EL INDICADOR

EDICIÓN Nº 17 · MAYO DE 2025
ISSN 2500-7955

¿Qué tanto estas preparado para enfrentar LA SEGURIDAD CIBERNÉTICA en tu empresa en este 2025?

UNA PUBLICACIÓN DE
BKF INTERNATIONAL
¡Comprometidos con el crecimiento empresarial!

BKF.COM.CO

Álvaro Enrique Chacón M.,
CISA, CDPSE, CSXF, CFC
Director Auditoría TI -BKF INTERNATIONAL

¿Qué tanto estas preparado para enfrentar la seguridad cibernética en tu empresa en este 2025?

El avance dinámico de la tecnología, el surgimiento de nuevas herramientas y la facilidad cada vez mayor para ser asequibles para quien requiere de ellas, deja expuesto y no se puede negar al surgimiento también de nuevas vulnerabilidades. Es aquí donde si usted se pregunta, ¿Si la tecnología continuará evolucionando vertiginosamente, entonces cuando será el declive de las amenazas emergentes?

Hoy por hoy escuchamos acerca del surgimiento de amenazas y ataques cibernéticos a diferentes entidades en el mundo, sin discriminar tamaño, complejidad o industria, vemos de frente como estos han conllevado a la discontinuidad de las operaciones de negocio, comprometiendo en consecuencia la reputación, confianza y la sostenibilidad a la cual estaban y venían acostumbradas estas entidades involucradas. No es de desconocer la gravedad de estas situaciones, máxime cuando se puede ver comprometida la economía de una región o industria.

Ahora bien, si a la fecha muchas de las organizaciones cuentan con medidas o procedimientos internos para dar tratamiento a estas amenazas, algunas otras con el acompañamiento de expertos que prestan el servicio para establecer las medidas de contención, en cuanto a la prevención, detección (monitoreo) y corrección de cara a las ciberamenazas, el lucro que viene en crecimiento para las organizaciones criminales que se ocupan de generar este tipo de amenazas, no se detiene ni se detendrá, por lo cual deberán las organizaciones en adelante convivir y concebir con más firmeza, y agilidad en sus planeaciones estratégicas como algo que llegó para quedarse.

El avance dinámico de la tecnología, el posicionamiento cada vez mas fuerte de la Inteligencia Artificial (IA) y el alcance a ella, así mismo el surgimiento de nuevas herramientas y la facilidad cada vez mayor para ser asequibles para quien requiera de ellas, deja expuesto y no se puede negar al surgimiento también de nuevas vulnerabilidades. Es aquí donde si usted se pregunta, ¿Si la tecnología continuará evolucionando vertiginosamene, entonces cuando será el declive de las amenazas emergentes? Pues la respuesta lastimosamente no será asoluta, tengo una buena noticia y otra no tan buena para usted. La buena noticia está que la nueva tecnología traerá nuevas y mejores soluciones para asistirnos en el atender estas adversidades de una manera más simple, sofisticada y previsible. La noticia no tan buena es que las ciberamenazas llegaron y estarán presentes para quedarse; por tanto, deberemos hacernos a procedimientos, normas o estándares nuevos, muy diferentes a los que seguramente tenemos en nuestro inventario y estructura organizacional.

¿Reconoces algunos de los siguientes?
Incorporar la experiencia en ciberseguridad a nivel de la Junta Directiva, permitiendo trascender de una postura netamente reactiva a una defensa proactiva,
- Contar con personal capacitado para enfrentar el reto y contener estas adversidades al margen, un Staff certificado, o terceros que en calidad profesional de expertos presten el servicio de ciberseguridad,
- Campañas cada vez más fuertes para sensibilizar a los funcionarios y usuarios de la organización,
- Incurrir en nuevos costos al presupuesto a nivel organizacional y no solo de TI,
-Endurecimiento (Hardening) en hard-

ware que guarde la robustez en configuración, almacenamiento y memoria, por cuanto demandará un mayor procesamiento concurrente de hilos en CPU, - Un software a modo de agente utlitario que tenga presencia en las instalaciones de servidores que gestionan información Core de negocio, el cual esté vigilante y configurado de cara al tratamiento de posibles vulnerabilidades. Algunas de estas herramientas conocidas son por ejemplo, IDS (Intrusion Detection System) o IPS (Intrusion Prevention System), que alertan a la central usuaria ante posibles eventos de riesgos, - Contar con mecanismos para el monitoreo automático permanente en la identificación de posibles amenazas, salientes como entrantes, y recurso humano que las clasifique y dé tratamiento, - Un programa de auditoría que tenga en su agenda la evaluación a los asuntos asociados a los mecanismos de prevención y detección instalados, - Contar con procedimientos alternos de contingencia "probados", es muy importante se pueda dar fe de ello.

Aun cuando muchos de los puntos anteriores nos suenen y parezcan conocidos, y que además parecieran ser suficientes, aunque mitigan de manera importante la exposición a posibles riesgos asociados al ciberespacio entre otros, para el 2025 vienen nuevos retos, debido al surgimiento de nuevas tecnologías aplicadas en este ámbito; varias de ellas impulsadas por la Inteligencia Artificial como seguramente ya se podía suponer. Algunas otras igualmente muy sofisticadas y de las cuales prometo tratarles de una manera simple en otro artículo, vienen relacionadas con las Interfaces de Programación de Aplicaciones, mejor conocidas como las API, las cuales no guardando una debida configuración se prestan para la posible extracción de datos y por si fuera poco, lo que se viene es todavía mas interesante como es el cifrado poscuántico.

Para esta ocasión sin embargo será importante reconocer algunas de las tendencias (sin ser las únicas en la actualidad) que debemos tener presente y en nuestro radar por supuesto, puede ser iniciando con las que esten a mejor alcance; lo cual ya auguraría un buen comienzo para implementar una ciberdefensa mas robusta, inteligente y proactiva.

1.Inteligencia Artificial (IA) y Aprendizaje Automático (ML): Estas tecnologías estarán contribuyendo cada vez más a la transformación de la ciberseguridad, donde sus algoritmos serán capaces de procesar grandes volúmenes de información. En consecuencia, producto de este volumen diverso de información estructurado o no, tendrán además la capacidad de analizar cada uno de los datos en tiempo real. Es aquí donde la respuesta automatizada a incidentes impulsada por el aprendizaje automático (Machine Learning) dotará a las organizaciones de la capacidad de responder a las amenazas con una rapidez sin precedentes, detectando patrones y anomalías que pudieran significar una amenaza potencial.

Es así como en conjunto con la IA nos ayudará a detectar, evadir o neutralizar las amenazas, pasando de medidas reactivas a estrategias proactivas, gracias a la detección de anomalías en tiempo real, la autenticación inteligente y la respuesta automática para dar tratamiento a posibles incidentes. Sin embargo, no todo es tan bueno, del otro lado veremos amenazas más sofisticadas e inteligentes impulsadas también por la IA, lo cual abarcará desde intentos de Ingeniería Social, Deepfake, hasta Malware automatizado que se adaptará de manera inteligente para eludir la detección. En este caso será muy importante estar al tanto de las últimas técnicas utilizadas con la IA y el disponer de medidas de seguridad más avanzadas, lo cual será esencial para evitar consecuencias mayores.

2. Privacidad de los datos: Según Garner estimó que para el 2024, aproximadamente el 75% de la población mundial iba a tener sus datos personales protegidos por normas de privacidad. La importancia de la privacidad de la data seguirá creciendo y será una inminente necesidad para que las organizaciones creen nuevos diseños, procedimientos y cuenten con instalaciones cuyo foco principal será el blindar la data sensible y la información que pudiera derivar de ella para quienes seamos los usuarios, tantos externos como internos. Según Garner, se prevé que el gasto en privacidad de datos registrará la mayor tasa de crecimiento en el presente año, por lo que se espera sea al interior de las organizaciones una prioridad de primer orden.

Desde lo que fue en el 2024 y será en adelante, está claro que la privacidad de los datos desempeñará un papel cada vez más fuerte y claro en el ámbito de la ciberseguridad. A medida que estas tendencias siguen evolucionando, incumbe a que las organizaciones deban mantenerse bien en alerta e informadas, ante el muy posible surgimiento de regulaciones en este ámbito. Las organizaciones deberán realizar auditorías periódicas para asegurarse de que cumplen todas las leyes pertinentes sobre privacidad de datos.

3. Arquitectura Zero-Trust: Este enfoque de seguridad cobrará mayor relevancia cada vez, donde su propósito principal reposará en no establecer ningún grado de confianza con ningún usuario o dispositivo informático dentro o fuera de la organización sin antes ser verificado, la posición de **<<verificar siempre, no confiar nunca>>,** estará ganando mayor relevancia. Este principio se está extendiendo ahora más allá de los muros de la red corporativa para abarcar a los trabajadores remotos, trabajar colaborativamente con otras organizaciones y con variados dispositivos IoT (Internet of Things). Esta expan-

sión no es más que un testimonio de la evolución del panorama de amenazas al que se enfrentarán las entidades digitales.

Ahora en el 2025, el modelo de confianza cero se ha transformado de venir siendo una configuración de seguridad de red puramente técnica, a un enfoque adaptable y holístico, pero, **¿qué es esto propiamente?,** pues como ejemplo ilustrativo puedo mencionar, un par de soluciones muy conocidas como es la incorporación de dispositivos BYOD (Bring Your Own Device) y la inclusión de técnicas MFA (Multi-Factor de Autenticación), como modelos de confianza cero que se adaptan a las nuevas formas de trabajar remotamente, haciendo uso de elementos de la nube o redes, hardware, usuarios y aplicaciones como parte integral de todo un entorno.

La flexibilidad y adaptabilidad de este enfoque fueron decisivas para ayudar a las organizaciones a responder al rápido cambio mundial hacia el trabajo remoto o a distancia. Ahora **¿qué es lo importante finalmente a este respecto?,** dejar claro que las empresas deben adoptar un enfoque de seguridad de confianza cero, en el que cada usuario y dispositivo deba ser tratado como potencialmente hostil, ya sea que opere dentro o fuera de la infraestructura corporativa. Esto sienta unas bases sólidas que mejorará las medidas de seguridad.

4. Blockchain: Esta tecnología no es un secreto su aplicabilidad para aquellas aplicaciones que requieren unos altos niveles de seguridad, como será ya en un futuro muy cercano, para el sector bancario y de la salud, donde los retos de un mercado cada vez más competitivo y cambiante les demandará en cuanto a la ciberseguridad sea una mayor tendencia para así incentivar a su uso.

5. Internet de las cosas (IoT): Dispositivos para el hogar y la oficina con microcomponentes electrónicos casi imperceptibles incluidos para ganar funcionalidad en la conectividad con otros dispositivos en conjunto, se disparará a nivel global como un acto de innovación en la competitividad comercial. Estos dispositivos vendrán con mejores capacidades para atender nuevas necesidades de los usuarios, que se inclinan por lo sofisticado e innovador, donde, como sabemos, una de sus características reposa en la simplicidad al usuario para ser configuradas, que en otras palabras termina significando el ser poco segura para su instalación y uso. Por ello, con el aumento de estas soluciones y dispositivos conectados, la IoT se volverá mucho más crítica en adelante y necesitará contar con mejores alternativas de seguridad, para proteger estos dispositivos y evitar sean vulnerados. Ejemplo de algunos son, los sistemas de seguridad basado en cámaras o CCTV, los sistema de monitoreo remoto basado en sensores (iluminación, temperatura, humedad, localizadores, la domótica, etc.),

6. Ciberresiliencia: Más allá de la prevención como es en la actualidad, para las organizaciones se volverá más común el contar con herramientas, procedimientos y acompañamiento de personal certificado con experiencia demostrada, que les facilitará la capacidad de recuperarse en una mejor ventana de tiempo, ante posibles incidentes que pudieran derivar de un ciberataque o ciberamenaza. En otras palabras, la connotación de criticidad tendrá un manejo más estructurado y a la vez muy posiblemente un poco más controlado al interior de un mejor número de organizaciones, pero que aún no se acerca al 50% de ellas.

Estas estrategias se esfuerzan por garantizar una rápida recuperación con una pérdida de datos y un tiempo de inactividad reducidos, haciendo de la ciberresiliencia una prioridad estratégica en 2025. A partir de este año, se aconseja a las organizaciones que se centren tanto en sus medidas de ciberseguridad como de ciberresiliencia, donde deben aspirar no sólo a una defensa sólida contra las ciberamenazas, sino además a un sistema de recuperación eficaz que les permita recuperarse con un daño mínimo.

EN RESUMEN

La ciberseguridad ha dejado de ser un tema exclusivamente técnico: hoy es un factor clave de continuidad y crecimiento empresarial. Las amenazas llegaron para quedarse, pero también lo han hecho las soluciones. Implementar una estrategia robusta, basada en inteligencia, prevención y resiliencia, no solo protegerá a tu organización, sino que le dará una ventaja competitiva real en un entorno digital cada vez más desafiante.

¿Estás listo para empezar a actuar?

Este artículo se elaboró producto de la participación en webinars y la lectura a material oficial en el sitio web de algunos de los líderes de la industria para temas relacionados con el conocimiento y experiencia de la Ciberseguridad en el mundo, con la intención de resaltar los asuntos más relevantes, para en términos simples pueda ser del alcance de quienes tengan interés en ganar un poco de conocimiento de estas tendencias y sea un punto de partida para efectuar una introinspección al interior de sus organizaciones y así aplicar posibles soluciones mitigantes.

Referencias

2025,ESET, https://www.eset.com/ve/tendencias-en-ciberseguridad/

2024,GARTNER.es,Las principales tendencias en ciberseguridad del 2024, https://www.gartner.es/es/tecnologia-de-la-informacion/tendencias/tendencias-ciberseguridad