

## VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

### IA Y RIESGOS DIGITALES

Gobernar lo inesperado, proteger lo esencial.



# ***Ciberdefensa impulsada por IA: Guías estratégicas reveladas***

*Rómulo Lomparte*

# AGENDA



# Agenda

Introducción

Estrategias de ciberseguridad

Ciberseguridad impulsada por IA

Conclusiones

Bonus: Caso



# INTRODUCCIÓN



# Introducción

*Mantenerse al día con los avances en ciberseguridad es crucial. El panorama de amenazas evoluciona rápidamente.*

*Esta concienciación es esencial para garantizar la eficacia sostenida de las medidas que protegen los datos y los sistemas.*

*Promueve la agilidad al definir procesos adaptables que evolucionan con las amenazas emergentes.*

*Esto permite que las operaciones de seguridad se adapten sin perder estructura ni control.*

*Estos esfuerzos se refuerzan con el uso de inteligencia artificial (IA) para fortalecer las defensas y adaptarse a las ciberamenazas cada vez más sofisticadas.*

*IA mejora la ciberseguridad al permitir la detección de amenazas en tiempo real y optimizar la detección de malware y phishing, así como el análisis del comportamiento del usuario (UBA).*



# Introducción

*El panorama cibernético exige guías de estrategia que unifiquen personas, procesos y tecnologías emergentes como la IA.*

*Aquí se presentan cinco guías, cada una aborda una amenaza importante de ciberseguridad:*

- *Ransomware*
- *Vulnerabilidades en la nube*
- *Phishing*
- *Ingeniería social*
- *Riesgo en la gestión de parches*



# ESTRATEGIAS DE CIBERSEGURIDAD



# Estrategias de ciberseguridad

*Una guía de seguridad es indispensable, especialmente ante las rápidas transformaciones en el ámbito de la seguridad de la información.*

## *Elementos clave de una guía de ciberseguridad:*

<b>Procedimientos predefinidos</b>	<ul style="list-style-type: none"><li>• Predefina y documente los procedimientos para responder a incidentes de seguridad específicos.</li><li>• Defina los pasos necesarios para identificar, contener, erradicar y recuperarse de los incidentes de seguridad.</li></ul>
<b>Clasificación de incidentes</b>	<ul style="list-style-type: none"><li>• Clasifique los sistemas según el tipo de incidente, su gravedad, impacto y naturaleza.</li></ul>
<b>Roles y responsabilidades</b>	<ul style="list-style-type: none"><li>• Identifique las responsabilidades y las expectativas de comunicación y colaboración del equipo de respuesta a incidentes.</li></ul>
<b>Herramientas y tecnologías</b>	<ul style="list-style-type: none"><li>• Incluya información sobre las herramientas y tecnologías que se utilizarán durante la respuesta a incidentes.</li></ul>
<b>Plan de comunicación</b>	<ul style="list-style-type: none"><li>• Proporcione orientación sobre cómo comunicarse internamente dentro de la organización, así como externamente con las partes relevantes, como clientes, socios y organismos reguladores.</li></ul>
<b>Consideraciones de cumplimiento</b>	<ul style="list-style-type: none"><li>• Aborde las consideraciones legales y de cumplimiento relacionadas con los incidentes de ciberseguridad.</li><li>• Esto incluye el cumplimiento de las leyes de protección de datos, los requisitos de notificación y las obligaciones legales.</li></ul>
<b>Análisis posterior al incidente</b>	<ul style="list-style-type: none"><li>• Incluya una sección sobre el análisis y la documentación posteriores al incidente. Esto implica revisar el proceso de respuesta a incidentes, identificar áreas de mejora y actualizar la guía de procedimientos.</li></ul>
<b>Capacitación y concientización</b>	<ul style="list-style-type: none"><li>• Incluir información sobre programas de capacitación y concientización para los empleados a fin de garantizar que conozcan las políticas de ciberseguridad y los procedimientos de respuesta a incidentes de la organización.</li></ul>
<b>Mejora continua</b>	<ul style="list-style-type: none"><li>• Revisar y actualizar periódicamente la guía de procedimientos para reflejar los cambios en el panorama de amenazas, la tecnología y la estructura organizativa.</li></ul>



# Estrategias de ciberseguridad

*El formato de una guía puede variar según el tamaño y naturaleza de la organización.*

*Para una pequeña empresa, una guía podría incluir un organigrama, políticas empresariales y correos electrónicos corporativos.*

*En cambio, las empresas más grandes suelen adoptar un enfoque más detallado mediante la creación de guías para cada departamento.*



# CIBERSEGURIDAD IMPULSADA POR IA



# Ciberseguridad impulsada por IA

*En la evolución de las estrategias de defensa la adopción de la IA, se está consolidando como una fuerza transformadora en la ciberseguridad.*

*La IA permite una protección inteligente y adaptativa contra amenazas complejas.*

*Mejora la detección de amenazas mediante el aprendizaje automático (ML) y análisis del comportamiento. Permite la identificación temprana de anomalías y posibles brechas de seguridad.*

*Los agentes de IA pueden ejecutar acciones del plan de defensa y consultar sensores, acelerando la detección de amenazas y garantizando una respuesta a incidentes automatizada y coherente.*

*Correlacionan alertas y ejecutan medidas de mitigación. Permiten a los analistas centrarse en incidentes de alta prioridad.*



# Ciberseguridad impulsada por IA

*El análisis basado en IA potencia la búsqueda de amenazas. Identifica patrones sutiles y factores de riesgo.*

*La integración de la inteligencia sobre amenazas y reconocimiento avanzado de patrones mejora las defensas contra amenazas internas, fraude y phishing.*

*Estas capacidades mejoran la postura de seguridad general y permiten una estrategia de defensa resiliente.*



# Ciberseguridad impulsada por IA

## **Ransomware**

*La mitigación del ransomware requiere un enfoque estratégico y multicapa que integre tecnología, procesos y personas.*

*Implica copias de seguridad con almacenamiento externo, actualizaciones frecuentes del sistema, parches y protección de endpoints.*

*Además, la segmentación de la red, estrictos controles de acceso y autenticación multifactor (MFA) pueden limitar el movimiento lateral y prevenir acceso no autorizado.*

*También incorporar programas de capacitación de usuarios, seguridad del correo electrónico y concientización sobre phishing que aborden el riesgo humano.*



# Ciberseguridad impulsada por IA

## ***Ransomware (cont.)***

*La IA puede fortalecer las defensas al detectar comportamientos sospechosos, predecir amenazas, automatizar respuestas y optimizar estrategias de copia de seguridad.*

*Las pruebas continuas, supervisión humana e integración de la IA en los planes de respuesta a incidentes mejoran la resiliencia general.*

*Finalmente, la colaboración con las fuerzas del orden y obtención de un seguro cibernético ayudan a mitigar el impacto de los incidentes de ransomware en caso ocurran.*

*La capacidad de agentes IA mejora la defensa contra ransomware.*



# Ciberseguridad impulsada por IA

## Ransomware (cont.)

### Ejemplo de guía contra ransomware:

#### Ataque típico de ransomware

- Infección
- Cifrado
- Rescate
- Demanda
- Pago
- Clave de descifrado

#### Activador crítico de IA

#### Acción del agente de IA

**Incorporación:** Integrar la IA en plataformas de gestión de información y eventos de seguridad (SIEM) y detección y respuesta en endpoints (EDR)

- Extracción autónoma de registros/telemetría de endpoints, redes y la nube.
- Ejecución automatizada de la guía de ataque (aislamiento de host, bloqueo de IP, desactivación de cuentas).

**Aprovechamiento:** Utilizar fuentes de inteligencia sobre amenazas mejoradas con IA.

- Analizar y correlacionar direcciones IP, dominios y hashes maliciosos con los registros.
- Enriquecimiento en tiempo real mediante inteligencia de fuentes abiertas (OSINT), dark web y fuentes comerciales.

**Capacitación:** Entrenar la IA sobre el ransomware y las vulnerabilidades de día cero.

- Aprender patrones de comportamiento (p. ej., cifrado, inyección)
- Pruebas autónomas en entornos aislados de modelos entrenados.

**Integración:** Combinar la IA con analistas humanos(intervención humana)

- Filtrar, enriquecer y resumir alertas para su revisión
- Recomendar estrategias basadas en el contexto y el historial
- Apoyar investigaciones interactivas de anomalías

**Validación:** Probar herramientas de IA periódicamente contra ataques simulados (equipo rojo).

- Simular comportamientos de adversarios para validar las defensas
- Autoevaluar la precisión de detección/respuesta y ajustar automáticamente los modelos



# Ciberseguridad impulsada por IA

## ***Vulnerabilidades en la nube***

*Cada vez, las empresas migran datos y sistemas a la nube, lo que aumenta su vulnerabilidad a las filtraciones de datos.*

*Mitigar estas vulnerabilidades requiere enfoque integral que proteja los datos, aplicaciones e infraestructura.*

*Implica seguir directrices de seguridad del proveedor de la nube e implementar gestión de identidades y accesos (IAM) con privilegios mínimos y autenticación multifactor (MFA).*

*El cifrado de datos, gestión robusta de claves, segmentación de red y firewalls protegen la información en reposo, en tránsito y a través de las redes.*



# Ciberseguridad impulsada por IA

## ***Vulnerabilidades en la nube (cont.)***

*Un enfoque para abordar las vulnerabilidades en la nube debe incluir auditorías, gestión de la configuración y aplicación de parches, monitorización en tiempo real, registro centralizado, respuesta a incidentes y verificación de terceros.*

*IA mejora la defensa de la nube al detectar configuraciones incorrectas, accesos anómalos y exposición de datos confidenciales, y recomendar controles de acceso inteligentes.*

*La combinación de la monitorización basada en IA con la supervisión humana, formación y estrategias de seguridad ayudará a defenderse de las amenazas en la nube.*

*Las guías de ciberseguridad basados en IA abordan las vulnerabilidades en la nube mediante activación de mecanismos de defensa autónomos*



# Ciberseguridad impulsada por IA

## Vulnerabilidades en la nube (cont.)

### Ejemplo de guía contra vulnerabilidades en la nube:

#### Vulnerabilidades típicas en la nube

- Filtraciones de datos
- Problemas de IAM
- Interfaces de programación de aplicaciones (API) inseguras
- Problemas con tecnologías compartidas
- Pérdida de datos
- Registro y monitorización insuficientes
- Riesgos legales y de cumplimiento normativo
- Vulnerabilidades en la cadena de suministro

#### Activador crítico de IA

#### Acción del agente de IA

**Monitorización:** Utilice SIEM basado en IA/ML y herramientas de detección nativas del proveedor de servicios en la nube (CSP)

- Correlacione anomalías en múltiples flujos de datos en tiempo real
- Ejecute automáticamente guías de detección (p. ej., aísle la carga de trabajo, marque actividad sospechosa)

**Control de acceso:** Implemente herramientas IA para políticas de acceso dinámicas basadas en el comportamiento.

- Ajuste dinámicamente las políticas según el comportamiento (p. ej., tráfico imposible, uso inusual de privilegios)
- Consulte el almacén de identidades en busca de anomalías y aplique autenticación adaptativa (multifactor reforzada)
- Desactive o ponga en cuarentena las cuentas de usuario sospechosas

**Seguridad de los datos:** Automatice la clasificación y protección de datos confidenciales con IA.

- Clasifique datos (información de identificación personal - IIP, datos financieros, direcciones IP) mediante escaneo con IA.
- Aplique automáticamente reglas de cifrado o prevención de pérdida de datos (DLP).
- Consulte sistemas de almacenamiento para detectar configuraciones incorrectas y corrija los datos expuestos.

**Respuesta a incidentes:** Implemente herramientas de orquestación, automatización y respuesta de seguridad (SOAR) con IA para planes de acción de la nube.

- Active y ejecute planes de acción SOAR (p. ej., aislamiento de host, bloqueo de IP, restablecimiento de credenciales).
- Consulte sensores forenses y recopile evidencia automáticamente.

**Confianza cero:** Aproveche la IA para la verificación de identidad y puntuación de sesiones.

- Verifique continuamente la identidad y las puntuaciones de confianza de las sesiones.
- Consulte la telemetría de dispositivos, uso y red para detectar señales de riesgo.
- Ajuste automáticamente los derechos de acceso en tiempo real según el nivel de confianza.



# Ciberseguridad impulsada por IA

## ***Ataques de phishing***

*Para mitigar los ataques de phishing, se requiere una combinación de controles técnicos, capacitación de usuarios y prácticas proactivas.*

*Para reducir el riesgo de correos electrónicos phishing, las empresas pueden implementar:*

- *filtrado avanzado de correo electrónico*
- *métodos de autenticación de correo electrónico como:*
  - *DMARC (Autenticación, Informes y Conformidad de Mensajes Basados en Dominio)*
  - *SPF (Marco de Políticas del Remitente)*
  - *DKIM (Correo Identificado por DomainKeys)*
- *filtrado web*
- *autenticación multifactor (MFA).*



# Ciberseguridad impulsada por IA

## ***Ataques de phishing (cont.)***

*Pueden realizar capacitaciones a los usuarios y simulacros para aumentar la concienciación sobre tácticas de phishing y prácticas de navegación seguras.*

*Los planes de respuesta a incidentes, software antiphishing y protección de endpoints permiten una detección y mitigación rápidas.*

*La colaboración, intercambio de inteligencia sobre amenazas y monitorización continua ayudan a identificar amenazas y patrones de phishing emergentes.*

*La IA amplifica los ataques de phishing mediante mensajes personalizados y automatizados.*



# Ciberseguridad impulsada por IA

## ***Ataques de phishing (cont.)***

*También puede reforzar las defensas mediante detección de anomalías, procesamiento del lenguaje natural (PLN) y reconocimiento de imágenes.*

*Estas herramientas con IA, junto con capacitación de los usuarios, autenticación y actualizaciones de seguridad continuas, pueden ayudar a garantizar una protección sólida contra amenazas de phishing.*

*Al combinar automatización, inteligencia sobre amenazas y UBA, las guías de ciberseguridad basadas en IA están transformando la defensa contra el phishing.*



# Ciberseguridad impulsada por IA

## Ataques de phishing (cont.)

### Ejemplo de guía contra ataque phishing:

#### Ataque de phishing típico

- Comunicación engañosa
- Suplantación de entidades de confianza
- Robo de credenciales
- Suplantación de identidad
- Archivos adjuntos maliciosos

#### Activador crítico de IA

#### Acción del agente de IA

#### Plataformas de seguridad con IA:

Implemente herramientas de detección de phishing basadas en IA.

- Consulte las pasarelas de correo electrónico, puntos finales y sensores de bandeja de entrada en la nube.
- Ponga en cuarentena automáticamente los correos electrónicos o enlaces sospechosos.
- Ejecute guías de procedimientos para bloquear dominios, URL y cuentas de remitente maliciosos.
- Enriquezca las alertas con información sobre amenazas para una evaluación más rápida por parte de los analistas.

**UBA:** Supervise las desviaciones en el comportamiento del usuario para detectar cuentas comprometidas.

- Consultar la identidad, puntos finales y telemetría de red para detectar anomalías (tráficos imposibles, uso indebido de privilegios, horarios de inicio de sesión atípicos).
- Aplicar controles adaptativos (autenticación multifactor, finalización de sesión, bloqueo temporal de cuentas).
- Ejecutar guías de procedimientos para notificar a los analistas y generar incidentes con puntuación de riesgo.
- Correlacionar las desviaciones con otras señales de ataque (p. ej., movimiento lateral).

**Simulaciones de capacitación:** IA para simular phishing para concientización.

- Lanzar automáticamente campañas de phishing simuladas a través de correo electrónico, chat y herramientas de colaboración en la nube.
- Consultar las respuestas de empleados y medir tasas de clics/aperturas.
- Generar automáticamente asignaciones de capacitación de usuarios basadas en el riesgo.
- Proporcionar a los analistas paneles que muestren las tendencias de susceptibilidad y el progreso a lo largo del tiempo.



# Ciberseguridad impulsada por IA

## ***Ingeniería social***

*La ingeniería social explota la psicología humana, confianza, urgencia o miedo.*

*Mediante capacitación en concientización, simulacros y cultura de denuncia, los empleados estarán preparados para reconocer y responder a las tácticas manipuladoras.*

*La autenticación multifactor (MFA), prácticas seguras de contraseñas y controles de acceso reducen el acceso no autorizado*

*El filtrado de correo electrónico, cifrado y canales de comunicación seguros refuerzan las defensas contra mensajes fraudulentos.*

*Los planes de respuesta a incidentes, auditorías, pruebas de penetración y evaluaciones de seguridad de dispositivos móviles y de terceros mejoran la resiliencia organizacional.*



# Ciberseguridad impulsada por IA

## ***Ingeniería social (cont.)***

*Los ciberdelincuentes están desarrollando ataques de ingeniería social cada vez más sofisticados mediante mensajes realistas, deepfakes y minería de datos.*

*Las herramientas de IA defensiva, capacitación, principios de confianza cero y comportamiento cauteloso en línea ayudan a mitigar este riesgo.*

*Defenderse de la ingeniería social requiere medidas de seguridad técnicas, capacitación de usuarios y respuesta proactiva, reforzada por guías de ciberseguridad basados en IA.*



# Ciberseguridad impulsada por IA

## Ingeniería social (cont.)

### Ejemplo de guía contra ingeniería social:

#### Tácticas típicas de ingeniería social

- Phishing
- Suplantación de identidad
- Pruebas previas
- Señuelo
- Intercambio de favores
- Acceso no autorizado a sistemas (tailgating / piggybacking)
- Búsqueda de información en contenedores de basura
- Ingeniería social inversa
- Ataques de suplantación de identidad basados en personas

#### Activador crítico de IA

#### Acción del agente de IA

#### Plataformas de seguridad con IA:

Utilice herramientas de IA que detecten patrones de engaño

- Consulte los sensores de red, terminales y correo electrónico en busca de indicios de engaño (p. ej., portales de inicio de sesión falsos, dominios falsificados).
- Ejecute guías de procedimientos para aislar sesiones sospechosas o bloquear recursos fraudulentos.
- Enriquezca automáticamente los hallazgos con información sobre engaño (p. ej., tácticas, técnicas y procedimientos [TTP] del atacante).
- Genere alertas priorizadas según la probabilidad de engaño.

**Capacite a empleados con ataques simulados por IA:** Exponga al personal a simulaciones de ingeniería social generadas por IA.

- Lanzamiento autónomo de simulaciones de phishing, smishing y vishing generadas por IA.
- Consulta de la interacción de los empleados (clics, aperturas, envío de credenciales) en tiempo real.
- Asignación automática de módulos de capacitación personalizados a usuarios de alto riesgo.
- Proporcionar a los analistas paneles con las tasas de éxito/fracaso de las simulaciones.

**Supervisión de comunicaciones de ejecutivos:** Uso de IA conductual para detectar intentos de suplantación de identidad.

- Consulta canales de comunicación por correo electrónico, chat y voz de ejecutivos en busca de anomalías (estilo, tono, discrepancias en los metadatos).
- Ejecución de guías de procedimientos para marcar o bloquear intentos sospechosos de suplantación de identidad antes de su entrega.
- Notificación automática a los equipos de seguridad sobre intentos de suplantación de identidad de ejecutivos con alta probabilidad de éxito.
- Correlación con inteligencia de amenazas externas (p. ej., dominios de atacantes conocidos, campañas de suplantación de identidad).

**Arquitectura de confianza cero:** Combinación de la verificación de identidad con la evaluación continua de riesgos.

- Consultar continuamente la telemetría de identidad, dispositivo y red para la puntuación de confianza.
- Ejecutar planes de acceso adaptativo (p. ej., autenticación multifactor reforzada, reautenticación, reducción de acceso) en tiempo real.
- Ajustar automáticamente las políticas en función del riesgo de la sesión (p. ej., accesos imposibles, intentos de escalada de privilegios).
- Proporcionar a los analistas paneles de control de riesgo a nivel de sesión para la supervisión.



# Ciberseguridad impulsada por IA

## ***Gestión de parches***

*Mitigar el riesgo relacionado con la gestión de parches requiere actualizar periódicamente el software, sistemas operativos y aplicaciones.*

*Las empresas pueden implementar herramientas automatizadas que identifiquen aplicaciones obsoletas y parches faltantes, lo que agiliza la remediación y aumenta la eficiencia.*

*Otros enfoques incluyen política de gestión de parches, inventario de activos y evaluación de vulnerabilidades que guíen la priorización e impacto en el negocio y probar parches en entornos controlados.*



# Ciberseguridad impulsada por IA

## **Gestión de parches (cont.)**

*La IA mejora la gestión de parches al automatizar la detección, priorización, programación y evaluación de riesgos, e integrar la inteligencia sobre amenazas para decisiones acertadas.*

*Sin embargo, una gestión de parches exitosa basada en IA aún depende de datos de calidad, supervisión humana y alineación con las políticas organizacionales.*

*Las guías de ciberseguridad impulsados por IA están redefiniendo la gestión de parches al combinar automatización, inteligencia y toma de decisiones con conciencia del riesgo.*

*Los agentes de IA integrados en las plataformas de gestión de parches pueden consultar continuamente los sensores del sistema y aplicaciones para detectar vulnerabilidades sin parchar y programar e implementar parches.*



# Ciberseguridad impulsada por IA

## ***Gestión de parches (cont.)***

*Al procesar información de inteligencia sobre amenazas, los agentes pueden correlacionar exploits, vulnerabilidades y exposiciones comunes (CVE) y campañas de malware con los inventarios de activos locales, lo que garantiza que los sistemas de mayor riesgo tengan prioridad para su corrección inmediata.*



# Ciberseguridad impulsada por IA

## Gestión de parches (cont.)

### Ejemplo de guía de gestión de parches:

#### Riesgos típicos de la gestión de parches

- Complejidad de los entornos de TI
- Gran cantidad de puntos finales
- Coordinación con proveedores
- Problemas de pruebas y compatibilidad
- Tiempos de inactividad no planificados
- Recursos limitados
- Resistencia de los usuarios
- Cumplimiento normativo
- Dificultades del teletrabajo
- Vulnerabilidades de día cero

#### Activador crítico de IA

#### Acción del agente de IA

**Incorporar:** Integrar la IA en las plataformas de gestión de parches existentes..

- Consultar sensores de sistemas y aplicaciones para detectar vulnerabilidades sin parchear
- Ejecutar guías para programar e implementar parches en puntos finales, servidores y cargas de trabajo en la nube
- Priorizar automáticamente los sistemas según la exposición, la criticidad o los requisitos de cumplimiento
- Validar la correcta aplicación de parches mediante comprobaciones posteriores a la implementación

**Aprovechar:** Combinar la IA con fuentes de inteligencia sobre amenazas para centrarse en las amenazas activas.

- Ingesta continua de datos sobre exploits activos, CVE y campañas de malware.
- Correlaciona las amenazas con los registros del entorno local y los inventarios de activos.
- Ejecuta guías para escalar y parchear los activos con mayor riesgo de sufrir exploits en producción.
- Bloquea automáticamente las IP/dominios maliciosos vinculados a vulnerabilidades sin parchear hasta que se apliquen los parches.

**Aumentar:** Utiliza IA para simular los efectos de los parches en entornos de pruebas (sandbox) antes de su implementación.

- Consulta la telemetría de los entornos de pruebas para probar los parches con cargas de trabajo representativas.
- Ejecuta guías para detectar automáticamente fallos de la aplicación, degradación del rendimiento o problemas de compatibilidad.
- Genera automáticamente puntuaciones de riesgo para cada parche en función del comportamiento observado.
- Comparte los informes con los analistas antes de la implementación en producción.

**Habilitar** Automatiza cuando sea seguro, pero mantén la supervisión humana para los sistemas de alto riesgo.

- Aplicar parches de forma autónoma a sistemas de bajo riesgo y bajo impacto.
- Marcar los sistemas críticos/de alto riesgo para su revisión humana antes de la ejecución.
- Ejecutar manuales de procedimientos para preparar planes de reversión en caso de fallo de los parches.
- Proporcionar a los analistas un panel de control que destaque la cobertura de la automatización frente a las aprobaciones pendientes.



**CONCLUSIONES**



# Conclusiones

*En el dinámico y complejo panorama, la defensa contra las ciberamenazas requiere estrategia que integre prácticas seguras en nube, gestión sólida de parches y formación de usuarios.*

*Políticas claras y guías de ciberseguridad bien definidos refuerzan la preparación de las organizaciones.*

*Los agentes de IA pueden ejecutar de forma autónoma acciones de las guías para acelerar la detección de amenazas y optimizar la respuesta a incidentes.*

*Mejoran la visibilidad y conocimiento al monitorizar el panorama de las ciberamenazas, incluyendo ransomware, vulnerabilidades en la nube, phishing, ingeniería social y entornos de parcheo.*

*Al automatizar estas tareas rutinarias y correlacionar la información en tiempo real, la IA permite a los equipos de seguridad centrarse en las amenazas de alta prioridad y su mitigación.*



# Conclusiones

*Sin embargo, esto es un arma de doble filo: los ciberdelincuentes también utilizan la tecnología para escalar, personalizar y enmascarar sus ataques.*

*La IA ya no es una simple mejora tecnológica. Es un imperativo estratégico para la ciberseguridad moderna.*

*Al integrar la IA en los marcos de defensa centrales, las organizaciones pueden anticiparse a las amenazas y construir una infraestructura digital más robusta.*



**BONUS: CASO**



# Bonus: Caso

**Imaginen que mañana, un gerente financiero recibe una videollamada de su CEO.**

- La voz es perfecta.
- El rostro es perfecto.
- El lenguaje corporal coincide.
- El supuesto CEO ordena transferir US\$ 250,000 para una adquisición urgente y confidencial.

Todo parecía legítimo... excepto por un detalle: **el CEO real estaba durmiendo en otro país.**

- El ataque fue realizado usando:
  - IA generativa de voz
  - Deepfake facial en tiempo real
  - Información obtenida de LinkedIn, entrevistas y redes sociales
- La transferencia ocurrió en menos de 15 minutos
- El bypass no fue técnico... fue psicológico

***La próxima gran vulnerabilidad no será el firewall. Será la confianza humana aumentada por IA.***



***¡Muchas gracias!***

*Rómulo Lomparte*  
*romulo.Lomparte@yahoo.com*

