Número 104 | Julio 2025

NTT DATA

Radar

El magazine de ciberseguridad

Data Security: el nuevo perímetro digital, inteligente y regulado

Por Jorge Trujillo Ramírez

En la actualidad, las reglas del juego han cambiado. En una economía que respira datos, no podemos enfocarnos en solo proteger bases de datos estáticas o prevenir ataques de *phishing*. Hoy en día, la seguridad de los datos está en el centro de una transformación radical, marcada por el creciente uso de las tecnologías emergentes como la inteligencia artificial (IA), *cloud* distribuido, IoT industrial y *machine learning*. En este nuevo entorno, proteger los datos no es solo una cuestión técnica o de cumplimiento, es una cuestión de liderazgo estratégico multisectorial. Los ciberataques no distinguen ni tamaño ni tipo de organizaciones. En lo que va del año, las brechas de seguridad están costando miles de millones a organizaciones que, paradójicamente, invertían millones en infraestructura.

Tecnologías emergentes: ¿nuevos activos o riesgos?

El uso de IA generativa, automatización robótica, dispositivos conectados y gemelos digitales está revolucionando sectores como salud, industria, banca y seguros. Pero también ha ampliado radicalmente la superficie de ataque.

- **En el sector salud:** la IA en diagnóstico clínico procesa datos sensibles en tiempo real. Una fuga puede tener implicancias éticas, legales y reputacionales graves.
- **En el sector de banca y seguros:** algoritmos de *scoring* de riesgo manejan datos personales y financieros que deben cumplir con GDPR, DORA y legislación local.
- **En el sector industrial:** sensores IoT y redes SCADA generan datos industriales críticos, muchas veces sin segmentación adecuada ni protección *cloud native*.

Las mismas tecnologías que potencian la eficiencia también abren nuevos riesgos.

Un nuevo escenario regulatorio

Las organizaciones enfrentan, además, el desafío de un mundo con un entorno regulatorio cada vez más exigente y cada vez más expuesto. Los marcos regulatorios están pasando del "deber ser" al "deber demostrar". Es decir, no basta con tener controles, ahora se exige evidencia continua de su eficacia. Algunos ejemplos de ello:

- **DORA (*Digital Operational Resilience Act*):** exige que bancos y aseguradoras gestionen riesgos de terceros, continuidad de negocio y pruebas de ciberseguridad.
- **NIS2 (UE) y versiones LATAM:** amplían el concepto de infraestructura crítica, incluyendo salud, minería, tecnología y energía.
- ***AI Act, Executive Orders, GDPR, LGPD* y sus equivalentes locales:** establecen responsabilidad clara sobre decisiones automatizadas y el uso ético de los datos.
- **Nuevas directrices sectoriales (como IEC 62443, NIST, HITRUST):** ahora se integran como requisitos en auditorías y licitaciones.

Datos protegidos es igual a negocio protegido

Las organizaciones que entienden que los datos han dejado de ser una responsabilidad exclusiva de las áreas de TI y que, por el contrario, son un activo estratégico y no solo un riesgo, están invirtiendo en tres frentes:

1. **Gobierno de datos:** saber qué se tiene, dónde está y quién accede.
2. **Cultura de seguridad:** capacitar al personal, no solo al área de TI.
3. **Gestión proactiva de riesgos regulatorios:** convertir el cumplimiento en una ventaja de mercado.

Y es aquí donde los **líderes de TI (CISO, CTO, CIO)** deben actuar:

- Diseñando arquitecturas seguras incluyendo el uso responsable de la IA Generativa y los datos (en entornos *cloud* y OT).
- Adoptando de forma adecuada las tecnologías de seguridad autónoma (ejemplo: EDR con IA, UEBA, DLP como servicio).
- Alineando y reforzando la cultura de ciberseguridad con la estrategia de negocio.
- Integrando ciberseguridad, cumplimiento y gobierno de datos en un solo modelo.

Conclusión:

Cada día, el valor de una organización se encuentra más ligado a la capacidad que tiene para proteger, gobernar y utilizar los datos en forma ética, responsable y confiable. Por ello, aquellas organizaciones que no consideran que proteger los datos es una extensión de la protección de su negocio no podrán triunfar en mundo donde cumplir ya no es suficiente, sino que se requiere liderar desde la confianza.

Jorge Trujillo Ramírez
Cybersecurity Project Leader

Ataques a “gigantes”, por pequeños “errores”

Cibercrónica por Aldemar Moreno Moreno

Hoy en día resulta inédito que grandes corporaciones con cargas de trabajo migradas a reconocidos proveedores *cloud* se vean afectadas por brechas de fuga de datos, en concreto después de inversiones importantes en soluciones de ciberseguridad, capacitación de personal y procesos de aseguramiento, así como de evaluación y monitorización en todo este tipo de plataformas.

Es lo que tienen en común empresas como Delta Airlines (Tecero: MoveIT – Ataque a Cadena de suministro), Toyota (Grupo Criminal: Medussa – Causa: ausencia de parches) o NPD - National Public Data (Grupo criminal: USDoD – Causa: vulnerabilidades en sitio web), solo por nombrar algunos ejemplos. El denominador común es la divulgación de datos sensibles expuestos cuyas medidas de prevención y protección se encuentran enunciadas en diferentes *frameworks* de aseguramiento y son tareas del día a día en las áreas de ciberseguridad.

No es precisamente que los atacantes hubieran utilizado técnicas sofisticadas para lograr acceder, cifrar y/o exfiltrar dicha información, al contrario, se han valido de técnicas de fácil aprendizaje por alguien con nivel medio de conocimiento en tecnología, con herramientas al alcance de todos. Vamos al detalle con un ejemplo reciente.

Hablemos del Ransomware CodeFinger que afecta a *buckets* en AWS. A diferencia de otros ataques como los que afectaron a Delta Airlines y que impactaron directamente una solución en la cadena de suministro con el producto MoveIT, de transferencia de datos segura (ataque que mencionamos en la cibercrónica de octubre de 2024), CodeFinger logra vulnerar relativamente fácil la información expuesta en el servicio S3.

Todo comienza con una simple enumeración de *access key* expuestos, o claves previamente comprometidas.

Utilizando dorks como: *"AWS_SECRET_ACCESS_KEY" OR "aws_access_key_id" site:github.com* y siendo un poco más específico en los parámetros de entrada, ya se pueden obtener extensos ejemplos de exposición de secretos para dar continuidad al siguiente paso, incluso mediante el uso de Shodan, GitGuardian u otros recursos se suelen recabar datos para diseñar el perfil de ataque e irlo perfeccionando. En este punto, el atacante ya puede verificar si las llaves obtenidas cuentan con los permisos “*s3:GetObject* and *s3:PutObject*”, en cuyo caso se procede con el siguiente paso:

- Proceder con la enumeración de *buckets* s3 y objetos para determinar si hay algún interés específico en la información que pueda hacer más cuantioso el pago del rescate.

- Una vez identificados los datos el siguiente paso es cifrar utilizando claves SSE con claves de cifrado simétrico AES-256. En este punto, las llaves que se generan son almacenadas por el atacante imposibilitando que el administrador del recurso pueda regenerarlas para intentar recuperar la información. Lo máximo que observa son los *logs* en CloudTrail, la creación de claves y un ID con el cuál nada se puede hacer de cara a una recuperación.

- Por último, se modifica el ciclo de vida del dato ajustando las políticas de retención del mismo, de tal suerte que en caso de no pagar el debido rescate se procede con eliminación de la *data* cifrada. Y la cereza del pastel es el mensaje personalizado que ya conocemos con la respectiva cuenta en bitcoins para el pago del rescate, así como términos y condiciones.

Al ser este ataque reciente, aún no se han divulgado nombres de empresas afectadas por el mismo, y es posible que durante varios meses no lo sepan mientras el atacante ejecuta su labor silenciosa de identificación, cifrado y perfeccionamiento del ataque.

Ahora bien, cuando hablamos de medidas simples o por lo menos ya conocidas, es preciso referirnos a los diferentes *frameworks* de aseguramiento. Dentro de las medidas relacionadas en CIS Benckmark para AWS o Azure, Nist Cibersecurity Framework, Cloud Control Matrix de CSA, Azure Security Benchmark, AWS Well Architected *framework,* entre otros, entregan detalladamente un compendio de controles y configuraciones específicas para la protección de los datos. Para seguir enfocándonos en las medidas de prevención ante CodeFinger el mismo CIS nos lo indica:

- **Utilizar *access keys* a corto plazo:** preferiblemente vincular a IAM (Identity and Access Management) y AWS STS (Security Token Service) con acceso a corto plazo.
- **Restringir** el uso de SSE-C a través de políticas IAM para prevenir la utilización por usuarios no autorizados y bajo condiciones específicas (por ejemplo, desde IPs permitidas, o por períodos cortos, etc).
- **Habilitar** el control de versiones y bloqueo de objetos para evitar la sobreescritura o eliminación de datos críticos.
- **Monitorizar y auditar el uso de claves en AWS:** esto incluye la revisión periódica de permisos, caducidad y alcance de servicios. Servicios como GuardDuty ofrecen inteligencia y analítica para detectar fácilmente cuando se puede estar materializando una amenaza.
- **Habilitar el registro de actividades:** a través de CloudTrail y enlazado a GuardDuty (o el sistema de inteligencia y análisis de datos de la organización). Cuanto más detallado, mejor, ya que permite recabar y entregar a herramientas de inteligencia patrones inusuales como cifrado masivo o cambios en las políticas de retención de datos.

Las anteriores medidas suelen ser de fácil implementación y son tareas del ABC de la operación de ciberseguridad en este tipo de infraestructuras. Sin embargo, vemos que su aplicación, evaluación de cumplimiento, análisis de postura, monitorización y alerta no están siendo aplicadas, incluso en grandes corporaciones. ¿Qué podríamos pensar de las condiciones de aseguramiento en pymes o entidades con poca conciencia del aseguramiento de los datos?

Debemos empezar por el aseguramiento básico, pero también debemos prepararnos para los desafíos que vienen con ataques que utilizan computación cuántica, más sofisticados, veloces y eficientes. Ante ellos, no bastará con los protocolos de aseguramiento “básicos” sino que tendremos que pensar en los nuevos mecanismos de protección.

En el caso de AWS ya se está hablando de Kyber para la gestión más segura de claves, TLS post-cuántico para conexiones seguras y Kyber en SSH para protección de datos en tránsito. Azure también está incorporando ML-KEM en las soluciones de Storage, KeyVault, aquellas que utilicen TLS 1.3. Tanto AWS como Azure se alinean con la publicación FIPS 203 de la NIST (lectura que se recomienda ampliamente para entender las implicaciones que puede conllevar este nuevo reto tecnológico). En ciberseguridad esta es la clave, seguir las prácticas líderes existentes, estudiar las tendencias, no menospreciar al oponente y leer atentamente las cibercrónicas.

Aldemar Moreno Moreno
Cybersecurity Consultant

Privacidad Diferencial, un control oculto pero muy necesario en los modelos de protección de datos analíticos

Artículo por Jaime Tovar Prieto

A pesar de que la seguridad de los datos y la información siempre ha sido una preocupación general, muchas personas obtienen tranquilidad al escuchar la afirmación “Protegemos su información”, pero pocos buscan entender cómo se logra esto. En vista de lo anterior, en este artículo de RADAR se abordará el concepto de Privacidad Diferencial, utilizado por grandes de la industria como Google, Apple y Microsoft, lo que indica su efectividad en la protección de la información.

¿Qué es la Privacidad Diferencial?

La Privacidad Diferencial es un marco matemático diseñado para proteger la privacidad de los datos. Permite realizar análisis sobre grandes conjuntos de datos sin revelar información sensible sobre individuos mediante la adición de "ruido" a los resultados. Este enfoque asegura que el resultado general sea el esperado, mientras que la información personal o sensible permanece oculta.

El modelo matemático aplicado a los datos busca extraer información útil y ejecutar análisis estadísticos sobre conjuntos que pueden contener información delicada (como datos personales, creencias, salud, religión o secretos corporativos), reduciendo la posibilidad de exponer datos y salvaguardando las responsabilidades mediante la debida diligencia, en cumplimiento con las regulaciones pertinentes sobre la captura y tratamiento de información.

La aplicación de este modelo de seguridad busca equilibrar de manera “tangible” la necesidad de obtener información a partir del análisis de grandes volúmenes de datos (Big Data) y la responsabilidad ética de proteger la privacidad de la información.

Sus orígenes

La base de este concepto se remonta a 1977, con Tole Dalenius, quien propuso la posibilidad de obtener información puntual de una base de datos sin revelar datos acerca de un individuo. En 2006, Cynthia Dwork, Frank McSherry, Kobbi Nissim y Adam Smith establecieron que, en muchos casos, es posible obtener información con un alto grado de precisión, garantizando al mismo tiempo un alto nivel de privacidad.

¿Ofuscar y privacidad diferencial, es lo mismo?

Desde un punto de vista superficial, se podría considerar que sí, sin embargo, no lo es.

Mientras que los enfoques tradicionales buscan anonimizar los datos utilizados en modelos analíticos, la Privacidad Diferencial se enfoca en limitar la cantidad de información expuesta que pueda inferirse o referenciarse a una persona.

Los modelos convencionales pueden ser ineficientes; aunque son efectivos en ciertos escenarios, pueden ser susceptibles a ataques de re-identificación. Para que este ataque sea efectivo, se necesita un vector adicional relacionado con la obtención de información extra. Un ejemplo de este tipo de ataque ocurrió en 2015, cuando la investigadora Latanya Sweeney, en su trabajo “Only You, Your Doctor, and Many Others May Know”, logró identificar el 43% de los pacientes registrados en un informe de datos médicos del estado de Washington, demostrando que un proceso de ofuscación es parcialmente efectivo para la protección de información.

Ahora bien, ¿cómo funciona?

Como se indicó al inicio, la Privacidad Diferencial se basa en un modelo matemático y, más específicamente, en el parámetro épsilon (ε) y en algunos casos el parámetro delta (δ). Épsilon refleja el presupuesto de privacidad, el cual es un número que define el nivel de ruido que se agrega a un conjunto de datos. Un valor menor de épsilon indica un mayor grado de protección, aunque sacrifica parte de la precisión del análisis, mientras que un valor más alto permite mayor exactitud, pero menor protección de la información.

Por su parte, delta refleja la probabilidad de que la garantía de privacidad falle o sea afectada, superando lo que se ha definido por épsilon. Delta es un número muy pequeño, cercano a cero (por ejemplo 10 a la -5, que es equivalente a 0.00001). Es importante señalar que la existencia de esta variable podría habilitar, en cierto grado, la posibilidad de fugas de información, pero, a cambio, permite mejorar resultados en ciertos casos.

Una propiedad fundamental de este modelo matemático es que los resultados del algoritmo deben ser los mismos, independientemente de si los datos de un individuo en particular están incluidos o no en el conjunto de datos.

El primer concepto relevante en la **Privacidad Diferencial** es la adición de ruido, que consiste en insertar datos aleatorios en el conjunto original, dificultando así la identificación de la influencia de un dato particular en el resultado final. Para la inyección o adición de ruido, se contemplan dos modelos principales:

- **Mecanismo Laplace:** agrega ruido aleatoriamente siguiendo una distribución de Laplace, que tiene una forma de pico y es sensible a los cambios. Este mecanismo se utiliza para la publicación de datos demográficos o médicos.
- **Mecanismo Gaussiano:** agrega ruido aleatoriamente siguiendo una distribución de Gauss, que presenta una forma de campana y es adecuado para proteger grandes volúmenes de datos.

Adicionalmente, existen otros mecanismos dentro de la **Privacidad Diferencial** que no agregan ruido, como:

- **Respuesta Aleatoria:** introduce aleatoriedad en las respuestas a preguntas sensibles.
- **Perturbación de Datos:** modifica el conjunto original de datos, introduciendo cambios intencionales en algunos valores.

Sin embargo, la Privacidad Diferencial tiene algunos puntos que requieren atención, tales como:

- Complejidad en la implementación
- Impacto en conjuntos de datos pequeños
- Errores en la implementación

Aplicaciones en la Industria

Google aplica este modelo de privacidad para capturar información de varios de sus productos, como los resultados de búsqueda en dispositivos Android y el uso de Google Cloud BigQuery. Este último es uno de los ejemplos más claros de este componente de seguridad, ya que permite añadir ruido a los resultados y proteger la confidencialidad.

Apple utiliza la información del análisis de dispositivos para recopilar datos sobre el uso de sus productos, como pulsaciones de teclas, errores y uso de emojis. Esta recopilación se procesa de tal manera que limita el número total de contribuciones que un usuario puede hacer, preservando su privacidad a lo largo del tiempo.

Conclusión

En resumen, la **Privacidad Diferencial** es un control esencial en la captura e ingesta de datos, ya que permite generar resultados útiles sin exponer información particular de individuos. Su aplicación no solo protege la privacidad, sino que establece un estándar ético que debe ser considerado al tratar con datos personales en la era digital.

Jaime Tovar Prieto
Cybersecurity Architect

El Puerto cuántico: cómo la logística empieza a beneficiarse de la computación cuántica

Espacio cuántico
por María Gutiérrez

Aunque de momento la computación cuántica no ha alcanzado un nivel de madurez que permita su despliegue generalizado en entornos productivos reales, (debido sobre todo a las limitaciones del *hardware* cuántico), ya se están produciendo avances significativos en sectores donde los problemas de optimización son especialmente complejos. No solo se trata de simular moléculas o romper criptografía, hay otros ámbitos que se benefician ya de esta tecnología, por ejemplo, la logística, y en especial la portuaria, con miles de contenedores moviéndose a diario, decisiones críticas que deben tomarse en segundos y múltiples restricciones operativas. Los puertos se están convirtiendo en escenarios ideales para probar algoritmos cuánticos, el Puerto de Los Ángeles, uno de los más grandes y congestionados del mundo, ha sido protagonista de uno de los casos de uso más relevantes hasta la fecha.

Uno de los primeros experimentos reales con computación cuántica aplicada a logística portuaria tuvo lugar gracias a la colaboración entre SavantX, empresa especializada en análisis predictivo y D-Wave systems pionera en computación cuántica del tipo *quantum annealing* (forma especializada de computación cuántica diseñada específicamente para resolver problemas de optimización combinatoria, extremadamente eficiente para problemas que consisten en encontrar el mínimo o máximo de una función con muchas variables interrelacionadas).

El reto al que debía enfrentarse era saber cuál es la mejor manera de reorganizar estos contenedores para que las grúas las encuentren más rápido. Este reto crece en complejidad a medida que aumentan los elementos y pronto se vuelven impracticables para los ordenadores clásicos. ¿El resultado? Según los responsables del proyecto se logró una mejora del 60 % en la eficiencia operativa, es decir, menos movimientos innecesarios, menos esperas, menos caos, menos costes..., el mensaje fue claro, la computación cuántica puede marcar una diferencia real en escenarios complejos.

El caso del puerto no es el único, otras empresas están empezando a explorar cómo los algoritmos cuánticos pueden ayudarles en sus cadenas logísticas. Por ejemplo, para la optimización de rutas de taxis durante eventos de alta demanda, para resolver problemas de planificación en fábricas donde se exploran problemas como el ensamblaje óptimo de componentes y la gestión de inventarios dinámicos. También en el entorno financiero para la optimización de carteras, detección de fraudes y valoración de derivados.

Y aunque los ordenadores cuánticos actuales tienen limitaciones importantes (son sensibles, requieren refrigeración extrema y no tienen aún la escala necesaria para resolver problemas masivos), pruebas como las realizadas en el puerto sirven para preparar el terreno y aprender cómo integrar estos nuevos enfoques con los sistemas clásicos. Mientras, grandes empresas trabajan para construir ordenadores más potentes, estables y accesibles.

Si el progreso sigue a este ritmo, muchos de los algoritmos que hoy se prueban en laboratorio podrían empezar a funcionar en producción antes de que finalice esta década, porque en un mundo donde cada segunda cuenta y cada ruta puede optimizarse, la computación cuántica empieza a dejar de ser solo una promesa.

El caso del puerto es solo un ejemplo de cómo estas tecnologías pueden empezar a resolver problemas del presente, Quizá no veamos mañana una red logística mundial 100 % cuántica, pero los primeros pasos están dados ...entre contenedores...

Seguridad de los datos en la época cuántica

Artículo por Cesar Huanayque Vilca

Mientras la computación cuántica promete revolucionar numerosos campos, desde la medicina hasta la ciencia de materiales, también presenta una amenaza existencial para los cimientos de la seguridad digital actual. Los algoritmos criptográficos que protegen las comunicaciones y los datos globales, como RSA y ECC, son vulnerables a los ataques de ordenadores cuánticos suficientemente potentes. En respuesta, emerge la Criptografía Post-Cuántica (PQC) como la contramedida esencial, ofreciendo una nueva generación de algoritmos resistentes a estas futuras amenazas y asegurando la confidencialidad de nuestra información en la próxima era tecnológica.

¿Qué es la Criptografía Post-Cuántica (PQC)?

La PQC se refiere al desarrollo de algoritmos criptográficos que son seguros contra ataques perpetrados tanto por ordenadores clásicos como por los futuros ordenadores cuánticos. A diferencia de la criptografía cuántica, que utiliza la física cuántica para la seguridad, la PQC se basa en problemas matemáticos que se consideran intratables incluso para un ordenador cuántico.

Una de sus principales ventajas es que estos nuevos algoritmos están diseñados para ser implementados en la infraestructura de TI clásica existente, facilitando la transición y protegiéndonos contra la amenaza inmediata de ataques como "Recolectar Ahora, Descifrar Después" (HNDL), donde los adversarios capturan datos cifrados hoy con la intención de descifrarlos en el futuro cuando dispongan de la tecnología cuántica necesaria.

La Estandarización del NIST

El Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. ha liderado un esfuerzo global para estandarizar algoritmos PQC robustos y fiables. Tras un proceso de evaluación que comenzó años atrás, en agosto de 2024, NIST anunció la finalización de los primeros estándares PQC:

- **FIPS 203 (ML-KEM):** un mecanismo de encapsulación de claves basado en retículos (CRYSTALS-Kyber) para el establecimiento seguro de claves.
- **FIPS 204 (ML-DSA):** un algoritmo de firma digital basado en retículos (CRYSTALS-Dilithium) para la autenticación.
- **FIPS 205 (SLH-DSA):** un algoritmo de firma digital basado en hashes (SPHINCS+), que ofrece una alternativa robusta.

El proceso continúa con algoritmos adicionales como **FALCON** y **HQC** (un KEM basado en códigos seleccionado en marzo de 2025), buscando diversificar las defensas criptográficas disponibles.

Estrategias de Protección de los datos en la Era Cuántica

La PQC debe aplicarse en todos los estados de los datos para garantizar una protección integral:

1. **Datos en Tránsito:** las comunicaciones (VPN, TLS, etc.) deben actualizarse para usar algoritmos PQC, como ML-KEM para el intercambio de claves y ML-DSA para las firmas digitales, asegurando así la confidencialidad y autenticidad.
2. **Datos en Reposo:** los datos almacenados se cifran con algoritmos simétricos robustos (como AES-256), pero las claves que protegen estos datos deben ser cifradas o "envueltas" utilizando un KEM post-cuántico.
3. **Datos en Uso:** la protección aquí es más compleja, pero muchos esquemas modernos de Cifrado Homomórfico (que permiten calcular sobre datos cifrados) ya se basan en problemas de retículos, lo que los hace inherentemente resistentes a la cuántica.

Finalmente, la transición a la Criptografía Post-Cuántica no es una simple actualización tecnológica; es una evolución estratégica fundamental para la seguridad a largo plazo. Aunque el "Día Q" —cuando un ordenador cuántico pueda romper la criptografía actual— es incierto, la amenaza de "Recolectar Ahora, Descifrar Después" es presente y real. Las organizaciones que comiencen hoy su viaje hacia la resiliencia cuántica no solo protegerán sus activos más valiosos, sino que también construirán una base de confianza digital más sólida y duradera para el futuro.

Cesar Huanayque Vilca
Cybersecurity Expert Architect

¿Cómo afecta la evolución de la huella digital del usuario en la postura de seguridad de la empresa?

Tendencias por Shirley Villacorta Aristondo

En las últimas cinco décadas, la forma en que conocemos y nos relacionamos con las personas ha evolucionado drásticamente. Hasta no hace mucho, establecer conexiones significativas dependía de nuestras habilidades interpersonales: "conversar, hablar y observar". Estos métodos, junto con un genuino interés y creatividad, facilitaban relaciones en las que cada interacción revelaba sorpresas y matices, sin la inmediatez que caracteriza la comunicación actual.

Sin embargo, en la última década hemos experimentado un cambio radical en nuestras conductas interpersonales. Hablar y observar se ha vuelto algo "vintage". Ahora, nuestras interacciones están predominantemente centradas en la información que elegimos compartir en el entorno digital, lo que ha propiciado un enfoque más analítico. Esta nueva dinámica incluye la búsqueda de información sobre la identidad y la huella digital de las personas, combinada con un uso intuitivo de OSINT (Open Source Intelligence), que amplía nuestro alcance para comprender a los demás.

Hoy en día, nos encontramos ante un panorama aún más complejo y desafiante, impulsado por la explosión de la Inteligencia Artificial (IA). Este uso de la IA ha reformulado radicalmente cómo interactuamos y nos conocemos. Así, el conocimiento que obtenemos sobre una persona proviene cada vez más de su huella digital y de las inferencias que la IA puede deducir a partir de datos sobre comportamientos, emociones e incluso rasgos psicológicos. De este modo, nos convertimos en representaciones digitales, resultado de un análisis algorítmico predictivo.

Presentación de Nuevas Amenazas

En este contexto, es urgente reflexionar sobre la necesidad de desarrollar propuestas efectivas para la protección de datos y el gobierno de identidades y privilegios. Con el aumento del uso de algoritmos e inteligencia artificial para interpretar nuestras características y comportamientos, surgen preguntas legítimas sobre privacidad, consentimiento y seguridad de la información personal. Nuevas amenazas han emergido en el entorno corporativo, como *deepfakes*, clonación de identidades biométricas, y suplantación de cuentas a través de BEC (Business Email Compromise) avanzados.

Colaboración en la Nueva Postura de Seguridad

Entonces, ¿cómo podemos contribuir a redefinir la postura de seguridad de la información en las empresas? Podemos centrarnos en tres aristas:

- **Nuevo Perímetro de Protección:** La configuración de protección ha cambiado, donde el usuario se convierte en el nuevo perímetro. Esto facilita el enfoque de *Zero Trust* basado en identidad.
- **Identidad Digital como Riesgo Corporativo:** La huella digital de nuestros colaboradores se ha convertido en un nuevo objetivo para los atacantes, quienes cuentan con mayores recursos para el perfilado y ejecución de ciberataques exitosos. Esperamos que entre 2025 y 2026 se conforme la adopción de soluciones de *Digital Risk Protection* y de *Identity Threat Detection and Response*.
- **Privacidad y Seguridad como un solo frente:** La privacidad y la seguridad deben trabajar como un solo frente. No habrá lugar para obstáculos en la postura de seguridad que ignoren la privacidad, o viceversa. La implementación estabilizada de *Privacy by Design* y *Security by Design* requerirá modelos de arquitectura de seguridad y el uso de herramientas de *Data Discovery*.

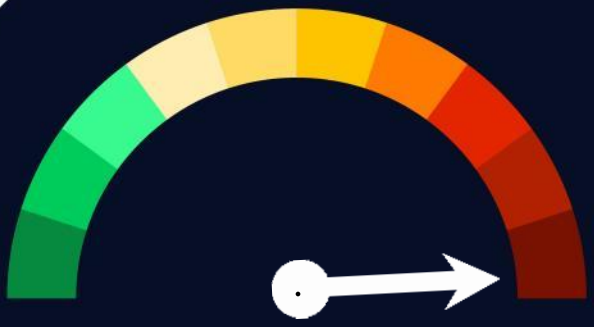
La era del riesgo sistémico digital y los desafíos asociados a la ciberseguridad requieren un enfoque proactivo y ético en la gestión de la información. A medida que avanzamos hacia un futuro digitalizado, es imperativo que se respeten las regulaciones y los derechos de cada individuo. En este sentido, la ciberseguridad ya no se limita a proteger sistemas; los programas de ciberseguridad también deben proteger a las personas y sus representaciones digitales, dado que estos elementos se han convertido en el nuevo perímetro que debe resguardarse.

Shirley Villacorta Aristondo
Cybersecurity Manager

Vulnerabilidades

Vulnerabilidad crítica de omisión de autenticación en Fortinet

Fecha: 28 de mayo de 2025
CVE: CVE-2025-22252



CVSS: 9.8

CRÍTICA

Descripción

Esta vulnerabilidad, con identificador CVE-2025-22252, consiste en una omisión de autenticación que permite a un atacante remoto obtener privilegios administrativos sin necesidad de credenciales válidas.

Esta falla pone en riesgo la integridad y disponibilidad de los sistemas afectados, ya que permite la toma completa de control, modificación de configuraciones sensibles y potencial robo de información confidencial.

Debido a su gravedad, con una puntuación de CVSS de 9.8, representa una amenaza crítica para las organizaciones que dependen de estos dispositivos en sus infraestructuras de red.

Solución

Fortinet publicó parches oficiales entre finales de mayo y principios de junio de 2025 que corrigen esta omisión de autenticación.

Se recomienda actualizar a las siguientes versiones:

- FortiOS 7.4.7 o superior
- FortiProxy 7.6.2 o superior
- FortiSwitchManager 7.2.6 o superior

Además, como medida temporal, se sugiere restringir el acceso administrativo mediante políticas de *firewall* y fortalecer la monitorización de accesos.

Productos afectados

Esta vulnerabilidad crítica afecta a varios productos Fortinet, entre los que destacan los siguientes:

- FortiOS (7.4.4 a 7.4.6 y 7.6.0)
- FortiProxy (7.6.0 a 7.6.1)
- FortiSwitchManager (7.2.5)

Referencias

- incibe.es
- fortiguard.fortinet.com

Vulnerabilidades

Vulnerabilidad de severidad alta en Google Chrome

Fecha: 2 de junio de 2025
CVE: CVE-2025-5419

CVSS: 8.8

ALTA

Descripción

Se ha detectado una vulnerabilidad de severidad alta que afecta a la versión 8 de Google Chrome.

Esta vulnerabilidad permitiría a un atacante, mediante una explotación *out-of-bound* la corrupción de memoria a través de una página HTML específicamente diseñada.

Esta es la segunda vulnerabilidad *zero-day* explotada activamente que Google ha tenido que parchear este año, siendo la primera en ser parcheada la vulnerabilidad CVE-2025-2783.

Solución

Google recomienda actualizar su navegador a las siguientes versiones:

- Actualizar a las versiones 137.0.7151.68 o 137.0.7151.69 para los usuarios de Windows o MacOS.
- Para los usuarios de Linux se recomienda actualizar a la versión 137.0.7151.68.

Productos afectados

La vulnerabilidad afecta a las siguientes versiones de Google Chrome:

- Versiones anteriores a la 137.0.7151.68.

Referencias

- thehackernews.com
- nvd.nist.gov

Parches de seguridad de Microsoft de junio para corregir 67 vulnerabilidades

Fecha: 10 de junio de 2025
CVE: CVE-2025-32711 y 66 más

Crítica

Descripción

Microsoft ha publicado parches en los que se corrigen 67 vulnerabilidades, siendo 2 de ellas de severidad crítica. Las vulnerabilidades identificadas más relevantes son las siguientes:

- CVE-2025-32711 (CVSS 9.3): afecta a M365 Copilot y permitiría a un atacante mediante *AI command injection* propagar información a través de una red.
- CVE-2025-47966 (CVSS 9.8): por otro lado, esta vulnerabilidad permitiría elevar privilegios en una red mediante la exposición de información clasificada a un usuario sin privilegios.

Por último, también destacan algunas vulnerabilidades de severidad alta:

- CVE-2025-47167 (CVSS 8.4): vulnerabilidad de confusión de tipos en Microsoft Office que permite ejecutar código de forma remota.
- CVE-2025-47957 (CVSS 8.4): esta vulnerabilidad de tipo *use after free* en Microsoft Word permitiría a un atacante realizar ejecución de código de forma remota.

Productos afectados

Las vulnerabilidades afectan a numerosos productos de Microsoft. Se puede encontrar el listado completo de los productos afectados en el siguiente enlace:

- msrc.microsoft.com

Solución

Desde Microsoft recomiendan aplicar el parche publicado para remediar las vulnerabilidades indicadas en el mismo.

Referencias

- msrc.microsoft.com
- thehackernews.com

Parche para la vulnerabilidad de ejecución remota en servidores WebDAV

Fecha: 10 de junio de 2025
CVE: CVE-2025-33053

Alta

Descripción

El parche para esta vulnerabilidad, que afecta a servidores con WebDAV en Microsoft IIS, Apache y Nginx, fue lanzado el 10 de junio de 2025 durante el Patch Tuesday de Microsoft.

La vulnerabilidad estaba siendo explotada por el grupo Stealth Falcon. Esta actualización soluciona un problema en la validación de rutas y nombres de archivos que permitía a atacantes remotos ejecutar código malicioso en el servidor mediante la manipulación del protocolo WebDAV.

Con este parche, se corrige la validación insuficiente que facilitaba la explotación, mejorando la seguridad del servidor. Además, Apache y Nginx publicaron sus propias actualizaciones para cerrar esta vulnerabilidad.

Productos afectados

Las versiones afectadas incluyen las siguientes:

- Microsoft IIS anteriores al parche liberado el 10 de junio de 2025
- Apache HTTP Server desde la 2.4.0 hasta antes de la versión 2.4.57
- Versiones de Nginx anteriores a la actualización de junio de 2025.

Solución

Se recomienda instalar los parches oficiales publicados por Microsoft, Apache y Nginx para corregir la vulnerabilidad. Además, se sugiere desactivar WebDAV donde no sea necesario y monitorizar los accesos para detectar posibles intentos de ataque.

Referencias

- incibe.es
- microsoft.com

Eventos

RAISE Summit 2025
8 - 9 julio

RAISE Summit 2025 se celebrará el 8 y 9 de julio de 2025 en el Carrousel du Louvre, París. El evento reunirá a líderes tecnológicos para compartir casos prácticos de implementación de IA e IA Generativa, con un *hackathon* de más de 300 participantes enfocado en soluciones reales. Contará con la participación de más de 150 inversores, impulsando las innovaciones disruptivas en IA.

Enlace

Data Center Asia 2025
15 - 17 de julio

Data Center Asia 2025 se celebrará del 15 al 17 de julio de 2025 en AsiaWorldExpo, Hong Kong (China), como evento central para infraestructura digital, *cloud*, IA y ciberseguridad en la región Asia-Pacífico. Reunirá a operadores de centros de datos, especialistas IT, expertos en seguridad y sostenibilidad, con más de 100 conferencias, paneles y stands de soluciones líderes. Se enfocará en innovaciones en eficiencia energética, diseño de instalaciones, IA y estrategias de protección frente a ciberamenazas.

Enlace

UserConf México 2025
16 – 17 de julio

UserConf México 2025 se llevará a cabo los días 16 y 17 de julio de 2025, en el Hilton México City Reforma en Ciudad de México. El evento reunirá a líderes y profesionales de IT para explorar las últimas tendencias en gestión IT y ciberseguridad, con talleres prácticos y sesiones técnicas. Habrá presentaciones de expertos y amplias oportunidades de *networking*.

Enlace

Recursos

➢ Handbook for Cyber Stress Tests

Handbook for Cyber Stress Tests publicado por ENISA ofrece una guía práctica para que autoridades nacionales y sectoriales evalúen la resiliencia cibernética de infraestructuras críticas bajo la directiva NIS2. Define las pruebas de estrés cibernético como evaluaciones dirigidas para medir la capacidad de soportar y recuperarse de incidentes graves, utilizando escenarios realistas y métricas de resiliencia. Presenta una metodología clara en cinco pasos: alcance y objetivos, diseño de escenarios, ejecución, análisis de brechas y seguimiento.

Enlace

➢ Likely Exploited Vulnerabilities

Likely Exploited Vulnerabilities (LEV) es una métrica propuesta por NIST que estima la probabilidad de que una vulnerabilidad ya haya sido explotada en la práctica. A diferencia de las listas KEV (Known Exploited Vulnerabilities) que registran casos confirmados, la LEV utiliza datos históricos para identificar vulnerabilidades con probabilidad real de haber sido explotadas. La metodología combina puntajes EPSS (Exploit Prediction Scoring System) a lo largo del tiempo para calcular la probabilidad acumulada de explotación pasada, mejorando así la priorización en la gestión de parches.

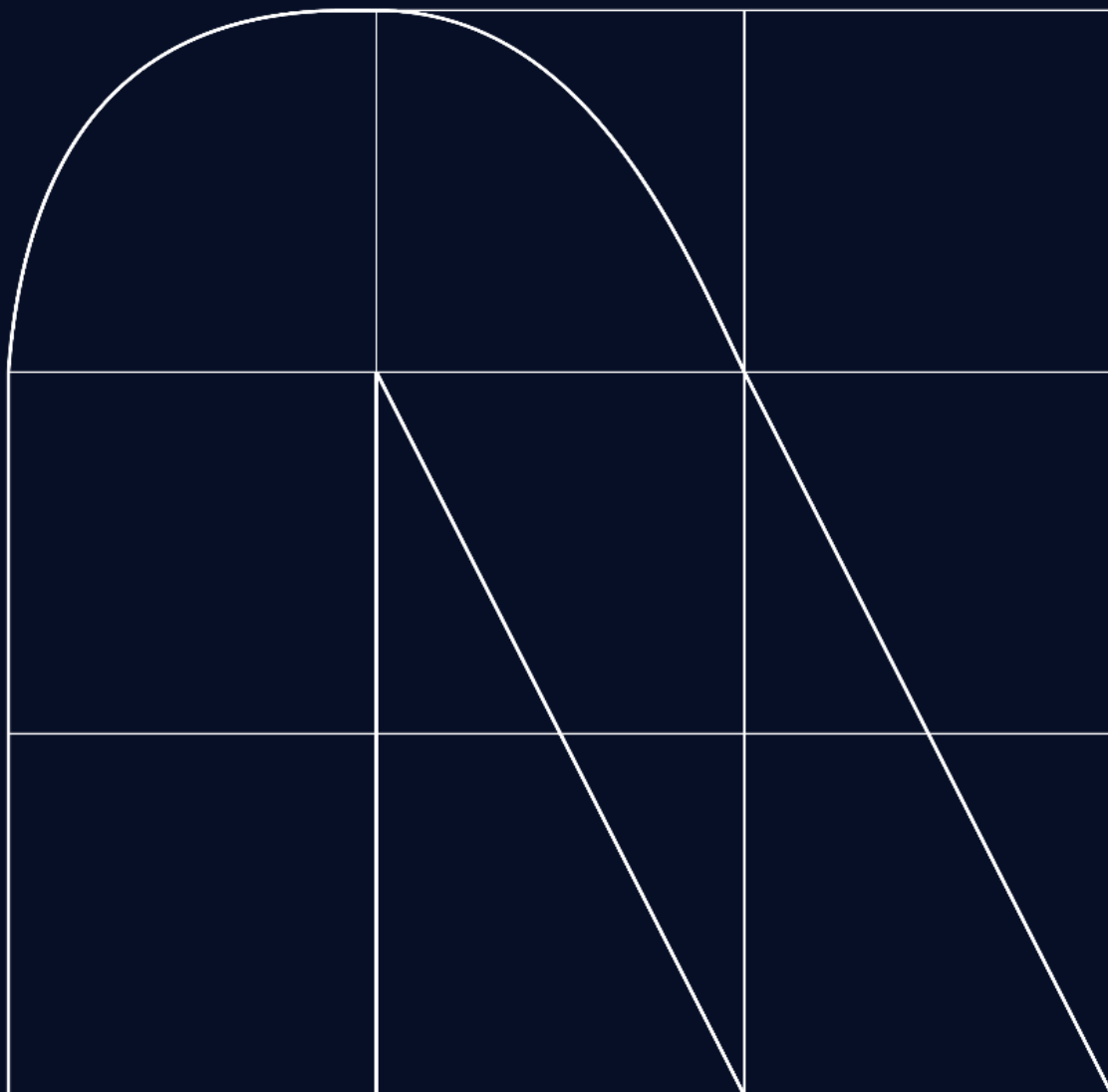
Enlace

➢ Guía de taller NIST sobre Usable Cybersecurity y Privacidad en tecnologías inmersivas

La Guía de taller virtual de NIST sobre Usable Cybersecurity y Privacidad en tecnologías inmersivas (IR 8557) aborda retos únicos en UX de seguridad y privacidad para realidad virtual/aumentada, explorando cómo interfaces inmersivas interactúan con datos biométricos y comportamentales. Incluye ponencias de investigación, panel de expertos y protocolos para integrar protección usable en entornos AR/VR.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com