Módulo 3. Ciberdelitos con IA

CÓRDOBA CREA FUTURO

La humanidad nunca ha dejado de evolucionar. Tras avanzar a lo largo de varios procesos históricos, actualmente nos encontramos inmersos en una etapa predominantemente tecnológica. Cabe resaltar que la aparición de Internet ha supuesto todo un hito, y ha marcado un antes y un después en nuestras vidas. Nos encontramos ante un nuevo medio de relacionarnos, de crear interconexiones entre las personas. Curiosamente, este fenómeno ha llegado a acaparar la esfera de lo social, económico, industrial, cultural y hasta lo puramente académico.

A raíz de la expansión y globalización de esta herramienta, han surgido canales de conexión que nos brindan información sobre usuarios de cualquier parte del mundo, y se utilizan motores de búsqueda que hacen simple la obtención de cierta información. Ha sido tan grande el impacto de Internet y las nuevas tecnologías que ambos conforman una de las bases de datos más grandes a nivel mundial. Esta herramienta, además de ayudar al crecimiento de las relaciones personales, ha hecho efectivo el flujo mercantil a nivel global.

Sin embargo, cabe aclarar que, desafortunadamente, muchas personas utilizan estas herramientas para facilitar datos a delincuentes o como medio para hacer efectivo algún daño a la información privada de las personas, a través de estafas, violación de la privacidad, robos, etc. Estas son acciones maliciosas, perseguidas en mayor o menor medida por todos los gobiernos, y pueden ser llevadas a cabo no solo por una persona individual, sino también grupos organizados encargados de cometer estos delitos.

La Real Academia define al ciberdelito como “delito que se comete a través de Internet” (Real Academia Española, s. f.).

En nuestro país, el sitio web Argentina.gob.ar define el ciberdelito del siguiente modo:

> “Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.
> Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como *cyberbulling*, *grooming*, *phishing* cometidos por ciberdelincuentes que actúan en grupos o trabajan solos” (Argentina.gob.ar, 2025).

Los delincuentes están aprovechando la IA en ciberseguridad para lanzar ataques más inteligentes, rápidos y dañinos que nunca. Desde correos electrónicos de *phishing* que parecen personales hasta *malware* que evade la detección, la IA está transformando el cibercrimen. Comprender cómo la IA empodera a los atacantes es el primer paso para contraatacar.

En Argentina, no existe un fuero digital tal como el Fuero Penal, Civil y Comercial, entre otros. En ocasiones, se traslada a la ley positiva del derecho al ciberespacio, que tiene sus propias normas. Es por ello que, para poder enfrentar el ciberdelito, es necesario que se entienda el contexto particular que tiene.

También es necesario aclarar que un informático, sin importar el nivel académico que tenga, goza de habilidades propias que son distintas a las que requiere la ciberseguridad. En un aprendizaje, seguramente al informático le resultará más fácil aprender sobre el ciberespacio. Es por ello que el alumno encontrará distintas ofertas académicas, tanto de nuevas carreras de grado como de posgrado, que contemplen estos nuevos espacios que superan lo digital para convertirse en algo más grande: el quinto dominio, es decir, el ciberespacio.

1. Ciberespacio

El ciberespacio es un espacio virtual global e interconectado, que abarca la infraestructura física (*hardware*, redes) y los componentes inmateriales (*software*, datos, servicios de Internet como la web y el correo electrónico), donde interactúan personas y sistemas, lo que crea un ámbito para la comunicación y la actividad socioeconómica más allá de la realidad física. Aunque a menudo se confunde con Internet, el ciberespacio es un concepto más amplio que engloba todas las redes y entornos digitales.

Componentes

- **Infraestructura**: servidores, cables, *routers*, *smartphones*, computadoras, redes inalámbricas.
- ***Software* y servicios**: sistemas operativos, aplicaciones, correo electrónico, páginas web, API.
- **Actores humanos**: usuarios que navegan, se comunican y realizan actividades.

Características

- **Virtual y relacional**: no existe físicamente, sino a través del intercambio de información y la interacción.
- **Expansivo**: crece constantemente con las nuevas tecnologías y usos.
- **Bifurcado**: tiene una base física (*hardware*) y una dimensión virtual (datos, servicios).

Origen del término

Fue acuñado por el escritor de ciencia ficción William Gibson en su novela *Neuromante* (1984), donde lo describía como una “alucinación consensual”.

En resumen, es la dimensión digital donde la información fluye y las interacciones humanas se dan a través de la tecnología, desde las redes más simples hasta la vasta red de Internet.

Son varios los factores que nos permiten estar conectados a Internet en todo momento, y esto se puede apreciar claramente por el uso de las redes sociales, correo electrónico, mensajería instantánea, entretenimiento, etc., lo que crea una convivencia compartida entre la vida real y el ciberespacio.

Para el autor, la legislación actual que regula el mundo físico no debería interpretarse de manera ni trasladarse sin mediaciones a las leyes del derecho positivo para ser aplicadas al ciberespacio, que es de naturaleza virtual. Si bien debemos ser conscientes de que hay una estrecha convivencia entre ambos, debe mantenerse la misma separación que hay entre el espacio exterior, con sus constelaciones y planetas, y nuestro mundo. Ya se probó, con varias pericias informáticas, que, si no se considera la perspectiva sugerida desde el punto de vista penal, un culpable puede convertirse en inocente o un inocente ser considerado culpable judicialmente.

Ciberdelito o cibercrimen

Los términos “ciberdelito” o “cibercrimen” son usados indistintamente. Por lo general, en el habla inglesa se usa la palabra *cybercrime* (cibercrimen), mientras que en nuestro país usamos la palabra “ciberdelito” para hacer referencia al mismo fenómeno.

El término “ciberdelito” es una conducta antijurídica realizada en un entorno digital, lo que a su vez implica que cualquier persona, empresa o ente, puede convertirse en víctima.

Una de las primeras formas de cometer cibercrímenes apareció mucho antes de la creación de las computadoras: se trataba de acciones ejecutadas por personas a través del *hackeo* de teléfonos.

Con la aparición masiva de computadoras y la creación de Internet, se han producidos varios ataques a lo largo de la historia. En los años 80, llegó la primera gran ola de delitos a raíz de la creación del correo electrónico. En los 90, con el crecimiento de los buscadores web, comenzaron los envíos de virus. Fue en el 2000 cuando comenzó a cobrar relevancia el delito cibernético, debido principalmente al posicionamiento de las redes sociales como tendencia masiva. Esto implicaba que el acceso a los datos comenzara a ser mucho más sencillo.

Hoy en día, los protagonistas son grupos organizados destinados a robar activos de personas individuales, empresas, bancos, etc.

A raíz del crimen organizado y con el crecimiento masivo de usuarios en redes sociales, comenzaron a tener lugar nuevos comportamientos que no pueden dejar de enmarcarse dentro del ordenamiento jurídico, lo que ha brindado un enfoque normativo. Es así que se establecen pautas y leyes internacionales destinadas a prevenir y castigar estos delitos.

Delitos de los que se puede ser víctima

Los ciberdelitos se cometen a través de dispositivos que tienen acceso a plataformas virtuales, como computadoras, teléfonos móviles, etc. Esto hace que seamos un blanco fácil de estos crímenes. En un principio, los ciberdelincuentes buscaban víctimas al azar; luego, mediante ingeniería social, empezaron a localizar e identificar a las víctimas; en la actualidad, da la impresión de que cuentan con distintos medios para obtener información precisa de las víctimas. También es importante saber que los ciberdelincuentes dejan una trazabilidad increíble, que se dilata rápidamente.

A continuación, presentamos algunas de las conductas reconocidas internacionalmente como crímenes informáticos.

- ***Hacking:*** acceso no autorizado a un sistema informático o equipo.
- ***Cracking***: modificación de *software* que tiene como finalidad eliminar los componentes de seguridad. La mayoría de estos casos se

adjudican a la distribución de copias duplicadas.

- ***Phishing***: técnica de engaño. El criminal simulará ser una persona o empresa, a través de una comunicación telefónica, mensajería instantánea, *e-mail* o redes sociales, e intentará así acceder a la información para cometer el delito.

- **Robo de identidad**: apropiación de la identidad de una persona, ya sea en público o en privado. Este delito lo sufren tanto personas físicas como jurídicas.

- **Ciberterrorismo**: acción de robar información a través de algún medio informático con la finalidad de cometer actos terroristas.

- ***Sniffer***: *apps* especiales que permiten captar datos que viajan en alguna red. Se les conoce como "rastreadores", y su función es meterse en el disco duro de los ordenadores conectados a una determinada red para extraer la información.

- **Propagación de *malware***: documentos, programas y mensajes maliciosos que pueden causar daños al equipo del usuario destinatario.

Herramientas utilizadas para robar datos

Existe un abanico de formas agravantes de cometer estos actos.

Las personas que hacen el daño suelen ser llamadas *hackers*. Son quienes llevan a cabo la acción de sustraer datos, activos o cualquier tipo de información que se utilizará para perjudicar al usuario víctima. Existen varios métodos para poder robar nuestros datos:

programas, portales de Internet, publicidades maliciosas o ciertas *apps* destinadas al crimen informático.

Hay herramientas que, dependiendo de quién y cómo las use, pueden ser de ayuda para convertirse en una potencial ciberarma. Algunas son:

- Nmap
- Wireshark
- Tor
- Red privada virtual (VPN)

A partir de estas herramientas, se accede a los datos de una persona física o jurídica a la que se desea perjudicar. Estas opciones de *hacking* tienen diferentes formas de actuar: algunas rompen el sistema de seguridad, otras se dedican a obtener contraseñas, ya sean sencillas o complicadas, pero todas tienen una misma finalidad: obtener datos para manipularlos.

Protección contra el cibercrimen

Como toda acción, tiene su contrapartida. No podemos pasar por alto que existen métodos para poder resguardarse de este tipo de crímenes. Solo hay que tener en cuenta ciertos detalles a la hora de salvaguardar la identidad.

Algunas de las opciones que permiten tener una mejor seguridad son las siguientes:

- VPN
- Nmap
- Activación del múltiple factor de autentificación

Como puede observarse, existen numerosas herramientas que pueden emplearse tanto con fines lícitos como ilícitos. Por ello, resulta fundamental contar con una formación sólida y ética en materia de ciberseguridad, ya que el uso indebido de estas herramientas no solo carece de fundamento ético, sino que también genera perjuicios.

¿Cuáles son los ciberdelitos y contravenciones más comunes?

Uno de los conceptos más importantes vertidos en el sitio web de Argentina.gob.ar (2025) es que los ciberdelitos se cometen “a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño”.

Algunos ejemplos que propone el sitio son:

“Ataques en tu navegación: desvían tu navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar tu sistema operativo, infectar tu teléfono y tu computadora, activar tu *webcam*, extraer datos, etc.

Ataques a servidores: pueden dañar o robar tus datos y negarte el acceso a tu información.

Corrupción de bases de datos: interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.

Virus informáticos: encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía.

Programa espía: alguno de los dispositivos tiene instalado un *software* que le permite encender y grabar con la cámara y el micrófono. También puede acceder a tu información personal sin autorización y sin que lo sepas" (Argentina.gob.ar, 2025).

Los ciberdelitos recurren a técnicas de ingeniería social para manipular a las personas mediante engaños o amenazas, con el objetivo de obtener datos personales o información perteneciente a terceros u organizaciones, apropiarse de recursos económicos, suplantar identidades o ejercer acoso en entornos digitales, incluido el de carácter sexual.

Algunos de los ejemplos que define el sitio web Argentina.gob.ar (2025) son:

"Phishing o vishing: —

los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar, y te piden los datos que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.

Ciberbullying: —

es el acoso por mensajería instantánea, *stalking* en WhatsApp, Telegram, Facebook Messenger y en las redes sociales con la intención de perseguir, acechar, difamar y atentar contra el honor e

integridad moral de una persona. Esto lo hacen a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, de la creación de memes o el etiquetado de tus publicaciones.

Grooming: —

se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores para posteriores chantajes o previo al abuso sexual.

Sextorsión: —

consiste en pedir dinero a cambio de no difundir en las redes imágenes generadas para un intercambio erótico consentido.

Ciberodio: —

son contenidos inapropiados que pueden vulnerar a las personas. Se considera ciberodio la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o el maltrato animal.

Pornografía infantil: —

se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita" (Argentina.gob.ar, 2025).

Se pueden consultar los delitos informáticos de Argentina en el sitio web de Argentina.gob.ar (https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos). Estos están tipificados en el Código Penal y son los siguiente:

Delitos informáticos contra la integridad sexual

"El Código Penal sanciona las siguientes conductas:

- producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir cualquier representación de una persona menor de 18 años dedicada a actividades sexuales explícitas o de sus partes genitales;

- tener representaciones de personas menores de edad de actividades sexuales explícitas o de sus partes genitales para distribuirlas o comercializarlas.

También sanciona el ciberacoso a personas menores de edad (*grooming*). Este delito consiste en tomar contacto con una persona menor de edad a través de medios de comunicación electrónica (redes, *mail*, chat, etc.) para cometer alguno de los delitos contra su integridad sexual" (Argentina. gob.ar, 2025).

Delitos informáticos contra la libertad

El Código Penal sanciona las siguientes conductas:

"Acceder, apoderarse, suprimir o desviar una comunicación electrónica que no le esté dirigida. La pena es mayor si el contenido de la comunicación electrónica se publica.

Acceder ilegítimamente a un sistema o dato informático de acceso restringido. La pena se agrava cuando el acceso es en perjuicio de un sistema o dato informático

de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Publicar indebidamente una comunicación electrónica no destinada a la publicidad cuando esto cause perjuicio a otros. No tiene responsabilidad penal el que actúa para proteger un interés público.

Revelar documentos informáticos oficiales que por ley deben ser secretos.

Acceder de manera ilegítima a bancos de datos personales, revelando información o insertando datos en un archivo de datos personales. Si el autor es funcionario público, sufre además pena de inhabilitación" (Argentina.gob.ar, 2025).

¿Qué es un documento para el Código Penal?

"Es la representación de actos o hechos sin importar el soporte utilizado para almacenarlo o transmitirlo. Pueden ser figuras o imágenes que se ven como dibujos, pinturas, fotografías,

retratos, películas cinematográficas, etc. Estas representaciones pueden estar en un soporte físico o en uno informático" (Argentina.gob.ar, 2025).

Delitos informáticos contra la propiedad

El Código Penal sanciona las siguientes conductas:

- "la estafa mediante el uso de tarjeta magnética o de los datos de la tarjeta;
- la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos;
- el daño informático, que consiste en alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; vender, distribuir, hacer circular o introducir en un sistema informático cualquier programa destinado a causar daños.

  La pena es mayor en caso de dañar datos, documentos, programas o sistemas informáticos públicos; causar daño en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público" (Argentina.gob.ar, 2025).

Delitos informáticos contra la seguridad pública que atentan contra los medios de comunicación

El Código Penal dice que estos son:

- “entorpecer las comunicaciones electrónicas;
- resistir violentamente el restablecimiento de una comunicación electrónica interrumpida” (Argentina.gob.ar, 2025).

Delitos informáticos contra la Administración pública

El Código Penal sanciona las siguientes conductas:

- “sustraer, alterar, ocultar, destruir o inutilizar registros o documentos electrónicos confiados a la custodia de un funcionario público o de otra persona en interés del servicio público".

Texto completo de la norma

Puedes acceder al texto completo de la norma entrando al siguiente enlace: https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/actualizacion#17

Normas complementarias

Ley 25.930: https://www.argentina.gob.ar/normativa/nacional/ley-25930-98807

Ley 26.904: https://www.argentina.gob.ar/normativa/nacional/ley-26904-223586

La Ley Olimpia en Argentina

La Ley Olimpia en Argentina (Ley 27.736), sancionada en octubre de 2023, es una legislación que reconoce y penaliza la violencia digital y la difusión no consentida de contenido íntimo, y la incorpora a la Ley 26.485 como una modalidad de violencia de género, para proteger la dignidad, reputación e identidad de las personas en entornos digitales. Obliga a las

plataformas a eliminar contenidos violentos y fortalece el acceso a la justicia para víctimas de ciberacoso y *doxing*[1].

[1] Ley 27.736. Ley Olimpia. Octubre de 2023.

CONTINUAR

2. Uso de la inteligencia artificial en ciberdelitos

Los ciberdelincuentes utilizan la IA para hacer sus ataques más sofisticados y difíciles de detectar. Algunas de las formas de amenazas más frecuentes son las siguientes:

- *Phishing* personalizado. La IA analiza datos de redes sociales para crear correos electrónicos de *phishing* muy convincentes, dirigidos a individuos específicos.
- *Deepfakes* y suplantación de identidad. Los *deepfakes* son vídeos, imágenes o archivos de voz manipulados con *software* de IA para parecer reales y auténticos. Los ciberdelincuentes pueden usarlos para extorsionar, cometer fraude o manipular a las víctimas para que realicen acciones perjudiciales.
- *Malware* inteligente. El *malware* impulsado por IA puede adaptarse y evitar ser detectado por los sistemas de seguridad tradicionales.
- Exploración de vulnerabilidades. La IA puede detectar rápidamente fallos en el *software* y las redes, que los atacantes pueden explotar antes de que se solucionen.

La IA como herramienta de ciberdelito

Esta tecnología abre nuevas oportunidades para diseñar, fabricar y compartir contenido extremadamente perturbador. La inteligencia artificial se consolidó como una herramienta de doble filo; mientras los ciberdelincuentes la emplean para crear fraudes digitales cada vez más complejos, empresas y gobiernos la utilizan como instrumento de defensa para activos y usuarios. Desde la mirada de los *hackers*, no existen fronteras. Posiblemente, se registren más *hackeos* en un país que en otro, no por la falta de tecnología para evitarlos, sino por otros factores estructurales. En Argentina, se observa una combinación de ciberdelito internacional, vinculado a la figura del *hacker*, y de ciberestafas locales asociadas a transacciones fraudulentas de gran magnitud. Entonces: si tenemos la tecnología para contrarrestarla, el recurso humano adecuado, las entidades provinciales y nacionales que nos protegen, y sin embargo el ciberdelito continúa en aumento (tanto el cotidiano como el internacional), con robo de la identidad, bases de datos de salud, etc., hay algo que no encaja.

La democratización de la inteligencia artificial abre un escenario en el que la creatividad delictiva encuentra nuevas oportunidades para desarrollarse, incluso en contextos que aparentan estar plenamente controlados. En este marco, surge un interrogante inevitable: si se sostiene la idea de que se dispone de los mejores recursos tecnológicos, ¿por qué los ciberdelincuentes continúan superando los mecanismos de control existentes?

Por ello, resulta necesario promover una creatividad orientada al desarrollo sostenible y a largo plazo, dado que los actores delictivos demuestran una capacidad constante para innovar y vulnerar los estándares actualmente vigentes.

Las imágenes generadas por IA son de gran calidad realista y han permitido la proliferación de *deepfake* a gran escala, principalmente contra referentes mundiales, como fue el caso del papa Francisco con campera de lujo.

Hay imágenes extraídas de redes sociales que son adulteradas y, según la edad, pueden tener una situación penal distinta para el acusado. Por ejemplo, si las imágenes adulteradas son de menores de edad, tendrían una calificación que va por un camino de protección a los menores; pero si las imágenes son de un adulto y hay comercialización, podría ir por el camino de promoción de la prostitución, si no se comercializa, es discutible, porque no hay figura específica (Álvarez, 2023), es posible que se pueda encuadrar en daños y perjuicios e invocando el derecho a la imagen, que es contemplado en el art. 53 del código civil. Sí es importante tener en claro que hay una gran falencia sobre normas y leyes que regulen sobre estas tecnologías que dinámicamente cambian y progresan.

Casos de este tipo abundan. A principios de julio, 15 estudiantes de la Facultad de Urbanismo de la Universidad de San Juan denunciaron que alguien estaba vendiendo fotos de ellas desnudas, solo que ellas jamás se habían sacado esas fotografías. Las publicaciones venían de un mismo perfil, y se aseguraba que con un *bot* de Telegram podía tomar las imágenes de chicas en las redes sociales y "desnudarlas" a través de inteligencia artificial. Ante la denuncia, la Justicia logró dar con la cuenta de correo electrónico asociada al perfil que hacía esas publicaciones bajo el alias "MarioMJohn68" y de allí sacar los datos para dar con la identidad del responsable: era un compañero de la facultad.

La herramienta que utilizó el detenido es una nueva forma de *deepfake*, que usa algoritmos de *deep learning* para analizar una imagen de una persona y generar una nueva imagen en la que la persona parece estar desnuda.

Un caso emblemático puede observarse en la red social X, que permitió la circulación de contenidos destinados a "desnudar" digitalmente a las personas, incluidos niños, lo cual en nuestro país constituye un delito. Frente a este escenario, surge el interrogante acerca de cuál es la respuesta jurídica adecuada. Sin embargo, y de manera preocupante, pese a la existencia de condenas vinculadas a la tenencia de pornografía infantil, en la práctica la respuesta resulta insuficiente o directamente inexistente.

Comprender la inteligencia artificial para la ciberseguridad

La inteligencia artificial para la ciberseguridad hace referencia al uso de tecnologías y técnicas de IA para mejorar la protección de los sistemas informáticos, las redes y los datos frente a ciberamenazas. La IA ayuda automatizando la detección de amenazas, analizando

grandes volúmenes de datos, identificando patrones y respondiendo a incidentes de seguridad en tiempo real.

Entre las aplicaciones clave de inteligencia artificial para la seguridad, se incluyen la detección de anomalías, *malware* e intrusiones, la prevención de fraudes, los resúmenes de incidentes, los informes para las partes interesadas, y la creación y utilización de técnicas de ingeniería inversa en los *scripts*. Al usar el aprendizaje automático, el aprendizaje profundo y el procesamiento del lenguaje natural, la inteligencia artificial aprende continuamente de los nuevos datos, y mejora su capacidad para identificar y mitigar las amenazas emergentes, reducir los falsos positivos y escalar los esfuerzos de seguridad de forma más eficaz. Los avances recientes en IA generativa han capacitado a los equipos con conclusiones controladas por datos, informes fáciles de producir y recomendaciones de mitigación paso a paso.

Usos de la IA en la ciberseguridad

Algunas consideraciones del uso de la IA en la ciberseguridad aplican en lo siguiente:

“Administración de identidad y acceso —

La inteligencia artificial se usa para la administración de identidad y acceso (IAM) con el fin de comprender los patrones en los comportamientos de inicio de sesión de los usuarios y mostrar comportamientos anómalos. También se puede usar para forzar automáticamente la autenticación en dos fases o un restablecimiento de contraseña cuando se cumplen determinadas condiciones. Y, si es necesario, las soluciones con tecnología de IA pueden impedir que un usuario inicie sesión si hay alguna razón para pensar que una cuenta se ha puesto en peligro.

Seguridad y administración de puntos de conexión —

Al reducir el trabajo manual, la inteligencia artificial ha ayudado a acelerar muchos procesos relacionados con la seguridad de los datos. Usando la inteligencia artificial, los equipos de seguridad pueden identificar y etiquetar rápidamente datos confidenciales en todo el entorno, ya sea que estén alojados en la infraestructura de la organización o en una aplicación en la nube. La inteligencia artificial también puede ayudar a detectar cuándo alguien está intentando mover datos fuera de la empresa y bloquear la acción o plantear el problema al equipo de seguridad.

Seguridad en la nube

Dado que las organizaciones usan varios proveedores de nube para la infraestructura y las aplicaciones, necesitan soluciones que proporcionen protección en todo el patrimonio. La inteligencia artificial une los datos de varios servicios en la nube para proporcionar una vista completa de los riesgos y vulnerabilidades en la nube de una organización. Esto ayuda a los profesionales de seguridad a abordar rápidamente las amenazas.

Seguridad de datos

Al reducir el trabajo manual, la inteligencia artificial ha ayudado a acelerar muchos procesos relacionados con la seguridad de los datos. Usando la inteligencia artificial, los equipos de seguridad pueden identificar y etiquetar rápidamente datos confidenciales en todo el entorno, ya sea que estén alojados en la infraestructura de la organización o en una aplicación en la nube. La inteligencia artificial también puede ayudar a detectar cuándo alguien está intentando mover datos fuera de la empresa y bloquear la acción o plantear el problema al equipo de seguridad.

Detección de ciberamenazas

Las soluciones de detección y respuesta extendidas (XDR) y administración de eventos e información de seguridad (SIEM) ayudan a los equipos de seguridad a descubrir ciberamenazas en toda la empresa. Para ello, ambas soluciones dependen en gran medida de la inteligencia artificial. Las soluciones XDR usan inteligencia artificial para supervisar puntos de conexión, correos electrónicos, identidades y aplicaciones en la nube para detectar comportamientos anómalos, correlacionar incidentes y exponerlos al equipo. Con modelos avanzados de inteligencia artificial, las soluciones XDR también pueden interrumpir los ataques avanzados, como *ransomware*, y proporcionar sugerencias para mejorar la cobertura de seguridad. Las soluciones SIEM usan la inteligencia artificial para agregar señales de toda la empresa, lo que proporciona a los equipos una mejor visibilidad de lo que sucede. Los equipos también usan la inteligencia artificial para generar conclusiones útiles a partir de la inteligencia contra amenazas, lo que les ayuda a adoptar un enfoque más proactivo para los riesgos cibernéticos.

Investigación y respuesta a incidentes

Durante la respuesta a incidentes, los profesionales de seguridad deben ordenar las montañas de datos para descubrir posibles ciberataques. La inteligencia artificial ayuda a identificar y correlacionar los eventos más útiles en varios orígenes de datos, lo que ahorra tiempo valioso a los

profesionales. La IA generativa simplifica aún más la investigación al responder preguntas y traducir el análisis al lenguaje natural" (Microsoft, s. f.).

IA para la ciberseguridad frente a la seguridad de la IA

Es importante distinguir entre dos conceptos relacionados pero diferentes: IA para la ciberseguridad y la seguridad para la inteligencia artificial.

"La IA para la ciberseguridad hace referencia al uso de herramientas de IA para mejorar la capacidad de una organización en detectar, responder y mitigar las amenazas a todo su entorno. Dado que la inteligencia artificial para la ciberseguridad puede analizar y correlacionar eventos entre varios orígenes, ayuda a las organizaciones a identificar patrones que indican posibles amenazas.

Por otro lado, la seguridad de la inteligencia artificial se centra en la protección de los propios sistemas de inteligencia artificial. Abarca las estrategias, herramientas y prácticas diseñadas para proteger los modelos, los datos y los algoritmos de IA frente a amenazas. Esto incluye garantizar que los sistemas de IA funcionen según lo previsto y que los atacantes no puedan aprovechar las vulnerabilidades para manipular salidas o robar información confidencial.

En resumen, IA para la ciberseguridad hace referencia al uso de sistemas de IA para mejorar la posición de seguridad general de una organización, mientras que la seguridad de IA consiste en proteger los sistemas de IA" (Microsoft, s. f.).

Ventajas de la inteligencia artificial para la ciberseguridad

"La inteligencia artificial ha sido realmente un cambio en la ciberseguridad, lo que facilita a los profesionales de la seguridad responder a un número cada vez mayor de ciberamenazas,

cantidades crecientes de datos y una superficie de ciberataque en expansión. Estas son algunas de las formas en que la inteligencia artificial para la ciberseguridad ayuda a los equipos a ser más eficaces:

Detección de amenazas más rápida

Muchas soluciones de seguridad, como SIEM o XDR, registran miles y miles de eventos que indican un comportamiento potencialmente anómalo. Aunque la gran mayoría de estos eventos son inofensivos, algunos no lo son, y el riesgo de pasar por alto una ciberamenaza potencial puede ser enorme. La inteligencia artificial ayuda a identificar los incidentes que realmente importan. También correlaciona actividades aparentemente no relacionadas en incidentes que indican una ciberamenaza potencial.

Informes simplificados

Las herramientas que usan la IA generativa pueden poner en correlación y analizar información de varios orígenes de datos para crear informes fáciles de entender que los profesionales de seguridad pueden compartir rápidamente con otros en la organización.

Identificación de vulnerabilidades

La inteligencia artificial ayuda a detectar puntos débiles en el entorno general, como dispositivos desconocidos y aplicaciones en la nube, sistemas operativos obsoletos o datos confidenciales desprotegidos.

Mejora de capacidades

Dado que la IA generativa ayuda a traducir los datos y el análisis de ciberamenazas al lenguaje natural, los analistas no necesitan saber cómo escribir consultas para ser productivos. Esto ayuda a los analistas júnior a asumir tareas más complejas. Además, la IA generativa proporciona pasos de corrección y otras recomendaciones que ayudan a los nuevos miembros del equipo a aprender rápidamente a responder eficazmente a los ciberataques.

Información accionable

Al agregar y analizar datos de diversos orígenes, como registros de seguridad, tráfico de red y fuentes de amenazas externas, la inteligencia artificial proporciona una vista completa del panorama de seguridad y revela patrones ocultos de ataque.

Reducción de falsos positivos y falsos negativos

La inteligencia artificial ayuda a reducir los falsos positivos y falsos negativos mediante técnicas avanzadas como el reconocimiento de patrones, la detección de anomalías, el reconocimiento contextual y el aprendizaje continuo. Estos sistemas proporcionan una toma de decisiones más matizada y evitan sobrecargar los equipos de seguridad con alertas irrelevantes.

Escalabilidad

La inteligencia artificial mejora significativamente la escalabilidad en ciberseguridad mediante la automatización de tareas, el procesamiento de grandes cantidades de datos en tiempo real y el aprendizaje continuo. A medida que crece el volumen y la complejidad de las ciberamenazas, la capacidad de la inteligencia artificial para escalar y adaptarse garantiza que los sistemas de ciberseguridad sigan siendo resistentes, eficientes y capaces de controlar las demandas de las infraestructuras de TI modernas" (Microsoft, s. f.).

Herramientas de ciberseguridad con tecnología de IA

La inteligencia artificial se ha integrado en varias herramientas de ciberseguridad para ayudar a mejorar su eficacia. Algunos ejemplos son:

- **"*Firewalls* e inteligencia artificial de próxima generación**. Los *firewalls* tradicionales toman decisiones sobre cómo permitir o bloquear el tráfico en función de las reglas definidas por un administrador. Los *firewalls* de próxima generación van más allá de estas funcionalidades, ya que usan la inteligencia artificial para aprovechar los datos de

inteligencia sobre amenazas y ayudar a identificar nuevas ciberamenazas.

- **Soluciones de seguridad de puntos de conexión mejoradas con la inteligencia artificial**. Las soluciones de seguridad de los puntos de conexión usan inteligencia artificial para identificar vulnerabilidades de los puntos de conexión, como un sistema operativo obsoleto. La inteligencia artificial también puede ayudar a detectar si se ha instalado *malware* en un dispositivo o si se están filtrando cantidades inusuales de datos hacia o desde un punto de conexión. Durante un ataque, la inteligencia artificial puede aislar automáticamente el punto de conexión del resto del entorno digital.

- **Sistemas de prevención y detección de intrusiones de red controlados por inteligencia artificial**. Estas herramientas supervisan el tráfico de red para detectar usuarios no autorizados que intentan infiltrarse en la organización a través de la red. Con la inteligencia artificial, estos sistemas procesan rápidamente grandes volúmenes de datos para identificar y bloquear a los ciberatacantes antes de que causen daños.

- **Soluciones de seguridad en la nube e inteligencia artificial**. Dado que muchas organizaciones usan varias nubes para su infraestructura y aplicaciones, puede ser difícil realizar un seguimiento de las ciberamenazas que se mueven entre diferentes nubes y aplicaciones. La inteligencia artificial ayuda con la seguridad en la nube mediante el análisis de datos de todos estos orígenes para

identificar vulnerabilidades y posibles ciberataques.

- **Seguridad de Internet de las cosas (IoT).** Al igual que los puntos de conexión y las aplicaciones, las organizaciones suelen tener muchos dispositivos IoT que son posibles vectores de ciberataques. La inteligencia artificial ayuda a detectar ciberamenazas en cualquier dispositivo IoT y también descubre patrones de actividad sospechosa entre varios dispositivos IoT.

- **XDR y SIEM**. Las soluciones XDR y SIEM extraen información de varios productos de seguridad, archivos de registro y orígenes externos para ayudar a los analistas a comprender lo que sucede en su entorno. La inteligencia artificial ayuda a sintetizar todos estos datos en conclusiones claras" (Microsoft, s .f).

Procedimientos recomendados para la IA para la ciberseguridad

"El uso de la inteligencia artificial para dar soporte a operaciones de seguridad requiere una planeación e implementación cuidadosa, pero con el enfoque adecuado, puede introducir herramientas que realicen mejoras significativas en la eficacia operativa y el bienestar de su equipo.

Desarrollar una estrategia

Hay numerosos productos y soluciones de inteligencia artificial para su uso en seguridad, pero no todos ellos serán adecuados para su organización. Es importante que las soluciones de inteligencia artificial se integren bien entre sí y con su arquitectura de seguridad o pueden terminar creando más trabajo para su equipo. Considere primero los mayores desafíos de seguridad y después identifique soluciones de inteligencia artificial que le

ayudarán a resolver esos problemas. Dedique tiempo a desarrollar un plan para integrar la inteligencia artificial en los procesos y sistemas actuales.

Integrar las herramientas de seguridad

La inteligencia artificial para la ciberseguridad es más eficaz cuando es capaz de analizar datos en toda la organización. Esto supone un reto si las herramientas funcionan en espacios aislados. Invierta en herramientas que trabajen conjuntamente y funcionen con su entorno actual sin problemas, como soluciones integradas de XDR y SIEM. O bien, si es necesario, asigne tiempo y recursos a su equipo para integrar herramientas, de modo que obtenga visibilidad completa en toda su infraestructura digital.

Administrar la privacidad y la calidad de los datos

Los sistemas de inteligencia artificial toman decisiones y proporcionan conclusiones basadas en los datos usados para entrenarlos y operarlos. Si hay errores en los datos o están dañados, la inteligencia artificial proporcionará información deficiente y tomará decisiones incorrectas. Durante la planeación, asegúrese de que tiene procesos implementados para limpiar los datos y proteger la privacidad.

Utilizar éticamente la inteligencia artificial

Muchos de los datos acumulados a lo largo de los años son inexactos, sesgados u obsoletos. Además, los algoritmos y la lógica de la inteligencia artificial no siempre son transparentes, lo que dificulta saber exactamente cómo genera conclusiones y resultados. Es importante asegurarse de que la inteligencia artificial no es la responsable final de la toma de decisiones si existe el riesgo de que trate injustamente a determinadas personas debido a datos sesgados. Más información acerca de la inteligencia artificial responsable.

Probar continuamente los sistemas de inteligencia artificial

Después de la implementación, pruebe periódicamente los sistemas para identificar problemas de sesgo o de calidad a medida que se generan nuevos datos.

Definir directivas para el uso de la IA generativa

Asegúrese de que los empleados y asociados comprenden las directivas de su organización para usar herramientas de IA generativa. Es especialmente importante que las personas no peguen datos reservados y confidenciales en solicitudes a la IA generativa, ya que existe el riesgo de que los datos se hagan públicos" (Microsoft, s. f.).

IA para soluciones de ciberseguridad

"La inteligencia artificial está impulsando cambios significativos en la ciberseguridad mediante la automatización de tareas, la mejora de la detección de amenazas, de la inteligencia y habilitando medidas de seguridad más proactivas y predictivas. A medida que el entorno de amenazas sigue evolucionando, la integración de la inteligencia artificial en la ciberseguridad se convertirá en una estrategia clave para las organizaciones que intentan anticiparse a los riesgos emergentes.

Puede empezar a incorporar inteligencia artificial en sus operaciones de seguridad, ahora, con soluciones de IA generativa, como Microsoft Security Copilot, que permite a los equipos responder de forma más eficaz y efectiva a las amenazas. Los agentes de Microsoft Security Copilot mejoran la seguridad y las operaciones de TI con automatización autónoma y adaptativa. Además, Seguridad de Microsoft ofrece varias soluciones con tecnología de IA para ayudarle a mejorar la eficacia de las operaciones de seguridad. A partir de ahora, su organización estará mejor preparada para mantenerse al día con las amenazas de hoy y mañana" (Microsoft, s. f.).

CONTINUAR

Referencias

Álvarez, R. (2023). *Preocupa el crecimiento del uso de deepfakes de famosas en sitios de videos para adultos*. TN. https://tn.com.ar/tecno/novedades/2023/10/25/preocupa-el-crecimiento-del-uso-de-deepfakes-de-famosas-en-sitios-de-videos-para-adultos/.

Argentina.gob.ar. (2025). *¿Qué es el ciberdelito?*. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito.

Microsoft. (2026). *¿Qué es la IA para la ciberseguridad?*. https://www.microsoft.com/es-ar/security/business/security-101/what-is-ai-for-cybersecurity.

Real Academia Española. (s. f.). Ciberdelito. En *Diccionario de la lengua española*. Recuperado el 28 de enero de 2026, de https://dle.rae.es/ciberdelito.

Bibliografía sugerida

Cert de España. (s. f.). *Glosario informático y de abreviaturas*. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=193.html

Zurdo, G. (2025). *La IA como herramienta del ciberdelito*. Clarín, https://www.clarin.com/opinion/ia-herramienta-ciberdelito_0_TTBkHHWKCr.html

Mazzia, Y. (2025). *El nuevo ciberdelito se sofistica gracias a la IA y ya afecta la seguridad de todo tipo de transacciones online*. https://www.forbesargentina.com/innovacion/el-nuevo-ciberdelito-sofistica-gracias-ia-ataques-ya-afectan-seguridad-cualquier-tipo-transacciones-online-n81744

Fortinet. (2026). *IA en Ciberseguridad: Definido y explicado*. https://www.fortinet.com/lat/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Global Cyber Alliance. (2026). *Antes de la ola de ciberdelincuencia con inteligencia artificial*. https://globalcyberalliance.org/es/antes-de-la-ola-de-ciberdelincuencia-con-ia/

Ministerio de Seguridad de la Nación. (2021). *Cibercrimen y delitos informáticos*. https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/2%20Cibercrimen.pdf

CONTINUAR