CEOE Empresas Españolas

Liderar
Defender
Impulsar
Promover

Digitalización, Innovación, Comercio e Infraestructuras

Panorama actual sobre el Impacto de la Inteligencia Artificial en la Ciberseguridad

Panorama actual sobre el Impacto de la Inteligencia Artificial en la Ciberseguridad

Contenido

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

1. Introducción

En la actualidad, el desarrollo y uso de la inteligencia artificial (IA) está experimentando un auge notable, especialmente en su vertiente generativa.

Dada la relevancia de esta tecnología, resulta esencial analizar las implicaciones que su implementación puede tener para las empresas y organizaciones en el ámbito de la ciberseguridad.

El objetivo de este documento es concienciar sobre la importancia de los avances en IA, cómo afectan a las empresas y cómo están transformando el panorama de la ciberseguridad, tanto desde la perspectiva de los ataques como de las defensas.

Si bien el potencial de la IA es indiscutible y su impacto en la ciberseguridad es cada vez más tangible, cabe señalar que algunas aplicaciones aún se encuentran en proceso de maduración antes de alcanzar su estado óptimo.

2. Impacto de la IA en la Ciberseguridad

La inteligencia artificial (IA) está revolucionando muchos aspectos de nuestras vidas y negocios, y la ciberseguridad no es una excepción. La IA, especialmente en su variante generativa, está siendo utilizada tanto para fortalecer las defensas cibernéticas como para potenciar los ciberataques.

Desde el lado de la defensa, la IA ofrece la capacidad de analizar grandes volúmenes de datos en tiempo real, detectar patrones sospechosos y responder a amenazas de manera más rápida y precisa que los métodos tradicionales. Por ejemplo, los sistemas de IA pueden identificar y neutralizar malware avanzado, reconocer intentos de phishing antes de que lleguen a los usuarios, y automatizar la respuesta a incidentes para reducir el tiempo de reacción.

Sin embargo, los mismos avances que hacen a la IA una herramienta poderosa para la defensa también la convierten en una herramienta peligrosa en manos de atacantes. La IA puede ser utilizada para crear ataques más sofisticados, realizar campañas de phishing altamente personalizadas y desarrollar deepfakes convincentes que pueden engañar a personas y sistemas[1]. Esto presenta nuevos

[1] ENISA THREAT LANDSCAPE 2024 | *"Herramientas de IA para ciberdelincuentes: Los actores de amenazas utilizaron herramientas como FraudGPT y grandes modelos lingüísticos para ser coautores de correos electrónicos fraudulentos y generar scripts PowerShell maliciosos."*

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

desafíos para la ciberseguridad, ya que las amenazas se vuelven más difíciles de detectar y mitigar.

Se estima que el mercado mundial de productos de ciberseguridad basados en IA alcanzará los 133.800 millones de dólares en 2030, frente a los 14.900 millones de dólares de 2021[2].

Según el informe[3] publicado por el Centro Nacional del Ciberseguridad del Reino Unido (NCSC):

- Es casi seguro que la inteligencia artificial (IA) aumentará el volumen y aumentará el impacto de los ciberataques en los próximos dos años.
- La amenaza para 2025 proviene de la evolución y mejora de las tácticas, técnicas y procedimientos (TTP) existentes.
- Todos los tipos de actores de amenazas cibernéticas, estatales y no estatales, calificados y menos calificados, ya están utilizando IA, en diversos grados.
- La IA proporciona un aumento de la capacidad en el reconocimiento y la ingeniería social, lo que casi con certeza hace que ambos sean más efectivos, eficientes y más difíciles de detectar.
- Es muy probable que los usos más sofisticados de la IA en las operaciones cibernéticas se restrinjan a los actores de amenazas con acceso a datos de entrenamiento de calidad, experiencia significativa (tanto en IA como cibernética) y recursos. Es poco probable que se realicen usos más avanzados antes de 2025.
- La IA reduce la barrera para que los ciberdelincuentes novatos, los hackers a sueldo y los *hacktivistas* lleven a cabo operaciones efectivas de acceso y recopilación de información. Es probable que este acceso mejorado contribuya a la amenaza global de *ransomware* en los próximos dos años.
- De cara a 2025 y más allá, es casi seguro que la mercantilización de la capacidad habilitada por la IA en los mercados penales y comerciales hará que la mejora de la capacidad esté disponible para la ciberdelincuencia y los actores estatales.

Por otro lado, según el informe " *STATE OF AI CYBER SECURITY 2024. Industry Perspectives on the Growing Role of AI in Cyber Security*", que recoge la opinión de más de 1.800 CISO y líderes de seguridad, señala que:

- El 74% de los encuestados está de acuerdo en que las amenazas cibernéticas impulsadas por IA están teniendo un impacto significativo en sus organizaciones.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

[2] https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html

[3] https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=AI%20lowers%20the%20barrier%20for,over%20the%20next%20two%20years.

- El 60% de los encuestados teme que sus organizaciones no estén adecuadamente preparadas para defenderse de los ataques impulsados por IA.
- El 96% de los participantes en la encuesta cree que las soluciones de seguridad impulsadas por IA mejoran significativamente la velocidad y la eficiencia de la prevención, detección, respuesta y recuperación.

Para finalizar cabe citar otro estudio, realizado en esta ocasión por KPMG y titulado *Perspectivas España 2024: Inteligencia Artificial y Digitalización*, en el que señala que "*para uno de cada tres empresarios y directivos (33%), la seguridad y la privacidad es uno de los retos que plantea la Inteligencia Artificial Generativa, se hace necesario aplicar un enfoque pragmático, que genere confianza en el cliente sin frenar el desarrollo de esta tecnología.*"

3. Riesgos Asociados

A medida que los sistemas de IA se vuelven más avanzados, los ciberdelincuentes también están aprovechando estas tecnologías para llevar a cabo ataques más sofisticados y efectivos. La capacidad de la IA para automatizar y personalizar ataques, generar contenido engañoso y evadir las defensas tradicionales plantea serias preocupaciones para la seguridad de las organizaciones.

Un aspecto alarmante es el uso de IA generativa para crear correos electrónicos de phishing altamente convincentes y deepfakes que pueden engañar tanto a personas como a sistemas automatizados. Además, la automatización de ataques mediante IA permite a los atacantes ejecutar campañas a gran escala con una eficiencia sin precedentes, aumentando la frecuencia y la sofisticación de los ataques.

Estadísticas recientes indican que **el 61% de las organizaciones creen que no pueden detectar intentos de brecha sin el apoyo de tecnologías de IA**, lo que subraya la dependencia creciente en estas herramientas para la defensa cibernética[4]. Sin embargo, esta misma dependencia puede convertirse en una vulnerabilidad si los sistemas de IA son manipulados o comprometidos por atacantes.

La preocupación por la privacidad también se ha intensificado con el uso de IA, ya que esta tecnología puede manejar y, potencialmente, exponer datos personales de manera no intencionada. **Alrededor del 39% de los expertos en ciberseguridad expresan que la implementación de IA podría agravar los problemas de privacidad**[5].

Además, la falta de regulaciones adecuadas para el uso de IA generativa y la aparición de nuevos tipos de ataques que las herramientas actuales no pueden detectar son otros riesgos significativos que las organizaciones deben considerar. **Un**

[4] All About AI
[5] All About AI

Calle Diego de León, 50
28006 Madrid
España
+34 915 663 400
info@ceoe.es
ceoe.es

33% de los expertos señala la carencia de un marco regulatorio robusto como un desafío importante[6].

3.1 Aumento de la sofisticación de los ciberataques.

Uno de los riesgos más preocupantes que ha traído consigo el exponencial crecimiento de la Inteligencia Artificial en los últimos meses, en particular, la inteligencia artificial Generativa, es el aumento de la sofisticación de los ciberataques.

La IA generativa ha comenzado a ser utilizada por ciberdelincuentes para mejorar y perfeccionar sus ataques. Tradicionalmente, los ciberataques dependían, en gran medida, de técnicas predecibles y patrones conocidos que los sistemas de seguridad podían identificar y bloquear. Sin embargo, con la IA generativa, los atacantes ahora pueden desarrollar métodos mucho más complejos y adaptativos.

A continuación, se muestran algunos **ejemplos de cómo la IA está aumentando la sofisticación de los ciberataques**:

1. **Phishing avanzado**: La IA generativa permite a los atacantes crear correos electrónicos de phishing que son casi indistinguibles de los correos electrónicos legítimos. Estos correos pueden personalizarse automáticamente para incluir detalles específicos sobre la víctima, aumentando la probabilidad de que esta caiga en la trampa. Por ejemplo, un correo podría parecer que proviene del jefe de la víctima, solicitando información sensible de manera urgente.

2. **Automatización de ataques**: La IA puede ser utilizada para automatizar la identificación de vulnerabilidades en sistemas y redes. Un atacante podría programar un sistema de IA para escanear miles de objetivos en busca de debilidades específicas, reduciendo el tiempo y el esfuerzo necesarios para lanzar un ataque exitoso.

3. **Malware evolutivo**: Utilizando IA, los atacantes pueden desarrollar malware que puede evolucionar para evadir las detecciones de los antivirus. El malware puede modificar su propio código y comportamiento en respuesta a las defensas que encuentra, haciéndose más difícil de detectar y eliminar.

4. **Ingeniería social automatizada**: La IA puede analizar grandes volúmenes de datos de redes sociales y otras fuentes para identificar información personal y profesional sobre una víctima. Esto permite a los atacantes diseñar campañas de ingeniería social altamente personalizadas y convincentes. Por ejemplo, un atacante podría usar IA para imitar el estilo de comunicación de un colega de la víctima y pedir acceso a sistemas internos.

[6] All About AI

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

5. **Ataques de suplantación de voz y video**: Con tecnologías de IA generativa, es posible crear audios y videos falsos que imitan a la perfección la voz y la apariencia de una persona. Estos deepfakes pueden ser utilizados para engañar a los empleados y hacerles realizar acciones perjudiciales, como transferencias de dinero a cuentas fraudulentas.

6. **Exfiltración de datos sigilosa**: La IA puede ayudar a los atacantes a extraer datos de manera sigilosa y eficiente. Por ejemplo, puede analizar patrones de tráfico de red para determinar la mejor manera de mover datos robados sin ser detectados, mimetizándose con el tráfico legítimo.

7. **Creación de Identidades Falsas:** La IA generativa puede ser utilizada para crear identidades falsas con fotos de perfil, documentos de identificación y datos personales ficticios. Estas identidades pueden ser utilizadas para abrir cuentas bancarias, registrar empresas fantasmas o realizar actividades fraudulentas sin ser detectadas.

8. **Simulación de Entornos de Prueba:** La IA generativa permite a los atacantes simular entornos de prueba que replican las redes y sistemas de una organización objetivo. Esto les permite experimentar y perfeccionar sus técnicas de ataque sin riesgo de detección, aumentando la eficacia de sus ciberataques.

9. **Desarrollos en Criptografía Ofensiva:** La IA generativa puede ser utilizada para desarrollar nuevas técnicas criptográficas que confundan y evadan las medidas de seguridad tradicionales. Esto incluye la creación de nuevos métodos de cifrado que son difíciles de descifrar y que pueden proteger las comunicaciones maliciosas de ser interceptadas.

10. **Emulación de Tráfico de Red:** Utilizando IA generativa, los atacantes pueden emular el tráfico de red legítimo para cubrir sus actividades maliciosas. Esto hace que sea más difícil para los sistemas de seguridad detectar comportamientos anómalos, ya que el tráfico malicioso se oculta entre el tráfico regular.

11. **Adaptación en Tiempo Real:** La IA generativa puede permitir a los atacantes adaptar sus métodos en tiempo real en respuesta a las defensas que encuentran. Por ejemplo, si un sistema de seguridad bloquea un tipo de ataque, la IA puede generar automáticamente una variante del ataque que evite la detección.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

3.2 Automatización de ataques.

La capacidad de la IA para automatizar y optimizar ciberataques representa un desafío significativo para la seguridad de las organizaciones.

La automatización de ataques con IA permite a los ciberdelincuentes lanzar campañas a gran escala con una rapidez y efectividad sin precedentes.

Anteriormente, los ciberataques requerían una cantidad significativa de tiempo y esfuerzo manual para identificar vulnerabilidades, diseñar exploits y ejecutar ataques. Hoy en día, con la ayuda de la IA, estos procesos pueden ser completamente automatizados, haciendo que los ataques sean más frecuentes, diversos y difíciles de prever.

A continuación, se muestran algunos **ejemplos de cómo la IA está automatizando los ciberataques:**

1. **Generación automática de exploits**: Una vez que se identifican las vulnerabilidades, la IA puede ayudar a generar y probar automáticamente exploits personalizados para aprovechar estas debilidades, reduciendo el tiempo y el esfuerzo necesarios para desarrollar ataques efectivos.
2. **Escaneo masivo de vulnerabilidades**: Las herramientas de IA pueden escanear miles de sistemas en busca de vulnerabilidades específicas en cuestión de minutos. Esto permite a los atacantes identificar objetivos potenciales de manera rápida y eficiente, aumentando sus oportunidades de éxito.
3. **Phishing a gran escala**: Los sistemas de IA pueden enviar correos electrónicos de phishing personalizados y dirigidos a millones de usuarios, adaptando los mensajes para maximizar las probabilidades de éxito. La IA puede analizar datos públicos y privados para crear mensajes altamente convincentes y específicos para cada destinatario.
4. **Ataques DDoS (Distributed Denial of Service) avanzados**: La IA puede coordinar y optimizar ataques DDoS, distribuyendo el tráfico malicioso de manera más efectiva para sobrecargar y desestabilizar los servidores objetivos. Esto permite que incluso atacantes con recursos limitados puedan lanzar ataques devastadores.
5. **Evasión de detección**: La IA puede aprender y adaptarse a las medidas de seguridad implementadas por las organizaciones, modificando sus técnicas de ataque en tiempo real para evitar ser detectada. Esto incluye cambiar patrones de tráfico, cifrar comunicaciones maliciosas y camuflarse como tráfico legítimo.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

6. **Ataques persistentes**: La IA puede mantener ataques persistentes a lo largo del tiempo, adaptándose continuamente a las defensas del objetivo. Esto incluye reintentar accesos fallidos con métodos nuevos y más sofisticados, asegurando que el ataque no cesa hasta que logra su objetivo.

7. **Ataques de suplantación de identidad (Deepfakes)**: La IA generativa puede crear audios y videos falsos (deepfakes) que imitan a la perfección la voz y la apariencia de una persona. Estos deepfakes pueden ser utilizados para engañar a los empleados y hacerles realizar acciones perjudiciales, como transferencias de dinero a cuentas fraudulentas o compartir información confidencial.

8. **Ataques Coordinados Multi-Vector:** La IA generativa permite coordinar ataques complejos que combinan múltiples vectores de ataque (phishing, malware, ingeniería social, etc.) para maximizar su efectividad. Estos ataques pueden ser lanzados simultáneamente o en una secuencia específica para sobrecargar las defensas de la organización objetivo.

4. Oportunidades y Beneficios

La inteligencia artificial (IA), incluida la IA generativa, **no solo presenta desafíos, sino también enormes oportunidades para fortalecer la ciberseguridad**. Utilizando IA, las organizaciones pueden mejorar significativamente su capacidad para detectar, prevenir y responder a ciberataques. Desde la automatización de la identificación de amenazas hasta la creación de defensas adaptativas, la IA permite a los sistemas de seguridad anticipar y neutralizar ataques con mayor rapidez y precisión que nunca.

Estas tecnologías avanzadas también facilitan el análisis de grandes volúmenes de datos para identificar patrones sospechosos y optimizar la respuesta a incidentes, proporcionando un entorno digital más seguro y resiliente.

4.1 Mejora en la detección de amenazas.

La IA generativa y otros algoritmos avanzados permiten a los sistemas de seguridad **identificar actividades maliciosas con una precisión y rapidez sin precedentes**. Tradicionalmente, la detección de amenazas dependía de firmas conocidas y patrones predefinidos, lo que dejaba a los sistemas vulnerables a ataques novedosos. Con la IA, es posible analizar vastas cantidades de datos en tiempo real, identificar comportamientos anómalos y predecir posibles amenazas antes de que se conviertan en problemas graves. Esta **capacidad de anticipación y respuesta proactiva** no solo mejora la seguridad, sino que también reduce los tiempos de respuesta a incidentes y minimiza el impacto de los ataques.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

A continuación, se muestran algunos **ejemplos de cómo la IA mejora la detección de amenazas:**

1. **Inteligencia de amenazas**: Los sistemas de IA pueden analizar grandes volúmenes de datos de inteligencia de amenazas provenientes de diversas fuentes, permitiendo la identificación temprana de nuevas tácticas, técnicas y procedimientos utilizados por los atacantes.

2. **Análisis en tiempo real**: La IA puede monitorear continuamente el tráfico de red y las actividades del sistema, detectando anomalías que podrían indicar un ataque en curso. Esto permite una respuesta inmediata y la mitigación de amenazas antes de que causen daños significativos.

3. **Detección de patrones de comportamiento**: Utilizando técnicas de aprendizaje automático, la IA puede aprender y reconocer patrones normales de comportamiento en una red, identificando desviaciones que podrían ser indicativas de actividades maliciosas, como el acceso no autorizado o exfiltración de datos.

4. **Correlación de eventos**: La IA puede correlacionar múltiples eventos de seguridad aparentemente inconexos para identificar patrones complejos de ataque. Esto ayuda a descubrir amenazas avanzadas y persistentes que podrían pasar desapercibidas con métodos de detección tradicionales.

4.2 Automatización de la respuesta a incidentes.

La IA no solo detecta amenazas, sino que también puede tomar decisiones automatizadas para contener y mitigar incidentes de seguridad. Esta capacidad no solo mejora la resiliencia de las infraestructuras digitales, sino que también libera a los equipos de ciberseguridad para que puedan enfocarse en tareas más estratégicas y complejas.

A continuación, se muestran algunos **ejemplos** de cómo la IA generativa está **automatizando la respuesta a incidentes**:

1. **Generación de contramedidas personalizadas**: La IA generativa puede crear automáticamente parches y soluciones específicas para vulnerabilidades recién descubiertas, permitiendo una respuesta inmediata y precisa a incidentes de seguridad.

2. **Desarrollo de playbooks de respuesta dinámicos**: Utilizando IA generativa, se pueden crear y actualizar continuamente playbooks de respuesta a

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

incidentes, basados en las mejores prácticas y adaptados a la evolución de las amenazas, asegurando que las organizaciones siempre cuenten con las estrategias más efectivas.

3. **Simulación de escenarios de ataque**: La IA generativa puede simular ataques y respuestas en entornos controlados, ayudando a identificar posibles puntos débiles y optimizar las estrategias de defensa antes de que ocurra un ataque real.

4. **Generación automática de informes de incidentes**: Tras un incidente, la IA generativa puede compilar y generar informes detallados y personalizados sobre lo ocurrido, facilitando el análisis post-incidente y proporcionando recomendaciones específicas para evitar futuras brechas.

5. **Respuesta adaptativa en tiempo real**: La IA generativa puede analizar el comportamiento de las amenazas en tiempo real y generar respuestas adaptativas, ajustando las medidas de defensa dinámicamente para contrarrestar las técnicas de los atacantes de manera efectiva.

4.3 Fortalecimiento de las defensas cibernéticas.

El uso de la Inteligencia Artificial, y en particular, de la Inteligencia Artificial Generativa, proporciona a empresas y organizaciones una defensa más proactiva y adaptable, permitiendo enfrentar las amenazas de ciberseguridad de manera más eficaz y con mayor resiliencia.

Esta capacidad de adaptación y evolución es esencial para **mantener la integridad y seguridad de las infraestructuras digitales** en un mundo donde los ciberataques son cada vez más sofisticados.

A continuación, se muestran algunos **ejemplos de cómo la IA generativa está fortaleciendo las defensas cibernéticas:**

1. **Desarrollo de firewalls inteligentes**: La IA generativa puede diseñar y ajustar automáticamente reglas de firewall basadas en patrones de tráfico en tiempo real, bloqueando actividades sospechosas y adaptándose a nuevas tácticas de los atacantes.

2. **Creación de honeypots dinámicos**: Utilizando IA generativa, es posible desarrollar honeypots (trampas para atacantes) que cambian y evolucionan constantemente, engañando a los atacantes y recopilando información valiosa sobre sus métodos y objetivos.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

3. **Actualización continua de sistemas de detección de intrusiones**: La IA generativa puede analizar datos de incidentes pasados y generar nuevas firmas y reglas para los sistemas de detección de intrusiones (IDS), mejorando su capacidad para detectar y prevenir intrusiones futuras.

4. **Generación de scripts de respuesta automática**: En función de las amenazas identificadas, la IA generativa puede crear scripts personalizados que ejecuten acciones defensivas específicas, como aislar dispositivos comprometidos o bloquear accesos no autorizados.

5. **Análisis predictivo de vulnerabilidades**: La IA generativa puede predecir posibles vulnerabilidades en sistemas y aplicaciones, generando informes y recomendaciones sobre parches y actualizaciones antes de que las vulnerabilidades sean explotadas por los atacantes.

4.4 Optimización de la gestión de riesgos.

La optimización de la gestión de riesgos mediante IA generativa proporciona a las organizaciones una herramienta poderosa para protegerse de las amenazas cibernéticas. Al ofrecer una **visión más precisa y proactiva de los riesgos**, estas tecnologías **permiten** a las empresas **tomar decisiones más informadas** y fortalecer su postura de seguridad en un entorno digital cada vez más complejo.

A continuación, se muestran algunos **ejemplos de cómo la IA generativa está optimizando la gestión de riesgos:**

1. **Generación de evaluaciones de riesgo personalizadas**: Utilizando IA generativa, las organizaciones pueden crear evaluaciones de riesgo adaptadas a sus entornos específicos, considerando factores únicos como la infraestructura de TI, los datos sensibles y las amenazas específicas de la industria.

2. **Análisis predictivo de riesgos**: La IA generativa puede analizar datos históricos y en tiempo real para prever posibles amenazas y vulnerabilidades, proporcionando recomendaciones sobre cómo mitigarlas antes de que se conviertan en problemas.

3. **Desarrollo de estrategias de mitigación**: La IA generativa puede sugerir estrategias de mitigación basadas en el análisis de riesgos, incluyendo la implementación de controles de seguridad, la adopción de nuevas tecnologías y la modificación de políticas internas.

4. **Optimización de recursos de seguridad**: La IA generativa puede ayudar a asignar recursos de seguridad de manera más efectiva, identificando áreas

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

prioritarias que requieren mayor atención y optimizando el uso de presupuestos y personal.

5. **Simulación de escenarios de riesgo**: La IA generativa puede crear simulaciones detalladas de posibles incidentes de seguridad, ayudando a las organizaciones a entender el impacto potencial de diferentes amenazas y a prepararse mejor para enfrentar eventos adversos.

4.5 Fortalecimiento de la Educación y Concienciación en Seguridad

La inteligencia artificial generativa está revolucionando la forma en que las organizaciones educan y conciencian a sus empleados sobre ciberseguridad. Estas tecnologías avanzadas permiten **desarrollar programas de formación personalizados, crear simulaciones de ataques realistas y ofrecer evaluaciones continuas que se adaptan dinámicamente a las necesidades individuales**.

Al proporcionar **feedback inmediato y recomendaciones de aprendizaje continuo**, la IA generativa asegura que los empleados no solo adquieran conocimientos teóricos, sino que también desarrollen habilidades prácticas y se mantengan actualizados frente a las amenazas emergentes. Esta capacidad de adaptación y personalización es clave para fortalecer la preparación y respuesta de las organizaciones ante los desafíos crecientes en el ámbito de la ciberseguridad.

A continuación, se muestran algunos **ejemplos de cómo la IA generativa está optimizando la Educación y Concienciación en Seguridad**:

1. **Generación de escenarios de entrenamiento personalizados:** La IA generativa puede crear escenarios de ataque específicos para el entrenamiento del personal, ajustándose a los roles y responsabilidades individuales dentro de la organización.

2. **Desarrollo de contenidos educativos dinámicos:** Utilizando IA generativa, se pueden crear materiales educativos que se actualizan continuamente en función de las amenazas emergentes, manteniendo al personal informado y preparado. Por ejemplo, mediante la generación de cuestionarios interactivos: que se actualizan automáticamente con nuevas preguntas basadas en las amenazas emergentes y los últimos incidentes de seguridad.

3. **Provisión de feedback inmediato**: La IA generativa puede proporcionar feedback inmediato y detallado durante las sesiones de formación, destacando las áreas de mejora y sugiriendo recursos adicionales para fortalecer las habilidades de los empleados.

4. **Recomendaciones de aprendizaje continuo:** Basándose en las evaluaciones y el desempeño, la IA puede generar recomendaciones personalizadas de

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

aprendizaje, incluyendo cursos, artículos y talleres que ayudarán a los empleados a mejorar su conocimiento y habilidades en ciberseguridad.

5. **Desarrollo de infografías y videos educativos:** Utilizando IA generativa, se pueden producir infografías y videos educativos que expliquen conceptos de ciberseguridad de manera clara y atractiva, mejorando la retención de información entre los empleados.
6. **Adaptación en tiempo real del plan de estudios:** La IA puede ajustar el plan de estudios en tiempo real basándose en la evolución de las amenazas y las necesidades de la organización, asegurando que los empleados siempre estén preparados para enfrentar los desafíos más recientes

5. Aplicación práctica y global de la IA en la Ciberseguridad para entornos corporativos o de negocio

Se ha analizado hasta ahora la importancia de identificar los métodos usados para atacar y proteger con Inteligencia Artificial (IA), así como los riesgos elevados que se pueden generar de forma exponencial, por el uso de la misma por parte de los atacantes, debido a la alta complejidad de los métodos creados con el pasar de los meses y años.

Por lo anterior, se hace primordial **identificar o tener una base de clasificación o segmentación de los entornos y los focos de ataques donde aplicaremos herramientas, métodos y modelos de IA avanzados**. Esto permitirá proteger de forma eficiente y detallada las zonas de servicios o infraestructuras de TI, sobre las cuales se despliegan o ejecutan servicios de procesamiento de información corporativa o incluso personal, garantizando la seguridad y los resultados esperados a nivel de integridad de los datos.

Lo anterior se puede lograr mediante el uso óptimo y apropiado, para lo cual se deben tener en cuenta la creación o el uso de una batería de herramientas, modelos de IA y la aplicación de una metodología o, en este caso, **un modelo robusto y estructurado que cubra todos los bloques de servicios**, tanto a nivel local (on-premises) como en el cloud, los cuales son utilizados durante el proceso de diseño, despliegue y gestión de servicios.

Hasta la fecha, y siendo uno de los muchos caminos que una organización puede tomar en el diseño e implementación de su plan de transición hacia arquitecturas de confianza cero, se han identificado de forma natural en la Gestión de la Seguridad de

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

la Información (SGSI) de cada organización o empresa los siguientes segmentos: **Identidad, Endpoints, redes, aplicaciones y datos**[7].

Como un elemento residual, pero relevante, se encuentra la **hibridación de los segmentos anteriores**, lo cual ha sido definido como prioritario por un gran número de empresas de diferentes sectores: infraestructuras críticas, financiero, gobierno, seguros y defensa, entre otros.

Según el orden de prioridad, cada segmento tiene su propia 'naturaleza' o complejidad, por lo que es necesario abordarlo de forma individual, identificando lo que se puede lograr con el uso de la IA (o IA Generativa) de manera pragmática.

En los siguientes puntos, se procederá a **particularizar**, teniendo en cuenta el análisis realizado hasta el momento en torno a los riesgo y oportunidades/beneficios, **la forma en la que se pueden abordar los retos que se plantean en cada uno de estos segmentos.**

- **Servicios de identidad**

Todos los entornos o segmentos de servicios que gestionan datos (como Endpoints, redes, aplicaciones y bases de datos) hacen uso de los servicios de identidad para acceder a estos. La IA, como tal, puede proteger cualquier identidad y garantizar un acceso estructurado a los servicios mencionados, clasificados como críticos, de forma óptima o avanzada. Al utilizar IA en los servicios de identidad, se pueden detectar patrones comportamentales anormales que buscan accesos no autorizados, con un beneficio adicional: la capacidad de suministrar una respuesta en tiempo real a un ataque y a situaciones o entornos complejos y multinube.

El uso de IA en los análisis de seguridad y protección de los servicios de identidad puede mejorar la identificación específica de las actividades y comportamientos de los usuarios dentro de las organizaciones o entidades, registrando y monitorizando tareas que se desvían de sus patrones comunes, como movimientos laterales entre servicios y escaladas horizontales o verticales de privilegios[8], que podrían indicar un ataque en curso o, incluso, preverlo antes de que suceda, debido al monitoreo de actividades preliminares típicas y la generación de alertas 'inteligentes' según estas.

Además, se puede ir más allá, bloqueando los servicios de identidad y proporcionando una ruta detallada para la solución del incidente.

De acuerdo con lo expuesto, **es posible generar políticas avanzadas de forma autogestionada con el uso de la IA**, para decidir si es necesario aplicar otro método

[7] *Zero trust maturity model*. (s/f). Cybersecurity and Infrastructure Security Agency CISA. Recuperado el 16 de agosto de 2024, de https://www.cisa.gov/zero-trust-maturity-model

[8] Escalada Horizontal: Un atacante accede a cuentas con privilegios similares a los que ya posee, permitiéndole acceder a diferentes datos o funcionalidades. Escalada Vertical: El atacante eleva sus privilegios de un nivel más bajo a uno más alto, como pasar de una cuenta de usuario estándar a una de administrador.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

adicional de autenticación, teniendo en cuenta variables como el dispositivo, el lugar de origen y el comportamiento del individuo.

En una fase final, y según los factores implicados en las actividades anteriores, **se puede crear una matriz de riesgos** con IA Generativa, obteniendo un beneficio real: una respuesta en tiempo real y una guía puntual para remediar los ataques a los servicios de identidad de la organización que sean comunes o constantes.

En conclusión, al utilizar la IA (Generativa), es posible evaluar continuamente el riesgo y la remediación asociada a las identidades y/o accesos. Lo anterior **permite a las organizaciones decidir, con conocimiento previo de los resultados esperados, si deben conceder o permitir ciertos accesos, basándose en un análisis de riesgos en tiempo real."**

- **Endpoints (Devices).**

Los Endpoints (Devices) pueden ser equipos o aplicaciones en entornos locales o en la nube. Teniendo esto presente, se puede usar la IA a nivel global para monitorizar e identificar las necesidades de protección de éstos de forma dinámica y con tiempos de respuesta muy cortos, en comparación con los tiempos anteriores al uso de esta tecnología.

A continuación, se presentan algunos aspectos en los que la IA protege de forma avanzada este segmento y en los que múltiples soluciones de ciberseguridad de distintos proveedores están disponibles o se están utilizando actualmente.

El uso de estas soluciones es vital dentro de las empresas y fundamental en la aplicación de sus planes de seguridad, para estar acordes a los ataques avanzados que enfrentan, muchos de los cuales son perpetrados con el mismo uso de la IA de forma malintencionada:

- Protección de identidades**:** Extrapolando el segmento anterior, en primera instancia, la IA logra proteger los servicios de identidad de los Endpoints, detectando intentos de acceso no autorizados en entornos locales (físicos) y en la nube (aplicaciones, servidores, máquinas virtuales, entre otros). Esto se logra mediante la aplicación de políticas de acceso adaptativas avanzadas y basadas en el riesgo, con una identificación previa utilizando casos similares (inferencia lógica mediante la comparación), así como parámetros corporativos, normativos, legislativos o incluso basados en las mejores prácticas existentes.
- Análisis de comportamiento: La IA ayuda a identificar comportamientos (también mediante inferencia) o actividades anómalas dentro de los dispositivos, lo que puede indicar la presencia de programas maliciosos o actividades no autorizadas. Esto se logra mediante la creación de modelos asociados a políticas de seguridad,

Calle Diego de León, 50
28006 Madrid
España
+34 915 663 400
info@ceoe.es
ceoe.es

categorías e identificación de controles críticos para la seguridad corporativa. Es en este contexto donde el aprendizaje automático mejora continuamente a medida que analiza más datos o variables (de aplicaciones o infraestructuras), categorizadas según el nivel de protección requerido en los Endpoints.

- Detección y respuesta a amenazas: Se utiliza la IA para analizar grandes volúmenes de datos y detectar patrones de comportamiento sospechosos en tiempo real dentro de cada dispositivo o Endpoint. Esto permite identificar y responder rápidamente a amenazas antes de que puedan generar alguna alteración en cada uno de los Endpoints de la organización, y por ende, afectar la operación normal de la empresa. Posteriormente, esta actividad se convierte en una herramienta de mejora continua, que permite generar de forma automática (IA Generativa) planes de seguridad particulares y estratégicos para la organización.
- Inteligencia sobre amenazas: El uso de IA (Generativa) permite realizar un registro y análisis de datos de amenazas globales e individuales, y posteriormente, suministrar inteligencia ejecutable o predictiva que logra prevenir ataques de forma proactiva, sin necesidad de seguimiento humano.
- Automatización de respuestas: La IA permite automatizar la respuesta a incidentes de seguridad sobre grandes volúmenes de dispositivos, según la criticidad de estos y lo que representan dentro de la organización a nivel de su actividad principal. Esto incluye la contención de amenazas, la remediación de vulnerabilidades sin intervención de operadores tipo SOC y el aislamiento de dispositivos, utilizando como base de conocimiento la información generada por millones de registros y respuestas aplicadas por múltiples usuarios empresariales. Esto reduce el tiempo de respuesta y remediación cuando se presenta un incidente en los dispositivos o Endpoints..

La implementación de estas tecnologías permite ofrecer una protección robusta y proactiva contra una amplia gama de amenazas cibernéticas dirigidas a los Endpoints, que son un objetivo principal de los ciberdelincuentes. De ahí la importancia del uso de la IA en este segmento: los Endpoints

- **Redes (Virtuales, locales).**

Los grandes volúmenes de datos procesados y transmitidos por medio de las redes locales o en la nube hacen de este segmento un pilar prioritario para el uso de la IA, con el fin de garantizar la integridad y disponibilidad en su funcionamiento.

Dado que este es uno de los vectores de servicios de TI más atacados, la IA permite gestionar grandes volúmenes de datos con un enfoque específico y aplicar los controles de seguridad correspondientes a los niveles de protección requeridos. A continuación, se detallan algunas actividades que pueden ser implementadas con IA:

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

- Análisis avanzado de tráfico: A diferencia de los sistemas de años anteriores, actualmente se puede usar la IA para crear patrones o, en su defecto, identificarlos cuando son anómalos, incluso en un entorno con alto tráfico y un volumen elevado de variables. En el mismo instante, se pueden crear tareas autónomas que realicen el seguimiento de datos con comportamientos maliciosos comunes y los aíslen o bloqueen en caso de que se incumpla alguna política durante la transferencia en la red, que es objeto de análisis.

- Aplicación de algoritmos predictivos: Como se ha mencionado, según la información previa o los comportamientos observados, en el caso de las redes, se pueden identificar los orígenes del ataque y el tipo de datos recibidos en nuestro entorno. Con ello, es posible realizar una protección predictiva basada en los modelos, por ejemplo, bloqueando la comunicación entre dos puntos si los datos procesados son de carácter personal o financiero, teniendo en cuenta solo el encabezado del documento o archivo enviado. Esto se lleva a cabo sobre millones de solicitudes con un rendimiento elevado y fluido, sin la intervención de un operador de seguridad cuando se presentan incidentes.

- Monitorización continua: En entornos ideales, las redes no tendrían caídas o fallas. Sin embargo, en casos de ataques avanzados (por ejemplo, DDoS), esta estabilidad se ve comprometida y pueden surgir intermitencias o cambios en rutas, puertos o medios de comunicación para la transferencia de datos. Ante esta situación, la IA puede adaptarse dinámicamente a estas contingencias, manteniendo el ambiente de comunicación inicial e incluso ampliando la monitorización a canales adicionales de forma automática, gracias a un buen entrenamiento de modelos para cada medio utilizado o contemplado.

- Análisis de amenazas a nivel global: El segmento de red, a diferencia de los demás analizados en este apartado, recibe miles o incluso millones de ataques o 'señales' por minuto, dependiendo del nivel de exposición al entorno público o interno. Aquí es donde se debe usar la IA como herramienta de clasificación automática de dichas amenazas. Esto permite crear segmentos de señales o ataques y generar un reporte coherente sobre la situación de los mismos, proporcionando una clasificación global sobre el nivel de exposición y criticidad de la organización, e identificando los tramos críticos de datos."

- **Aplicaciones**

El uso de la IA en entornos de aplicaciones sigue rutas concretas para su implementación, permitiendo una protección tanto proactiva como reactiva de este segmento:

- Desarrollo seguro: Durante el proceso de creación o desarrollo de aplicaciones, especialmente aquellas destinadas a entornos corporativos críticos o no, se deben aplicar numerosos controles orientados al diseño y la programación de la

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

aplicación. Estas tareas se pueden optimizar y agilizar mediante la utilización de recursos y funciones de IA en las herramientas de creación del producto de software. A continuación, se detallan los aspectos más relevantes:

- *Verificación de código seguro:* Existen herramientas prediseñadas en el mercado que utilizan IA para validar de manera detallada cada sección del código, comparándolo con códigos potencialmente vulnerables o dañinos. Con esta técnica, se logra reducir la posibilidad de lanzar una versión insegura del producto. Para este caso en particular, existen dos tipos de verificación o análisis: estático y dinámico.

- *Desarrollo mejorado o potenciado:* Con el uso de la IA, se puede gestionar y escribir código fuente con sugerencias para una mejor versión del código o función que se esté creando, indicando incluso el código completo en su versión más segura, basado en el contexto del resto del código de la aplicación. Adicionalmente, se pueden realizar revisiones globales para identificar módulos que puedan presentar fallas que se conviertan en vulnerabilidades de seguridad. Esto permite presentar recomendaciones para un plan de mejora continua del producto en desarrollo o ya desplegado.

- *Pruebas de rendimiento y funcionamiento:* Con el uso de IA se pueden crear una serie de validaciones y modelos de testeo segmentados según los frameworks existentes en el mercado o asociados a normativas legales y contextos locales de calidad. Una vez creados o desplegados, pueden ser utilizados de forma automatizada para repetir constantemente las tareas asociadas.

- *Validación de librerías y dependencias:* Uno de los problemas más comunes es el uso de librerías de terceros o propias con vulnerabilidades no reconocidas. La IA se puede emplear para realizar análisis periódicos sobre estas, identificando vulnerabilidades concretas asociadas a la versión actual y ejecutando la actualización de las mismas

- <u>Gestión y Mantenimiento:</u>

  - *Pruebas de seguridad:* La IA alcanza su máximo potencial en este ámbito, ya que es necesario aplicar pruebas de seguridad tanto para el entorno estático como para la infraestructura de la aplicación, con el fin de garantizar la integridad de su entorno. Esto se logra utilizando métodos de aprendizaje automático avanzados. Posteriormente, se integran pruebas específicas del producto en uso para identificar las áreas de seguridad que requieren tests periódicos, también de manera automática. Según los resultados obtenidos, la IA generativa puede proporcionar al administrador del producto los pasos o controles necesarios para mejorar la postura

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

de seguridad de la solución (por ejemplo, escaneo de puertos, análisis estático, entre otros).

- *Seguridad contra el acceso no autorizado:* En el caso de aplicaciones corporativas críticas, se pueden desarrollar modelos de IA que permitan identificar y categorizar los ataques más comunes (y nuevos) mediante accesos no autorizados a la aplicación, bloqueándolos sin intervención humana. A medida que los ataques aumentan, el modelo se vuelve más maduro, lo que disminuye el tiempo de respuesta ante incidentes (por ejemplo, protección contra phishing).

- *Monitorización avanzada:* Este aspecto es de vital importancia, ya que la IA, al aplicarse, permite identificar patrones poco comunes que están fuera del contexto de la infraestructura de la aplicación. Cuando se produce un ataque, la IA puede generar bloqueos, aplicar medidas de remediación en segundos y proporcionar un informe que incluya las acciones de mitigación implementadas, así como posibles mejoras en el contexto de la organización.

- *Detección avanzada de amenazas:* Cuando una aplicación está en uso, puede recibir y procesar una gran cantidad de información "expresada" en lenguaje natural que, para el software en sí, no representa un peligro. Sin embargo, con modelos de IA, es posible identificar tanto las amenazas relacionadas con ataques directos a los servicios que soportan la aplicación como las amenazas a los datos que forman parte de la información (por ejemplo, DNI, direcciones, información bancaria). Estos datos son clasificados como confidenciales o sensibles dentro de la aplicación.

- **Datos**

La IA ha mejorado y, en muchos casos, ampliado el alcance y la capacidad de análisis para proteger los datos y gestionarlos de forma segura. A continuación, revisamos algunas actividades en las que ha impactado y cómo aplicarlas:

- Ciclo de vida: La IA actual permite participar de forma proactiva en todas las fases del ciclo de vida de los datos (generación y captura, almacenamiento, tratamiento, análisis y visualización) dentro de una organización. Actúa como un guardián, garantizando en tiempo real el cumplimiento de los parámetros y estándares de calidad, identificando las inconformidades y generando la acción técnica específica que debe ejecutarse para remediarlas, todo esto en un corto plazo (minutos). Cabe destacar que en la fase de "Análisis y Visualización", la IA ha potenciado la capacidad de incluir consultas en lenguaje natural, reduciendo así el costo en especialistas de datos.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

- Clasificación de la información y datos: Antes del uso de la IA, uno de los mayores desafíos era la clasificación de los documentos procesados y almacenados en los puestos de trabajo u otros entornos donde es común manejar grandes volúmenes de archivos con datos. Actualmente, la IA puede ejecutar esta tarea en tiempo récord, incluso en el momento en que se copian los archivos o la información dentro de los repositorios, o durante el procesamiento de los datos en las aplicaciones corporativas. Para aplicar la IA a esta actividad, es necesario parametrizar los valores de la herramienta a utilizar, teniendo en cuenta el marco de trabajo, estándares o leyes del país correspondiente. Esto garantiza el cumplimiento de los tiempos de almacenamiento, la gestión de datos sensibles y los perfiles de usuarios no autorizados. Adicionalmente, se puede identificar el nivel de seguridad de la información y emitir alertas de acceso no autorizado de forma automática. La IA permitirá procesar todo tipo de archivos (textos, bases de datos, PDF, imágenes escaneadas, entre otros formatos).

- Prevención de Pérdida de Datos (DLP): En este ámbito, se deben aplicar controles según las normativas vigentes de cada país, así como estándares ISO, mejores prácticas o controles proactivos específicos del sector en el que opera la organización. Los controles soportados por IA permiten alcanzar niveles avanzados de respuesta, como detectar y actuar frente a la modificación no autorizada de un documento debidamente clasificado, entre millones de ellos, o identificar la transferencia de información y datos sensibles independientemente del formato en que se gestionen. Además, durante la transferencia de la información por la red, la IA puede identificar si se trata de datos críticos o sensibles y actuar en consecuencia.

- Gobernanza, Riesgos y Cumplimiento (GRC): Con el uso de la IA, se puede realizar un análisis completo del estado y cumplimiento normativo. Para ello, es necesario diseñar un modelo de cumplimiento normativo (normas, estándares, leyes, mejores prácticas) aplicable a la organización e implementarlo en el entorno de la aplicación. Esto permitirá a la IA gestionar el conocimiento necesario para generar recomendaciones y rutas de solución ante cualquier incumplimiento identificado dentro del contexto normativo típico de la organización o del sector de negocio.

- Gestión dinámica y adaptativa de la seguridad de los datos: Antes de la era de la IA, uno de los mayores inconvenientes era la dificultad para identificar riesgos y aplicar políticas relacionadas sin intervención manual. Con el uso de la IA, es posible identificar previamente una serie de tareas y políticas orientadas a proteger los datos procesados de forma constante dentro de la organización. La IA analiza el contexto y decide qué política o control aplicar, aumentando el flujo de los procesos de seguridad según las necesidades o la

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

interacción del usuario con los datos. Se pueden crear políticas y controles personalizados según los riesgos identificados por la propia IA.

El uso de la IA en la gestión segura y la protección avanzada de los datos ha permitido alcanzar un nivel de automatización y análisis elevado. Esto incluye la capacidad de verificar millones de archivos en poco tiempo y de manera contextual, según los niveles de acceso asignados a los usuarios finales, al tiempo que se aplican normativas y controles de cumplimiento asociados a la clasificación dinámica de los datos.

6. Recomendaciones para Empresas y PYMES

Para enfrentar los riesgos y aprovechar las oportunidades que la inteligencia artificial (IA), en particular la IA generativa, ofrece en el ámbito de la ciberseguridad, las empresas y PYMES deben adoptar una serie de recomendaciones prácticas que pueden integrarse dentro de los Sistemas de **Gestión de la Seguridad de la Información (SGSI) de cada organización o empresa,** en el que se recoge el conjunto de políticas, procedimientos, herramientas, actividades asociadas y controles que se utilizan para proteger la información de una organización.

En este sentido, el Grupo de Trabajo sobre Ciberseguridad de la Comisión de Sociedad Digital de CEOE elaboró en su momento un documento ("Aproximación a la adecuación normativa en materia de ciberseguridad") en el que se realizaba una recopilación, no exhaustiva, de actuaciones a desarrollar para despliegue y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI), siguiendo las directrices que se recogen en la norma ISO 27001, según su última actualización del año 2022. A modo de resumen, y partiendo del imprescindible **compromiso e implicación de la dirección** de la organización, el despliegue y mantenimiento de un SGSI implicaría:

1. Definición del **alcance** (activos, proceso y áreas afectadas)
2. Definición del **contexto** del SGSI: descripción del entorno de operación e identificación de partes interesadas.
3. Desarrollo de una **Política de Seguridad de la información general**: creación de un marco para la definición de los objetivos; reconocimiento del compromiso de atender los requerimientos, reconocimiento del compromiso de mejora continua**, planificación de la comunicación.**
4. Asignación de **funciones y responsabilidades**
5. **Estrategia de comunicación**
6. **Análisis y tratamiento de riesgos**
7. **Definición de objetivos**

Calle Diego de León, 50
28006 Madrid
España
+34 915 663 400
info@ceoe.es
ceoe.es

8. **Soporte**: **dotación de los medios materiales y humanos** necesarios para la correcta y efectiva implementación del SGSI y para su mejora y evolución continua.
9. Planificación de la **evaluación del desempeño del SGSI y actuación** para su continua mejora y actualización.
10. **Documentación**

Particularizando en las medidas relacionadas con la Inteligencia artificial a incorporar en el SGSI, se pueden encontrar, entre otras, las siguientes:

1. **Formación, Capacitación y capacitación continua**:
    - Invertir en la formación continua de los empleados sobre las mejores prácticas de ciberseguridad y las nuevas amenazas emergentes;
    - Proporcionar capacitación específica sobre cómo funciona la IA y cómo puede ser utilizada tanto para proteger como para atacar sistemas.
    - Fomentar una cultura organizacional que valore la ciberseguridad como una responsabilidad compartida
2. **Implementación de Tecnologías:**
    - Adoptar soluciones de IA que permitan la detección y respuesta automatizada a incidentes de seguridad.
    - Implementar firewalls que utilicen IA generativa para adaptarse a nuevas amenazas en tiempo real (asegurando el adecuado funcionamiento del sistema de IA y la correcta configuración previa del firewall.)
    - Desplegar honeypots que evolucionen constantemente para atraer y analizar ataques.
3. **Automatización de la Respuesta a Incidentes**:
    - Utilizar IA generativa para desarrollar y ejecutar respuestas automáticas a incidentes, como el aislamiento de dispositivos comprometidos.
    - Crear scripts adaptativos que la IA pueda ajustar según la naturaleza del incidente.
4. **Optimización de la Gestión de Riesgos**:
    - Generar evaluaciones de riesgo específicas para la organización utilizando IA generativa.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es

- Implementar simulaciones detalladas de posibles incidentes para preparar mejor a la organización frente a amenazas reales.

5. **Evaluación y Mejora Continua**:
    - **Auditorías de seguridad**: Realizar auditorías y evaluaciones periódicas del estado de seguridad de la organización para identificar y corregir vulnerabilidades.
    - **Actualización de tecnologías**: Mantener actualizadas todas las soluciones de seguridad y tecnologías de IA para asegurarse de que se beneficien de las últimas innovaciones y mejoras, siempre comprobando que tras la actualización el funcionamiento sea análogo al esperado.
    - **Adaptación continua de políticas de seguridad**: Emplear IA generativa para revisar y ajustar continuamente las políticas de seguridad en función de los nuevos descubrimientos y la evolución de las amenazas, manteniendo una postura de seguridad robusta y actualizada.

Calle Diego de León, 50
28006 Madrid
España

+34 915 663 400
info@ceoe.es
ceoe.es