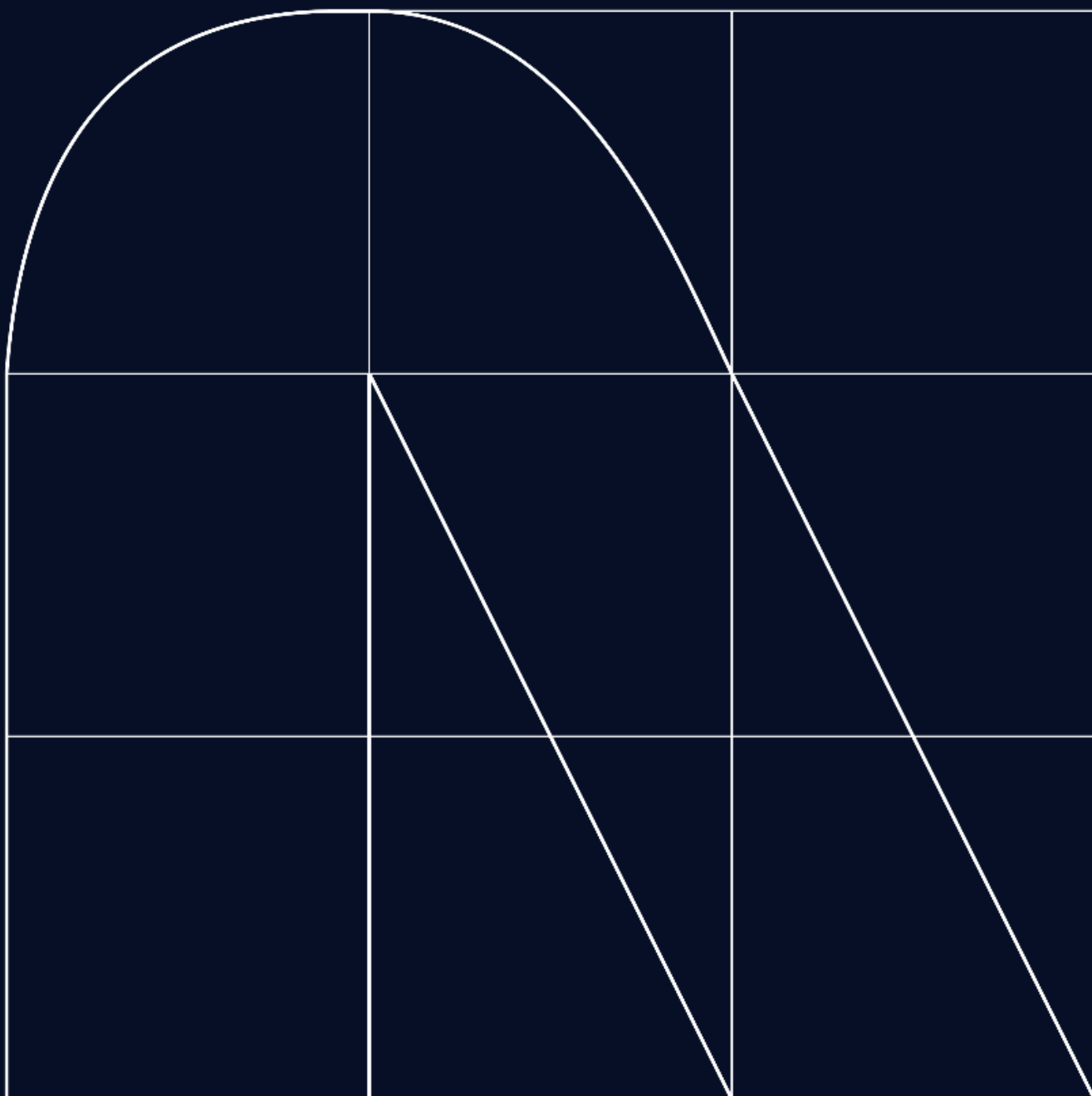
Número 86 | Enero 2024

NTT DATA

# Radar

## El magazine de ciberseguridad



# 2024: un nuevo inicio en el proceso de transformación digital

Por Maria Pilar Torres Bruna

Empezamos un nuevo año, el 2024, y tecnológicamente hablando, todo apunta a que será un año apasionante. Cuando pensábamos que las empresas habían dado un gran paso en su transformación digital (como resultado de la pandemia y de la modernización que está impuso para poder seguir trabajando de manera remota), y que nos venían unos años más bien de estabilización, volvemos a tener esa sensación de que estamos en un nuevo comienzo del camino. Se nos viene una nueva revolución, que vendrá liderada por la adopción de la inteligencia artificial.

Desde las áreas de seguridad hemos visto cómo nuevos proyectos de IA, aunque sea a modo prueba de concepto, irrumpen en el negocio. Lo cierto es que más del 70% de las organizaciones, al menos a nivel de America Latina, reconocen la IA como un motor de cambio en la transformación que nos viene. Se percibe una preocupación desde el punto de vista de la seguridad y la privacidad. Preocupación que ya ha pasado a ser una ocupación para distintos gobiernos que están regulando el uso de la inteligencia artificial y entidades bien reconocidas como la NIST, la agencia de protección de datos personales en España o la red iberoamericana de protección de datos.

Y en esta situación, solo nos queda hacer lo que hemos hecho siempre: hacer de la ciberseguridad una palanca clave para la transformación digital. Y para ser esa palanca de cambio pensamos que los siguientes puntos deben estar muy presentes en el año que empieza:

- Debemos acompañar la adopción de los proyectos de IA asegurando que cumplen con un marco de seguridad y privacidad que evita sesgos y tiene en cuenta datos completos y de fuentes fiables. No importa si el país en el que estamos no hay todavía una regulación vigente. Escojamos un buen marco de buenas prácticas para estar listos para una futura normativa y posicionarnos ante nuestros clientes como consumidores de IA responsable.
- Adoptemos la propia IA para aumentar los niveles de seguridad en la compañía. Muchas tecnologías ya traen consigo el uso de la IA. Hay que maximizar ese uso y detectar puntos aún no cubiertos por ella para definir como eficientar esa funcionalidad.
- El análisis de riesgos cuantitativo puede ser un gran aliado para demostrar que la inversión en seguridad, en proyectos de IA y en proyectos en general, no sólo no es un coste, sino que trae mejores resultados en el medio plazo. Quizá sea el momento para realizar el análisis sobre los escenarios de riesgo de mayor impacto para la organización.
- No demos de pensar en el futuro. La ciberseguridad ha dejado de ser un aspecto del CISO para ser una cuestión de resiliencia organizacional. Está en manos de todos.

En NTT DATA estamos convencidos de que se viene un año emocionante para los que trabajamos en ciberseguridad. Esperamos acompañarlos para seguir creciendo este maravilloso ámbito. ¡Feliz año 2024! ¡Les deseamos un año ciber-seguro!

**Maria Pilar Torres Bruna**
Directora de Ciberseguridad

# Los ciberataques ponen en jaque la seguridad de las infraestructuras médicas

Cibercrónica

En el entramado global de la atención médica, una amenaza digital silenciosa ha desencadenado una vulnerabilidad sin precedentes en la intersección de la tecnología y la salud. En el cierre del 2023, los ciberataques han aumentado drásticamente, siendo las infraestructuras críticas de la salud unas de las más afectadas, poniendo en peligro la estabilidad de clínicas, hospitales, entidades prestadoras de servicios de salud y laboratorios. Los defensores de la salud deben proteger un sistema frágil que busca fortalecer la salud global.

Al cerrar noviembre en Nueva Jersey, el sistema de salud local anunció interrupciones, marcando otro episodio en la cadena de eventos que ha afectado la infraestructura médica. La priorización de cirugías según urgencia resalta la vulnerabilidad cruda de un sistema esencial que sostiene no solo diagnósticos y tratamientos, sino la misma existencia.

Simultáneamente, en Tulsa, Oklahoma, el Centro Médico Hillcrest se convirtió en epicentro de un devastador ataque de ransomware, postergando procedimientos vitales y sumiendo a miles de pacientes en la incertidumbre sobre su salud. La realidad de que nuestras vidas están entrelazadas con las complejidades digitales de la atención médica se volvía más apremiante que nunca.

> Estos ataques representan una amenaza directa para la vida y salud de millones, dejando pacientes en espera y generando costos económicos devastadores

Se siguió expandiendo a Nashville, Tennessee, cuando Ardent Health Services, responsables de 30 hospitales en seis estados, desconectaron su red después de un ciberataque también a finales de noviembre. Ambulancias desviadas, procedimientos suspendidos; la columna vertebral de la sociedad, la atención médica, incapacitada ante los ataques. La misma amenaza desgarradora se hizo presente en Colombia en septiembre de 2023, cuando más de 50 instituciones estatales, incluida la Superintendencia Nacional de Salud, reportaron ciberataques bajo la ominosa modalidad ransomware, afectando gravemente la prestación de servicios a la ciudadanía por varias instituciones de salud.

Estos eventos críticos revelan una verdad escalofriante: el corazón palpitante de la atención médica es vulnerable a ataques digitales que amenazan no solo la infraestructura, sino directamente la salud y el bienestar de las comunidades. En este escenario, la ciberseguridad no es solo una capa adicional, sino una línea de defensa esencial para proteger la integridad de la atención médica global. Mientras estos incidentes resaltan las grietas en el sistema, también instan a una acción colectiva e inmediata para preservar la confianza y la eficacia de los servicios de salud, asegurando las ciber amenazas no eclipsen nuestra capacidad de curar y cuidar.

A nivel mundial, cientos de ciberataques han surgido, desde naciones desarrolladas hasta menos favorecidas, en una danza ejecutada por ciberdelincuentes con objetivos más allá del lucro económico, buscando desestabilizar y aterrorizar a la sociedad. La gravedad de la situación exige medidas inmediatas.

Estos ataques representan una amenaza directa para la vida y salud de millones, dejando pacientes en espera y generando costos económicos devastadores. La colaboración internacional se erige como un pilar fundamental en esta batalla, donde la información sobre amenazas debe compartirse ágil y transparentemente para fortalecer las defensas colectivas.

La implementación de **estrategias de respuesta rápida, tecnologías de inteligencia artificial y aprendizaje automático** se torna esencial para detectar patrones de ataques antes de que se materialicen. La lucha contra esta oscura amenaza digital requiere no solo innovación tecnológica, sino también un cambio cultural y una conciencia constante en todos los niveles de la atención médica. La inversión en innovaciones defensivas es imperativa para construir un escudo robusto contra aquellos que buscan desangrar la salud mundial a través de oscuros recovecos digitales. La victoria se celebra no solo en la protección de datos, sino en la preservación de la esencia misma de nuestra existencia: la salud y el bienestar de la humanidad.

En el **inicio del 2024**, nos enfrentamos al reto de convertir desafíos pasados en oportunidades de cambio y mejora, especialmente en la defensa contra amenazas cibernéticas en la salud. La colaboración internacional y la innovación tecnológica son fundamentales para un futuro más seguro, respaldadas por una creciente conciencia colectiva sobre la importancia de la ciberseguridad en el ámbito médico.
Este año nos insta a traducir lecciones aprendidas en la batalla cibernética en medidas más efectivas y a construir un escudo más fuerte contra amenazas digitales. Que el 2024 sea un período de transformación positiva, donde la unión global, la tecnología avanzada y la conciencia constante nos conduzcan a una ciberseguridad fortalecida y, en última instancia, a una atención médica más segura y confiable para todos.

Pero no solo el sector salud se está viendo afectado por los implacables ciberdelincuentes, ya que en estas fechas un antiguo malware ha regresado con más fuerza y nuevas y novedosas maneras de vulnerar sectores públicos, empresariales y a nosotros como usuarios de internet. Por esto, no está de más mencionar un RAT que ha resurgido con fuerza: **el NetSupport RAT**. Los Troyanos de Acceso Remoto (RAT) son maestros en la orquestación del caos, proporcionando al atacante un control absoluto sobre la máquina infectada. Al infiltrarse en un sistema, este malware establece un puente virtual, permitiendo al intruso dirigir el dispositivo a distancia, de manera comparable a herramientas como el Protocolo de Escritorio Remoto (RDP) o TeamViewer.

NetSupport RAT, antaño una herramienta legítima de administración remota conocida como NetSupport Manager, ha renacido como una amenaza latente en manos de actores maliciosos. Los expertos en seguridad observan con inquietud su drástico aumento en infecciones, siendo víctimas sectores críticos como la educación, el gobierno y los servicios empresariales. La propagación de NetSupport RAT se gesta mediante artimañas diversas, desde actualizaciones fraudulentas hasta descargas clandestinas. Este troyano destaca por su versatilidad al afectar desde neófitos cibernéticos hasta adversarios avezados, convirtiéndose en una amenaza de alcance amplio y sutil.

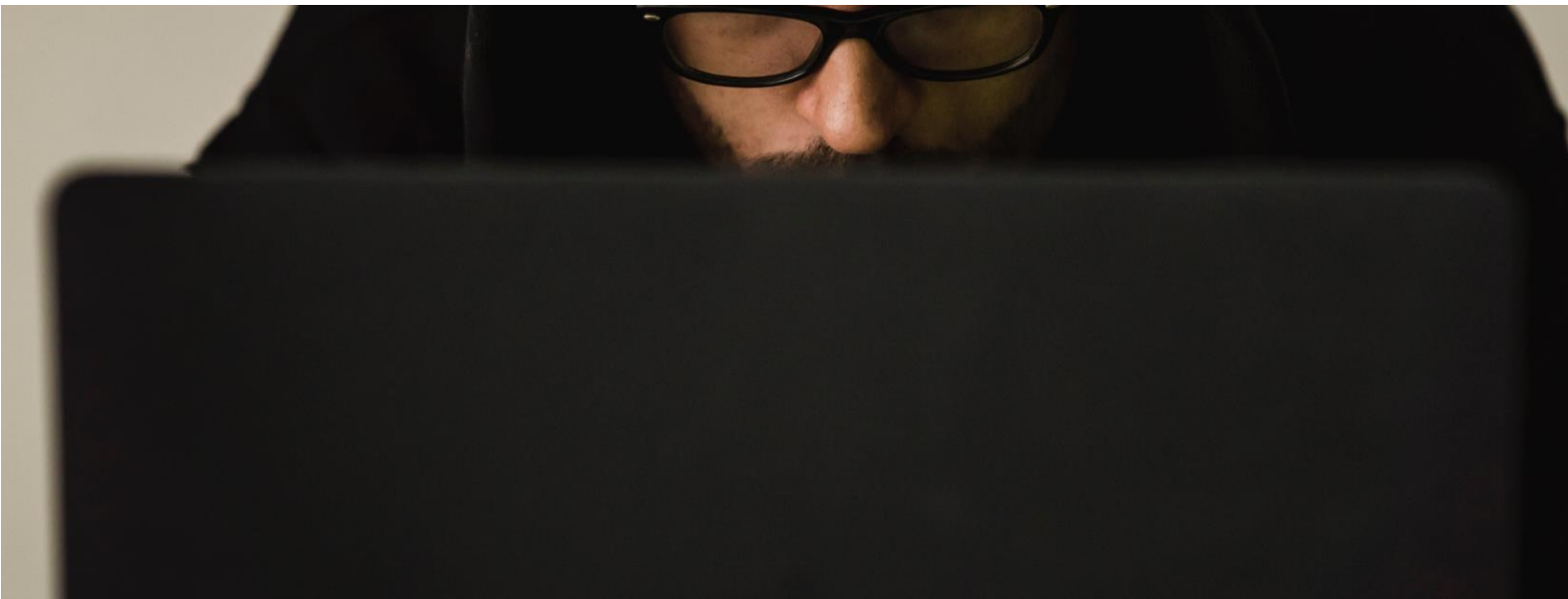
El modus operandi de NetSupport RAT implica el engaño de víctimas, persuadiéndolas para que descarguen actualizaciones falsas de navegadores desde plataformas comprometidas. Esta táctica de infección, adaptable y astuta, deja una huella sutil pero inconfundible en el lienzo siempre cambiante de la ciberseguridad.Frente a este resurgimiento sigiloso, la ciberseguridad demanda una aproximación vigilante y estratégica. La concientización del usuario se erige como un escudo esencial, educándolos sobre tácticas de phishing y la precaución al descargar actualizaciones. Implementar soluciones de seguridad avanzadas y mantener la infraestructura tecnológica actualizada se convierten en barreras cruciales para frenar la embestida de NetSupport RAT.

**El NetSupport RAT puede desencadenar consecuencias devastadoras** una vez que logra infiltrarse en un sistema. Los atacantes, armados con este malware, pueden ejecutar diversas acciones maliciosas, como el robo de datos sensibles, el control remoto del sistema afectado e incluso la interrupción de servicios esenciales. Este conjunto de capacidades amenaza no solo la confidencialidad de la información, sino también con ocasionar pérdidas financieras y dañar la reputación de las víctimas. La presencia de NetSupport RAT se ha detectado en diversos sectores, desde la educación hasta los servicios empresariales. Escuelas, universidades, entidades gubernamentales y empresas han sido blanco de este troyano de acceso remoto, lo que subraya la amplitud de su amenaza. NetSupport RAT emplea una variedad de métodos para propagarse, incluyendo el phishing, la inyección de código y la descarga manual del malware. La diversidad de estrategias hace que la detección y prevención sean desafíos constantes en este juego estratégico en el ciberespacio.

En este escenario, **la defensa contra el renacimiento de NetSupport RAT** requiere medidas preventivas sólidas. La concientización del usuario, una política estricta de actualizaciones, inversión en soluciones de seguridad avanzadas, actualización constante de sistemas y la implementación de sistemas de monitoreo continuo son recomendaciones clave para mitigar el riesgo y proteger el entorno cibernético. La colaboración entre la comunidad de ciberseguridad se erige como una fortaleza compartida, uniendo fuerzas para comprender y neutralizar amenazas emergentes. En este juego dinámico entre atacantes y defensores, cada medida de mitigación constituye un paso crucial hacia la preservación de la integridad digital en este mundo interconectado.

**Martín Bedoya**
Lead Analyst Cybersecurity

**Orlando Ospina**
Analyst Cybersecurity



# Bienvenido año 2024. Las tendencias en ciberseguridad ¿cambiaran?

TENDENCIAS

Al terminar el año, se nos hace costumbre evaluar la perspectiva de ciberseguridad en las empresas, y se observa que a pesar de que tienen procesos continuos de evaluación de riesgos, no logran reducir su exposición a las amenazas, ello debido a que aún persisten en enfoques poco realistas, aislados y centrados en herramientas.

Forbes ha indicado que, para finales del 2024, el costo de los ataques cibernéticos a la economía global superará los 10,5 billones de dólares. Esto números demuestran una creciente necesidad sobre el tema de ciberseguridad, y su prioridad estratégica a nivel individual y organizacional. Nos hemos venido preparando para afrontar nuevas tendencias y tecnologías en nuestras organizaciones, hablar del internet de las cosas (IoT), Big Data, 5G y ahora la Inteligencia Artificial (IA), nos lleva a pensar no solo en nuevas oportunidades de negocio, sino también en nuevas formas en que los ciberdelincuentes pueden atacarnos, pero nada más alejado de la realidad cuando observamos que esas “nuevas formas” siguen siendo las mismas que “combatimos” año a año:

Por ejemplo, organizaciones como CISA (Cybersecurity & Infraestructure Security Agency) y ENISA (European Union Agency for Cybersesurity) coinciden en señalar que considerando el impacto y la frecuencia con que se pueden realizar o identificar las diversas amenazas, podemos considerarlas en los siguientes grupos:

- Ransomware
- Malware
- Ingeniería social
- Amenazas contra los datos
- Amenazas contra la disponibilidad
- Manipulación de la información
- Ataques a la cadena de suministro (supply chain)

A medida que las organizaciones enfrentan una lucha por mantenerse al día con un panorama de amenazas en constante evolución, los líderes de ciberseguridad suelen recurrir a enfoques reactivos que solo persiguen en forma constante las amenazas y buscan reducir algún posible incidente. Ello, es contrario a una estrategia de iniciar y madurar programas con un nuevo enfoque para poder comprender de una forma más proactiva la superficie de ataque a la que se encuentran expuestos, creemos que esto les permitiría priorizar mejor sus esfuerzos y medir los progresos a lo largo del tiempo.

**Las recomendaciones en esta situación son:**

• Hay que asegurar que los resultados de la gestión de exposiciones contribuyan a múltiples partes de las organizaciones de seguridad y TI diseñando un programa para gestionar un conjunto más amplio de exposiciones.

• Considerar escenarios de exposición a amenazas utilizando áreas que sean emergentes y se asocien a su gestión de la superficie de ataque, así como a una postura de seguridad.

• Integrar una gestión continua de exposición a amenazas y que cada ciclo se adhiera a un proceso de cinco pasos (alcance, descubrimiento, priorización, validación y movilización), asociado a su flujo de gestión de incidentes.

**Jorge Trujillo**
CyberSecurity Specialist

# Cifrado en capa de aplicación como estrategia para robustecer la postura de seguridad

El cifrado se ha consolidado como una herramienta fundamental para salvaguardar la confidencialidad de la información. A través de mecanismos matemáticos, es posible transformar un conjunto de datos para impedir que actores no autorizados puedan comprenderlos. Este proceso es fundamental a la hora de proteger el tráfico de los sistemas que se despliegan a través de internet.

El protocolo TLS (Transport Layer Security) desempeña un papel crucial al asegurar la información transmitida en las comunicaciones entre un servidor y un cliente, es el encargado de agregar el candado al navegador en lo que se conoce como HTTPS. Operando en la capa de transporte, este protocolo se encarga de cifrar la totalidad del canal de comunicación mediante suites de cifrado.

Actividades como el intercambio de claves, autenticación mutua, cifrado y revisión de integridad mediante hashes son procesos que se llevan a cabo gracias a TLS, lo que permite garantizar confidencialidad, integridad y no repudio, verificando que las partes involucradas sean quienes dicen ser y no puedan negar la autenticidad de la información intercambiada. Este proceso integral de cifrado constituye un componente esencial en la protección contra amenazas y posibilita un intercambio seguro de datos.

Aunque el protocolo TLS garantiza un canal de comunicación cifrado a través de internet, es importante tener en cuenta que el cifrado se aplica exclusivamente al canal. Esto significa que, en la práctica, existe la posibilidad de capturar y manipular la información abusando de la confianza del protocolo TLS. Por tanto, como medida de defensa en profundidad, el cifrado en capa de aplicación permite agregar un control adicional para proteger los datos de las peticiones que viajan a través de internet.

Los Proxys HTTPS son herramientas que permiten ejecutar ataques conocidos como "Man In The Mide" (Hombre en el Medio), debido a que tienen la capacidad de interferir en el protocolo TLS abusando de la excesiva confianza de este en el navegador. Estos proxis posibilitan a un atacante observar y alterar los parámetros que se envían desde un cliente hacia el servidor en una aplicación web o móvil aun cuando la información se encuentra protegida por TLS. Dado que estas herramientas son ampliamente conocidas por adversarios, es necesario considerar estrategias adicionales de seguridad que permitan proteger el tráfico.

La captura del tráfico de red de una aplicación web o móvil introduce una serie de amenazas que deben tenerse en cuenta desde el diseño de la solución. Inyecciones de código, ataques de fuerza bruta, enumeración de usuarios o secuestros de sesión son ataques comúnmente conocidos que pueden efectuarse gracias a la posibilidad de inspeccionar el tráfico de las aplicaciones.

Para contrarrestar estas amenazas potenciales es posible implementar cifrado en capa de aplicación. Este control se enfoca en proteger la confidencialidad de los parámetros que se envían en las peticiones y las respuestas del servidor. Para lograrlo las fábricas de software deben implementar este control directamente en la aplicación, esto quiere decir, en el código fuente del backend y del frontend.

Los programadores pueden utilizar dos conceptos fundamentales de la criptografía: el cifrado simétrico y asimétrico. Un algoritmo de cifrado simétrico implica el uso de una única clave tanto para el proceso de cifrado como el descifrado. Este enfoque, aunque eficiente, plantea el desafío de compartir de manera segura la clave entre las partes de la comunicación. Por otro lado, los cifrados asimétricos utilizan un par de claves: una pública y otra privada. La clave pública se comparte abiertamente, mientras que la clave privada se mantiene en secreto. La información cifrada con la clave pública solo puede descifrarse de manera efectiva con la clave privada correspondiente.

La elección del tipo de algoritmo de cifrado a utilizar debe definirse desde la fase de diseño de la aplicación. Por un lado, el cifrado simétrico, siendo más ligero, permite cifrar los datos más rápido. Sin embargo, conlleva el riesgo de que la clave compartida sea capturada y el adversario logre descifrar la comunicación.

Para resolver este problema, los programadores pueden implementar mecanismos de ofuscación por obscuridad para ocultar la clave. En su contraparte, el cifrado asimétrico brinda mayor seguridad, ya que la clave de descifrado no se comparte. A pesar de esto, los algoritmos de cifrado asimétrico requieren una mayor capacidad de cómputo debido a la complejidad algorítmica, lo que puede impactar seriamente en el rendimiento y la experiencia de usuario de la aplicación. De allí que la implementación de cifrado en capa de aplicación debe ser un control que deberá implementarse a partir de un análisis y conocimiento profundo de las necesidades de negocio.

Es importante considerar que no aplicar cifrado en capa de aplicación introduce diversas amenazas para las aplicaciones. Sin embargo, la fundación OWASP, que es una comunidad abierta relacionada con la seguridad en aplicaciones, no profundiza sobre este control en sus diferentes marcos metodológicos, esto puede deberse al impacto en el rendimiento de la aplicación y en el costo de implementación para la fábrica de software.

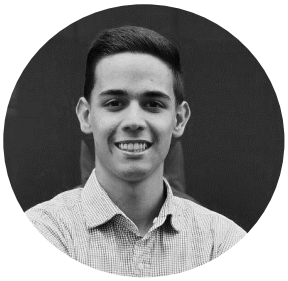
Históricamente, la seguridad y rendimiento han ido en caminos opuestos, no obstante, en los últimos años, las capacidades de cómputo han experimentado un aumento de potencia significativo y una reducción de costos considerable gracias a la nube, haciendo que la implementación de cifrado en capa de aplicación sea más viable.

Por otro lado, encontrar programadores que implementen criptografía puede ser un desafío para las fábricas de software, la necesidad de programadores más experimentados incrementa el costo por hora-desarrollo, estos costos han sido una barrera significativa para la adopción generalizada del cifrado en capa de aplicación. No obstante, en la actualidad se observa un cambio en este panorama gracias al aumento de librerías *OpenSource* y de documentación relacionada sobre cómo cifrar en lenguajes de programación para la web.

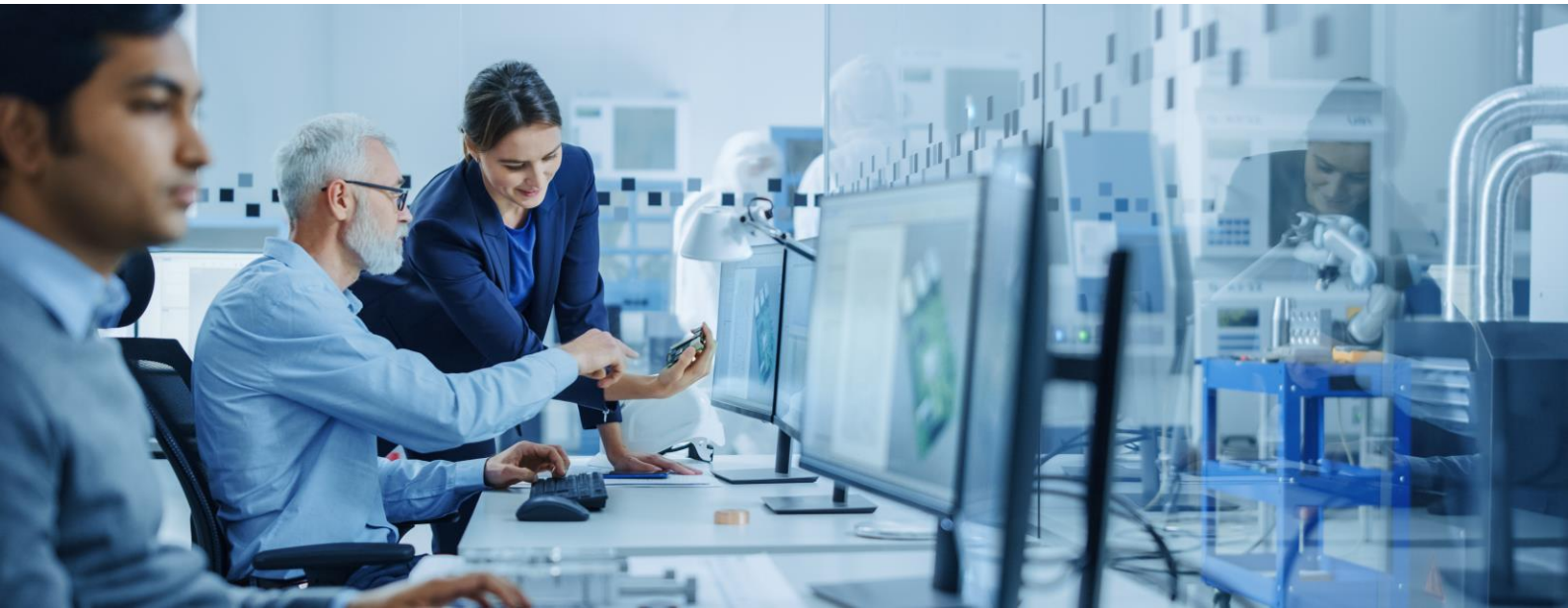
A pesar de este avance, OWASP aún no ha incluido la interceptación de tráfico como un criterio de vulnerabilidad para las aplicaciones web; sí lo hizo en su momento para las aplicaciones móviles, sin embargo, es un control que depreciaron posteriormente. Las prioridades y enfoques de seguridad cambian con el tiempo a medida que evolucionan las tecnologías y las amenazas cibernéticas. Es crucial para las fábricas de software seguir prácticas de seguridad actualizadas y anticiparse a los cambios del entorno tecnológico que introduce nuevas amenazas. Es probable que OWASP incorpore este control en sus próximas actualizaciones.

En resumen, el protocolo TLS, aunque valioso para la proteger el canal de comunicaciones, no es suficiente para garantizar la protección de la información contra interceptaciones. Por lo tanto, la implementación de cifrado en capa de aplicación es una estrategia de seguridad que puede ser utilizada por las fábricas de software para robustecer su postura de seguridad y elevar el nivel de madurez en seguridad de las aplicaciones. Cada día la implementación de este control es más económica y sus beneficios son fácilmente medibles, pues la motivación de un adversario por comprometer una aplicación puede verse disminuida cuando no solamente debe evadir TLS, sino una capa de cifrado adicional.

**Martín Bedoya**
Lead Analyst Cybersecurity



**José Cianci**
Analyst Cybersecurity



# Neobancos y tendencias en ciberseguridad: desafíos y oportunidades

En los últimos años la industria financiera ha experimentado una gran transformación digital lo que ha dado lugar entre otros aspectos a la llegada de los neobancos, que son entidades financieras que ofrecen sus servicios bajo un esquema totalmente digital, sin las tradicionales sucursales físicas, apostando por una diferenciación en la agilidad y practicidad para el enrolamiento de usuarios, así como en la adquisición y uso de sus productos.

A medida que los neobancos van posicionándose en el mercado y van sumando cada vez más usuarios, la ciberseguridad emerge como un elemento clave en este nuevo panorama financiero. En este artículo, exploraremos algunos de los principales desafíos y oportunidades a los que se enfrentan hoy en día los neobancos, en el ámbito de la ciberseguridad:

**Desafíos que deben tener en cuenta los Neobancos**

**Autenticación reforzada:** la autenticación segura es esencial en un entorno financiero completamente digital, implementar medidas como la autenticación multifactorial y tecnologías biométricas se vuelve crucial para asegurar los procesos de validación de identidad de los usuarios, así como la ejecución segura de las operaciones.

**Aumento y evolución de amenazas cibernéticas**: su propuesta de valor 100% digital los convierte en un blanco bastante atractivo para ataques cibernéticos como phishing, Ransomware, denegación de servicios, fraudes en línea, entre otros; lo cual podría comprometer seriamente la seguridad de la información financiera y personal de los usuarios.

**Almacenamiento en la nube**: la gran mayoría de los neobancos almacenan datos en la nube a fin de facilitar el acceso y la agilidad en sus servicios, lo cual requiere implementar medidas de seguridad más avanzadas para proteger estos datos.

**Privacidad de datos personales:** la recopilación y manejo de datos son fundamentales para la operación de los neobancos, garantizar la privacidad y seguridad de esta información personal resulta crucial para construir y mantener la confianza de sus clientes.

**Cumplimiento normativo:** a medida que los neobancos se expanden, enfrentan desafíos en términos de cumplimiento normativo ya que las regulaciones de ciberseguridad y privacidad también están evolucionando y siendo cada vez más exigentes con este tipo de propuestas innovadoras en el mercado financiero; en ese sentido, los neobancos deben adaptarse y asegurar el cumplimiento de dichas regulaciones a fin de evitar posibles multas o sanciones.

**Educación del usuario:** la concientización y educación del usuario son componentes clave en la defensa contra amenazas cibernéticas. Los neobancos deben proporcionar información clara sobre las mejores prácticas de seguridad, identificación de posibles amenazas y cómo los usuarios pueden protegerse.

**Oportunidades en medio de los desafíos**

Así como existen múltiples desafíos en ciberseguridad, los neobancos también tienen la oportunidad de destacar y construir la confianza de los usuarios mediante la adopción de medidas proactivas.

Tienen una amplia gama de opciones para invertir en herramientas de seguridad y tecnologías emergentes, como inteligencia artificial, machine learning, inteligencia de amenazas, entre otros, para anticipar amenazas y fortalecer sus defensas.

Además, pueden sumar y/o mejorar sus capacidades a través de proveedores expertos que ofrecen conocimientos especializados y soluciones avanzadas para los diferentes desafíos que deben abordar en cuanto a Ciberseguridad.

En conclusión, a medida que los neobancos abren nuevas posibilidades en el panorama financiero, la ciberseguridad se convierte en un pilar fundamental de su éxito y sostenibilidad. La adopción de tecnologías emergentes y apoyo en proveedores expertos en seguridad cibernética les permitirá prosperar en un entorno cada vez más dinámico y amenazante. La clave radica en la capacidad de mantener un equilibrio entre la innovación y la seguridad para ofrecer servicios financieros digitales confiables.

**Milagros Silvia**
Expert Consultant Cybersecurity

**Si quieres recibir este PDF mensualmente en tu correo, suscríbete a la newsletter de RADAR para estar al día de todas las novedades sobre la ciberseguridad.**

# Gestión de la Continuidad de Negocio: IT y OT

La Gestión de la Continuidad de Negocio (GCN) es el conjunto de actividades, procesos, herramientas, personas y controles previamente definidos, estructurados, documentados y probados, que tienen como objetivo garantizar la continuidad mínima, previamente acordada, de los servicios y/o áreas que dan soporte al negocio, cuando uno o más recursos relevantes para la organización no estén disponibles. La GCN permite a la organización tener un menor impacto, una cierta previsibilidad y una adecuada continuidad de sus actividades.

La Gobernanza Corporativa tiene principios. Uno de ellos exige la sostenibilidad. Como tal, la existencia de la GCN es responsabilidad del Órgano de Dirección y/o del Consejo de Administración.
1. Transparencia: Informar y poner a disposición la información correctamente.
2. Equidad: Trato justo y no discriminatorio.
3. Rendición de cuentas: Responsabilidad.
4. Continuidad corporativa: Sostenibilidad de la organización.

**Tipos de recursos**

Para una mejor estructuración, implementación y mantenimiento de la GCN, es importante identificar qué tipos de recursos existen y cuáles deben considerarse.

**Recursos de Tecnología de la Información (IT):** son recursos en los que la información o los datos son los principales elementos para considerar en sus diversas formas y presentaciones. Este conjunto de recursos es el más conocido y utilizado en las organizaciones. Es el más avanzado en términos de procesamiento y comunicación. Tiene una elevada madurez en materia de seguridad.

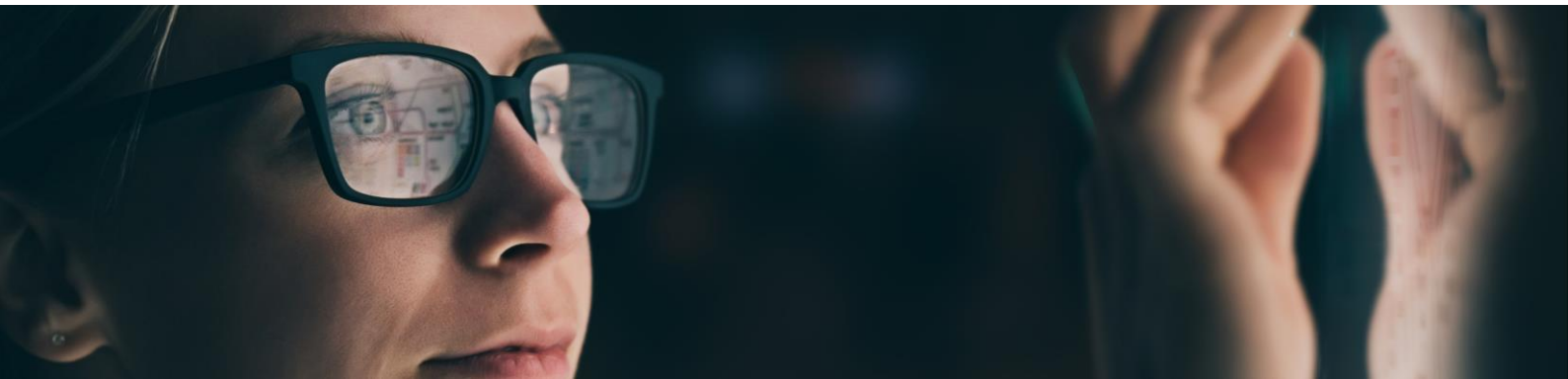
**Recursos de Tecnología Operativa (OT):** cuando el recurso a considerar no es, esencialmente, de naturaleza de información o datos. En este grupo se consideran los equipos con algún procesamiento para las áreas industrial, sanitaria y agroindustrial. Son recursos del Internet de las Cosas (IoT). Existen muchos tipos de equipos.

Considerando los controles de confidencialidad, integridad, disponibilidad, legalidad, no repudio y fiabilidad, todos ellos son importantes para el funcionamiento de las organizaciones. Sin embargo, existe un direccionador de seguridad para cada tipo de tecnología. Para las tecnologías de la información, la prioridad es la confidencialidad. Para las tecnologías operativas, la prioridad es la disponibilidad. Luego están los demás controles.

La seguridad para la Tecnología de la Información es más madura y cuenta con equipos, aplicaciones, legislación y normas definidas. La seguridad para la Tecnología Operativa es menos madura, debido a su necesidad de seguridad. Hasta hace poco, la Tecnología Operativa se ocupaba del entorno de las máquinas industriales, con un funcionamiento muy limitado a un equipo o grupos de equipos normalmente en una fábrica. Con el desarrollo del Internet de las Cosas (IoT), el ámbito de la Tecnología Operativa se ha vuelto más sofisticado y ha ido más allá del entorno industrial. La agroindustria está utilizando sensores de suelo para indicar la humedad y otros factores en grandes campos, así como para controlar su maquinaria. El sector sanitario está utilizando equipos de examen, operaciones a distancia con robots o máquinas intracorpóreas como marcapasos y chips que recogen información del cuerpo. Las ciudades inteligentes están creciendo y generando instalaciones y cuidando la privacidad de los ciudadanos.

Pero, tanto si se trata de Tecnología de la Información como de Tecnología Operativa, deben existir Planes de Continuidad de Negocio. Los macro controles son los mismos. Sin embargo, en cada uno de ellos habrá una aplicación específica para la información o las "cosas" inteligentes.

Los pasos que se describen a continuación son orientativos y deben utilizarse siempre teniendo en cuenta las características del entorno que se desea proteger. Son las siguientes (siguiente página)



**Identificación de amenazas:** todas las posibles amenazas deben ser identificadas. Sin embargo, se deben definir las amenazas que serán consideradas para el plan.

**Ámbito y escenario**
El ámbito es la gama de recursos y entornos que se tendrán en cuenta. El escenario es el momento y las condiciones concretas de la posible situación de indisponibilidad.

**Priorización de recursos**
Es la definición del orden de prioridad y tiempo para la recuperación de los recursos. El Tiempo Máximo de Recuperación (RTO) y el Punto de Recuperación (RPO) se identifican teniendo en cuenta la pérdida de datos. Esta priorización puede ser identificada por un proceso de Análisis de Impacto en el Negocio (BIA), un requisito contractual, un requisito legal o una definición del Consejo de Administración.

**Selección de la estrategia**
Se trata de definir la solución alternativa para el recurso o el entorno. Se tendrán en cuenta las prioridades y el coste de la aplicación de la solución alternativa.

**Estructuración y elaboración del plan**
Se trata de diseñar los equipos, el flujo, las actividades, las responsabilidades y la documentación.

**Planificación y realización de pruebas**
Se trata de la planificación, preparación, estructuración, autorización, ejecución y evaluación de las pruebas.

**Mantenimiento del plan**
Se trata de la planificación y las normas de actualización periódica y actualización específica.

**Plan de crisis y plan de comunicación**
Desde el punto de vista de la GCN, el Plan de Crisis y el Plan de Comunicación existen para apoyar y posibilitar la actuación holística de todas las áreas de la organización. Por supuesto, pueden tener una vida independiente, pero en la práctica complementan y posibilitan la eficacia de los demás planes.

**Plan de crisis:** conjunto de acciones y controles que debe planificar la organización cuando se produce un acontecimiento inesperado que puede tener un impacto negativo en la organización.

**Plan de comunicación**: este plan garantiza la existencia de comunicación interna dentro de la organización y también (principalmente) la comunicación de la organización con el entorno externo, como la prensa, los clientes, los accionistas, los órganos de supervisión o similares.

**La Gestión de la Continuidad de Negocio** debe diseñarse y construirse específicamente para cada organización y cada situación organizativa. No existe un "plan prefabricado". Los profesionales implicados en la gestión de la continuidad de las actividades deben tener conocimientos y experiencia en planes y situaciones de contingencia.

**Edison Goncalves**
Cybersecurity evangelist

# Eventos

### SANS Cloud Defender 2024 (Live Online) (8 - 13 Enero)

El SANS Cloud Defender 2024 se llevará a cabo en línea del 8 al 13 de enero. Este curso ofrece una formación de inmersión diseñada para que los profesionales de seguridad y/o informática interesados puedan aprender a construir, desplegar y gestionar infraestructuras, plataforma y aplicaciones seguras en la nube.

**Enlace**

### CSA AI Summit (17 - 18 Enero)

El CSA AI Summit es un destacado evento que busca reunir a expertos en la industria con el fin de brindar orientación sobre temas críticos de Inteligencia Artificial (IA) y su impacto en la ciberseguridad. Durante 2 días, ofrece información clave sobre cómo la IA generativa puede beneficiar a la ciberseguridad, cómo la están utilizando los ciber atacantes y las directrices que se deben considerar para un uso responsable.

**Enlace**

### SANS Cyber Threat Intelligence Summit & Training 2024 (29 de Enero - 5 de Febrero de 2024)

El SANS Cyber Threat Intelligence Summit &Training es un evento que se lleva a cabo en Washington DC, Estados Unidos del 29 de enero al 5 de febrero. Este evento, al cual se puede acceder también vía online, tiene como objetivo que los interesados en la industria puedan adquirir nuevas perspectivas y aprender de casos de estudio que desafían los supuestos de la inteligencia de ciberamenazas, dando lugar a un cambio en su comprensión.

**Enlace**

# Recursos

**Certificate of Competence in Zero Trust (CCZT) FAQ:**
El Certificate of Competence Zero Trust (CCZT) es un recurso líder en la industria que proporciona a los profesionales de la tecnología, los conocimientos esenciales para comprender y aplicar los principios de Zero Trust. En el documento FAQ elaborado por Cloud Security Alliance (CSA), podrá encontrar más información acerca de los beneficios del CCZT y cómo acceder a éste.

Enlace

**Mitigación de riesgos de seguridad en aplicaciones basadas en LLM de Generación de Recuperación Aumentada (RAG, por sus siglas en inglés)**

La Generación de Recuperación Aumentada es una técnica eficaz utilizada por los ingenieros de IA para desarrollar aplicaciones basadas en grandes modelos lingüísticos (LLM). Sin embargo, se ha identificado que la falta de controles de seguridad en las aplicaciones LLM basadas en RAG puede plantear riesgos si no se abordan adecuadamente. Debido a ello, el artículo elaborado por Cloud Security Alliance, tiene como objetivos: (i) analizar la arquitectura RAG, (ii) identificar los potenciales riesgos de seguridad en cada etapa; y, (iii) brindar recomendaciones técnicas para mitigar dichos riesgos, sirviendo así de guía práctica para los desarrolladores.

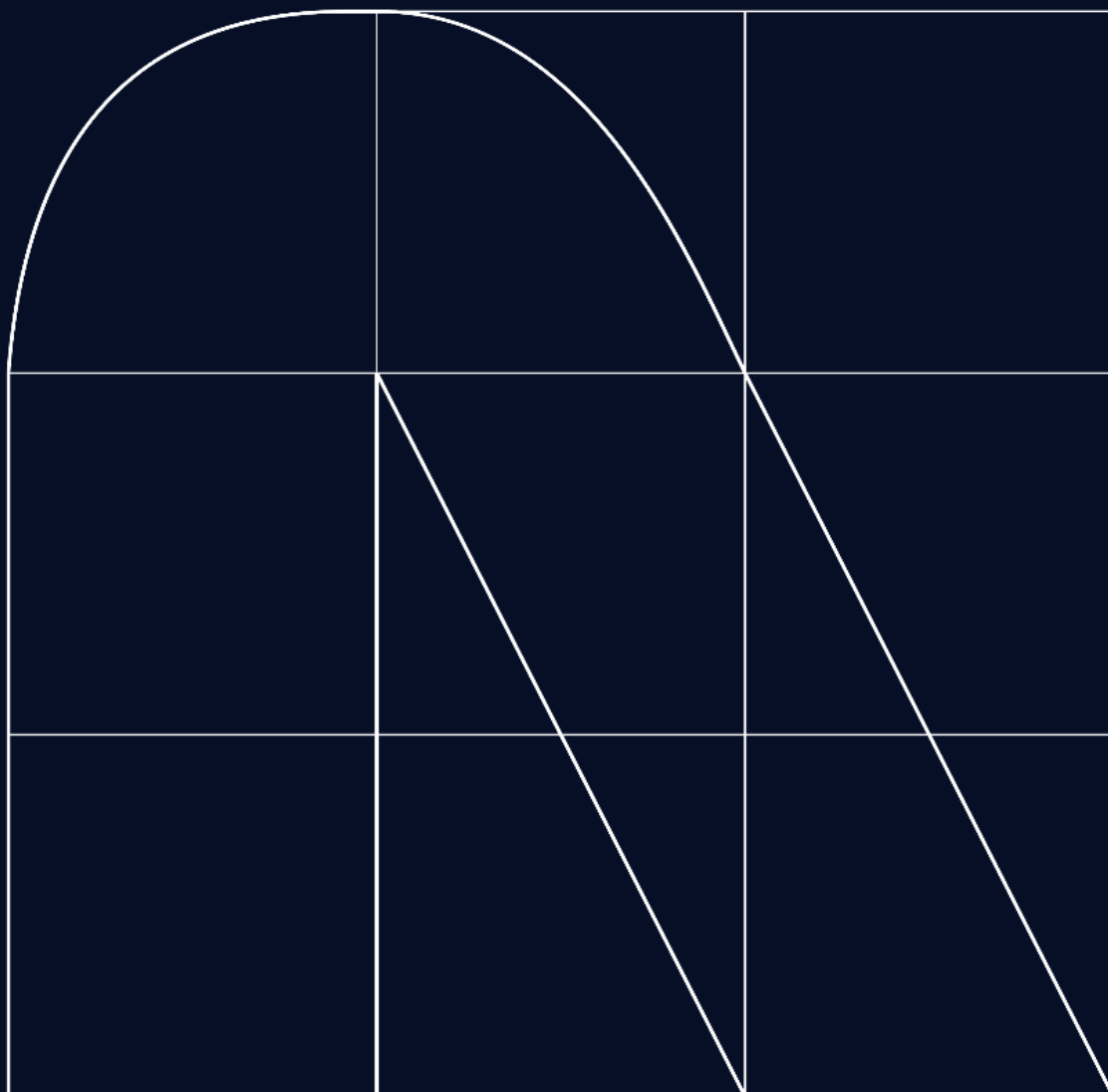
Enlace

**GPT-4 Turbo**

OpenAI anuncia el lanzamiento de GPT-4 Turbo, una nueva generación del modelo grande de lenguaje, LLM en inglés, que promete superar las debilidades de los anteriores, GPT-3.5 y GPT-4, ser más rápido y barato. Esta nueva versión alcanza una longitud de contexto de 128.000 tokens, es decir, la cantidad de texto que admite y comprende cuando se le hace una pregunta al chatbot. Además, puede aceptar imágenes como entradas en la API Chat Completions, lo que permite casos de uso como generar subtítulos, analizar imágenes del mundo real en detalle y leer documentos con figuras.

Enlace





**Powered by the cybersecurity NTT DATA team**

es.nttdata.com