios similares. El Ponemon Institute e IBM informaron que la combinación de la IA y la automatización fue el mejor factor en la reducción de los costes generales de una vulneración de datos.[9] De modo similar, un estudio de IBV sobre la seguridad zero trust concluyó que el 61 % de las organizaciones líderes utilizaron la automatización y orquestación de la seguridad para reducir los costes operativos y de capital en materia de seguridad.[10]

Estos resultados ofrecen pruebas convincentes de por qué los líderes de seguridad están adoptando la IA y la automatización en la totalidad del ciclo de vida de la seguridad. A continuación, exploraremos cómo los líderes están mejorando el desempeño en dos áreas importantes: la protección y prevención, y la detección y respuesta.

Si a una empresa le lleva 230 días naturales detectar incidentes cibernéticos, responder a ellos y recuperarse una vez que ocurren sin usar la IA, al usarla, podría reducir ese tiempo hasta en 99 días.



**Capítulo 2**

# La IA impulsa el desempeño en todo el ciclo de vida de la seguridad

Junto con el modelo de responsabilidad compartida inherente en la seguridad del cloud y la integración de TI inherente en un enfoque zero trust, la IA combinada con la automatización representa una capacidad fundamental para las operaciones de seguridad de aquí en adelante.

La IA con fines de seguridad y la automatización pueden generar aportes significativos enriquecidos con datos contextuales e históricos, y facilitar una mayor coordinación y colaboración con los colaboradores dentro y fuera de la organización. Esto libera a los recursos capacitados para investigar amenazas antes de que tengan la posibilidad de madurar. Al mejorar el desempeño en los procesos de protección y prevención, y detección y respuesta, la IA y la automatización pueden tener un gran impacto en la resiliencia cibernética general de la organización.

Para entender mejor esta influencia, examinamos el modo en que los adoptantes están usando la IA y la automatización en todo el ciclo de vida de las operaciones de seguridad, tanto en sus procesos de protección y prevención como de detección y respuesta. Esta información nos ayudó a evaluar cómo la combinación de estas tecnologías impulsa la eficacia y eficiencia operativas. También nos ayudó a explicar cómo el desempeño mejorado puede ofrecer beneficios comerciales a posteriori, como una mayor productividad y una mejor experiencia del empleado.

Al mejorar el desempeño de las operaciones, la IA y la automatización ayudan a fortalecer la resiliencia cibernética general.

## Protección y prevención: uso de la IA para mitigar riesgos, controlar los costes y desarrollar confianza

### Los desafíos

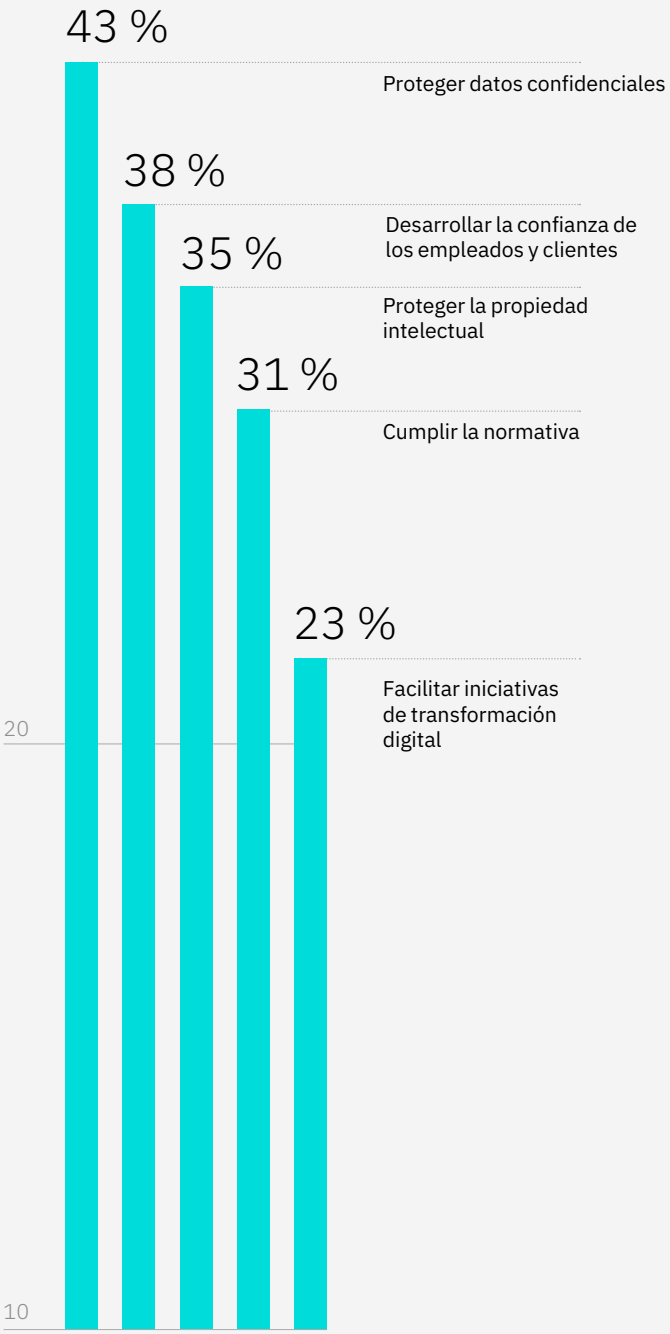
A medida que la cantidad de trabajadores remotos y aplicaciones y servidores basados en el cloud se ha expandido en los últimos años, también lo ha hecho la cantidad de endpoints y aplicaciones que se deben supervisar. Los ciberdelincuentes están explotando los servicios conectados para crear nuevos vectores de amenaza, y los ataques están evolucionando del phishing oportunista a campañas de ransomware coordinadas, donde una empresa se mantiene como rehén hasta que paga. El ransomware fue clasificado como el principal tipo de ataque observado por IBM X-Force® en 2021, mientras que las operaciones de phishing fueron la principal vía de peligro y estuvieron presentes en el 41 % de los ataques.[11]

Esta sofisticación cada vez mayor de las amenazas de ciberseguridad afecta a las empresas y sus clientes. Para ganar y aumentar la confianza de los clientes, colaboradores y empleados, los adoptantes de la IA están priorizando de manera proactiva la reducción de riesgos, la protección de los datos confidenciales y la preservación de la propiedad intelectual (consulte la Figura 4).

FIGURA 4

**IA en guardia**

Los adoptantes de la IA buscan proteger los datos de la empresa y los clientes y preservar la confianza




*P: ¿Cuáles son los principales impulsores de la IA en su organización? (Objetivos que se centran en la protección y la prevención).*

## La propuesta de valor de la IA

Quizás la ventaja comercial más significativa se desprende de la combinación de la IA y la automatización con un modelo zero trust. Para la protección y prevención, estas capacidades deshacen los silos operativos y mejoran la visibilidad del patrimonio digital de la organización: los datos, los dispositivos, los usuarios, la red, las cargas de trabajo, las aplicaciones y las interacciones entre colaboradores en todo el ecosistema.

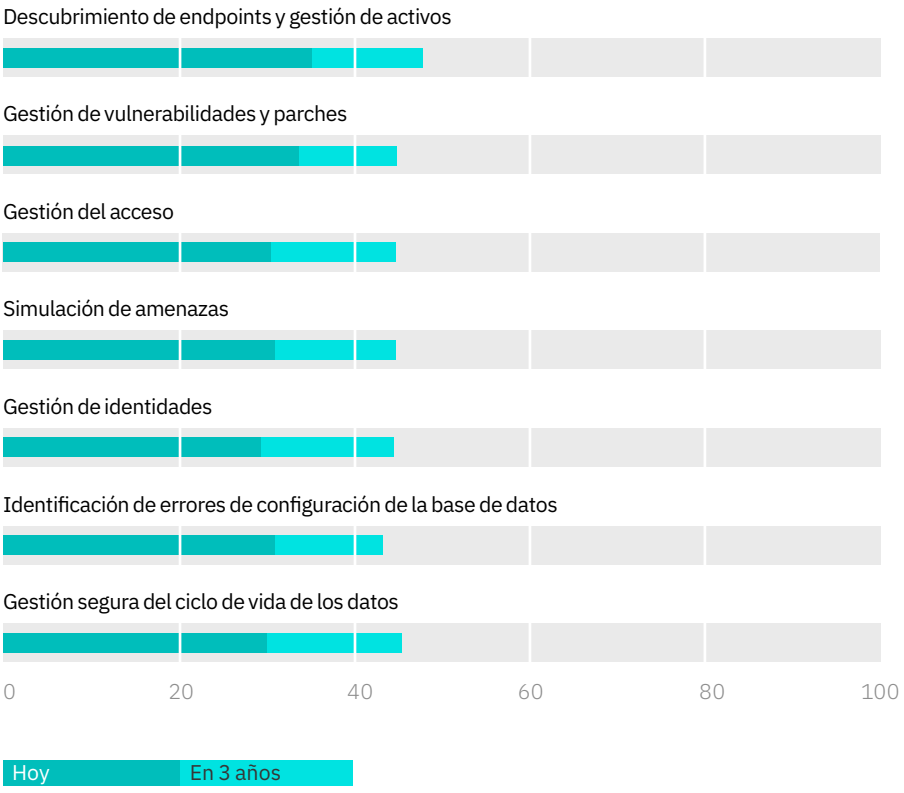
La IA y la automatización pueden facilitar esta visualización realizando descubrimientos y clasificaciones de datos confidenciales con regularidad de forma local, en el endpoint, en tránsito y en el cloud. Las tecnologías permiten que las empresas usen datos de recursos y metadatos para recrear la totalidad del contexto de una interacción determinada, así como para comprender dónde residen los datos más confidenciales, quiénes tienen acceso a ellos (y cómo), quién está accediendo a ellos (y cuándo) y qué están haciendo con los datos. Esto puede ayudar a alcanzar los estándares de la protección de datos y el cumplimiento normativo, y a respaldar la supervisión y el control del acceso a repositorios de datos muy confidenciales.

En la búsqueda de esta visión más holística de sus entornos digitales, los adoptantes de la IA han identificado el descubrimiento de endpoints y la gestión de activos como su principal caso de uso de la IA. El 35 % está implementando la IA y la automatización en esta función y planea aumentar el uso al menos al 50 % en 3 años (consulte la Figura 5). A esto le sigue la gestión de vulnerabilidades, al 34 %. Los adoptantes de la IA esperan aumentar su uso de la IA para la protección y prevención en un 40 %, en promedio, en los próximos 3 años. (Consulte “Cómo la IA ayuda a proteger y prevenir”).

FIGURA 5

### Implementación de la IA con fines de protección y prevención

Los adoptantes están usando la IA para expandir su visión de un conjunto de activos digitales cada vez mayor




*P: ¿Qué casos de uso de la automatización con IA se están implementando en la actualidad? ¿Y en 3 años? (Casos de uso que se centran en la protección y la prevención).*

**Perspectiva**

# De qué manera la IA ayuda a proteger y prevenir

Con estos cinco casos de uso principales, los adoptantes de la IA están invirtiendo en proteger el valor subyacente de sus negocios, concentrándose en la reducción de riesgos y la prevención de ataques, al mismo tiempo que construyen confianza.

**IA para el descubrimiento de endpoints y la gestión de activos.** Bajo el radar de las políticas de seguridad tradicionales de las organizaciones operan dispositivos no autorizados, lo que los hace difíciles de detectar. La IA puede aprender el contexto, el entorno y los comportamientos asociados con los tipos de activos específicos, los servicios de red y los endpoints, y las empresas luego pueden limitar el acceso a dispositivos autorizados e impedir el acceso de dispositivos no autorizados y no gestionados.

**IA para la gestión de vulnerabilidades.** Las evaluaciones de vulnerabilidades con tecnología de IA pueden ayudar a identificar dispositivos configurados de forma inadecuada, para que los administradores puedan eliminarlos o volverlos a configurar. Si bien el escaneo activo de vulnerabilidades en entornos de tecnología operativa (TO) puede desestabilizar los sistemas, las organizaciones pueden usar IA y automatización para realizar una supervisión pasiva. La IA también puede ayudar a priorizar el parcheo de vulnerabilidades brindando información sobre exploits armados, para que los clientes puedan adoptar un enfoque basado en riesgos en la gestión de vulnerabilidades.

**IA para la gestión de acceso.** Las empresas pueden usar la IA para auditar el acceso a los datos y servicios por parte de usuarios y aplicaciones. Una vez que se establece la titularidad de los recursos confidenciales, la IA puede coordinar las actividades en el plano de control, supervisando comportamientos, alertando sobre anomalías, generando información contextual, enviando alertas e iniciando acciones con fines de remediación.

**IA para la simulación de amenazas.** Los simuladores de amenazas pueden conectarse a endpoints de software de toda la red de una organización para emular el ciclo de vida de un incidente de ciberseguridad. Esto permite evaluar la defensa en materia de seguridad en vivo sin interactuar con endpoints o servidores de producción, lo que permite a las empresas identificar y cerrar brechas en su sistema de defensa sin afectar sus operaciones.

**IA para la gestión de la identidad.** Las operaciones de seguridad zero trust ejercen una mayor demanda sobre la infraestructura de TI y las capacidades de autenticación de seguridad; en particular, debido a la necesidad de resolver la identidad casi en tiempo real. Si bien zero trust puede representar una mejora significativa en las capacidades operativas, también plantea nuevos desafíos para la capacidad operativa y la coordinación de las operaciones (por ejemplo, admite que los trabajadores remotos utilicen varios dispositivos desde diferentes lugares). La IA puede mejorar los servicios de autenticación creando un perfil de usuario único basado en una combinación de comportamientos históricos, datos contextuales y políticas basadas en roles.

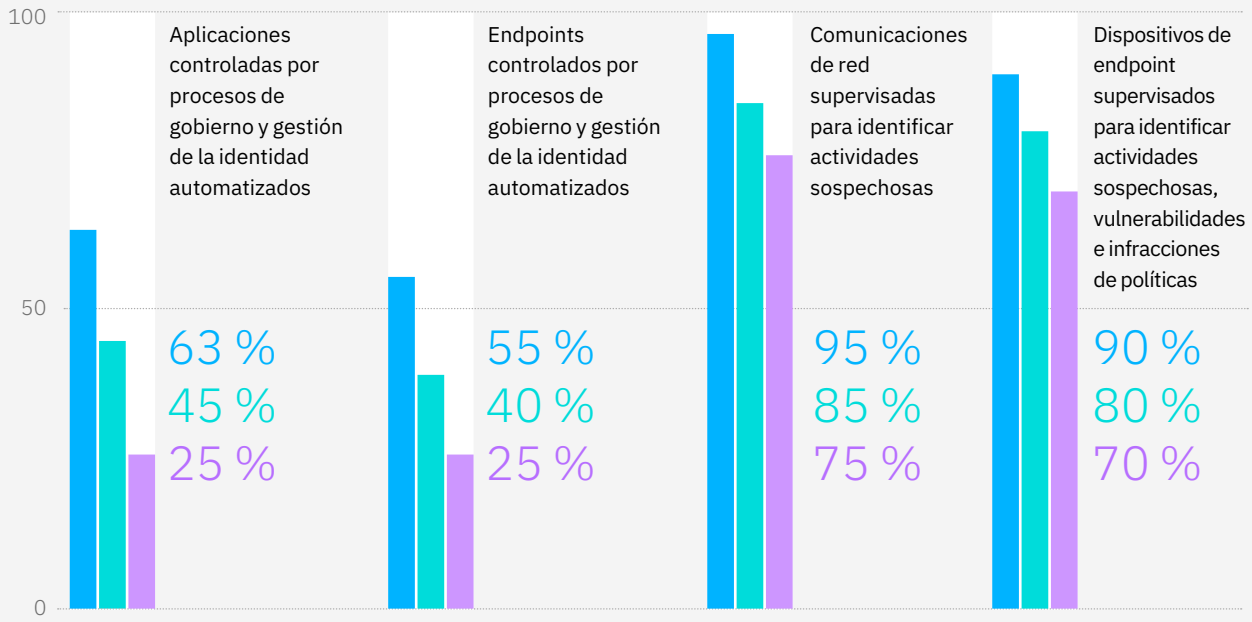
La automatización con IA está mejorando la capacidad de las organizaciones de proteger un mayor número de sus endpoints y aplicaciones y de aumentar la supervisión de las comunicaciones de red (consulte la Figura 6). Los adoptantes de IA con mejor desempeño informan de que están implementando la gestión y el gobierno automatizados de la identidad en el 63 % de sus aplicaciones y el 55 % de sus endpoints. Gracias a la IA, estos porcentajes suponen un aumento de un 67 % más aplicaciones y un 50 % más endpoints. Esto permite una mayor visibilidad de la huella de las operaciones en expansión que depende de servicios que abarcan varios clouds.

FIGURA 6

**Expansión de la visibilidad**

La automatización permite a los adoptantes de la IA controlar y supervisar más activos

Porcentaje de activos controlados y supervisados con IA




25 % de los adoptantes de la IA con mejor desempeño
Media proporcional de adoptantes de la IA
25 % de los adoptantes de la IA con menor desempeño

Incluso el término medio de los porcentajes notificados para estas áreas refleja cantidades sólidas de aplicaciones y endpoints controlados con la automatización, con muchas más ventajas disponibles a medida que el desempeño mejora. Los adoptantes de la IA informan de un progreso aún mejor al usar la IA y la automatización para vigilar las comunicaciones de red y los dispositivos de endpoint para detectar actividades sospechosas. Los adoptantes de la IA con mejor desempeño afirman que están usando la IA para supervisar el 95 % de las comunicaciones de red y el 90 % de los dispositivos de endpoint.

El verdadero valor de la protección y prevención radica en algo inherentemente difícil de medir: la evitación. Dada la información más relevante y oportuna del desempeño de todos los activos digitales, los equipos de seguridad pueden evitar amenazas con más eficacia, mitigar riesgos y proteger y preservar los beneficios de sus organizaciones, así como también, la reputación de sus marcas.

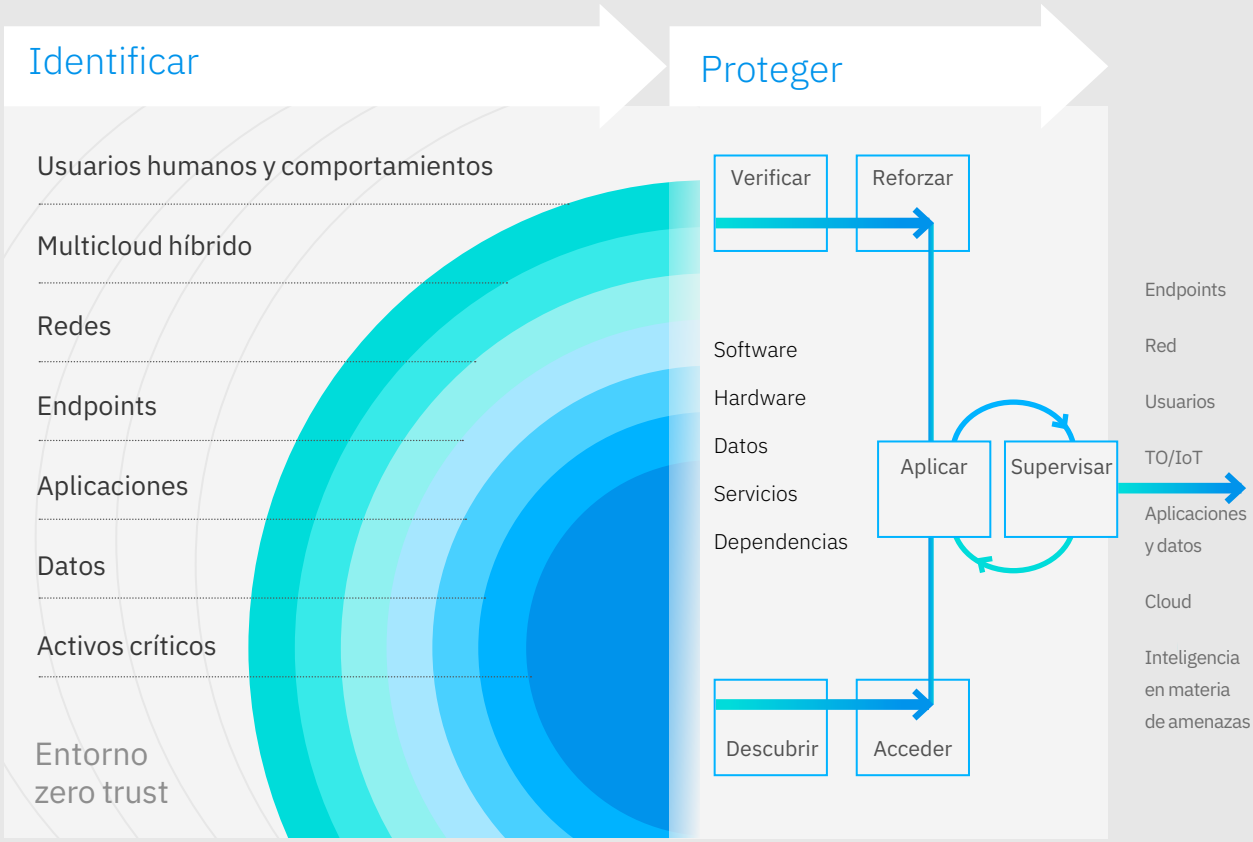
Los adoptantes líderes de la IA están usando la automatización para controlar el 63 % de sus aplicaciones y el 55 % de sus endpoints.

**Perspectiva**

# La combinación de IA y automatización permite mejores controles de seguridad

## Protección y prevención

La IA admite la supervisión de varias capas en los entornos multicloud

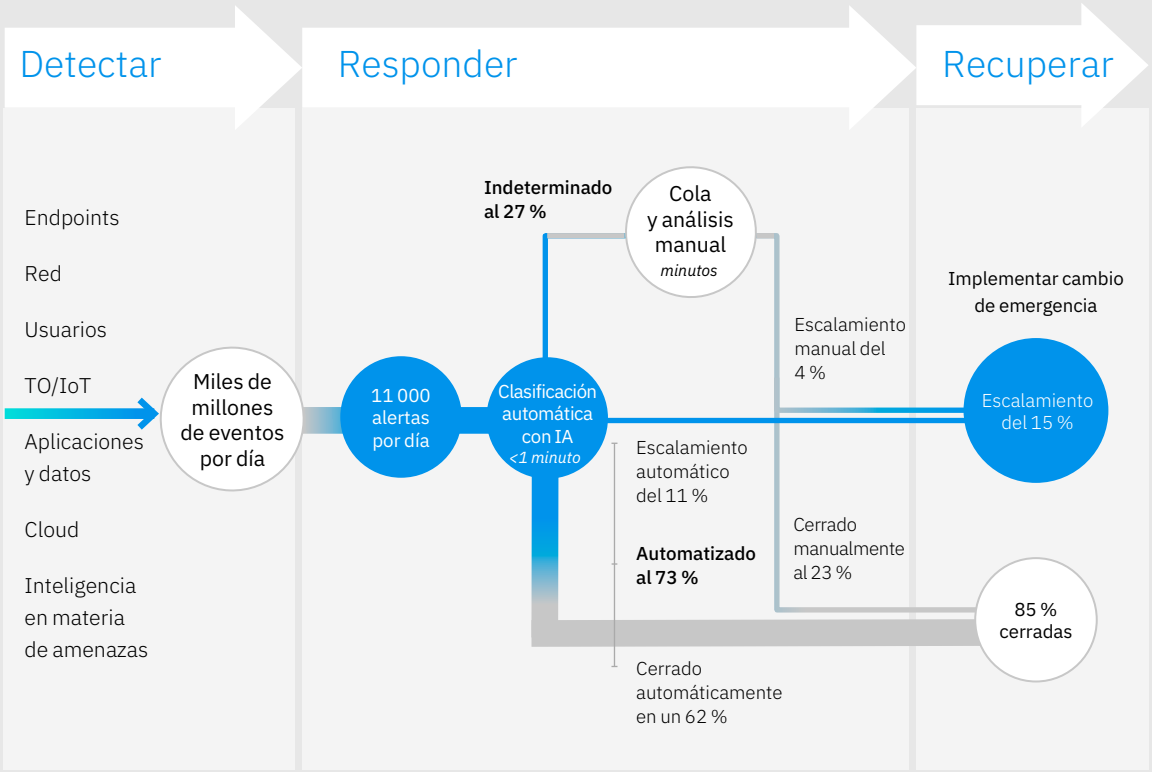


**Perspectiva**

# La combinación de IA y automatización mejora el desempeño de las operaciones de seguridad

## Detección y respuesta

El uso de IA y automatización puede condensar las métricas de desempeño




## La experiencia del analista del futuro

| Sin IA | Con IA y automatización |
|---|---|
| 8 herramientas/filtros | 1 filtro |
| 19 pasos | 6 pasos |
| Tiempo de respuesta en horas/días | Tiempo de respuesta en minutos |

*Fuente: IBM Security Services, basado en un análisis de datos de desempeño agregados de 2021.*
*Nota: se espera que los umbrales de desempeño representados mejoren de forma continua.*

## Detección y respuesta: uso de la IA para impulsar la productividad y acelerar la recuperación

### Los desafíos

El bienestar de la empresa no solo se basa en la protección y prevención de incidentes, sino en cuán rápido puede detectarlos, responder a ellos y recuperarse una vez que ocurren. Los principios basados en zero trust sugieren que los profesionales de la seguridad deben presuponer que sus organizaciones ya han sido vulneradas y volverán a sufrir vulneraciones en el futuro.

Hay varias cuestiones que llevan a los impulsores principales a usar la IA en las actividades de detección y respuesta. Como se mencionó anteriormente, la impronta digital en rápida expansión de la mayoría de las organizaciones, el traslado a modelos de negocios cada vez más abiertos y el aumento pronunciado de la cantidad de empleados remotos están generando una cascada de nuevos eventos de seguridad. Muchas organizaciones de seguridad simplemente no tienen la capacidad de supervisar y gestionar manualmente tales eventos y de actuar en respuesta a ellos de forma rápida y eficaz.

La escasez de cibertalento complica la situación. La falta de empleados cualificados tiene un gran impacto en la posición de la empresa en relación con la seguridad, tanto en términos del uso eficiente de recursos para mejorar el tiempo de respuesta como a la hora de aprovechar la experiencia para fortalecer la calidad de los resultados en cuanto a seguridad.

Según EMSI, una empresa nacional de análisis laborales, por cada 100 puestos de ciberseguridad que se necesitan cubrir, solo hay 68 candidatos cualificados, muchos de los cuales ya tienen empleos muy rentables.[12] Un estudio reciente de IBV determinó que las organizaciones necesitan 150 días para cubrir una vacante de ciberseguridad con un candidato capacitado.[13] Los nuevos analistas de primera línea, que necesitan apoyo operativo adicional para hacer su trabajo de forma eficaz, no alivian necesariamente la escasez de talento. Con frecuencia, no tienen experiencia en la industria y necesitan tiempo para desarrollar verdaderamente confianza y madurez en sus habilidades de investigación y evaluación de amenazas.

La IA y la automatización pueden ayudar a estos analistas con la gestión de conocimientos, la gestión de casos y las capacidades de apoyo operativo (por ejemplo, chatbots de primera línea y repositorios de conocimientos de lenguaje natural). El resultado neto es revolucionario: la combinación del criterio humano y la IA junto con la automatización aumentan la capacidad de inteligencia. (Consulte “IA más automatización: una revolución del talento”).

**Perspectiva**

# IA más automatización: una revolución del talento

El conocimiento cibercultural y el talento en materia de ciberseguridad desempeñan una función fundamental en el logro de resultados comerciales y de seguridad. Los programas de IA exitosos no hacen que el talento se vuelva obsoleto. Por el contrario, aumentan la eficacia de los analistas de seguridad y el alcance de los trabajadores con conocimientos en seguridad. Al abrir las puertas a un modelo de participación más flexible, la IA alivia algunas de las limitaciones de los recursos y las habilidades que actúan como factor decisivo en los resultados de seguridad positivos y negativos.[14]

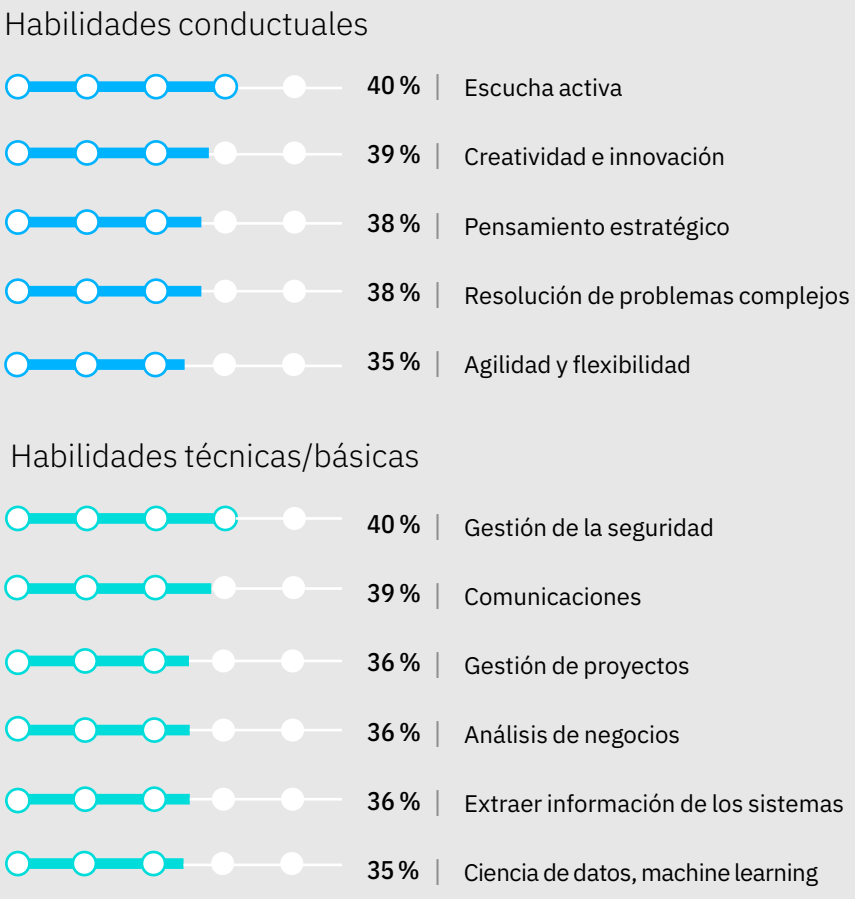
Los adoptantes de IA están experimentando una demanda intensa de nuevo talento. En los últimos 12 meses, incorporaron un 15 % neto de empleados nuevos en ciberseguridad y atribuyen el 40 % de este cambio a su adopción de IA con fines de seguridad. Los encuestados nos informaron de que hubo cambios en las habilidades requeridas en el 34 % de las funciones de seguridad, el 35 % de los cuales fueron impulsados directa o indirectamente por la adopción de IA.

Al combinar factores humanos con tecnología, los adoptantes de la IA pueden cerrar la brecha de recursos de manera directa reinvirtiendo en la plantilla de ciberseguridad. Las organizaciones pueden desarrollar el talento de manera nativa, haciendo que la automatización se trate en menor medida de la optimización de costes y en mayor medida de la especialización y mejora de la experiencia laboral, lo que ayuda a los empleados a ampliar sus competencias.

Los adoptantes de la IA priorizan una combinación de habilidades técnicas y conductuales en sus empleados. Desde una perspectiva de comportamiento, el 40 % expresa que la escucha activa es la cualidad más importante que los empleados necesitan como consecuencia de la IA. El 39 % sostiene lo mismo en relación con la innovación y la creatividad. En cuanto al aspecto técnico, el 40 % considera que las habilidades de gestión de la seguridad son las más importantes, mientras que el 39 % se centra en las habilidades de comunicación (consulte la figura). Esta mayor flexibilidad en la integración de habilidades técnicas y sociales es una de las áreas más prometedoras de las nuevas propuestas de valor de la IA.

**La IA demanda una combinación de habilidades**

Los empleados de ciberseguridad necesitan habilidades técnicas y sociales para lograr el éxito con la IA




*P: ¿Qué habilidades necesita su personal de ciberseguridad para desarrollarse o mejorar como consecuencia de la IA?*

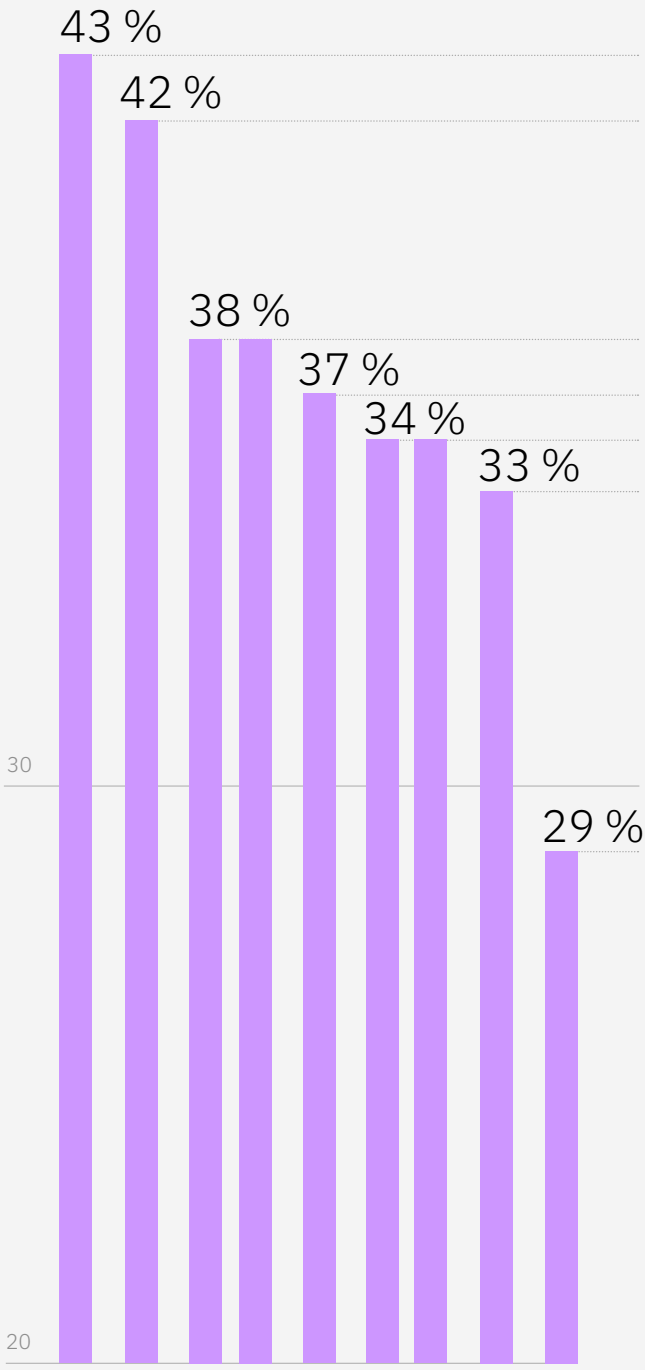
En respuesta a los desafíos relacionados con el personal, los adoptantes de la IA están implementando IA y automatización para mejorar la productividad y la experiencia laboral de los sobrecargados recursos. De hecho, el 43 % sostiene que aumentar la productividad de los recursos cibernéticos es uno de los principales factores que impulsa el uso de la IA. El 42 % informa que reducir los eventos de seguridad, los incidentes y las vulneraciones es un objetivo, y el 38 % se centra en usar la IA para mejorar la precisión de los analistas de ciberseguridad (consulte la Figura 7).

En conjunto, la IA y la automatización pueden tener un drástico impacto positivo en la capacidad de responder al elevado volumen y frecuencia de los eventos de seguridad, lo que constituye un factor clave a la hora de mejorar el entorno laboral del analista de seguridad. Al entender mejor qué amenazas requieren más atención, los analistas pueden desligarse de la clasificación de rutina y concentrarse en las actividades de investigación de amenazas de mayor valor. En última instancia, el resultado será: una mayor capacidad y especialización de la plantilla de ciberseguridad.

FIGURA 7

## Impulsar la productividad

Los adoptantes de la IA aspiran a mejorar la eficacia de los analistas en la detección y la respuesta




Aumentar la productividad de los recursos de ciberseguridad

Reducir los eventos e incidentes de ciberseguridad y las vulneraciones

Mejorar la precisión de los analistas de ciberseguridad

Acelerar la detección y reducir los tiempos de respuesta

Reducir la dependencia y reimplementar recursos de ciberseguridad

Mejorar la visibilidad de los datos de ciberseguridad empresariales

Predecir ciberataques

Identificar posibles problemas de ciberseguridad no visibles para los humanos

Reducir los costes de ciberseguridad

*P: ¿Cuáles son los principales impulsores de la IA en su organización? (Objetivos centrados en las operaciones, la detección y la respuesta).*

## La propuesta de valor de la IA

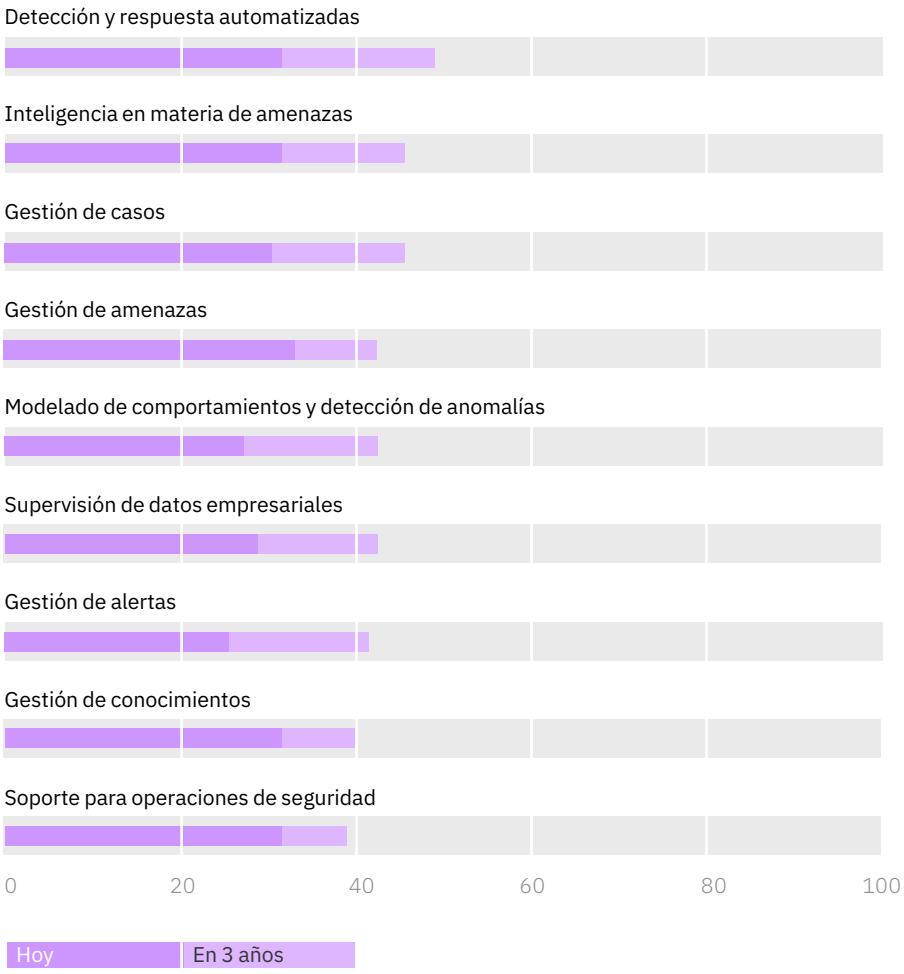
El secreto para mejorar la productividad es ayudar a la plantilla, aplicando tecnología donde puede ser más eficaz. Por ejemplo, la detección de amenazas es un caso de uso ideal para reducir los métodos manuales y lograr una mayor eficacia por medio de la IA y la automatización. Los procesos de investigación automatizados y controlados por la IA pueden proteger datos y activos de gran valor de forma selectiva, así como segmentos de la red y servicios de cloud. Al ofrecer una mayor visibilidad de las comunicaciones de red, el tráfico y los dispositivos de endpoint, la IA y la automatización ayudan a mejorar la capacidad de identificar posibles amenazas, lo que permite a los recursos de ciberseguridad tomar decisiones mejores y más informadas de manera sistemática.

Los adoptantes de la IA reconocen el potencial de usar la IA y la automatización para la gestión de amenazas. El 34 % señala que este es su principal caso de uso de la IA para actividades de detección y respuesta (consulte la Figura 8). A esto le sigue la detección y la respuesta automatizadas, que se convertirán en lo más implementado en tres años, según el 49 %. Y, al igual que los casos de uso con fines de protección y prevención, los adoptantes esperan aumentar su uso de la IA para casos de uso de detección y respuesta una media del 40 % aproximadamente en los próximos 3 años. (Consulte la perspectiva “Uso de la IA para detectar y responder más rápido”).

FIGURA 8

**Aplicar IA con fines de detección y respuesta**

Los adoptantes están usando la IA para identificar amenazas más rápido y responder de forma proactiva a los ciberataques




*P: ¿Qué casos de uso de la automatización con IA se están implementando en la actualidad? ¿Y en 3 años? (Casos de uso que se centran en la detección y la respuesta).*

# Uso de la IA para detectar y responder más rápido

Los adoptantes de la IA están usando IA y automatización para mejorar de manera significativa la productividad de su plantilla de ciberseguridad, lo que se mide por medio de varios indicadores de desempeño clave. Estos cinco casos de uso demuestran cómo.

**Detección y respuesta automatizadas.** La IA con fines de seguridad y la automatización permiten automatizar la recopilación, la integración y el análisis de los datos de cientos y hasta miles de puntos de control, sintetizando los registros del sistema, los flujos de red, los datos de endpoints, las llamadas a la API del cloud y los comportamientos de los usuarios. Junto con la gestión de amenazas y la priorización de alertas, las organizaciones pueden complementar las soluciones de telemetría existentes con las capacidades de detección y respuesta de endpoints (EDR, por sus siglas en inglés) y detección y respuesta extendidas (XDR, por sus siglas en inglés). Estas capacidades permiten que los equipos de operaciones de seguridad entiendan por completo el contexto de las excepciones de seguridad, establezcan prioridades y dediquen recursos suficientes a la investigación de amenazas de alto impacto.

**Inteligencia en materia de amenazas.** La inteligencia en materia de seguridad impulsada por la IA permite a las organizaciones analizar flujos de datos en directo para detectar comportamientos anómalos en tiempo real. Combinar información de seguridad entre dominios, integrando señales de telemetría internas con fuentes de inteligencia externas, da como resultado una inteligencia práctica en un margen de actuación, lo que mejora la eficacia de las políticas de seguridad, en especial aquellas asociadas con amenazas emergentes. Además, las capacidades de captura de registros se pueden extender aplicando los mismos procedimientos en distintos entornos del cloud, lo que permite identificar configuraciones irregulares que podrían señalar firmas de ataques más elusivas, como amenazas persistentes avanzadas (APT, por sus siglas en inglés) y ataques de día cero.

**Gestión de casos.** La funcionalidad de gestión de casos del área de seguridad permite a un equipo de seguridad recopilar información sobre actividades sospechosas y escalar las investigaciones con información detallada relacionada con el caso y registros. Implementar IA puede aumentar la velocidad y el volumen de los datos procesados e integrar técnicas de ciencias de datos, lo que permite la identificación y la clasificación automatizadas de los datos de los documentos. Dado que la IA puede entender el contexto, puede agrupar datos por tema sin una clasificación previa. Esto ayuda a los equipos de seguridad a usar datos reconocidos como relacionados para sacar conclusiones y hallar similitudes que no son evidentes.

**Gestión de amenazas.** La IA ayuda a los analistas a clasificar las alertas con eficacia, centrándose primero en las más importantes, y les ayuda a distinguir los resultados falsos negativos de los falsos positivos y a reducir en gran medida las posibilidades de pasar por alto incidentes críticos. También clasifica y prioriza amenazas para desencadenar alertas basadas en firmas de ataque, indicadores de compromiso (IOC, por sus siglas en inglés) e indicadores de comportamiento (IOB, por sus siglas en inglés).

**Modelado de comportamientos y detección de anomalías.** Los modelos de seguridad de IA automatizada pueden reconocer comportamientos anómalos, evaluar vulnerabilidades de forma dinámica y señalar actividades anómalas, todos posibles indicadores de compromiso. Luego, machine learning puede recomendar opciones de remediación sobre la base de un amplio espectro de factores, como variables situacionales, precedentes históricos o fuentes de inteligencia de amenazas, seguidas de actualizaciones en la administración de la política en puntos de control específicos.

Los adoptantes de la IA informan de una reducción exitosa en el tiempo para detectar incidentes y responder a ellos (consulte la Figura 9). En comparación con las estimaciones de desempeño anteriores a la implementación de la IA, los adoptantes informan de que la media proporcional de días para detectar incidentes se redujo en un 12 %, mientras que la media proporcional de días para responder a incidentes y recuperarse tras ellos se redujo en un 11 %. Al analizar a quienes tienen un mejor desempeño, vemos la verdadera oportunidad de que la IA y la automatización ofrezcan mejoras significativas. El 25 % de los adoptantes de la IA con mejor desempeño informa que ha usado la IA para reducir el tiempo para investigar incidentes en casi un tercio y el tiempo para responder y recuperarse en casi un cuarto. También ha reducido los tiempos de permanencia en un 45 %.

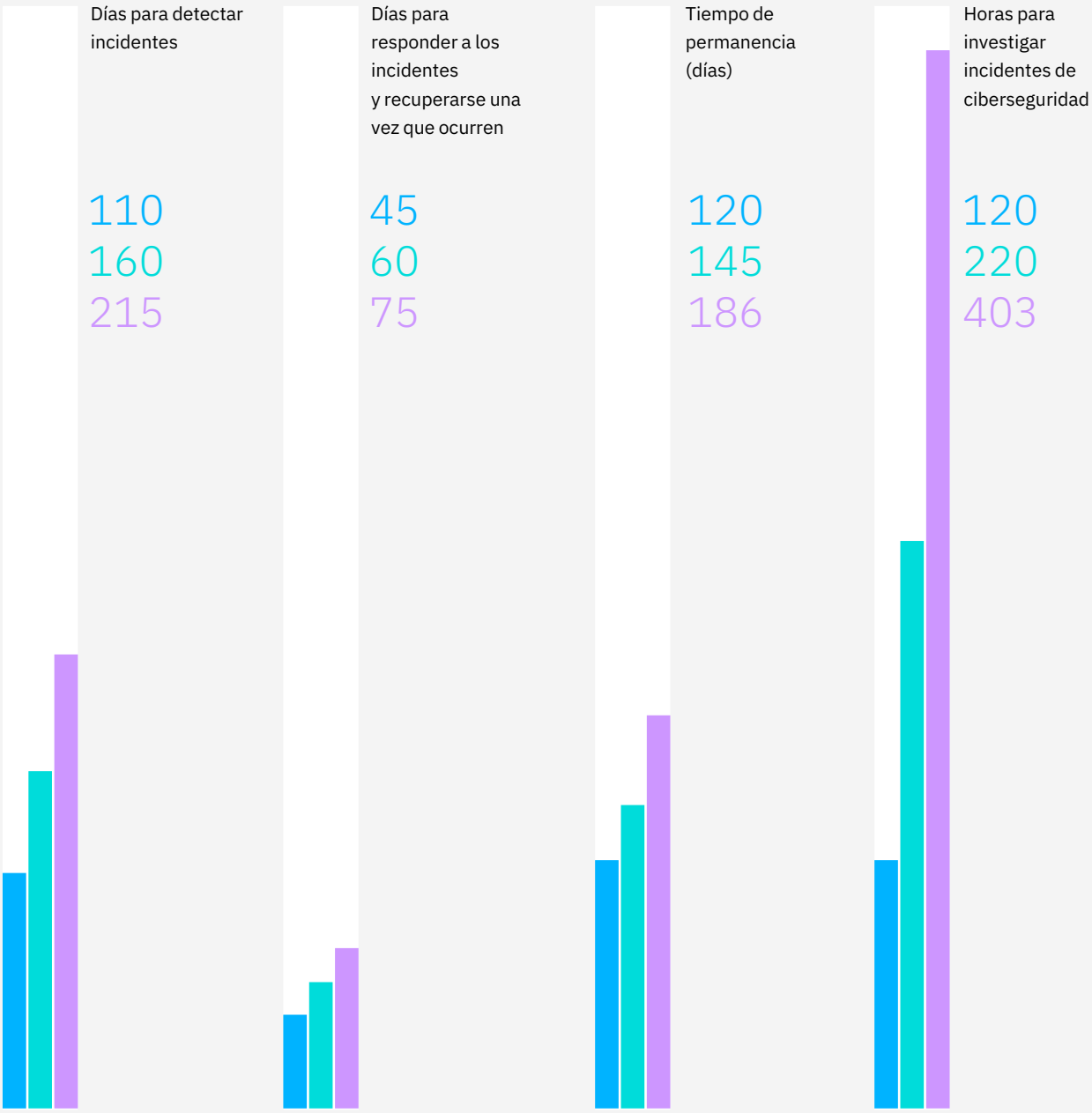
Los adoptantes de la IA están demostrando que implementar IA y automatización en todo el ciclo de vida de las operaciones de seguridad mejora las capacidades de protección y prevención, y mejora su desempeño en materia de detección y respuesta. Su éxito revela cómo las organizaciones pueden usar la IA para mejorar en gran medida la resiliencia cibernética general durante tiempos complejos. (Consulte el caso práctico “IA más automatización: mejor entorno laboral y mejor desempeño”).

Los adoptantes de la IA con mejor desempeño reducen el tiempo para investigar incidentes de ciberseguridad en casi un 30 %.

FIGURA 9

## Acelerar la recuperación

Quienes tienen un mejor desempeño
tienen una mejor detección
y mejores tiempos de respuesta
a los incidentes de seguridad




25 % de los adoptantes de la IA con mejor desempeño
Media proporcional de adoptantes de la IA
25 % de los adoptantes de la IA con menor desempeño

*Las barras más cortas representan un mejor desempeño*

**Caso práctico**

# Proveedor global de servicios de seguridad gestionados

## IA más automatización: mejor entorno laboral y mejor desempeño

Un proveedor de servicios de seguridad administrados que presta servicio a cientos de clientes globales de diferentes industrias estaba sufriendo problemas de capacidad recurrentes, a pesar de tener operaciones de seguridad modernizadas con un cloud híbrido y capacidades zero trust. “La superficie de ataque no para de crecer”, dijo uno de los analistas de seguridad principales del cliente. “Vemos las dos caras del problema: demasiada información de demasiadas fuentes o la falta de información relevante en el momento adecuado, cuando es más importante”.

La escasez de habilidades y especialización empeora el panorama. “Estamos compitiendo por talento difícil de encontrar y cualquier ventaja puede ayudarnos”, dijo el ejecutivo líder del cliente. Usando metodologías de design thinking e IBM Garage™, los líderes del cliente comenzaron a estructurar la oportunidad en términos de resultados comerciales. “Queríamos crear una mejor experiencia de trabajo para nuestros analistas. También queríamos ver cómo una mayor automatización podría mejorar el desempeño del equipo”, dijo el ejecutivo del cliente.

Un equipo integrado de operaciones y desarrollo formuló cuatro objetivos primordiales:

- Reducir el ruido para que los analistas se puedan concentrar en las alertas de alto valor.
- Reducir el tiempo de clasificación, compilando datos contextuales, metadatos y registros de servicio para recrear fielmente el entorno de amenazas.
- Acelerar las investigaciones por medio de un mayor contexto y datos/metadatos de más valor.
- Complementar las recomendaciones precisas con explicaciones y razonamiento.

Después de casi un año, el cliente mejoró drásticamente su eficacia operativa de las siguientes maneras:

- Automatizando la clasificación del 73 % de las alertas, a partir de un 40 %, con un nivel de confianza superior al 90 %.
- Reduciendo la superficie total de ataque y el riesgo asociado en aproximadamente el 50 % usando controles zero-trust específicos de la carga de trabajo.
- Reduciendo el tiempo de permanencia del atacante y los plazos de vulnerabilidad en un 50 %.
- Reduciendo los incidentes de seguridad en un 75 % y duplicando el tiempo medio para las vulneraciones.

Mientras que la IA impulsa la automatización, el impacto de la solución en el lado humano de la ecuación es, quizás, más poderoso. La combinación de IA y automatización libera a los analistas para que se concentren en amenazas de mayor impacto, como los ataques de día cero, la detección de APT, la detección de amenazas y el análisis forense. Los analistas de seguridad ofrecen opiniones continuas para que la solución sea más inteligente, pero, también, más fácil de entender para el humano. El ejecutivo del cliente resume el impacto para la empresa: “Para nosotros, la capacidad de combinar la automatización con un mejor entorno de trabajo para nuestro equipo marcó la diferencia”.

Capítulo 3

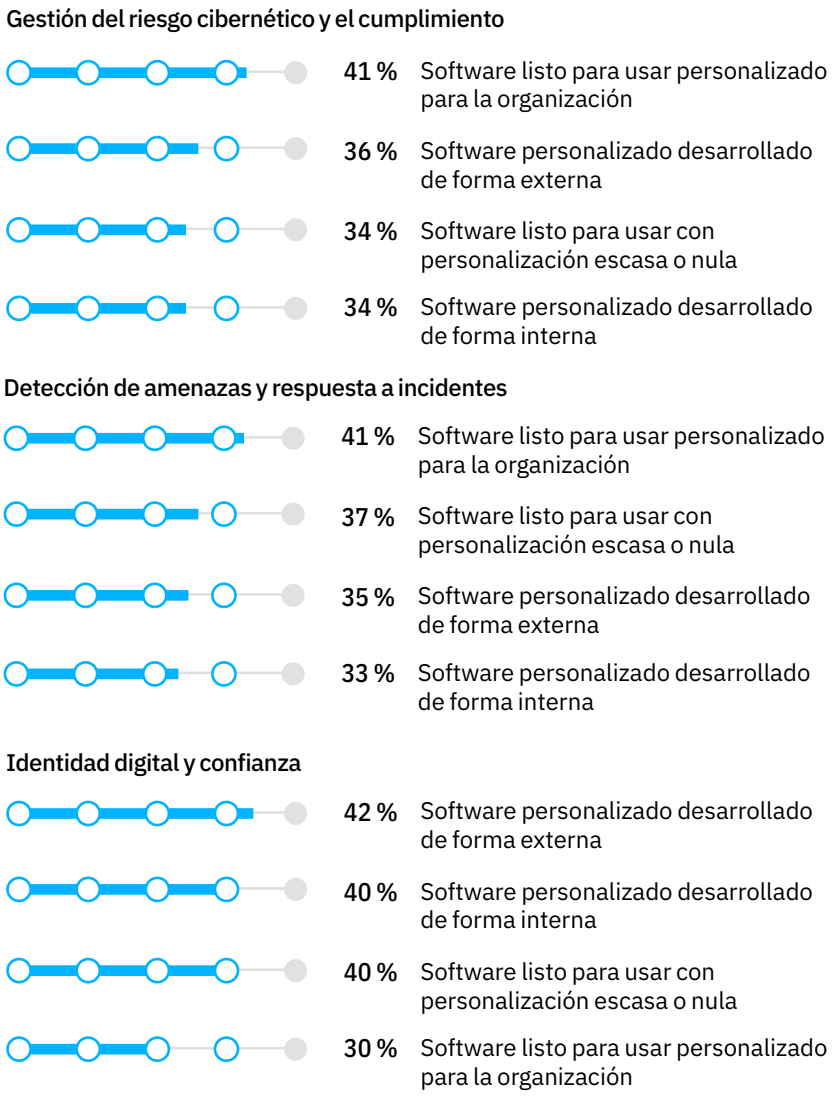
# Planificación de la hoja de ruta para adoptar la IA con fines de seguridad

A medida que analiza la integración de perspectivas de IA y automatización en sus operaciones de seguridad, considere cómo podría lucir una implementación exitosa. Los adoptantes de la IA están usando una combinación de soluciones listas para usar y herramientas personalizadas. Más adoptantes de la IA informan de que el software listo para usar y configurable es el tipo de implementación más exitoso para el riesgo cibernético y el cumplimiento, así como para la detección de amenazas y la respuesta a incidentes (consulte la Figura 10). Pero, en cuanto a la identidad digital y la gestión de confianza, los adoptantes de la IA dicen que el software personalizado, ya sea de forma interna o externa, ha permitido obtener mejores resultados.

FIGURA 10

**Habilitación de la IA con fines de seguridad**

Las implementaciones más exitosas suelen involucrar algún tipo de personalización




*P: ¿Cómo describiría la implementación de tecnología de IA en su organización para la gestión del riesgo cibernético y el cumplimiento? (Seleccione las tres opciones principales).*

*P: ¿Cómo describiría la implementación de tecnología de IA de su organización para la detección de amenazas y la gestión de respuestas a incidentes? (Seleccione las tres opciones principales).*

*P: ¿Cómo describiría la implementación de tecnología de IA de su organización para la gestión de la identidad digital y la confianza? (Seleccione las tres opciones principales).*

Las soluciones de seguridad altamente configuradas y desarrolladas de forma personalizada pueden ofrecer mayores capacidades y beneficios, aunque los costes continuos asociados con el desarrollo y soporte deben incluirse en su presupuesto de operaciones de seguridad.

Aunque algunas industrias podrían beneficiarse de las aplicaciones de seguridad de IA especializadas (por ejemplo, los bancos y mercados financieros), es necesario analizar minuciosamente los costes de soporte continuo, los requisitos de personal y los cronogramas de parches, en particular para el mantenimiento y la gestión de vulnerabilidades. La decisión de personalizar una solución debe reflejar un motivo comercial convincente basado en una posición frente a los riesgos de la organización en evolución y las posibles vulnerabilidades en materia de seguridad.

Una solución de IA personalizada debe tener en cuenta los costes de soporte continuos.

# Manual de acción

**Implementación de la IA con fines de seguridad y la automatización para obtener valor comercial**

Incluso la organización de seguridad más exitosa es un trabajo en curso. La naturaleza dinámica de las operaciones y el surgimiento continuo de nuevos vectores de amenaza requieren que priorice la preparación y la resiliencia. No se trata de si su organización será vulnerada, sino de cuándo y en qué medida.

De manera similar, debe reconocer que los modelos de IA deben seguir aprendiendo y que sus equipos de seguridad deben seguir alimentándolos con información nueva relativa al desempeño. Este compromiso con el aprendizaje continuo influye en los resultados que puede conseguir.

Para los adoptantes de la IA, el desempeño en materia de seguridad está afectando tanto a la eficacia operativa como al valor comercial, y está creando un entorno laboral más poderoso y adaptable para los analistas de seguridad. En conjunto, estos factores pueden tener un impacto significativo en la resiliencia cibernética general de la organización.

Ya esté poniendo a prueba estas funciones por primera vez o expandiendo la funcionalidad de sus aplicaciones existentes, hay tres recomendaciones que pueden orientar estos esfuerzos.

## 1

## Evaluar su desempeño según métricas de seguridad clave

Identificar los impulsores de la mejora en seguridad

- Entender la apremiante lógica estratégica para implementar funciones de IA y automatización en sus operaciones de seguridad, y actualizar su estrategia de ciberseguridad y riesgo cibernético para reflejar este cambio en las prioridades. ¿Se trata de reducir los incidentes de ciberseguridad y las vulneraciones o de reducir los costes por medio de eficacias operativas? ¿O se trata, tal vez, de mejorar la confianza de clientes, empleados o colaboradores?

Identificar áreas de mejora basándose en comparaciones de referencias

- Examinar métricas clave de riesgo y seguridad para la protección, la prevención, la detección y la respuesta, y comparar el desempeño de su organización con sus homólogos. Las brechas representan áreas en las que puede centrar las iniciativas de mejora y donde la IA y la automatización pueden ser más útiles.
- Para realizar comparaciones, algunas organizaciones ofrecen servicios formales de análisis comparativo. También puede identificar métricas de seguridad por medio de recursos en línea, como Ponemon Institute, Gartner, Forrester, IDC, SANS Institute, Cloud Security Alliance (CSA), etc.

## 2

## Priorice las mejoras de seguridad que aportan mayor valor y se alinean con sus principales objetivos de seguridad

Establezca prioridades basadas en el impacto e intente lograr mejoras en las mediciones de desempeño clave

- Evalúe los posibles beneficios que se pueden lograr mejorando el desempeño en cada una de sus métricas de desempeño clave. Esto ayuda a ver qué áreas pueden ofrecer mayor valor en términos de factores operativos, como coste, eficacia, calidad y tiempo. Si se da por hecho que las áreas potenciales se alinean con su estrategia de seguridad, sus mediciones deberían contribuir al máximo al logro de sus objetivos estratégicos.

Identifique los usos de la IA más propensos a mejorar el desempeño

- Entienda las mediciones de desempeño más asociadas con la protección y prevención, y la detección y respuesta. Por ejemplo, para la protección y prevención, una medición clave es la cantidad de aplicaciones y endpoints controlados por la gestión automatizada de la identidad o los endpoints. Para la detección y respuesta, el tiempo de permanencia es una métrica importante.
- Considere los usos de la IA en ambas áreas más propensos a ofrecer las mejoras en el desempeño y los beneficios comerciales que ha definido como más importantes. Use estas prioridades para definir las hojas de ruta de la IA con fines de seguridad y la automatización en su organización. Determine sus fortalezas e identifique dónde puede aprovechar a los colaboradores para expandir su experiencia. Por último, seleccione el modelo de implementación de la IA con más probabilidades de ser exitoso, ya sea configurando una solución existente o desarrollando una solución especializada, y en qué medida desea depender de terceros para el desarrollo y el soporte.

## 3

## Desarrollar facilitadores clave de iniciativas de mejora de la seguridad

Definir una estrategia de IA con fines de seguridad y un plan de operaciones acorde

- Implementar, controlar y gestionar sus usos de la IA en línea con las estrategias de seguridad y riesgo cibernético más amplias de su organización. Asegurarse de que estas se reflejen en las políticas operativas, los controles y los procesos.

Determinar y desarrollar las habilidades conductuales y técnicas que su organización necesita para tener éxito

- Analizar el impacto de la automatización en su plantilla de ciberseguridad. ¿Percibirán la automatización como una amenaza o como una oportunidad? ¿Cuál es la forma correcta de llevar a cabo esta conversación?
- Al analizar qué hace que la IA con fines de seguridad y la automatización sean exitosas, tenga en cuenta los componentes de desarrollo y retención, como el entorno laboral, la demanda de especialización y experiencia, y la mejora o la renovación de habilidades asociadas. ¿Qué combinación de habilidades se requiere en un entorno de IA y automatización?
- Determine en qué área la IA y la automatización pueden aportar el mayor beneficio a su plantilla de ciberseguridad. Identifique brechas y ofrezca capacitaciones basadas en la función para desarrollar y mejorar las habilidades conductuales y técnicas que se requieren. Tenga en cuenta los factores humanos, como el aprendizaje experiencial y las simulaciones de ciberseguridad para desarrollar habilidades, mientras ofrece experiencia real y práctica, utilizando servicios de colaboradores internos o externos.
- Por último, supervise su progreso. A medida que se implementan nuevos usos y funciones de la IA, valide su desempeño real en comparación con referencias específicas para determinar la eficacia relativa de varias inversiones.

# Acerca de los autores


*Sridhar Muppidi*

Director de tecnología
IBM Security
linkedin.com/in/smuppidi
muppidi@us.ibm.com


Sridhar es socio de IBM y director de tecnología (CTO) de IBM Security. Es responsable de impulsar la estrategia técnica, la arquitectura y la investigación de la cartera de productos y servicios de IBM Security para ayudar a los clientes a administrar su defensa contra amenazas y a proteger sus activos digitales. Es un líder técnico orientado a los resultados con 25 años de experiencia en desarrollar productos de seguridad, ofrecer arquitectura de soluciones a los clientes, impulsar estándares abiertos y liderar equipos técnicos.


*Lisa Fisher*

Líder global en investigación de referencias;
TI, seguridad y cloud
Líder de IBM Institute for Business Value,
Oriente Medio y África
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com


Lisa es responsable de producir investigaciones de referencia para todas las industrias y regiones, para prever y estructurar el impacto de las tecnologías en las empresas desde las perspectivas de la ciberseguridad y el riesgo cibernético. Lisa trabaja en Sudáfrica.


*Gerald Parham*

Líder en investigación global;
CIO y responsable de seguridad
IBM Institute for Business Value
linkedin.com/in/gerryparham/
gparham@us.ibm.com


Gerald dirige las áreas de investigación en materia de seguridad y sistemas de información en IBM Institute for Business Value. Se centra en las estrategias cibernéticas, el asesoramiento de la Junta y la seguridad al nivel del ecosistema, en particular, la relación entre estrategia, riesgo, seguridad abierta, confianza y valor comercial. Tiene más de 20 años de experiencia en liderazgo ejecutivo, innovación y desarrollo de propiedad intelectual.

## Acerca de la información de referencia

La información de referencia ofrece datos para ejecutivos sobre negocios importantes y temas tecnológicos relacionados. Se basa en el análisis de datos de desempeño y otras mediciones de referencia. Para obtener más información, comuníquese con IBM Institute for Business Value escribiendo a global.benchmarking@us.ibm.com.

## IBM Institute for Business Value

Durante dos décadas, IBM Institute for Business Value ha ejercido como grupo de reflexión para generar nuevas ideas de IBM. Lo que nos inspira es producir perspectivas estratégicas informadas por medio de tecnología y respaldadas por la investigación que ayudan a los líderes a tomar decisiones comerciales más inteligentes.

Desde nuestra posición única, en la intersección de los negocios, la tecnología y la sociedad, encuestamos a miles de ejecutivos, consumidores y expertos por año, e interactuamos con ellos, para resumir sus perspectivas en información creíble, inspiradora y que nos permite actuar.

Para mantenerse conectado e informado, regístrese para recibir el boletín de noticias de IBM por correo electrónico en ibm.com/es-es/ibv. También puede seguir a @IBMIBV en Twitter y encontrarnos en LinkedIn, en https://ibm.co/ibv-linkedin

## El compañero correcto para un mundo en constante cambio

En IBM, colaboramos con nuestros clientes, combinando la perspectiva comercial, la investigación avanzada y la tecnología para darles una ventaja clara en el entorno actual que cambia rápidamente.

## Informes relacionados

**Getting started with zero trust security (Primeros pasos con la seguridad zero-trust)**

McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher y Gerald Parham. “Getting started with zero trust security” (Primeros pasos con la seguridad zero-trust). IBM Institute for Business Value. Julio de 2021. ibm.co/zero-trust-security

**The new era of cloud security (La nueva era de seguridad en el cloud)**

Thompson, Shue-Jane, Shamla Naidoo, Shawn Dsouza y Gerald Parham. “The new era of cloud security: Use trust networks to strengthen cyber resilience” (La nueva era de seguridad en el cloud: uso de redes de confianza para fortalecer la resiliencia cibernética). IBM Institute for Business Value. Abril de 2021. ibm.co/cloud-security-cyber-resilience

**AI ethics in action (Ética de la IA en acción)**

“AI ethics in action: An enterprise guide to progressing trustworthy AI” (Ética de la IA en acción: una guía empresarial para el progreso de la IA de confianza). IBM Institute for Business Value. Abril de 2022. ibm.co/ai-ethics-action

## Metodología de estudio e investigación

IBM Institute for Business Value se asoció con APQC (American Productivity and Quality Center) para encuestar a 1000 ejecutivos con responsabilidad general sobre la ciberseguridad de la TI y la tecnología operativa (TO), así como la seguridad de la información en sus organizaciones. Los encuestados representaban 16 sectores, incluidos mercados financieros y bancos, artículos electrónicos y software, administración, seguros, medios de comunicación y entretenimiento, comercio minorista y servicios. Estaban distribuidos en cinco regiones globales: África y Oriente Medio, Asia Pacífico, centro y sur de América, Europa, Estados Unidos y Canadá. Incluyeron empresas que no aplican la IA en sus procesos de la función de seguridad.

Se les pidió a los encuestados que proporcionaran información sobre la aplicación actual y planificada de la IA en sus procesos de ciberseguridad y riesgo cibernético, así como sobre el desempeño de sus funciones de seguridad. Dado que hay muchos factores que influyen en el desempeño, pedimos a los adoptantes de la IA (las 637 empresas que ponen a prueba, implementan, operan u optimizan la IA en al menos un proceso de seguridad) que proporcionaran sus estimaciones sobre cómo la IA había influido en los indicadores de desempeño clave (KPI) habituales de la función de seguridad y riesgo cibernético. Esto nos permitió calcular el rango de desempeño en cada indicador de desempeño clave, así como el rango de impacto que la IA tuvo en cada indicador.

Los indicadores de desempeño clave que se incluyen en este informe se definen de la siguiente manera:

**Tiempo de permanencia:** es el tiempo que transcurre entre un ataque o situación comprometida y su descubrimiento o detección.

**Tiempo medio (en días naturales):** plazo para responder a incidentes de ciberseguridad y recuperarse, que comienza cuando se detecta un incidente y se establece su alcance. Incluye actividades para eliminar la amenaza y restaurar los sistemas afectados al estado previo al incidente, la evaluación, la supervisión y la validación de los sistemas afectados, y las operaciones de restauración.

**Tiempo medio (en horas):** plazo para investigar los incidentes de ciberseguridad. Comienza cuando una alerta de seguridad se somete a investigación y finaliza cuando la investigación termina.

**Coste de ciberseguridad como porcentaje del coste de TI:** incluye los costes de TI en relación con la aplicación, la seguridad de datos y el cloud, la administración de acceso a la identidad, la protección de la infraestructura, la gestión de riesgos integrada, los equipos de seguridad de red, demás software de seguridad de la información, servicios de seguridad y software de seguridad para el consumidor. Incluye todos los costes de los procesos para respaldar las operaciones empresariales y excluye la depreciación/amortización (basado en el flujo de caja) y la “TI revendida”.

**Retorno de la inversión en seguridad (ROSI):** se expresa como porcentaje y equivale a: [la pérdida total estimada en USD] x [el coste total de la ciberseguridad (la mitigación porcentual lograda con las soluciones o los esfuerzos en materia de ciberseguridad)] - [el coste total de la ciberseguridad (el coste total de las soluciones o los esfuerzos de ciberseguridad)] / [coste total de ciberseguridad (el coste total de las soluciones o los esfuerzos en materia de ciberseguridad)].

**Coste de una vulneración de datos:** incluye los gastos directos e indirectos que conlleva la detección, el escalamiento, la notificación y las actividades de respuesta a la vulneración de datos. El coste promedio de una vulneración de datos se calcula de la siguiente manera: [cantidad anual de vulneraciones multiplicada por todos los factores de coste]/[cantidad anual de vulneraciones].

Los rangos de desempeño que se utilizan en este informe se definen de la siguiente manera:

Los adoptantes de la IA con mejor desempeño son aquellos cuyo desempeño está en el percentil 75 o 25 de cada métrica, dependiendo de si es mejor tener un valor más alto o más bajo para una medición específica. Si, para una métrica particular, es mejor que un valor sea más alto, entonces los adoptantes de la IA con mejor desempeño (el 25 %) serán las organizaciones que se encuentran en el percentil 75. El 75 % de los encuestados tiene un desempeño inferior y el 25 % está en este nivel o por encima. Si es mejor que el valor sea más bajo, entonces los adoptantes de la IA con mejor desempeño serán los que se encuentren en el percentil 25. El 25 % de los encuestados tiene un desempeño de este nivel o inferior y el 75 % está por encima. La media proporcional es el valor intermedio en la distribución de respuestas; la mitad de los encuestados tienen un desempeño por debajo de este nivel y, la otra mitad, por encima.

# Reconocimientos

IBV desea expresar su agradecimiento al distinguido equipo de investigadores de seguridad de IBM Research, que está explorando el impacto de las nuevas tecnologías y las innovaciones aplicadas en todo el ciclo de vida de la seguridad. Este equipo incluye a J.R. Rao, Marc Stoecklin e Ian Molloy. También queremos agradecer a Srini Tummalapenta y Charles Henderson, que compartieron amablemente su experiencia para explicar los temas principales. Este informe no hubiera sido posible sin la generosa contribución de estos colegas.

Nuestro agradecimiento a Mary O'Brien y Chris McCurdy por liderar un equipo global de profesionales de seguridad en IBM Security. Nuestros colegas en IBM Security han proporcionado sugerencias valiosas y realistas basadas en su interacción con cientos de clientes internacionales. Su trabajo aporta una base fundamental para gran parte de nuestra investigación.

Por último, queremos agradecer a nuestros compañeros de IBV que nos ayudaron a crear estos materiales. Ellos son Dave Zaharchuk, Kirsten Palmer, Heba Nashaat, Sherihan Sherif, Joanna Wilkins, Angela Finley y Kathy Cloyd. Todas las semanas, IBV publica nuevos informes de liderazgo basados en investigaciones primordiales. Cada informe cuenta con el respaldo de un equipo heterogéneo de profesionales de investigación, creativos y analíticos que colaboran para hacer realidad estos materiales.

# Notas y fuentes


1 Turton, William, and Kartikay Mehrota. “Hackers Breached Colonial Pipeline Using Compromised Password.” Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Holmes, Aaron; “Ransomeware gangs targeted 3 different US water treatment plants this year in previously unreported attacks, according to federal agencies.” Insider. October 16, 2021. https://www.businessinsider.com/3-us-water-treatment-plants-attacked-by-ransomware-gangs-report-2021-10

2 Vigliarolo, Brandon. “Report: Pretty much every type of cyberattack increased in 2021.” TechRepublic. February 17, 2022. https://www.techrepublic.com/article/report-pretty-much-every-type-of-cyberattack-increased-in-2021/; 2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/es-es/security/data-breach/threat-intelligence/

3 “SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president.” Reuters. February 14, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R; Robertson, Paul. “Best of 2021—Worldwide Hack: Microsoft Exchange Server Zero-Day Exploits.” Security Boulevard. December 27, 2021. https://securityboulevard.com/2021/12/worldwide-hack-microsoft-exchange-server-zero-day-exploits/; Torres-Arias, Santiago. “What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what’s at stake.” The Conversation. https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

4 “The 2021 CIO Study. The CIO Revolution: Breaking barriers, creating value.” IBM Institute for Business Value. November 2021. ibm.co/c-suite-study-cio

5 Schneier, Bruce. “The Coming AI Hackers.” Harvard Kennedy School, Belfer Center for Science and International Affairs. April 2021. https://www.belfercenter.org/publication/coming-ai-hackers

6 “AI & Cybersecurity: Balancing Innovation, Execution & Risk.” Pillsbury Law and The Economist Intelligence Unit. September 9, 2021. https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

7 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

8 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.co/security/data-breach. “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” Identity Theft Resource Center. January 24, 2002. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

9 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.com/es-es/security/data-breach

10 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

11 “2022 IBM X-Force Threat Intelligence Index.” I BM Security. February 2022. ibm.com/es-es/security/data-breach/threat-intelligence/

12 Hatton, Tim. “The Cybersecurity Talent Shortage: An Urgent Threat.” EMSI. March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/

13 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

14 Brandenburg, Rico and Paul Mee. “Cybersecurity for a Remote Workforce.” MIT Sloan Management Review. July 23, 2020. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

**IBM España, S.A.**
Santa Hortensia, 26-28
28002 Madrid

Elaborado en los Estados Unidos de América | Junio de 2022



Este documento fue impreso en papel reciclado sin cloro por una imprenta con certificación de Cadena de Custodia del Consejo de Administración Forestal (FSC, por sus siglas en inglés) con tintas ecológicas. La energía utilizada para producir este papel e impresión procede de energías ecológicas renovables. Le pedimos que recicle este material.


9NGZA7GK-ESES-01

IBM