DOCUMENTOS SiC
Nº 42
JUNIO 2024

Microsoft

El compromiso con la seguridad y la oportunidad de la IA para la protección

Raquel Hernández
Directora de Soluciones de Seguridad de Microsoft España

Elena García Díez
Chief Security Advisor de Microsoft España

SFI, Iniciativa Futuro Seguro

Copilot for Security, la mano derecha del analista

NIS2 y DORA: tecnología y servicios para cumplir

Más de 15.000 *partners* globales y 10.000 especialistas propios en ciberseguridad avalan su papel estelar como proveedor confiable de empresas y estados

Microsoft apuesta por la IA para alimentar el proceso de mejora continua de la gestión de la seguridad en sus servicios y productos

Microsoft siempre ha tenido en su ADN trabajar por "un mundo más seguro". Así se plasma en su declaración de intenciones, denominada 'Iniciativa Futuro seguro', presentada a finales de 2023 y actualizada este año, y en un portafolio donde cada vez tiene más peso la IA, para anticiparse y hacer frente a un panorama de amenazas complejo y cambiante. Se trata de un hito que ha puesto en valor su director ejecutivo, Satya Nadella, quien se ha dirigido también a todos los empleados enfatizando un compromiso sin parangón por "priorizar la seguridad por encima de todo".

"Todos somos defensores", recuerda Microsoft en uno de sus más recientes informes sobre el panorama de amenazas. A un año de celebrar cuatro décadas de vida, la multinacional de Redmond es, sin duda, uno de los grandes referentes mundiales en seguridad cibernética en la actualidad. Con más de 10.000 expertos en este área de 120 países, equipos rojos y azules dedicados, centros de operaciones 24x7 y miles de socios de toda la industria, la empresa continúa aprendiendo y evolucionando para proteger a los más de 860.000 clientes corporativos que apuestan por ella.

Cyber Defense Operations Center de Microsoft

Nuevo enfoque

La seguridad ha estado presente en Microsoft desde sus comienzos hace casi cuatro décadas. A finales de 2023, su presidente **Brad Smith** dio un paso más presentando la 'Iniciativa Futuro Seguro' (SFI), un nuevo enfoque para buscar "la próxima generación de protección y un nuevo mundo de seguridad para nuestros clientes y la industria" para hacer frente a "la creciente velocidad, escala y sofisticación de los ciberataques, que van más allá de lo visto antes".

A él se sumó la carta que escribió, en mayo, a todos los empleados su director ejecutivo, **Satya Nadella**, quien quiso reforzar la apuesta por la "seguridad por encima de todo" (*Security Above All Else*) de la multinacional recordando que "cada tarea que asumimos (desde una línea de código hasta un proceso de cliente o socio) es una oportunidad para ayudar a reforzar nuestra propia seguridad y la de todo nuestro ecosistema". Y es que, "la ciberprotección es un deporte de equipo y acelerar SFI no es solo la tarea número uno de nuestros equipos de seguridad: es la principal prioridad de todos y la mayor necesidad de nuestros clientes", recordó.

Además, en la compañía cada vez tiene más protagonismo la IA para la defensa y la proactividad frente a todo tipo de adversarios. Así, en uno de sus recientes informes de 'Cyber Signals', en colaboración con OpenAI, explora el impacto de la IA en el panorama de la ciberseguridad y detalla cómo proteger las plataformas de IA de intentos de abuso. Además, anuncia sus principios sobre el uso de este tipo de herramientas para rastrear y bloquear amenazas persistentes avanzadas de estados-nación, manipuladores y sindicatos cibercriminales.

"Si perdemos la confianza en la forma con la que utilizamos la tecnología para trabajar, jugar y vivir, entonces sería un futuro muy distópico", ha manifestado su Corporate Vice President, Security, Compliance, Identity, and Management, Microsoft Corporation, **Vasu Jakkal.** "Por eso, Microsoft está en seguridad. Porque creemos que este es el mayor problema que hay que resolver desde el punto de vista tecnológico".

IA responsable y segura

De hecho, dos aspectos que preocupan especialmente a los CEOs en relación con la IA, son la seguridad y la ética. Según datos de IDC, un 77% de las organizaciones considera que confiar en proveedores con una estrategia de IA responsable es imprescindible para poner en marcha proyectos de este tipo. Por ello, una IA responsable y segura es uno de los grandes requisitos para su despliegue en las organizaciones. En este sentido, Microsoft está realizando un gran esfuerzo global, a través de notables inversiones en infraestructuras y servicios, así como en la disponibilidad de guías de implementación y documentación sobre las mejores prácticas en esta área.

Además, entre sus grandes apuestas destaca la de construir un 'escudo cibernético' basado en IA. Para ello, cuenta con numerosos recursos, como su red global de centros de datos, destacando su Centro de Inteligencia de Amenazas (MSTIC) y el Centro de Análisis de Amenazas (MTAC), que utilizan herramientas y técnicas avanzadas de IA. "Se trata de ganar la batalla frente al cibercrimen y su uso cada vez más intensivo de la IA", recuerdan desde la multinacional.

Más capacidades

Y es que, a pesar de que los atacantes ya están utilizando estas tecnologías para mejorar los mensajes y técnicas de *phishing* y las operaciones de influencia con imágenes sintéticas, la IA también permite activar estrategias de defensa, al automatizar y ampliar las capacidades de detección, respuesta, análisis y predicción de amenazas. Además, los especialistas de Microsoft recuerdan que la inteligencia artificial también puede facilitar que los modelos de lenguaje masivo (LLM) generen información y recomendaciones en lenguaje natural a partir de datos complejos, lo que ayuda a que los analistas sean más efectivos.

Su uso en la red global de centros de datos de Microsoft permite "detectar amenazas a una velocidad tan rápida como la propia Internet". "Aunque los 8.000 millones de personas del planeta pudieran buscar juntos evidencia de ataques cibernéticos, nunca podríamos seguir el ritmo. Pero la IA cambia las reglas del juego".

A ello se suma la compartición de prácticas de IA responsable con más de 15.000 *partners* de seguridad en todo el mundo. ●

Ingeniera industrial y graduada en Administración y Dirección de Empresas, Raquel Hernández es, desde finales de 2023, Directora de Soluciones de Seguridad de Microsoft. Cuenta con una amplia experiencia en el sector y un profundo conocimiento del mercado local para hacer frente a la enorme oportunidad que representa la ciberprotección para los proyectos de digitalización e implantación de IA en las organizaciones españolas, con el objetivo de hacer "un mundo más seguro".

"Copilot for Security es la primera solución especializada que pone la IA generativa en manos de profesionales de todos los niveles de experiencia"

Raquel Hernández

Directora de Soluciones de Seguridad de Microsoft España

– ¿Cómo resumiría el enfoque de la gestión de la ciberseguridad de Microsoft?

– Nuestro compromiso es hacer el mundo más seguro para garantizar que las personas y organizaciones consigan más a través del uso de la tecnología. Tenemos un plan de inversión, presentado en 2021, de más de 20.000 millones de dólares a cinco años en seguridad, protección de datos y gestión de riesgos para proporcionar una protección de extremo a extremo.

La seguridad siempre ha sido muy importante, y ante el aumento y la complejidad de los ciberataques, es ahora la prioridad de la compañía. Las personas y las organizaciones requieren avances continuos en nuestro compromiso sobre cómo protegemos, detectamos y respondemos a las amenazas. Estos compromisos definen nuestro enfoque de ciberdefensa.

– La Iniciativa Futuro Seguro, ¿en qué supone un antes y un después en ciberprotección corporativa?

– La velocidad, escala y sofisticación de los ciberataques requieren una nueva respuesta global. Por eso, lanzamos la Iniciativa Futuro Seguro donde nos comprometimos a desarrollar un 'ciberescudo' basado en IA. Nuestra red global de centros de datos y el uso de modelos avanzados de IA nos sitúan en una posición destacada para poner esta tecnología al servicio de los CISOs. Además, nos guiamos por tres principios: seguridad prioritaria en el diseño, seguridad habilitada por defecto y seguridad de las operaciones en cuanto a monitorización y controles.

"Nuestra red global de centros de datos y el uso de modelos avanzados de IA nos sitúan en una posición destacada para poner esta tecnología al servicio de los CISOs de las organizaciones".

– La IA lo está cambiando todo. ¿Qué aporta Microsoft Copilot for Security?

– Es la primera solución para seguridad que pone la IA generativa en manos de profesionales de todos los niveles de experiencia. Aunque los ataques han aumentado un 67% en los últimos cinco años, no hay suficientes profesionales expertos. En el mundo hay cuatro millones de vacantes sin cubrir. La IA responde a este reto. Copilot for Security es capaz de generar recomendaciones en lenguaje natural a partir de datos complejos. Los usuarios que la han usado han experimentado un aumento del 7% en precisión en todas las tareas y un 22% más de rapidez a la hora de completarlas. Estas cifras muestran los beneficios tangibles de integrar la IA en las prácticas de ciberseguridad.

– Microsoft es "el primer proveedor de seguridad que ofrece gestión de seguridad de la IA de extremo a extremo, protección contra amenazas, seguridad de datos y gobernanza para la IA". ¿Qué le diferencia?

– Reunimos ventajas clave: 78 billones de señales diarias que procesamos para construir nuestra inteligencia sobre amenazas, datos a gran escala; la plataforma integral de seguridad más completa que hace uso de IA responsable y segura, campo que también lideramos: somos la empresa de seguridad más grande del mundo y la que más invierte en este campo; además contamos con los certificados de conformidad para el nuevo Esquema Nacional de Seguridad con nivel alto, para más de 170 servicios de nube. Esto incluye también todos nuestros servicios de IA, como Microsoft Copilot for Security, lo que nos convierte en el primer proveedor de nube que certifica un servicio de estas características. Las organizaciones que inviertan en IA para reforzar la seguridad se mantendrán como líderes en sus industrias. En Microsoft, nos comprometemos a empoderarlos con las mejores soluciones.

– Uno de sus retos es "construir alianzas a largo plazo con los clientes, promoviendo una transformación digital segura". ¿Cómo se está materializando? Ha sido notable el presentado con Telefónica…

– Estamos logrando muchos avances. La ciberseguridad es una responsabilidad compartida que nos afecta a todos. Contamos con un ecosistema de 15.000 *partners* globales de seguridad que trabajan conjuntamente con nosotros en acompañar a más del millón de clientes que usan nuestra tecnología. El acuerdo con Telefónica Tech implica la integración de nuestras soluciones avanzadas de seguridad e IA con su experiencia en la operación de la ciberseguridad. Los clientes se beneficiarán de una gestión de la seguridad proactiva, integrada, automatizada y en tiempo real.

– ¿Qué opina de las normativas europeas?

– Es esencial un marco regulatorio potente que proteja a los usuarios y promueva los usos positivos y responsables de la tecnología. Colaboramos estrechamente, a escala nacional y europea, con los reguladores y todas nuestras soluciones cumplen con la normativa actual. Esto nos permite validar la robustez de nuestras soluciones y ponerlas al servicio de nuestros clientes –a los que también ayudamos a adoptar las medidas necesarias–, con los máximos estándares de confianza y seguridad. ●

Ingeniera de Telecomunicaciones y hasta hace poco CISO de una destacada multinacional tecnológica, Elena García ha llegado a Microsoft para "ayudar a empresas y administraciones públicas, nacionales y europeas, a avanzar en su estrategia de seguridad y mejora de su ciberresiliencia". Convencida del valor que aportan el trabajo de los responsables de la información y los roles directivos para desplegar estrategias que pongan a la ciberseguridad en un plano global, en esta entrevista desgrana los grandes retos de la compañía para hacer un mundo digital confiable, frente a un panorama de amenazas cambiante y complejo.

"Manejar 78 billones de señales relativas a eventos de seguridad en el SOC aporta a Microsoft un valor diferencial en inteligencia de amenazas y protección"

Elena García Díez

Chief Security Advisor en Microsoft

– ¿Cómo ha sido la transición desde CISO a Chief Security Advisor (CSA) en Microsoft? ¿Con qué tipo de clientes y sectores va a focalizar más su trabajo?

– Como sociedad, vivimos en un momento de continua evolución tecnológica en la que las amenazas vienen también evolucionando en su complejidad e impacto. Ahí los profesionales de este mundo tecnológico, también los de ciberseguridad, estamos obligados a estar en continua evolución para dar respuesta a nuevas preocupaciones y necesidades.

Tras años de experiencia en el sector tecnológico y de la ciberprotección, desde posiciones en sector público y privado, me incorporo al equipo de Microsoft en un proyecto y momento apasionante para hacer frente a la enorme oportunidad que representa la ciberseguridad para los proyectos de digitalización e implantación de IA en las organizaciones españolas de todo tipo y sector.

Personalmente, en esta etapa trabajaré la ciberseguridad desde una posición muy complementaria respecto a mis experiencias anteriores. Un reto que abordo con ilusión y grandes expectativas de contribuir al desarrollo de todo el ecosistema.

"Los datos de nuestros clientes son de nuestros clientes, no se utilizan para entrenar otros modelos de IA y están protegidos de acuerdo con la regulación de privacidad y el EU Data Boundary, que recientemente hemos actualizado".

– Desde su amplia trayectoria, habiendo trabajado también, durante más de una década para Inteco (actual Incibe), ¿cómo está percibiendo la evolución de la IA, su adopción por parte de las organizaciones y sus riesgos?

– La IA es una nueva oportunidad de evolución tecnológica y, como tal, aporta nuevas capacidades a amenazas y atacantes, pero al mismo tiempo, emerge como ayuda a las compañías para desplegar estrategias más innovadoras de defensa.

Además, la IA viene a revolucionar y es una nueva variable disruptiva de lo que eran ya los procesos de transformación digital. Tenemos que aplicar ahora, mejor que nunca, las lecciones aprendidas de revoluciones tecnológicas anteriores. Asimismo, promover la adopción responsable de esta tecnología es clave para que realmente haga más eficientes y seguras a las organizaciones.

Si hay algo que preocupa a los CEOs de las organizaciones, en cuanto a la IA, es la seguridad y la ética: un 77% considera que confiar en proveedores con una estrategia de IA responsable es imprescindible para poner en marcha sus proyectos de IA.

Una aproximación de seguridad de extremo a extremo, como la gestión de seguridad de la IA que promueve y proporciona Microsoft, es clave para el éxito de su adopción ya que contempla protección contra amenazas, seguridad de datos y gobernanza.

– Como ex CISO, ¿qué valoración hace de la propuesta de Microsoft en lo referente a la IA aplicada a la ciberseguridad?

– Para Microsoft la seguridad es lo primero. Su apuesta es una combinación de tecnología y talento humano, donde la Inteligencia Artificial juega un papel fundamental para seguir la acelerada evolución cualitativa y cuantitativa de las ciberamenazas.

La compañía ha dado un importante paso con Microsoft Copilot for Security, la primera solución de IA generativa para seguridad del sector. Además, es un proveedor de confianza para las organizaciones. Manejar 78 billones de señales relativas a eventos de seguridad sobre las que nuestros más de 10.000 ingenieros operan el SOC de Microsoft aporta sin duda un valor diferencial a la inteligencia de amenazas y protección.

– Soberanía digital y soberanía del dato. ¿Puede colaborar Microsoft con el Estado español en la salvaguarda de ambos espacios?

– Sin duda. De hecho, estamos colaborando con el gobierno de España en este sentido. Respondemos como actor importante en la industria y ofrecemos soluciones que permiten a las organizaciones tener un mayor control sobre sus datos, garantizando la soberanía digital de los mismos. Los datos de nuestros clientes son de nuestros clientes, no se utilizan para entrenar otros modelos de IA y están protegidos de acuerdo con la regulación de privacidad y el EU Data Boundary, que recientemente hemos actualizado.

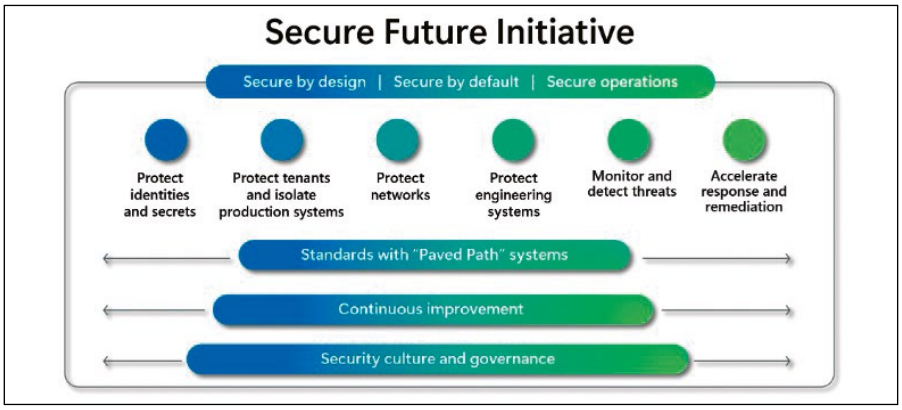
Los pilares: ciberseguridad basada en inteligencia, ingeniería de software e impulso a la aplicación de estándares internacionales

Ciberprotección por encima de todo: hacia un Futuro Seguro

Frente al ritmo, la escala y la complejidad crecientes de las ciberamenazas, con alrededor del 40% de los ataques estadonación de los últimos dos años dirigidos a infraestructuras críticas, según el Informe de Defensa Digital de Microsoft, la compañía ha decidido dar un gran paso en su estrategia con la finalidad de poner la seguridad por delante y transformar la manera en que diseña, construye, prueba y opera su tecnología, para proteger a sus clientes y su propia infraestructura. Así, en noviembre de 2023, presentó lo que ha denominado **'Iniciativa Futuro Seguro'** (SFI), que supone "un fuerte compromiso de varios años para ayudar a garantizar que ofrecemos productos y servicios seguros y dignos de confianza, permitiendo a nuestros clientes alcanzar sus objetivos de transformación digital y proteger sus datos y activos de actores maliciosos", destacó su Corporate Vice President and Chief Cybersecurity Advisor, Microsoft Corporation, **Bret Arsenault**. Para ello, se focalizará en tres pilares: la ciberseguridad basada en la IA), los avances en ingeniería de software y el impulso a una mayor aplicación de estándares internacionales.

Avances en IA e ingeniería

Así, la compañía se ha comprometido a crear un "ciberescudo" basado en IA para ponerla al servicio de la ciberseguridad, a través de su amplia red de centros de datos y el uso de modelos avanzados de IA, desarrollando unas capacidades que también se están extendiendo a los clientes ya que, a través de las tecnologías de seguridad de la firma, pueden extraer y analizar datos de una variedad de fuentes.
Microsoft busca, además, desarrollar un nuevo estándar de seguridad que esté presente en la forma en que se diseña, construye, prueba y funciona su tecnología. Así, entre otras acciones, ha evolucionado su ciclo de vida de desarrollo de seguridad (SDL), que creó en 2004, a un 'SDL dinámico' o dSDL. Esto le permite aplicar procesos sistemáticos para integrar de forma continua la ciberprotección contra los patrones de amenazas emergentes a medida que los ingenieros programan, prueban, implementan y operan sus sistemas y servicios. Este proceso se puede complementar con otras medidas, como las de análisis de código seguro impulsado por IA y el uso de GitHub Copilot para auditar y probar el código fuente ante amenazas avanzadas. Junto a ello, Microsoft también proporcionará a sus clientes configuraciones predeterminadas más seguras para la autenticación multifactor (MFA). Y es que, uno de sus grandes objetivos es fortalecer la protección de la identidad y los accesos ante ataques altamente sofisticados.



La compañía ha evolucionado su enfoque para que sus productos y servicios se guíen por tres principios: seguridad por diseño, seguridad por defecto y seguridad en la operación.

Aplicación eficaz de las normas internacionales

La multinacional también está redoblando sus esfuerzos para aglutinar a gobiernos, sector privado y sociedad civil en torno a la aplicación efectiva de los principales estándares que impulsan la ciberseguridad.

Evolución constante

En mayo, la compañía decidió ampliar su Iniciativa integrando las recomendaciones recientes de la Junta de Revisión de Seguridad Cibernética (CSRB) del Departamento de Seguridad Nacional (DHS) de EE.UU., así como sus lecciones aprendidas sobre ciberincidentes para garantizar que su enfoque de ciberseguridad sigue siendo sólido y adaptado a un panorama de amenazas en evolución. **Charlie Bell,** Executive Vice President, Microsoft Security, lo justifica así: "Microsoft desempeña un papel central en el ecosistema digital mundial y esto conlleva la responsabilidad fundamental de ganarse y mantener la confianza. Debemos y haremos más".
La evolución del enfoque SFI pasa, de esta forma, por que los productos y servicios se guíen por tres principios: seguridad por diseño, seguridad por defecto y seguridad en la operación. Unos propósitos que implican trabajar en seis grandes frentes: la protección de identidades y secretos; la protección de los *tenants* y el aislamiento de los sistemas de producción; la protección de las redes; la protección de los sistemas de ingeniería; y la aceleración de la respuesta y la implementación del remedio. Dentro de cada pilar, la compañía llevará a efecto medidas de gran impacto.

Gobernanza mejorada

Microsoft también está tomando medidas importantes para refinar la gobernanza efectiva de la seguridad, incluidos varios cambios organizativos y supervisión, controles e informes adicionales. "Estamos cumpliendo estos objetivos a través de un nuevo nivel de coordinación con un modelo operativo que alinea a los líderes y equipos con los seis pilares de SFI, con el fin de impulsar la seguridad de manera completa y romper los silos tradicionales", indica Bell. Y es que, por ejemplo, está implementando un nuevo marco de gobierno de seguridad, encabezado por el Director de Seguridad de la Información (CISO), además de inculcar una cultura encaminada a priorizar las buenas prácticas de seguridad en toda la organización.

Inteligencia generativa para ayudar al analista del SOC

Gestión global y protección tecnológica integrada de extremo a extremo

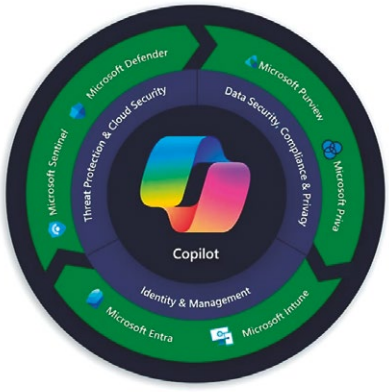
Con un enfoque integrado y aprovechando las capacidades de la IA y la automatización en su portafolio de productos y servicios, Microsoft es una de las empresas que ha sabido desmarcarse del resto para erigirse como un referente, especialmente a la hora de aplicar la IA Generativa a la ciberseguridad. Sin duda, uno de los principales hitos de la compañía en este sentido ha sido el lanzamiento de lo que se ha convertido en su propuesta más innovadora: **Microsoft Copilot for Security**, que ha integrado en toda su cartera de productos de protección y que cuyo uso es abierto de forma general.

Se trata de su gran apuesta basada en datos a gran escala e inteligencia sobre amenazas, incluyendo más de 78 billones de señales de seguridad procesadas por Microsoft cada día. En ella también incluye grandes modelos de lenguaje (LLM), ampliando las habilidades de los profesionales, así como permitiéndoles colaborar de manera más efectiva, tener mayor visibilidad y responder más rápido.

Y es que, Copilot for Security multiplica la fuerza de todo el portafolio de Microsoft Security, que integra más de 50 categorías dentro de seis familias de productos para ofrecer una seguridad de extremo a extremo y sin fisuras. Su implementación hace posible proteger un entorno corporativo desde cualquier perspectiva: seguridad, cumplimiento, identidad, administración de dispositivos y privacidad. "En la era de la IA, es más importante que nunca tener una solución unificada que elimine las brechas de protección creadas por herramientas aisladas", señalan desde la compañía.

Especialmente destacada es la integración de Copilot en productos como Microsoft Defender, para la detección, investigación y respuesta a amenazas; en Microsoft Entra, para prevenir los compromisos a la identidad de los usuarios; en Microsoft Sentinel, para priorizar las alertas más críticas; en Microsoft Purview, para proteger y gobernar los datos; y en Microsoft Intune, para una gestión más eficiente de los *endpoints*, entre otros.

De hecho, Microsoft ya ha podido comprobar sus ventajas: con ella, los analistas de seguridad experimentados han sido un 22% más rápidos y un 7% más precisos en todas las tareas al usar esta herramienta, entre otros datos recogidos en su segundo estudio económico de Copilot for Security.



Microsoft Security portfolio

AI alcance de cualquier organización

Para facilitar su adopción, Microsoft ofrece Copilot for Security en un portal inmersivo independiente o integrado en productos de seguridad existentes. Es multilingüe y puede procesar y responder en ocho idiomas a todo tipo de indicaciones. Asimismo, cuenta con un modelo de pago por uso para que esté al alcance de cualquier organización. A ello, se suma un ecosistema amplio y global de más de 100 socios, formado por proveedores de servicios de seguridad gestionados y proveedores de software independientes.

Protección de extremo a extremo

Junto a ello, cabe destacar que, durante la celebración de la pasada Conferencia RSA, Microsoft presentó novedades que le convierten "en el primer proveedor de seguridad que ofrece gestión de seguridad de la IA de extremo a extremo, protección contra amenazas, seguridad de datos y gobernanza para la IA".

Copilot for Security multiplica la fuerza de todo el portafolio de Microsoft Security, que integra más de 50 categorías dentro de seis familias de productos.

Además de dar a conocer la integración de Copilot for Security en toda su cartera de protección, la compañía hizo públicas, entre otras, nuevas funcionalidades en dos de sus soluciones más importantes para los equipos de seguridad, **Microsoft Defender** y **Microsoft Purview**, con las que ayuda a proteger y controlar las aplicaciones de IA generativa.

Así, en su plataforma de protección de aplicaciones nativa de la nube (CNAPP) de Microsoft Defender for Cloud, los equipos de ciberprotección pueden identificar su infraestructura de IA, como *plugins*, SDK y otras tecnologías, gracias a las capacidades de gestión de seguridad en plataformas como Microsoft Azure OpenAI Service, Azure Machine Learning y Amazon Bedrock. Además, facilita la respuesta a incidentes con la integración nativa de estas señales en Microsoft Defender XDR, entre otras características.

A ello se le unen las mejoras en Microsoft Purview AI Hub que, ahora, en versión *preview*, ofrece información tal como datos confidenciales compartidos con aplicaciones de IA, el número total de usuarios que interactúan con este tipo de aplicaciones y el nivel de riesgo asociado a ello. Incluso, ofrecerá información sobre el mal uso de la IA. Además, Purview incluye nuevas evaluaciones de cumplimiento de la IA.

Operaciones de seguridad

En paralelo, Microsoft ha incluido nuevas características y capacidades para los SOC, destacando **Microsoft Security Exposure Management**, una solución que ayuda a los equipos a identificar exposiciones de riesgo e implementación de controles de seguridad esenciales insuficientes. Y en **Sentinel**, ha desarrollado Optimizaciones SOC para orientar de forma personalizada y ayudar a gestionar los costes, aumentar el valor de los datos y mejorar la cobertura frente a las técnicas de ataque más comunes. Todo, como parte de un gran portafolio en constante evolución.

Controlar y proteger el uso de la IA

Asimismo, Microsoft ha activado en su cartera de soluciones capacidades para descubrir sus riesgos (como fugas de datos confidenciales y usuarios que acceden a aplicaciones de alto riesgo), proteger las aplicaciones de IA en uso y los datos confidenciales sobre los que razonan o generan, así como gobernar su uso detectando cualquier infracción de políticas regulatorias u organizativas. De esta forma, las organizaciones pueden trabajar con todo tipo de datos, ya sean críticos o no, de forma segura y responsable.

Microsoft se prepara para su designación como "proveedor externo de servicios de TIC críticos"

Tecnología y servicios para facilitar el cumplimiento de las exigencias de NIS2 y DORA

La UE concibe la ciberseguridad como uno de los pilares de la transformación digital socioeconómica, algo que se evidencia con el desarrollo y aprobación de normativas de gran impacto. Una de ellas es la directiva NIS2, en vigor desde enero de 2023, que perfecciona el camino marcado con su predecesora (NIS), proporcionando medidas para impulsar un adecuado nivel común de ciberprotección en la UE, y que los estados miembros deberán transponer con fecha límite de 17 de octubre de este año. Entre sus novedades, destaca la ampliación del alcance de sus medidas a 15 sectores y a más de 160.000 empresas.

Junto a NIS2, cabe destacar la Ley de Resiliencia Operacional Digital (DORA), un reglamento especial, que será de aplicación a partir del 17 de enero de 2025. Su objetivo es armonizar y reforzar la ciberseguridad del sector financiero (bancos, compañías de seguros y empresas de inversión) y sus proveedores, y garantizar que dicho sector sea resiliente ante contingencias graves de su entorno operativo debidas a ciberataques, fallos de TI u otros riesgos. No cabe duda de que trabajar para cumplir estas normativas requiere preparación y colaboración en todos los niveles de una organización.

Directiva NIS2

La preparación para NIS2 puede requerir un esfuerzo considerable ya que, por ejemplo, exige implementar una serie de elementos clave como parte de sus medidas, incluyendo la seguridad de la cadena de suministro, las políticas de control de acceso y la gestión de activos, así como el uso de soluciones de autenticación multifactorial, el principio de confianza cero, la gestión de incidentes y los planes de recuperación empresarial, entre otros.

Para facilitar la adaptación, Microsoft ofrece un enfoque que "combina conocimiento técnico, estrategias innovadoras y un profundo conocimiento legal", indica su General Manager, Data Security, Compliance, and Privacy, Microsoft Corporation, **Herain Oberoi**. "Nuestra estrategia para NIS2 aborda toda la gama de riesgos asociados con la tecnología de la nube. Y estamos comprometidos a garantizar que los servicios en la nube de Microsoft establezcan el punto de referencia para el cumplimiento normativo y la excelencia en ciberseguridad en tecnología", añade. Además, el cumplimiento de NIS2 se alinea con los mismos principios de Zero Trust abordados por las soluciones de seguridad de Microsoft, a través de Microsoft Sentinel, Microsoft XDR y Microsoft Defender, entre otras.

DORA y la industria financiera

La Ley de Resiliencia Operativa aplica a entidades de la industria de servicios financieros (FSI) que operan en la UE y a sus terceros TIC proveedores que prestan servicios en la UE, independientemente de dónde operen estos últimos. También, se aplica a los proveedores externos críticos (CTPP) designados por las Autoridades Europeas de Supervisión. De hecho, por primera vez, se designarán "proveedores de servicios críticos de TIC de terceros" o CTPP considerados críticos para el sistema financiero. Microsoft se está preparando para ser designada como "proveedor externo de servicios de TIC críticos" y está en disposición de cumplir con las disposiciones de DORA y ayudar a las instituciones financieras reguladas a cumplirla.

En este último sentido, cabe señalar que las entidades financieras de la UE deben considerar bajo DORA una serie de áreas principales, entre las que se encuentra un marco de gestión de riesgos de TIC. Para ello, Microsoft ya ofrece capacidades integradas de gestión de riesgos de TIC en sus servicios actuales. Por ejemplo, con Microsoft Defender for Cloud, Microsoft 365 Service Healh Dashboard, Microsoft Secure Score, Azure Service Health y Microsoft Purview.

Además, se les exige una serie de requisitos sobre la gestión, clasificación y presentación de informes de incidentes de TIC, para los que la compañía proporciona capacidades con Microsoft Defender. Además, Microsoft 365 Compliance Center y Azure Sentinel proporcionan funcionalidades para la detección, investigación, generación de informes y gestión de incidentes, alineándose con los requisitos para la notificación y respuesta. La Ley también introduce la realización de pruebas de resiliencia operativa digital y Microsoft ya permite a los clientes hacerlo a través de Microsoft Cloud Penetration Testing Rules of Engagement y sus programas de Bug Bounty.

Certificados para el ENS

En lo que toca a la legislación española vigente para el sector público y sus proveedores, cabe destacar que, recientemente, Microsoft ha renovado sus certificados de conformidad para el nuevo Esquema Nacional de Seguridad (ENS) con nivel alto, para más de 170 servicios de nube de Microsoft para Azure, Microsoft 365, Microsoft 365 para Educación y Dynamics 365 (incluyendo Power Platform).

"Estamos comprometidos a garantizar que los servicios en la nube de Microsoft establezcan el punto de referencia para el cumplimiento normativo y la excelencia en ciberseguridad en el mundo de la tecnología". Herain Oberoi

Esta certificación se ha ampliado también a la plataforma Microsoft Azure AI Studio y a todos los servicios de IA sobre Azure, además de a la solución de seguridad potenciada con IA, Microsoft Copilot for Security. De esta manera, la compañía se convierte en el primer proveedor de nube que certifica un servicio de estas características.

Además de estos servicios, han recibido esta certificación Microsoft Copilot para Microsoft 365, y Microsoft Copilot Studio, entre otros, complementando así su oferta de cumplimiento del ENS en este ámbito.

Microsoft

Microsoft Copilot for Security:

La primera herramienta de IA generativa para la operación de Seguridad e IT en el mundo

Para más información accede a:
https://aka.ms/copilotforsecurity