Cómo escalar el valor de la IA al negocio: Select

CanalesTI agosto 2024 / Número 514

CanalesTI

:(

Your PC ran Into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about these issue and posible fixes visit http://www.windows.com/stopcode

If you call a support person, give them this info:
Stop Code: CRITICAL_PROCESS_DIED

FALLO DEL SIGLO

CIMBRA LA CIBERSEGURIDAD

Más poderoso

Eaton Power Xpert 9395P

200 - 1200 kVA

UPS doble conversión, diseñado para mantener energía estable, ininterrumpida y limpia.

EATON

Powering Business Worldwide

Solicita más información:

AlejandroALavin@eaton.com

CELEBRA

45 AÑOS

INGRAM MICRO®

FALLO DEL SIGLO

CIMBRA LA CIBERSEGURIDAD

El jueves 18 de julio por la madrugada se registró una falla en máquinas con Windows provocada por una actualización defectuosa del proveedor de ciberseguridad Crowdstrike, la cual causó desconexiones de operación e impactos significativos en las empresas más grandes del mundo, en sectores como aerolíneas, aeropuertos, trenes, sistemas de pago, de salud, energía y medios de comunicación, incluyendo México.

La empresa de ciberseguridad responsable de ésta que definen especialistas como "la mayor interrupción informática de la historia", asegura que no se trata de un incidente de seguridad o un ciberataque, sino de un "error humano" al no verificar el buen funcionamiento de la actualización, la cual es usada por sistemas operativos como Linux, Mac y Windows. Pero el defecto sólo se encontró en servidores Windows, lo que se tradujo en la aparición de la temida "pantalla azul" que impedía su correcto funcionamiento.

Las fallas continuaron días después de que el CEO de CrowdStrike, George Kurtz, asegurara que el problema fue solucionado por sus ingenieros. Reiteró que la caída se debió a un "error" en una actualización que tuvo un problema de compatibilidad con el sistema operativo Windows, que afectó el acceso a las aplicaciones y servicios de Microsoft 365.

CrowdStrike, que es proveedor de ciberseguridad del 70 por ciento de las empresas más grandes del mundo consideras por la revista Fortune, se disculpó y aseguró que están trabajando para evitar que este tipo de incidentes vuelvan a ocurrir en el futuro. La empresa publicó una serie de recomendaciones para que sus clientes puedan recuperar sus sistemas lo antes posible, pero especialistas aseguran que esto puede llevarse días o semanas, ya que los "parches" se tendrían que hacer de manera manual o semi manual.

Troy Hunt, un experto australiano en ciberseguridad, lo catalogó como "la mayor interrupción informática de la historia", si bien no culpó a Microsoft sino a Crowdstrike.

Se salvó Rusia, entre otros países, en parte porque las sanciones occidentales hicieron que Microsoft dejara de prestarles servicio con motivo del operativo militar en Ucrania. Desde entonces, Rusia pasó a usar sus propios sistemas informáticos, como Astra Linux, cuyo desarrollo se aceleró en los años posteriores a las primeras sanciones occidentales por la reunificación de Crimea, quizá previendo que era cuestión de tiempo que Occidente encontrara más razones para seguir sancionándola.

Microsoft indicó en la red social X que la empresa estaba "trabajando para redirigir el tráfico afectado a sistemas alternativos para aliviar el impacto de una manera más rápida" y dijo que observaban "una tendencia positiva en la disponibilidad del servicio".

La empresa afirma que "está investigando" la incidencia global. "Somos conscientes de un problema que afecta a los dispositivos Windows debido a una actualización de una plataforma de software de terceros (en referencia a Crowdstrike). Anticipamos que se llegará a una resolución", indicaron a Europa Press fuentes de la compañía.

En entrevista con Canales TI, el especialista en ciberseguridad, Luis Díaz, advirtió que este gigantesco incidente tendrá repercusiones graves en la reputación de la industria de

Helder Ferrão,

Estratega Industrial de Akamai LATAM

tecnología. Por lo que en breve tendremos que ver cambios significativos en la estructura de desarrollo, comercialización y uso de toda la infraestructura que hoy es basamento de la actividad humana del siglo XXI.

Por su parte, Amit Yoran, presidente y director general de Tenable opinió ante medios: "Esta caída sin precedentes evidencia cuán dependientes son nuestros sistemas críticos de que el software opere todo el tiempo como debe. Este es un perfecto caso de estudio sobre por qué nadie debe depender de un solo proveedor, ya sea CrowdStrike, Microsoft o cualquier otro.

Aunque hasta el momento no tenemos motivos para creer que esto fue el resultado de un ciberataque, es un severo recordatorio del amplio impacto que la tecnología puede tener en nuestra vida diaria. Esto también hará que los directores de TI y los profesionales de seguridad dejen de aplicar actualizaciones automáticas de proveedores a ciegas. Los días de la auto-actualización se han sometido a un escrutinio masivo."

Las consecuencias

Helder Ferrão, Estratega Industrial de Akamai LATAM., afirma que es posible se haya generado una especie de preocupación por parte de las personas, sin embargo es importante recordar que la nube y el internet funcionan sin problemas el 99% del tiempo; sin embargo, cada empresa tiene un manual para manejar las interrupciones de TI para garantizar una recuperación rápida y una interrupción mínima.

Estos manuales abarcan desde la preparación, detección y notificación, respuesta inmediata, hasta resolución, lo que garantiza que las empresas tengan un enfoque estructurado y proactivo para gestionar y resolver cualquier incidente. Para los equipos de TI, el objetivo número uno es el rápido análisis de la causa raíz y luego determinar el mejor camino hacia la solución.

Son situaciones que pueden suceder en el mercado, los riesgos digitales existen y los ataques seguirán existiendo, por lo que es vital no subestimar los desafíos y las complejidades para mantener este vasto tejido digital en funcionamiento de manera segura, y seguir protegiéndonos con los mecanismos más desarrollados. Por ello, no cree que vaya a haber ningún impacto en la confianza, pero sí demuestra la importancia de todos los puntos de atención y gestión del entorno tecnológico

.Jonny López, Consulting Sales Engineer LATAM en Cradlepoint, asegura que las fallas de seguridad, como la que vivimos en semanas recientes, ciertamente pueden afectar la percepción pública sobre la eficacia de los productos de ciberseguridad y en particular sobre las partes involucradas. Sin embargo, las empresas que demuestran transparencia, rapidez en la respuesta y un compromiso firme con la mejora continua pueden mantener y hasta aumentar la confianza de sus clientes a largo plazo; en este sentido es importante entender que la ciberseguridad es un campo en constante evolución y cada incidente proporciona lecciones valiosas y oportunidades para fortalecer las defensas.

Es así como los responsables de TI deben asegurarse de contar con la tecnología adecuada y sobre todo con planes de continuidad de negocio y recuperación ante incidentes, mismos que deben estar alineados con las mejores prácticas y establecer protocolos de atención de emergencias.

La recomendación siempre estará orientada a la implementación de la tecnología apropiada pero también aconsejamos prestar especial atención a los procesos, personas y políticas de seguridad que al final van mucho más allá de la implementación de una u otra solución y realmente es allí donde se establece la forma en la que se implementa y opera la estrategia completa de manera integral.

Por otra parte, vale la pena tener en cuenta la importancia de tecnologías agentless (sin agente) que no requieren de la instalación de una aplicación en la computadora del usuario, con esto se logran prevenir muchas de las amenazas de Día Cero y otras más comunes de una manera no invasiva, sin intervenir el funcionamiento del sistema operativo, protegiendo al mismo tiempo la información sensible y previniendo la ejecución de código malicioso en el dispositivo del usuario. A fin de aprovechar esta tecnología para aislar oportunamente los recursos críticos de la empresa, previniendo la entrada de código malicioso y evitar la filtración de datos lo cual es pieza clave para mantener la privacidad e integridad de la información de la empresa.

David González, Investigador de seguridad del laboratorio de Eset en Latinoamérica, explica que el fallo afectaría más temporalmente la percepción de seguridad, pues fue un incidente a nivel mundial que involucró muchísimas fallas de sistemas críticos.

David López Agudelo,

vicepresidente de ventas USA/Latam de Appgate

Y aunque será una afectación temporal, se debe de empezarse a ganar de nuevo la confianza por parte de las empresas que manejan la ciberseguridad. Deben aprender a gestionar las crisis por las que están pasando, y también aprender a mejorar sus procesos. De ahí que una transparencia, una buena comunicación con sus clientes, canales y una correcta implementación de sus soluciones, son claves para restaurar esta confianza.

Por su parte, María José Albarrán, directora de Canales para Fortinet México, dijo que esto no afectará la confianza, todo lo contrario. Puede ayudar a generar más conciencia.

La gente que antes no tenía presente que la ciberseguridad puede afectar la operación de países o aeropuertos, ahora es más consciente y esto hace que volteen a ver qué significa la seguridad digital, cómo estar protegidos e incluso tener un plan estratégico para gestión de riesgos y ciberseguridad.

Gustavo Valdez, Director de General de Ikusi en México, asegura que la clave es entender que la ciberseguridad es un ecosistema en el que la tecnología, las regulaciones y las prácticas organizacionales deben trabajar en conjunto para proteger procesos críticos de negocio derivados de la digitalización de los mismos. La IA, cuando se utiliza adecuadamente, puede fortalecer este ecosistema, ayudando a las organizaciones a ser más resilientes frente a las amenazas cibernéticas.

Ueric Melo,Security Awareness & Privacy Manager, Latin America and Caribbean de GENETEC, afirmó que, además de afectar la reputación de CrowdStrike, la industria de ciberseguridad actualmente es fundamental para cualquier organización.

El propio incidente y la disrupción que causó muestran cómo somos dependientes de los sistemas de tecnología de la información y de la conectividad entre estos sistemas y sus usuarios. Por eso, es impensable poner un sistema, dispositivo conectado o cualquier solución tecnológica en producción sin considerar los riesgos cibernéticos y, entre otras cosas, implementar las herramientas adecuadas para mitigar los riesgos identificados. Observando la evolución tecnológica de los últimos años y también las amenazas cibernéticas, queda evidente que las herramientas de ciberseguridad son, y seguirán siendo, sumamente necesarias.

Es natural que surja este tipo de pensamiento, ya que una solución que debería ayudar a proteger los activos de las empresas fue responsable de causar uno de los mayores "apagones cibernéticos" de la historia. Pero no podemos dejar de añadir a esta ecuación cuáles serían los riesgos asumidos al no utilizar esta u otras herramientas de ciberseguridad.

Jonny López,

Consulting Sales Engineer – LATAM en Cradlepoint

Felix Lopez; Gerente de Ingeniería MAPS, menciona que este incidente pudo generar a algunas empresas dudas y llevarlos a cuestionar la confiabilidad de los productos de ciberseguridad. Sin embargo, es importante recordar que ningún sistema está libre de errores y que estos pueden ocurrir en cualquier tipo de software, incluyendo el software de seguridad. Considerando las miles de actualizaciones que se dan en todos los sistemas, incluyendo los de ciberseguridad, podemos esperar que los fabricantes de productos de ciberseguridad tomarán esto como una oportunidad de construir mecanismos más eficientes de validación para mantener o reforzar la confianza de sus clientes.

Marijus Briedis, CTO de NordVPN, asegura que este suceso podría servir de llamada de atención al sector. Es posible que veamos procedimientos de prueba más rigurosos, diversificación de las soluciones de seguridad y una mejor planificación de la recuperación en caso de catástrofe. Aunque puede haber algunos problemas de confianza a corto plazo, sobre todo para CrowdStrike, el incidente demuestra en última instancia la importancia de la ciberseguridad en nuestro mundo digital.

Es probable que las organizaciones se conviertan en clientes más exigentes, que demanden mayores niveles de fiabilidad y mejores salvaguardas. A largo plazo, esto podría conducir a prácticas de ciberseguridad más sólidas y resistentes en todos los ámbitos.

Jorge López, Vicepresidente para Latinoamérica de Tanium, afirma que este es un momento desafiante para muchos de nuestros clientes globales. Las organizaciones más innovadoras y preocupadas por la seguridad del mundo confían en Tanium porque hemos desarrollado una gestión de cambios disciplinada, segura y automatizada en todos los aspectos de nuestra solución para ayudar a prevenir interrupciones en las operaciones comerciales de nuestros clientes. Revisamos constantemente

David González,

Investigador de seguridad del laboratorio de Eset en Latinoamérica

todos los aspectos de nuestra postura de implementación y, considerando el incidente reciente, nos aseguramos activamente de continuar perfeccionando nuestros propios modelos de seguridad.

Rick Vanover, VP de Estrategia de producto de Veeam, añade que esta interrupción destaca las dependencias de las nubes públicas hiperescalables, Internet y más para servicios críticos líderes. En esta era de ofertas de software como servicio (SaaS) impulsadas en la nube; este es un riesgo que asumimos. En términos generales, los servicios de nube pública hiperescalables ofrecen mejor disponibilidad que la mayoría de las organizaciones pueden ofrecer en sus propias prácticas de centros de datos. Aunque un buen historial es reconfortante, es importante tener un proceso probado para manejar escenarios como este y disminuir las interrupciones comerciales.

Seguirá el crecimiento

Genetec explica que el crecimiento de la industria de ciberseguridad es consistente año tras año, así como el aumento del costo causado por el cibercrimen. En 2023, la inversión en ciberseguridad fue de 167 mil millones de dólares estadounidenses, mientras que el costo del cibercrimen fue de 8,1 billones. La previsión para 2024 es que las inversiones lleguen a los 183 mil millones de dólares, mientras que el costo del cibercrimen superará los 9,2 billones.

Para ponerlo en perspectiva, si el cibercrimen fuera un país, sería la tercera mayor potencia económica del mundo. Y estos indicadores no muestran señales de retroceder. Factores externos, como incidentes cibernéticos, continuarán afectando esta y otras industrias, pero el avance, tanto en volumen como en sofisticación de los ataques, en teoría, impide la retracción o incluso la desaceleración de las inversiones en esta área.

En el caso específico del apagón de CrowdStrike, el incidente puede incluso tener un efecto inverso, haciendo que más empresas busquen nuevas y diferentes soluciones de ciberseguridad, ya sean estas medidas tecnológicas, de gobernanza u otras.

Un ejemplo práctico de motivación para un aumento en este tipo de búsqueda podría ser el hecho de que agentes maliciosos han creado diversas campañas de phishing, promoviendo una falsa corrección para el problema, explotando el momento crítico y la conmoción causada para inducir al

usuario a instalar algún componente malicioso en su entorno. Además, se han mapeado al menos 27 dominios maliciosos registrados con el objetivo de estafar a los usuarios explotando este tema, ya sea ofreciendo una falsa solución o incluso prometiendo la corrección del problema.

Esto nos muestra que los adversarios son rápidos, están atentos y muy actualizados, lo que significa que no podemos, en ninguna circunstancia, bajar la guardia. Muy al contrario, es necesario fortalecer nuestras medidas de seguridad, ya sean físicas, administrativas o incluso tecnológicas.

David López Agudelo, vicepresidente de ventas USA/Latam de Appgate, afirma que hoy en día, donde todo es digital, este error que generó graves consecuencias, no hace más que reafirmar la importancia de soluciones confiables y que aseguren la continuidad de la operación, con todos los respaldos necesarios para que esto ocurra.

Por lo mismo, es fundamental que los CISOs estén presentes en los directorios de las empresas y en las más altas esferas de decisión, para que así una visión segura siempre sea puesta en la balanza a la hora de definir el rumbo de una entidad particular.

Para Cradlepoint, el hecho de que el crecimiento del mercado de soluciones de seguridad cibernética ha sido impulsado por la creciente digitalización y la imperativa necesidad de proteger datos y sistemas críticos, así como por la evolución de los ataques. Incidentes como éste subrayan la importancia de invertir en una estrategia de ciberseguridad robusta y pueden, paradójicamente, impulsar aún más el crecimiento del mercado al evidenciar la necesidad constante de innovar y mejorar.

Las empresas probablemente redoblarán sus esfuerzos y presupuestos en seguridad para evitar futuras vulnerabilidades. La ciberseguridad debe estar a la vanguardia de la planeación e implementación digital de las organizaciones.

De acuerdo con el estudio "State of Connectivity 2024 in Mexico" de Cradlepoint, muchos tomadores de decisiones empresariales mexicanos no están familiarizados con los últimos estándares de 'Ciberseguridad 2.0', más relacionados con la gestión de redes seguras e inteligentes que con los esquemas tradicionales de firewalls, lo que podría explicar porque menos del 40% de las empresas en México utilizan accesos de red bajo el principio de cero confianza (Zero Trust), y la adopción

Ueric Melo,

Security Awareness & Privacy Manager, Latin America and Caribbean de GENETEC

de tecnologías SASE (Secure Access Service Edge) aún está por debajo del 30%.

Sergio Navarro, Director de Preventa de IQSEC, dice que aunque una falla puede causar preocupaciones a corto plazo, el crecimiento del mercado de seguridad cibernética probablemente continuará. Los ciberataques son cada vez más sofisticados y frecuentes, lo que aumenta la demanda de soluciones de seguridad robustas. Este incidente subraya la importancia de invertir en ciberseguridad y puede incluso impulsar un crecimiento adicional a medida que las organizaciones buscan fortalecer sus defensas.

Para Fortinet, si el mercado ya traía una tendencia de crecimiento año con año, esto, sin duda, lo impulsará aún más. El hecho de que haya sido un caso que recibió tanta atención y cobertura, contribuye a que, como mencionaba antes, la gente sea más consciente, lo cual implica un crecimiento en esta área. Las empresas deben empezar a considerar a la ciberseguridad dentro de su estrategia de negocios, y definitivamente sucesos como este ayudan a resaltar su importancia en todos los ámbitos.

Fabio Assolini, director del Equipo Global de Investigación y Análisis para América Latina en Kaspersky, agrega que, a partir del posible rediseño en la infraestructura de seguridad de TI de las organizaciones, es probable que el mercado de ciberseguridad también se reconfigure para seguir creciendo pues, después de todo, es un sector crítico en un mundo cada vez más interconectado, donde las organizaciones están obligadas a protegerse.

Dentro de esta reconfiguración, podría aumentar el uso de servicios de seguridad multicloud por parte de las empresas, es decir, tener más de un proveedor de ciberseguridad en la nube o de forma híbrida, preferencialmente en distintas zonas geográficas, para mantenerse blindadas en caso de incidentes.

Para implementar esta estrategia, las compañías deberán incrementar sus presupuestos de ciberseguridad, lo que representará un reto, pero también una inversión redituable en el largo plazo.

Tener una amplia oferta de soluciones de ciberseguridad no sólo beneficia al mercado, sino que también eleva los niveles de seguridad de las empresas para evitar ciberincidentes. Los proveedores de ciberseguridad deberán esforzarse al

máximo para ayudar a sus clientes a responder de inmediato a cualquier incidente.

Como reacción de los clientes, destaca NordVPN, es posible que aumente la demanda de soluciones de varios proveedores y de redundancias. Las empresas podrían dudar a la hora de poner todos los huevos en la misma cesta, por así decirlo. En realidad, esto podría impulsar el crecimiento en algunos segmentos del mercado, ya que las organizaciones buscan diversificar su pila de seguridad.

Jorge López.

Vicepresidente para Latinoamérica de Tanium

También podría producirse un aumento de la demanda de soluciones de recuperación ante desastres y continuidad de negocio. El incidente de CrowdStrike ha puesto de manifiesto los puntos débiles de las estrategias de copia de seguridad de muchas organizaciones, lo que podría impulsar la inversión en este ámbito.

Para Tanium, después de cada incidente importante, los líderes recurren a sus equipos de TI con la pregunta: "¿Cómo podemos evitar que esto suceda?"; y debemos estar concientes de que los riesgos continuarán existiendo de diferentes maneras y la protección es actualmente más necesaria que nunca, es por eso que reiteramos la necesidad de que contar con una plataforma confiable para proporcionar información flexible, autónoma y en tiempo real debería ser un requisito clave en todos los entornos.

La plataforma debe tener salvaguardas incorporadas desde el diseño con una gestión de cambios rigurosa y los más altos estándares de control de calidad y, en ese sentido, la plataforma de Tanium proporciona el poder de la certeza: precisamente cuándo y dónde es más difícil encontrar esa certeza.

Por su parte, Andrés Cariño, Cloud Solutions Director en Oracle, afirma que no ve un impacto negativo en el crecimiento o la percepción generalizada de confianza del sector.

Dada el crecimiento constante de los ataques de seguridad que sufren las empresas alrededor del mundo, más que frenar el crecimiento, lo que ocasionan impactos como este; es un interés e intención por tener mayor conocimiento de estos temas y, por ende, continuar creciendo. En todo caso, el impacto puede afectar a un proveedor, pero impulsar a otro con capacidades similares.

Gustavo Valdez,

Director de General de Ikusi en México

Los cambios necesarios

Ricardo Villadiego, CEO & fundador de Lumu Technologies, comenta que las prácticas de seguridad que se deberían implementar en el futuro parten de tener el control de las operaciones como algo fundamental. Esto se logra entendiendo cómo están funcionando cada uno de los componentes de la estrategia de ciberseguridad, teniendo visibilidad completa que brinde certeza sobre el riesgo de terceros y eliminando la dependencia de fabricantes de tecnología, también conocido como platformization.

Siempre debe de existir un plan de ciber resiliencia, asegura Eset. No solamente se debe contar con un proveedor de servicios o en este caso de ciberseguridad, sino también otras alternativas. Lo que se ha visto es que muchas veces no hay compatibilidad entre diferentes marcas vendors y eso evita tener alternativas.

Contar con un plan C permitirá reforzar ese tipo de de prácticas de resiliencia, por ejemplo. Muchas veces se liberan parches y nos son probados, simplemente son lanzados en automático. Esto debe de pasar por una serie de pruebas en entornos bajos, para que, de existir una falla inmediatamente sea reportarla al vendor y corregirlo.

Esto ya debe de entrar dentro de las políticas de seguridad de cada una de las empresas. Lo siguiente también es tener una parte de capacitación y concientización hacia todos los empleados sin importar el nivel sobre las amenazas. La importancia de por qué actualizar los sistemas independientemente si son móviles o de escritorio. Tener una respuesta rápida sobre incidentes. También cuentan con una política de seguridad en actualizaciones. Finalmente, involucrar no solamente a los internos, sino también a los que están fuera, a los socios.

Para Akamai es importante que todas las empresas empiecen a cambiar su enfoque sobre la ciberseguridad, no deben preguntar si los van a atacar, deben de preguntarse cuándo los van a atacar, para siempre estar preparados, ser conscientes de que el riesgo siempre está presente.

Lo más importante en todas las organizaciones es la preparación ante cualquier situación, y la prevención activa de cualquier reto que pueda vulnerar los

sistemas. En Akamai, empleamos una combinación de sistemas automatizados avanzados y operadores humanos capacitados para abordar y resolver problemas que la automatización por sí sola no puede resolver.

Es así como contamos con un sólido marco de gestión de incidentes que aborda rápidamente los fallos. Este marco está diseñado para reducir significativamente el posible tiempo de inactividad. Contar con mecanismos de red que contengan posibles fallas es vital; por ejemplo, implementamos también estrategias para evitar problemas en cascada, lo que mantiene la estabilidad general y resiliencia de la red.

A su vez, Veeam agrega que es preciso ser consciente de qué servicios de nube pública de hiperescala se utilizan en una oferta que está poniendo como parte de su pila de servicios. Asegurarse de saber si algún servicio que se está utilizando está interrumpido y comunicarlo en consecuencia. Y, finalmente, preguntar si la empresa puede continuar con una interrupción prolongada. Si no puede, identificar qué alternativas deberían incrementarse para la cobertura.

Ikusi destaca lo esencial de que las empresas tengan visibilidad o lo que conocemos en el nicho como observabilidad de sus activos, para detectar, identificar y mitigar rápidamente riesgos y amenazas potenciales. Se deben adoptar estrategias de seguridad basadas en capas que incluyan medidas de prevención, detección y respuesta a incidentes, así como fomentar una cultura de seguridad dentro de la organización, asegurando que todos los empleados estén capacitados y conscientes de las mejores prácticas de ciberseguridad.

Asimismo, las auditorías de seguridad regulares y las pruebas de los controles de seguridad pueden ayudar a identificar debilidades antes de que sean explotadas.

Una de las prácticas que más recomienda Kaspersky para las empresas y proveedores de servicios de ciberseguridad es contar con una red de homologación, esto significa tener un ambiente aislado dentro de su infraestructura para probar las actualizaciones de cualquier solución de ciberseguridad, u otra herramienta de TI, e identificar si existe algún problema antes de que estas actualizaciones sean distribuidas a toda la empresa y, si es el caso, a la de su cadena de suministro; esto puede ayudar a reducir riesgos de algún fallo o amenaza de seguridad. De la misma

Sergio Navarro,

Director de Preventa de IQSEC

forma, en este tipo de entornos aislados, es posible analizar objetos sospechosos y detectar comportamiento malicioso para prevenir amenazas.

Para MAPS hay varias prácticas importantes a tomarse en cuenta como: Gestión de parches y actualizaciones: Es fundamental mantener todos los sistemas, aplicaciones y dispositivos actualizados con las últimas versiones y parches de seguridad, con un sistema de gestión que permita tomar acciones de reparación inclusive.

Realizar evaluación y gestión de riesgos: Las organizaciones deben realizar evaluaciones regulares de riesgos para identificar y abordar las vulnerabilidades en sus sistemas y redes. Esto incluye la realización de pruebas de penetración y auditorías de seguridad.

Tener un plan de respuesta a incidentes y recuperación: Las organizaciones deben tener planes de respuesta a incidentes y recuperación ante desastres. Esto incluye la identificación de los roles y responsabilidades durante un incidente de seguridad, la creación de un plan para la comunicación durante y después de un incidente, y la creación de un plan para la recuperación y la continuidad.

Implementar políticas de mínimos privilegios: Esta política implica dar a los usuarios y sistemas sólo los privilegios que necesitan para realizar sus tareas. Esto puede ayudar a limitar el daño a los equipos y sistemas. Al mismo tiempo, no debe tomarse como una receta, pues cada organización es única, por lo que es necesario adaptar estas prácticas a las necesidades específicas de cada una.

Para NordVPN la diversificación es crucial. Depender demasiado de un único proveedor o solución crea un único punto de fallo. Las empresas deben aplicar un enfoque de seguridad por capas, utilizando múltiples herramientas y proveedores para crear redundancia y reducir el riesgo.

Los procedimientos de prueba y despliegue son esenciales. Este incidente pone de relieve la importancia de los procesos de control de calidad, incluidas las pruebas A/B para las actualizaciones. Las organizaciones deben implementar despliegues escalonados para los sistemas críticos, lo que permite la detección temprana de problemas antes de que afecten a toda la infraestructura.

Hay que dar prioridad a la recuperación en caso de catástrofe y a la planificación de la continuidad de la actividad. Este incidente pilló desprevenidas a muchas organizaciones, revelando lagunas en sus estrategias de copia de seguridad. Es crucial comprobar periódicamente los planes de recuperación en caso de catástrofe: no hay que dar por sentado que funcionarán cuando sea necesario.

La mejora de los sistemas de supervisión y alerta podría ayudar a detectar problemas más rápidamente. Las organizaciones deben tener visibilidad en tiempo real del estado de sus sistemas y ser capaces de identificar y responder rápidamente a las anomalías.

Seguridad y nuevas tecnologías

Si bien la automatización promete rapidez para resolver problemas, también promete resolver de manera activa anomalías que puedan surgir, cuando se cuenta con personal capacitado para resolverlos de forma integral. Akamai afirma que sus nuevos sistemas están diseñados para autorrepararse y automatizar los procesos de recuperación, minimizando así la necesidad de intervención humana. Este enfoque garantiza una resolución rápida de problemas comunes y mejora la confiabilidad general del sistema. Y cuando existan incidentes que requieren de ejecución manual, intervienen operadores capacitados, guiados por procedimientos detallados que garantizan que los problemas se resuelvan de manera eficiente.

Por su parte, la inteligencia artificial, especialmente su capacidad de aprendizaje, irá reconfigurando lo que ya conoce y funciona como una herramienta importante para la evolución de las nuevas soluciones. La IA es una herramienta que puede mejorar el desempeño de los empleados y el servicio al cliente, mientras se mantiene la interacción humana. Marcos de IA responsables, capacitación de empleados y pautas transparentes son los principios que generan confianza. Akamai analiza continuamente los incidentes pasados para perfeccionar y mejorar sus estrategias de resiliencia. La empresa adapta de esta forma su enfoque en función de las amenazas y experiencias en evolución, garantizando que sus sistemas sigan siendo sólidos y confiables.

Para Fortinet, la automatización, como tantos otros fenómenos que van pasando en temas de tecnología, son herramientas que van creciendo, se van popularizando y se van utilizando cada vez más.

La automatización, como tal, requiere de muchos procesos y tiene que estar acompañada siempre de ciberseguridad, control, confianza y respuesta a incidentes. En realidad, no debería de afectar porque no es algo que se pueda parar, es algo que viene constante y se mantendrá así a futuro. Como decíamos antes, lo importante es que las empresas tengan ya esta consciencia

Ricardo Villadiego,

CEO & fundador de Lumu Technologies

y empiecen a incluir la ciberseguridad en sus procesos de automatización, implementación de nuevas tecnologías y procesos, etc.

La IA es un punto crucial en ciberseguridad y temas de respuesta a incidentes. Cada vez es más utilizada en el desarrollo de soluciones, actualizaciones y otros puntos vitales en el negocio, y va a seguir evolucionando para poder ayudar a los equipos técnicos a mantener las redes seguras, actualizadas, con los protocolos de seguridad al día, etc.

Ikusi dice que también es importante reconocer que, con el aumento de la automatización, surgen nuevos desafíos, como que las soluciones automatizadas sean bien diseñadas y probadas antes de su implementación.

La automatización debe ser vista como una herramienta complementaria y un proceso continuo que apoya a los profesionales de la ciberseguridad, permitiéndoles concentrarse en problemas más complejos y de mayor prioridad.

La confianza en la automatización se puede fortalecer mediante la implementación de prácticas sólidas de gestión de riesgos y una constante innovación en seguridad tecnológica.

Por su parte, la inteligencia artificial tiene el potencial de desempeñar un papel crucial en la mejora de la ciberseguridad. La IA puede ayudar a identificar patrones de comportamiento anómalos, detectar amenazas emergentes y responder a los incidentes de manera más eficiente.

Antes de la llegada de la IA, la detección y respuesta a amenazas cibernéticas solían depender en gran medida de los esfuerzos humanos, lo que a menudo resultaba en tiempos de respuesta lentos y una mayor exposición al riesgo.

La ciberseguridad es un componente esencial en la era digital y la protección de datos es una prioridad crítica para las empresas por lo anterior, es importante colaborar con expertos en ciberseguridad que ayuden a realizar pruebas y a establecer el plan de trabajo ideal.

A medida que la IA continúe evolucionando, su capacidad para predecir y prevenir ataques cibernéticos mejorará, proporcionando una capa adicional de protección, sin embargo, es importante seguir monitoreando y regulando el uso de IA para asegurar que se utilice de manera ética y efectiva.

A su vez, Genetec explica que existe la posibilidad de que haya una reducción en la confianza en los procesos automatizados de actualización. Sin embargo, las actualizaciones de sistemas, aplicaciones y firmware de dispositivos son fundamentales, ya que, además de ofrecer nuevos recursos y mejoras, también traen correcciones de fallos y vulnerabilidades.

Para equilibrar esta situación, existen algunos recursos que los usuarios pueden adoptar, como, por ejemplo, utilizar herramientas que permitan definir la priorización de parches de actualización.

De esta manera, solo las actualizaciones críticas con correcciones de fallos de seguridad se implementarían automáticamente el primer día, mientras que todas las demás actualizaciones quedarían en un área de "espera" por un período definido. Así, el usuario podría interrumpir el proceso automático de actualización en caso de una falla generalizada, como la que ocurrió el pasado día 19. Si no se toma ninguna acción al final de ese período, la actualización se instalaría automáticamente.

Nord VPN concuerda en que este incidente puede hacer tambalear cierta confianza en la automatización, especialmente en la ciberseguridad. Muestra cómo una pequeña actualización automatizada puede causar rápidamente problemas generalizados. Pero la automatización sigue siendo crucial para responder rápidamente a las amenazas, así que no podemos abandonarla. En su lugar, es probable que veamos esfuerzos para hacer que la automatización sea más inteligente y segura.

Las empresas podrían empezar a lanzar actualizaciones de forma más gradual, mejorar sus sistemas para detectar comportamientos inusuales y contar con una mayor supervisión humana. El objetivo es mantener la velocidad y la eficacia de la automatización al tiempo que se reduce el riesgo de fallos a gran escala. Al final, lo más probable es que este acontecimiento nos empuje a perfeccionar nuestros sistemas automatizados en lugar de alejarnos de ellos.

Sin embargo, la automatización en ciberseguridad ofrece muchos beneficios, incluyendo la capacidad de responder rápidamente a los incidentes de seguridad, agrega MAPS.

Aunque, como cualquier tecnología, la automatización no está exenta de riesgos, aunque este incidente puede haber afectado la confianza en la automatización, no necesariamente significa que la automatización sea por definición insegura o poco fiable. Con las estrategias de gestión de riesgos adecuadas, la automatización puede seguir desempeñando un papel esencial en la mejora de la eficiencia y eficacia de la ciberseguridad.

De la misma forma, la Inteligencia Artificial (IA) tiene un gran potencial para mejorar la ciberseguridad en las PC, servidores y redes. Sin embargo, recordemos que la IA no es una solución mágica para todos

Felix Lopez,

Gerente de Ingeniería MAPS

los problemas de ciberseguridad. Aunque la IA puede ser una herramienta valiosa, también es esencial contar con políticas y prácticas de seguridad sólidas, y un equipo de seguridad bien formado y equipado. Además, como cualquier tecnología, la IA también puede ser susceptible a errores y vulnerabilidades, por lo que es importante utilizarla de manera responsable y con una comprensión clara de sus limitaciones.

Tanium dice que las organizaciones deben preparar sus entornos para lo inesperado. Invertir en herramientas que respalden una respuesta dinámica y extensible aumentará la resiliencia frente a errores y fallas inesperadas.

Tener una plataforma confiable y de misión crítica con la capacidad de proporcionar información flexible, autónoma y en tiempo real debería ser un requisito clave en todos los entornos ya que a medida que el negocio cambia constantemente, también lo hace la necesidad de que la TI y la seguridad evolucionen con él. Estamos mejorando la plataforma Tanium XEM con la introducción de Gestión Autónoma de Terminales (AEM por sus siglas en inglés). Tanium AEM mejorará la plataforma central de Tanium con un conjunto de características distintivas que transforman la forma en que los equipos de TI y seguridad deciden y ejecutan cambios de forma segura en su entorno, a escala y en tiempo real.

Contar con una plataforma confiable y de misión crítica con la capacidad de proporcionar información flexible, autónoma y en tiempo real, debería ser un requisito clave en todos los entornos. Independientemente de qué protección de endpoints o solución EDR se utilice, las organizaciones más sofisticadas y conscientes de la seguridad implementan la plataforma Tanium XEM como elemento fundamental de un enfoque de defensa en profundidad.

Al final, la automatización de los procesos es un fenómeno inevitable y con muchas más virtudes que defectos, dice Appgate. En ese sentido, la confianza en la misma no debería verse afectada por un incidente en particular.

Asimismo, la Inteligencia Artificial (IA) asoma como un aliado fundamental en

la ciberseguridad de acá en adelante, si es que se utiliza de buena manera. Se espera que haya una mayor sofisticación y precisión en cuanto a ataques, por lo que Appgate cree necesario tener una postura proactiva en la implementación de medidas de ciberseguridad, que aprovechen tecnologías como la IA y tengan el respaldo de tecnologías como Zero Trust Network Access (ZTNA), lo cual ayudará a prevenir todo tipo de ataques de manera integral.

Sergio Navarro, Director de Preventa de IQSEC, también comenta que la automatización es una herramienta poderosa para mejorar la eficiencia y la rapidez en la respuesta a incidentes de seguridad. Pero debe implementarse con cuidado y supervisada adecuadamente. La confianza en la automatización puede mantenerse alta si las organizaciones aseguran que sus soluciones automatizadas son robustas, confiables y complementadas con la supervisión humana.

La IA puede ayudar a predecir y prevenir ataques antes de que ocurran, mejorar la detección de anomalías y proporcionar análisis de riesgos más precisos. Sin embargo, es crucial mejorar y actualizar los algoritmos para enfrentar nuevas amenazas emergentes. Pero, particularmente, en el caso de un fallo de actualización, la IA podría ayudar poco, pues cuando un error humano es el que produce el incidente, probablemente la IA lo considere normal.

Para Oracle la automatización y la seguridad cubren necesidades complementarias en la agenda de TI. Ambas son necesarias, porque ayudan a tener una operación más ágil. En este sentido, el paso a seguir es reforzar las precauciones y el control sobre las herramientas y, particularmente, sobre la orquestación que se ejecuta, para conocer el impacto de las mismas en el ecosistema de TI.

La IA ya se implementa en cierto grado o forma en todos estos rubros, brindando un apoyo importante para su correcto funcionamiento. La IA es una tecnología que sigue evolucionando y que seguramente cada vez más podrá apoyar en la resolución de problemas de este tipo, sin embargo, siempre es importante contar con un equipo de seguridad bien conformado, que cuente con las habilidades y conocimientos necesarios para, en conjunto, potencializar el resultado.

Lumu concuerda en que la automatización no es mala; por el contrario, permite lograr eficiencias y enfocar a los equipos en tareas que agreguen más valor para las organizaciones. Los ciberdelincuentes no tienen miedo de automatizar sus ataques, lo que genera problemas es no tener control y visión estratégica de lo que se quiere automatizar. En ciberseguridad el tiempo es vital, los líderes de de la operación están buscando automatizar cada vez más tareas de la operación porque

Marijus Briedis,

CTO de NordVPN

les permite ser ágiles frente a las amenazas en constante evolución, pueden medir más fácil los resultados de la estrategia y pueden desarrollar el talento reduciendo la cantidad de procesos manuales y fatiga por tareas repetitivas.

La IA ya es parte de nuestro día a día desde hace varios años, ya está integrada en los dispositivos de uso diario. Lo que realmente hace la diferencia en ciberseguridad es darle un uso estratégico, como por ejemplo, facilitar la cacería de amenazas, automatizar tareas de operación de ciberseguridad, reducir los tiempos de respuesta ante incidentes, identificar a tiempo el riesgo cibernético que un tercero o proveedor puede insertar en una organización e incluso, facilitar la orquestación de herramientas de defensa e incluso detectar problemas de compatibilidad a tiempo.

Lo aprendido hacia el futuro

Para MAPS el incidente con CrowdStrike ofrece varios puntos importantes a considerar para las empresas:

1. Pruebas de calidad: Antes de lanzar cualquier actualización o nuevo software, es crucial realizar pruebas exhaustivas para identificar y solucionar cualquier problema potencial. Esto puede ayudar a prevenir incidentes que puedan afectar a los usuarios.

2. Planes de respuesta a incidentes: Tener un plan de respuesta a incidentes bien definido puede ayudar a las empresas a manejar eficazmente cualquier problema de seguridad que surja. Esto incluye tener procedimientos claros para la identificación, contención, erradicación y recuperación.

3. Capacidad de Resiliencia y recuperación: Los incidentes de seguridad pueden ocurrir, incluso con las mejores medidas de protección. Por lo tanto, es importante que las empresas tengan planes de recuperación para restaurar rápidamente después de un incidente.

4. Inversión en seguridad: Este incidente subraya la importancia de invertir adecuadamente en seguridad. Esto no sólo incluye la inversión en tecnologías de

seguridad, sino también en la formación del personal, en la creación de una cultura de seguridad y en la implementación de políticas y procedimientos de seguridad adecuados.

Este incidente puede verse como una oportunidad de aprendizaje para mejorar las prácticas de seguridad y la resiliencia de las empresas.

Fortinet agrega que nadie está exento de este tipo de problemas, todos corremos el riesgo de que el negocio quede fuera por algún tipo de error en los sistemas.

En segundo lugar, los sistemas almacenan cantidades enormes de información, y a veces no sabemos ni qué es exactamente lo que está almacenado o en dónde.

Por ende, las empresas deberían contar con un inventario de activos digitales que les permita tener un control de qué información están almacenando, en dónde está cada cosa guardada, qué es lo que se necesita respaldar y qué áreas o datos importantes podrían no estar bien protegidos para poder tomar acciones sobre ello.

Aunado a lo anterior, con base en este análisis es importante que las empresas definan qué pasa si algo deja de funcionar, cuáles son las pérdidas potenciales, cuánto podría sostener su operación en caso de alguna falla, y qué es necesario respaldar.

Es importante, como he mencionado en puntos anteriores, contar con un plan bien estructurado de respuesta ante incidentes, qué vamos a hacer si pasa, cómo lo vamos a tratar, cómo y en cuánto tiempo podríamos regresar a la normalidad.

Al final, hay que entender que probablemente no nos estamos sentando a analizar lo valioso que tenemos en nuestros sistemas, todos los datos que sostienen el negocio, cómo estar mejor protegidos y qué hacer ante algún tipo de incidencia.

Ante esto, es necesario que las compañías que no lo están haciendo empiecen a enfocar su atención en la parte de ciberseguridad, incluyéndola en su estrategia de negocio a través de un plan integral que incluya tecnología y educación, y capacitación para cada miembro de la organización; sea parte del equipo técnico o no.

Para Ikusi, se debe enfatizar la importancia de la colaboración y la transparencia en el manejo de incidentes de seguridad, asegurando que la información relevante se comparta rápidamente para mitigar daños.

También deben invertir en la capacitación continua para mantenerse al tanto de las amenazas y tendencias emergentes, así como adoptar un enfoque proactivo, no solo reaccionando a incidentes, sino también

Andrés Cariño,

Cloud Solutions Director en Oracle

anticipándose a posibles amenazas y desarrollando estrategias para enfrentarlas.

De igual forma, entender la necesidad de una integración más profunda entre la IA y la automatización en las soluciones de seguridad implementadas de manera responsable y ética. Asimismo, es fundamental mantener un enfoque centrado en el cliente, asegurando que las soluciones de seguridad sean accesibles, comprensibles y fáciles de implementar para todas las organizaciones.

Genetec dice que una lección importante que deben aprender todas las empresas que desarrollan tecnología es que las herramientas son solo una parte de cualquier solución.

Es muy importante que un desarrollador tenga procesos muy claros y bien definidos, robustos, probados y validados periódicamente para minimizar el riesgo de que fallas como esta sean publicadas e implementadas en producción sin ser identificadas en ninguna de las etapas del proceso de desarrollo, como la verificación del código, el control de calidad, las pruebas en un entorno controlado.

Además, todos los componentes de la cadena de suministro deben poseer políticas de seguridad estrictas, tanto internas como para todos sus proveedores. Esta política debe garantizar que los procedimientos mencionados anteriormente sean cumplidos por todas las partes involucradas.

Otra medida importante es la ejecución de auditorías a estos proveedores para validar que todas las reglas acordadas estén realmente siendo cumplidas y bien ejecutadas.

De igual forma, como cualquier proceso, es muy importante seguir un ciclo de mejora continua, revisando las políticas y procesos de auditoría frecuentemente y aplicando correcciones y mejoras siempre que sea necesario.

En este tipo de escenario, especialmente donde las tecnologías (y las amenazas) evolucionan a una velocidad exponencial, es vital que cualquier documento que defina políticas, reglas o procesos sea un documento vivo, multidisciplinario y que pueda seguir el ritmo de esta evolución.

Para Cradlepoint, las empresas de ciberseguridad y de cómputo deben

aprender la importancia de la resiliencia y la adaptabilidad. Este tipo de eventos resaltan la necesidad de:

1. Implementar soluciones integrales: Que combinen diversas capas de seguridad para proteger contra una amplia gama de amenazas.

2. Mantener un enfoque de prevención de amenazas avanzadas y de Día Cero tanto en perímetro extendido como en la dorsal del centro de datos.

3. Alinear la estrategia a las mejores prácticas: Implementar metodologías que involucren personas, tecnología y procesos ajustados a la realidad y capacidades de cada organización, esto implica contar con protocolos de atención y mitigación de incidentes, planes de recuperación y continuidad del negocio.

4. Mantener la transparencia: Comunicar abiertamente sobre las vulnerabilidades y los pasos tomados para resolverlas.

5. No omitir ningún paso: Por más obvio que parezca, y por más confianza que se tenga en el equipo y/o en los procesos, cumplir a cabalidad con los protocolos de prueba, controles de cambios antes de sacar a producción cualquier producto, plataforma o sistema de información; esto reducirá la posibilidad de cometer errores.

6. Fomentar la colaboración: Trabajar estrechamente con otras empresas y organismos reguladores para compartir información y mejores prácticas.

7. Invertir en innovación continua y educación: Permanecer a la vanguardia tecnológica para anticiparse a las nuevas amenazas.

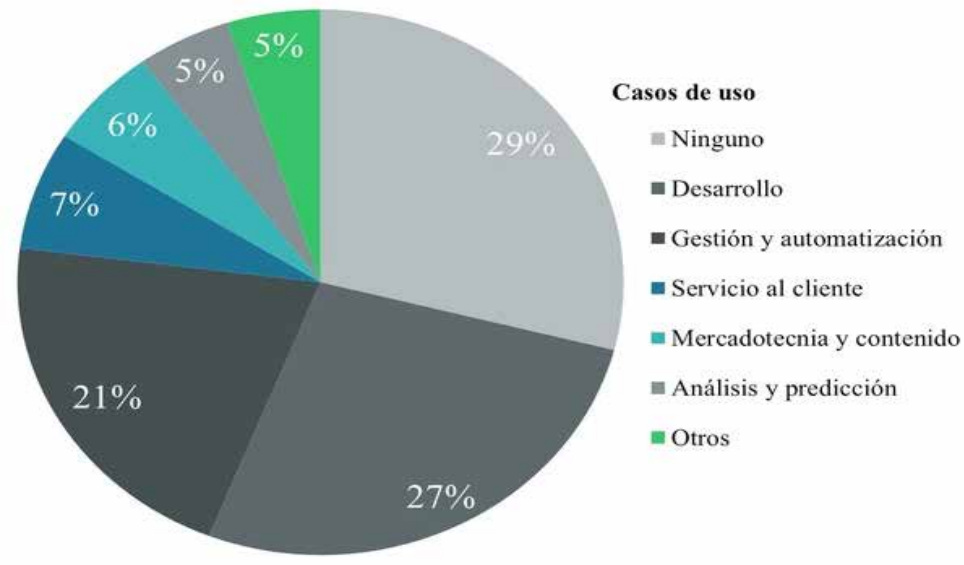
Finalmente, Tanium vaticina que el mundo de la tecnología aprenderá mucho más en las próximas semanas y meses. Tras este error se continuará informando las mejores prácticas de entrega de software y se mejorarán los programas de investigación, innovación y desarrollo, para ayudar a prevenir interrupciones en las operaciones comerciales de los clientes, así como perfeccionando los modelos de seguridad.

Cómo ESCALAR el valor de la IA al negocio

La IA generativa es una "arma de doble filo" su facilidad de uso estimula la generación de múltiples casos en organizaciones, sin embargo, sin una gestión de datos adecuada no sólo no se generaliza el impacto, sino que puede ser nociva para el negocio.

Se multiplican los casos de uso

Los casos de uso de la IA en la industria TIC mexicana se están generalizando, tanto para uso interno como para ofrecer soluciones al cliente. En un sondeo reciente con empresas de TIC, los participantes destacan el desarrollo de código y la gestión y automatización de operaciones como los más frecuentes, muchos basados en herramientas de IA generativa



Sin embargo, a pesar de todo el entusiasmo que se ha desatado en la industria TIC, alrededor de un tercio de las empresas aún no utilizan inteligencia artificial al interior de su empresa o para apoyar a sus clientes.

Impacto y factores que lo determinan

La evidencia de una contribución significativa al negocio de los casos de uso de la IA generativa en el mundo es escasa. McKinsey destaca que sólo 15% de las compañías encuestadas indicaron que el uso de IA generativa ha generado un impacto significativo en las utilidades de sus empresa.

En otro sondeo reciente con la industria mexicana de TIC realizado por Select, 43% de los participantes señalaron que han experimentado poco o ningún impacto de la IA en las organizaciones. Sin embargo, existe un grupo pequeño pero importante de empresas que han experimentado impactos positivos de la IA en la productividad, la atención, experiencia y aseguramiento de la calidad para el cliente, la optimización de procesos

y en el uso de redes sociales para promocionar productos y servicios.

En ese mismo sondeo, las empresas subrayan que el costo, la carencia de casos de uso específicos, la falta de interés y la disponibilidad de datos de calidad son los factores que determinan el bajo impacto de la IA en las organizaciones.

Recomendaciones estratégicas

El valor potencial del uso de la IA es enorme, pero para capturarlo es necesario que la industria TIC apoye a sus clientes a elevar la escala y operar continuamente los casos de uso.

El surgimiento de IA generativa está forzando a lideres empresariales a rediseñar sus estrategias y plataformas de datos; aquellos que tengan éxito en esta tarea lograrán maximizar el valor monetario, tanto al negocio del usuario como al negocio de los integradores.

Por ejemplo, datos continuos sobre la experiencia integral del cliente a lo largo de sus interacciones con una empresa son cruciales para mejorarla, pero difíciles de desarrollar y actualizar. Por ello, es necesario fortalecer las capacidades de orquestación, automatización y facilidad de uso de los datos y mantenerlos incorruptibles (MLOPs).

De la literatura5 hemos sintetizado una serie de recomendaciones estratégicas que los integradores y usuarios deben seguir para elevar la contribución al negocio de la IA y en particular de la IA generativa:

- Enfocarse en aplicaciones de impacto y viables
- Orquestar interacciones con fuentes de datos e integrar operaciones para escalar
- Anticipar costos: gestión del cambio y operación son los mayores
- Controlar proliferación de herramientas; escoger la del aliado en la nube
- Crear equipos que generen valor no sólo modelos
- Seleccionar los datos correctos no los perfectos
- Usar herramientas6 para mejorar, catalogar, etiquetar y definir interrelaciones
- Reusar código para acelerar desarrollo y crear una plataforma transversal
- Escalar IA con seguridad: estándares y mejores prácticas de codificación

Conclusiones

Los casos de uso de la IA en la industria TIC mexicana se están generalizando, tanto para uso interno como para ofrecer soluciones al cliente; sobre todo la IA generativa. Sin embargo, la evidencia de su contribución a las utilidades de un negocio es aún limitada. Muchas empresas de la industria TIC en México señalaron que no han experimentado ningún tipo de impacto de la IA. Para escalar el impacto de la IA, los integradores y sus clientes deben fortalecer las capacidades de orquestación, automatización y facilidad de uso de los datos y mantenerlos incorruptibles.

EL USO RESPONSABLE DE LA IA

Ni negro, ni blanco — como todo en esta vida, el panorama de la IA está teñido de grises y de matices. Es entonces justo allí, en medio de todas aquellas tonalidades, que sale a relucir el humanismo tecnológico, buscando adornar el paisaje con pinceladas de justicia y de moral. Después de todo, un gran poder siempre conlleva a una gran responsabilidad.

No perdamos el rumbo. Basta ya de cuestionarnos si la Inteligencia Artificial es "buena" o "mala", "protagonista" o "antagonista".

No demos un salto al vacío

En ocasiones, como generación, nos resulta difícil dimensionar las proporciones de aquellos eventos históricos en los que estamos inmersos, aquellos de los cuales formamos parte. Pero lo cierto es que, ante el galopante avance de la IA, el mundo está por experimentar acelerados cambios a un ritmo vertiginoso que no se veía desde el despliegue de la imprenta, hace ya más de seis siglos. Ante el alboroto tecnológico, la UNESCO ha liderado valiosos esfuerzos a fin de garantizar que la ciencia y la tecnología se desarrollen dentro de un marco ético.

Entender y, más que nada, regular hasta dónde llega el límite de aquella delgada línea en la que como humanidad nos balanceamos entre lo correcto y lo incorrecto, es responsabilidad de todos. Particularmente, las grandes corporaciones tienen la obligación moral de calibrar su llamada brújula ética en función de adquirir mejores prácticas en el uso de las nuevas tecnologías, adhiriéndose a estrictas regulaciones en materia de protección de datos y del derecho a la privacidad.

Encontrar el norte en dirección a un mundo más inclusivo, sostenible y pacífico a partir del buen uso de la IA es una tarea loable, pero compleja (complejísima). Si me lo preguntan, aquella brújula debería siempre apuntar a un uso tecnológico que, en medio de su afán por afinar y automatizar procesos, no comprometa la privacidad, la reputación ni la dignidad de las personas.

Bien dijo Maite López Sánchez, profesora de la Universitat de Barcelona y coordinadora del máster interuniversitario de inteligencia artificial que "la transparencia y el respeto a la privacidad son cualidades que solemos exigir a las instituciones públicas, pero con frecuencia olvidamos pedírselos también a quienes desarrollan algoritmos".

Si bien los avances en materia de IA han sabido acelerar y perfeccionar procesos y tareas diarias -desde facilitar diagnósticos médicos hasta posibilitar comunicaciones más personalizadas y eficaces entre las empresas y sus consumidores-, ya estamos lo suficientemente viejos como para saber que no todo lo que brilla es oro. No por nada, en los más recientes años, han salido

Janeth Rodríguez,
VP Revenue Latam de Infobip

a flote diversos y profundos dilemas éticos que nos han invitado a reflexionar antes de saltar al vacío.

Algoritmos que sesgan

Así es, la IA tiene el potencial de reproducir nocivos prejuicios y sesgos y de exacerbar desigualdades latentes. Basta con realizar una rápida búsqueda en Google para darse cuenta del poder que yace tras la automatización y el sesgo del conocimiento. Hagan el ejercicio. Escriban "cuáles son los mejores líderes mundiales" en su motor de búsqueda predilecto y verán cómo su pantalla se inunda de golpe de fotografías de hombres.

Ahora escriban en su buscador "colegialas" y comparen los resultados versus el término "colegiales"; seguramente su primera búsqueda les arrojará imágenes sexualizadas de adolescentes con diminutas faldas, mientras que la segunda les mostrará estudiantes comunes y corrientes. Indudablemente, el uso de los algoritmos representa un riesgo real de reforzar estereotipos de género. Cabe resaltar que lo mismo aplica para sesgos étnicos, raciales y de todo tipo.

Para estas alturas, creer que la tecnología es imparcial resulta un tanto ingenuo. La realidad es que los motores de búsqueda procesan macrodatos priorizando aquellos resultados con una mayor cantidad de clics.

Ya habiendo dicho esto, visto desde un ángulo constructivo, si bien tanto las personas como la IA contribuyen a alimentar sesgos de diversa índole, la IA también tiene el potencial de corregir y de reversar encasillamientos mandados a recoger. Como siempre, la respuesta está en las manos de las personas que hacen uso de las tecnologías.

Educación desechable

Como madre, muchas veces me cuestiono acerca de las profundas implicaciones que tendrá todo este auge tecnológico en el futuro de los jóvenes en época de escolaridad. Y es que, lastimosamente, nos estamos enfrentando a una generación de estudiantes propulsados por un dañino plagio digital que, además de ser instantáneo, muchas veces resulta inexacto.

Tal es el caso de ChatGPT, una IA revolucionaria y prometedora que puede

jugarnos a favor o en contra por extraer contenido de diversas fuentes, fidedignas y dudosas, para arrojar respuestas que en ocasiones no hacen otra cosa más que divulgar la desinformación. Pero, ojo, no me malinterpreten, soy fiel creyente de que aquellos profesionales que se resistan a montarse en la ola de estas nuevas tecnologías inevitablemente terminarán por naufragar. El arte está en saber navegar dicha ola con gracia, estilo y -claro- ética.

Ni todo rosa, ni todos espinas

A la lista de desafíos éticos que he mencionado se le suman muchos otros, como lo son los dilemas en materia de propiedad intelectual y derechos de autor; impactos significativos en el territorio de las artes y la creatividad humana; prácticas invasivas de vigilancia ("Big Brother is watching you"), entre muchos otros. Pero, entonces ¿qué hacemos? Taparnos los ojos y echarnos a llorar no es una opción.

La óptica lo es todo. ¿Qué tal si, por ejemplo, en lugar de enfocar nuestra crítica hacia todos los trabajos que, potencialmente, podrían desaparecer y ser reemplazados por la IA, nos concentramos en explorar todos aquellos nuevos roles que podrían surgir a partir de ella? Y es que, si lo piensan, muchos de los cargos actuales (esos mismos de los que hacemos alarde en nuestros perfiles de LinkedIn) ni siquiera existían hace una o dos décadas. Sí, el cambio asusta, es normal, pero no por eso debemos paralizarnos.

Tech for Good, calibrando nuestra brújula

El concepto de Tech for good surge entonces como esa luz esperanzadora que, además de prometer eficiencia, reducción de costos y autonomía, pone sobre la mesa nuestra escala de valores y nuestra humanidad misma.

Desde mi rol como VP de Revenue para LATAM en Infobip, he podido ser testigo de primera mano de cómo la tecnología puede impactar positivamente en la vida de las personas, actuando como catalizadora en temas de inclusión y dignidad humana.

Muchas veces me he visto conmovida por casos de éxito que respaldan nuestras soluciones, pero también nuestra esencia. Tal fue el caso, por ejemplo, de Redes da Maré, la organización gubernamental brasilera que con la ayuda de Infobip pudo reforzar y automatizar un programa de protección alimentaria, distribuyendo canastas alimentarias a 40 mil familias en las favelas de Maré durante la pandemia. Y ni qué decir de Unicef, a quienes ayudamos a reducir el abandono de donantes en un 33% mediante un uso inteligente de nuestras tecnologías.

Una aliada, no una enemiga

Resistirnos al cambio únicamente nos hará nadar a contracorriente. No hay vuelta atrás. La IA ha llegado, ha tocado a nuestras puertas y se ha sentado a la mesa — en nuestras manos está darle una buena lección de modales.

Más poderoso

Eaton Power Xpert 9395P

200 - 1200 kVA

UPS doble conversión, diseñado para mantener energía estable, ininterrumpida y limpia.

EATON

Powering Business Worldwide

Solicita más información:

AlejandroALavin@eaton.com

CELEBRA

45 AÑOS

INGRAM MICRO®