Gartner

La IA en el ámbito de la ciberseguridad: define tu rumbo

Minimiza los cambios disruptivos, gestiona los riesgos y aprovecha el valor de la IA.

Deja atrás el bombo publicitario y aprovecha al máximo el valor de la IA en la ciberseguridad

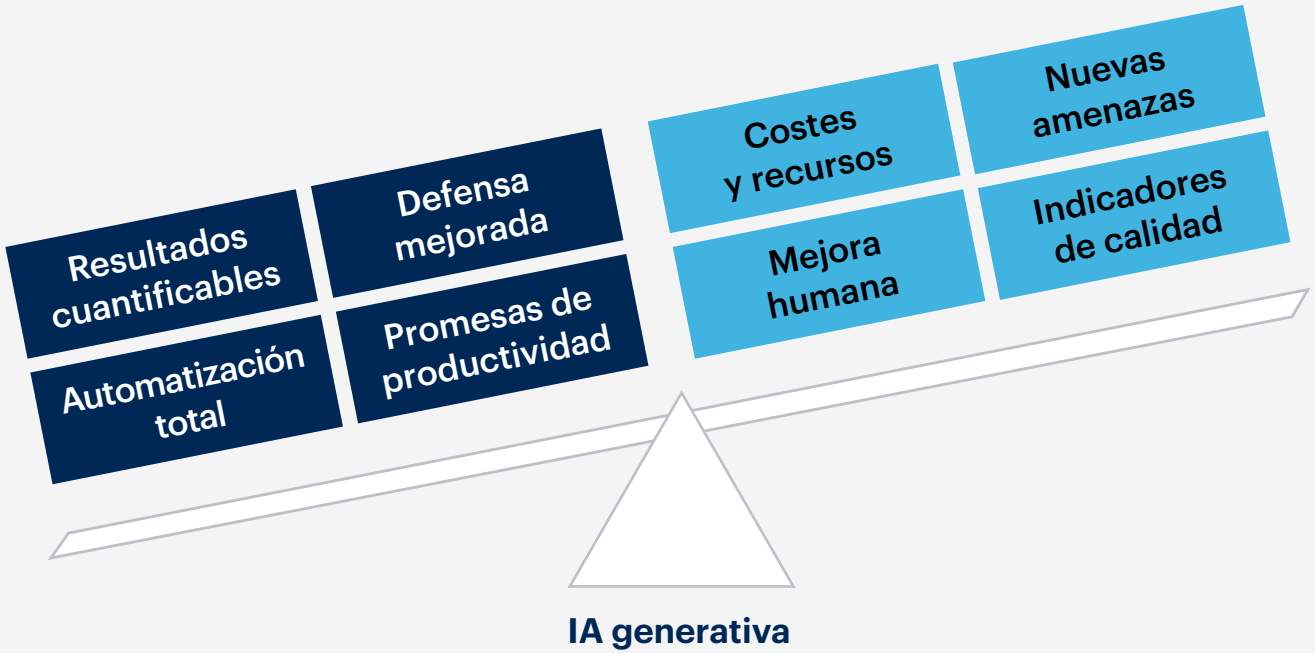
Como es habitual, la expectación en torno a la IA y la IA generativa en el ámbito de la ciberseguridad ha provocado cambios disruptivos en las empresas. Además, ha traído consigo nuevos niveles de riesgo y distracción a un panorama de seguridad ya de por sí desafiante. Y, a pesar del revuelo, la IA aún no ha cumplido todas sus promesas.

Sin embargo, lo que ayer era un caos mañana es una oportunidad. Más allá de todo el ruido, reside la verdadera oportunidad de aprovechar el valor de la IA.

La IA puede transformar, y lo hará, la manera en que las organizaciones operan, incluida la seguridad. Mientras tanto, a medida que los retos de la IA se hacen más evidentes y las aplicaciones de la IA continúan madurando, concéntrate en:

- Determinar el impacto de la IA
- Priorizar las principales áreas de riesgo
- Aprovechar al máximo el valor de la IA
- Anticiparte a los cambios futuros

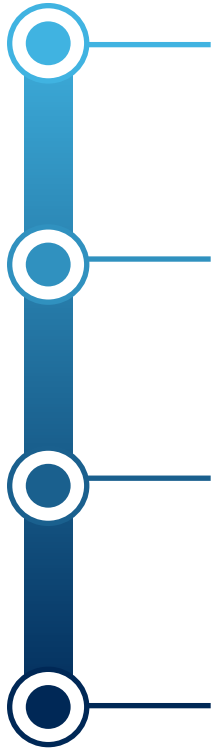
Equilibrar la realidad de la ciberseguridad con las expectativas de la IA generativa



Fuente: Gartner

Determina el impacto de la IA

Según el análisis que hemos realizado, **casi el 90 % de las empresas** todavía están explorando o probando la IA generativa, y la mayoría aún no ha implementado controles técnicos o políticas de AI TRiSM (gestión de la confianza, el riesgo y la seguridad de la IA), lo cual genera una oleada de cambios en el ámbito de la seguridad. Los responsables de empresa están notando estos efectos de diversas maneras:



De forma directa y urgente

- Uso no gestionado e incontrolado de datos confidenciales en aplicaciones de terceros
- Infracciones de derechos de autor y daños a la marca asociados

De forma directa y sobredimensionada como urgente

Anuncios prematuros y exagerados diseñados para generar interés en la IA generativa

De forma indirecta y alarmante

- Preocupaciones sobre posibles riesgos para la privacidad y la aparición de agentes malintencionados
- Aparición de nuevas superficies de ataque derivadas de prácticas empresariales alteradas

De forma indirecta y latente

- La adopción en curso de la IA generativa requiere una adaptación constante en materia de seguridad
- Las futuras regulaciones y requisitos de cumplimiento exigen la preparación del equipo de seguridad
- Incertidumbre sobre las futuras brechas de habilidades y los retos en la gestión del talento

Define tu rumbo

La incorporación de la IA generativa requerirá nuevos principios de gobernanza o la modificación de los existentes, junto con una hoja de ruta de ciberseguridad bien definida que integre consideraciones sólidas centradas en la IA.

El alcance de la gobernanza de la IA en tu organización dependerá de su nivel de madurez, pero puedes y deberías centrarte en estas tres hojas de ruta al mismo tiempo:

1. **Adapta la estrategia de seguridad de las aplicaciones a la IA**
   Asegúrate de seguir implementando prácticas de desarrollo seguras, al tiempo que proteges las nuevas superficies de ataque tanto en el tiempo de ejecución como a lo largo del ciclo de desarrollo. Implementa tecnologías que refuercen la privacidad y evalúa las nuevas técnicas de IA generativa para mejorar la seguridad de las aplicaciones.
2. **Integra las nuevas tecnologías de IA en la ciberseguridad**
   Ten en cuenta el impacto de la IA actual y futura en tu hoja de ruta a tres años.
3. **Incluye las consideraciones de la IA en los programas de gestión del riesgo**
   Los requisitos en cuanto a las habilidades necesarias evolucionarán con el tiempo. Los indicadores, los registros de riesgos y la exposición a amenazas también lo harán.

Las 3 principales preocupaciones de los responsables de ciberseguridad sobre el uso de la IA generativa y los riesgos asociados:

Acceso de terceros a datos confidenciales

Uso de la IA generativa y posibles vulneraciones de la seguridad de los datos

Toma de decisiones erróneas

Fuente: Gartner

Implementa soluciones de gestión de la confianza, el riesgo y la seguridad de la IA (AI TRiSM)

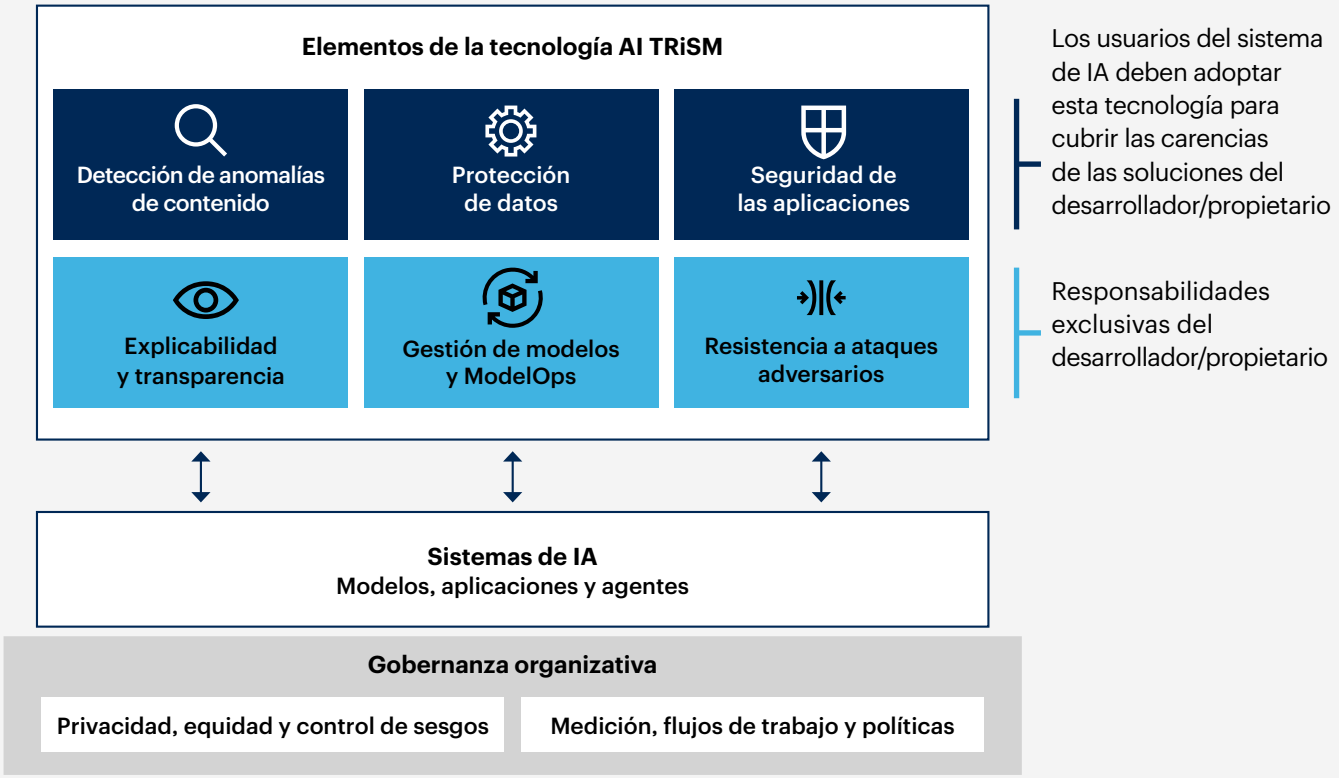
Los riesgos de la IA generativa aumentan con el uso de grandes modelos de lenguaje (LLM) alojados externamente y otros modelos de IA generativa, ya que las empresas no pueden controlar directamente los procesos de aplicación ni la manipulación y almacenamiento de los datos.

Los modelos locales alojados y controlados internamente también presentan riesgos, especialmente cuando se carece de controles de seguridad y gestión de riesgos.

Gestiona el riesgo con la gestión de la confianza, el riesgo y la seguridad de la IA (AI TRiSM), un marco de controles y facilitadores de confianza que proporcionan de manera continua lo siguiente:

1. Detección de anomalías de contenido
2. Gobernanza y protección de datos
3. Reducción de los riesgos de seguridad de las aplicaciones

Tecnología de gestión de la confianza, el riesgo y la seguridad de la IA



Fuente: Gartner

Prioriza la protección de las aplicaciones de IA generativa

Garantiza la aplicación de controles de seguridad esenciales para la web, SaaS, infraestructura en la nube como servicio (IaaS) y plataformas como servicio (PaaS). Luego, toma medidas para proteger las aplicaciones de IA generativa.

Utilización de aplicaciones web y aplicaciones SaaS

- ☐ Política de uso aceptable (PUA) de la IA generativa
- ☐ Lista de verificación de los requisitos de seguridad para validar, aprobar e integrar las aplicaciones SaaS
- ☐ Norma de seguridad de los datos para proteger los datos confidenciales en la nube pública
- ☐ Producto de Security Service Edge (SSE) para garantizar la seguridad en el uso de las aplicaciones web y las aplicaciones SaaS

Aplicaciones empresariales alojadas en la nube

- ☐ Norma de seguridad para el uso seguro de la nube pública
- ☐ Tecnologías de seguridad para la protección de aplicaciones web y en la nube
- ☐ Capacidades de seguridad específicas para aplicaciones personalizadas
- ☐ Controles de detección de bots para garantizar que solo las personas accedan a las aplicaciones de IA generativa
- ☐ Capacidades para proteger los terminales de API tanto internos como externos

Céntrate en 3 áreas clave de riesgo

La IA generativa promete traer numerosos beneficios, como una mayor eficiencia y productividad. Sin embargo, también introduce tres nuevas categorías de riesgo.

Detección de anomalías de contenido

- Uso inaceptable o malicioso
- Alucinaciones
- Riesgo de resultados inexactos, ilegales, que infrinjan los derechos de autor o resulten perjudiciales

Protección de datos

- Filtración de datos
- Contenidos y datos de usuario comprometidos
- Gobernanza de la política de privacidad y protección de datos
- Evaluaciones del impacto en la privacidad
- Cumplimiento de la normativa regional

Seguridad de las aplicaciones

- Ataques adversarios a través de consultas
- Ataques a bases de datos vectoriales
- Acceso de hackers

Define tu rumbo

La AI TRiSM es un esfuerzo colaborativo: la IA, la seguridad, el cumplimiento y las operaciones deben unirse para implementar nuevas medidas de AI TRiSM. Empieza por estas acciones:

- [ ] Crea un grupo de trabajo organizativo o una unidad especializada para gestionar tus esfuerzos de AI TRiSM.
- [ ] Trabaja con toda la organización para gestionar los mejores conjuntos de herramientas posibles como parte de un programa integral de AI TRiSM.
- [ ] Define políticas de uso aceptable. Establece sistemas para registrar y aprobar de manera metódica las aplicaciones de los usuarios y el uso de documentos.
- [ ] Supervisa continuamente el uso en relación con los objetivos establecidos y ajusta los parámetros de uso de manera constante.

Para 2026, las empresas que implementen controles TRiSM en las aplicaciones de IA consumirán al menos un **50 % menos** de información inexacta o ilegítima que conduzca a una toma de decisiones errónea.

Fuente: Gartner

Cómo los CIO pueden maximizar el potencial de la IA generativa

La IA generativa promete transformar una amplia gama de procesos empresariales y de seguridad. Estas son las acciones que, como CIO, deberías priorizar para aprovechar al máximo su valor:

- ☐ **Registra, supervisa y gestiona el consumo de IA** de aplicaciones y funciones de IA generativa de terceros.
- ☐ **Actualiza los requisitos de selección de proveedores y tecnologías** para abordar los retos de privacidad, derechos de autor, trazabilidad y explicabilidad.
- ☐ **Actualiza las prácticas de seguridad de las aplicaciones y los datos de IA** para integrar nuevas superficies de ataque.
- ☐ **Realiza pruebas de concepto antes de integrar la IA generativa en los programas de ciberseguridad,** con el objetivo de potenciar las capacidades de los empleados en lugar de reemplazarlos.
- ☐ **Supervisa los cambios en el panorama de las amenazas,** como la disminución de la precisión de la detección y del rendimiento de los controles de seguridad existentes. Asegúrate de tener acceso a información precisa sobre los cambios en el panorama de amenazas. Planificar escenarios hipotéticos para futuros ataques de IA generativa es complejo y puede que no sea la forma más provechosa de emplear los recursos.

Durante 2025, la IA generativa provocará un repunte en los recursos de ciberseguridad necesarios para protegerla, lo que supondrá un **aumento de más del 15 % en el gasto en seguridad de las aplicaciones y los datos.**

Fuente: Gartner

Cómo los CISO pueden maximizar el potencial de la IA generativa

Estas son las acciones que, como CISO, deberías priorizar para aprovechar al máximo su valor:

- ☐ **Evalúa estas tecnologías como cualquier otra herramienta** para valorar si generan nuevos riesgos con los datos confidenciales.
- ☐ **Define los resultados óptimos esperados** a fin de evaluar cómo la IA puede mejorar los indicadores de seguridad existentes sin tener que crear otros nuevos.
- ☐ **Realiza experimentos con nuevas funciones** de los proveedores de seguridad existentes, empezando por casos de uso específicos y bien definidos en las áreas de operaciones de seguridad y seguridad de las aplicaciones.
- ☐ **Aplica el marco AI TRiSM** al desarrollar nuevas aplicaciones propias o al usar aplicaciones de terceros que utilicen grandes modelos de lenguaje (LLM) e IA generativa.
- ☐ **Prepara y capacita a los equipos** para hacer frente tanto a los efectos directos (privacidad, propiedad intelectual, seguridad de las aplicaciones de IA) como a los indirectos (otros equipos que utilizan la IA generativa, como RR. HH., finanzas o aprovisionamiento) derivados del uso de la IA generativa en la empresa.

Para 2028, la adopción de aumentos generativos reducirá la brecha de habilidades, **lo que eliminará la necesidad de educación especializada en el 50 % de los puestos de ciberseguridad de nivel inicial.**

Fuente: Gartner

Define tu rumbo

Estos son los siguientes pasos que deberías dar:

- ☐ **Evalúa** las tecnologías de IA y decide los resultados óptimos que espera lograr tu organización con ellas.
- ☐ **Mantén y perfecciona** las capacidades de detección y respuesta ante amenazas inciertas y ambiguas.
- ☐ **Invierte** en gestión de la exposición e inteligencia sobre amenazas para identificar los riesgos más relevantes.

Una tercera parte (34 %) de las organizaciones tienen previsto implementar la IA generativa en los próximos 12 meses.

Fuente: Gartner

Puestos de liderazgo clave para desarrollar con éxito una estrategia y un plan de implementación de la IA

CIO/Responsable de tecnología

El CEO, el resto de responsables de empresa y la junta directiva esperan que el CIO desarrolle una estrategia formal de IA (o nombre a un líder de IA) y logre con éxito:

- Establecer un objetivo de IA para toda la empresa, identificar casos de uso y cuantificar los beneficios y riesgos.
- Alinear los equipos empresariales y de tecnología, además de modificar las competencias organizativas para apoyar la IA.
- Designar a un líder de IA para coordinar las ideas y fomentar la innovación.

CISO/Responsable de seguridad + equipo

El responsable de ciberseguridad debe garantizar que la ciberseguridad y la privacidad de los datos sean una parte esencial de la estrategia de IA y lograr con éxito:

- Proporcionar una supervisión general del programa en términos de seguridad y riesgo.
- Anticipar y tomar medidas contra las consecuencias imprevistas, como las vulneraciones de la seguridad de los datos o las infracciones de los derechos de autor.
- Actualizar continuamente las habilidades y la preparación para hacer frente a nuevas amenazas.

CDAO/Responsable de análisis de datos + equipo

Se espera que el responsable de análisis de datos guíe a sus organizaciones en la preparación de los datos para la estrategia de IA y logre con éxito:

- Identificar casos de uso de la IA para la gestión de análisis de datos aumentados.
- Aprovechar las prácticas de análisis de datos existentes y establecer políticas de gobernanza de análisis de datos para la IA.
- Desarrollar nuevas fuentes de valor a partir de los datos aprovechando la IA.
- Preparar los datos para la IA.

Responsable de arquitectura empresarial + equipo

Se espera que el responsable de arquitectura empresarial genere un valor empresarial tangible a partir de la IA y que logre con éxito:

- Ser el propietario y responsable de toda la hoja de ruta de la infraestructura de IA.
- Controlar las decisiones de inversión en arquitectura tecnológica de IA.
- Dirigir la toma de decisiones sobre la adopción de soluciones de IA para impulsar los resultados empresariales.

Responsable de ingeniería de software + equipo

El responsable de ingeniería de software debe comprender a fondo las implicaciones de la tecnología de IA y lograr con éxito:

- Aclarar los resultados empresariales deseados respecto a la integración de la IA.
- Definir buenas prácticas de ingeniería de IA en toda la organización.
- Transformar los productos, servicios y experiencias, y adoptar un enfoque que dé prioridad a la IA en las hojas de ruta.

Nuestra investigación ha revelado varias ideas sobre cómo **posibilitar que cada función tome medidas eficaces para obtener resultados con la IA que aporten valor.**

	1 Establece un objetivo de IA que esté alineado con los objetivos de la empresa	2 Selecciona casos de uso y realiza pruebas	3 Incorpora la IA en la tecnología y las operaciones empresariales
CIO/Responsable de tecnología	**Elige cuidadosamente dónde centrar los esfuerzos en materia de IA** mediante el seguimiento de las buenas prácticas recomendadas por Gartner para seleccionar los indicadores empresariales con un mayor impacto.	**Alinea los objetivos empresariales con las pruebas piloto** mediante el estudio del valor empresarial potencial y la viabilidad, y evaluando el impacto disruptivo y la posible consecución de los objetivos estratégicos.	**Impulsa la adopción de la IA en la empresa,** convirtiéndola en una práctica de innovación mediante la designación de líderes específicos, la asignación de recursos y financiación y el establecimiento de barreras de protección y gobernanza.
CISO/Responsable de seguridad + equipo	**Anticípate a los atacantes sofisticados** mediante el uso del modelado del comportamiento de la IA para mejorar las capacidades de detección de amenazas.	**Identifica los mejores casos de uso de la IA** mediante la valoración de la viabilidad y la reducción de riesgos, y el uso del recurso AI Use-case Prism for Cybersecurity de Gartner.	**Gestiona de manera más eficaz el riesgo de la IA,** con equipos que trabajen en proyectos de IA evaluando las consideraciones de ciberseguridad en cada fase del desarrollo.
CDAO/Responsable de análisis de datos + equipo	**Impulsa la alineación** mediante la cuantificación del valor esperado de la IA con un KPI específico y estableciendo indicadores de avance y retraso para supervisarlo.	**Prioriza mejor los casos de uso** mediante la selección de las dimensiones del valor empresarial, el refinamiento de los casos de uso y el fomento del compromiso y las decisiones.	**Impulsa de manera eficiente la entrega de IA** mediante la potenciación de las capacidades de los equipos interdisciplinarios con expertos en datos, el uso de técnicas más apropiadas y el mantenimiento de una deuda técnica baja.
Responsable de arquitectura empresarial + equipo	**Crea un ecosistema de IA eficaz** mediante la identificación de áreas en las que se pueda investigar en mayor profundidad y el desarrollo de planes y estrategias de IA.	**Planifica las iniciativas de IA de manera más estratégica** mediante el uso del enfoque de modelado de capacidades en cuatro pasos de Gartner para establecer una infraestructura de IA óptima.	**Consigue los resultados empresariales deseados y evita fallos** mediante el seguimiento del enfoque de cinco fases de Gartner para la ejecución de la IA.
Responsable de ingeniería de software + equipo	**Realiza las operaciones de desarrollo de aplicaciones de manera efectiva** mediante la adopción de prácticas de ingeniería de software con IA.	**Maximiza el valor de la IA** mediante la identificación de áreas en las que las pruebas de software puedan beneficiarse más de la IA y generar un mayor impacto, como en las pruebas visuales.	**Genera ideas innovadoras** mediante la combinación de la experiencia humana con la IA generativa para mejorar la exploración y comprensión del espacio de soluciones.

Información práctica y objetiva

Descubre estos recursos y herramientas complementarios:

Insights

Tendencias en ciberseguridad: optimización para mejorar la resiliencia y el rendimiento

Descubre cómo las principales tendencias reflejan la necesidad de programas más ágiles y adaptables.

Herramienta

Evaluación comparativa del valor empresarial de la ciberseguridad de Gartner

Explora nuevas medidas estandarizadas para compararte con otras organizaciones del sector, reducir los riesgos y alcanzar los objetivos empresariales.

Insights

Crea una hoja de ruta de ciberseguridad resiliente para tu empresa

Mantén a tu equipo centrado en los proyectos que sustentarán los objetivos de la empresa y en abordar los riesgos.

Webinar

Explora la evolución de los riesgos y los retos de seguridad en los sistemas de IA empresarial

Aprende a proteger la IA y a implementar las medidas necesarias para evitar fallos en la IA.

Accede a otros conocimientos sobre IA de Gartner:

Elabora una estrategia de IA que impulse el valor para tu empresa

Prepárate para la IA: lo que todo responsable de TI debe saber y hacer

Guía fundamental de los datos preparados para la IA

Ciberseguridad e IA: mejora la seguridad y gestiona los riesgos

¿Ya eres cliente?
Obtén acceso a más recursos en tu portal de cliente. Iniciar sesión

Conecta con nosotros

Obtén conocimientos prácticos y objetivos que permitan una toma de decisiones más acertada y un mejor desempeño a la hora de abordar las principales prioridades estratégicas. Contacta con nosotros para hacerte cliente:

EE. UU.: 1 855 811 7593

Internacional: +44 (0) 3330 607 044

Hazte cliente

Obtén más información sobre Gartner para responsables de ciberseguridad
gartner.com/en/cybersecurity

Entérate de las últimas novedades

Acude a una conferencia de Gartner
Ver conferencias

Gartner®