Número 108 | Noviembre 2025

NTT DATA

Radar

El magazine de ciberseguridad

NIS2 y DORA: un único marco de gobierno para Europa

Por Carlos Chavarría

La Unión Europea se dirige hacia un marco común en materia de ciberseguridad. La actualización de la directiva NIS2 y la creación del reglamento DORA buscan unificar el gobierno a través de la implicación del personal de la capa ejecutiva, la gestión del riesgo, la gestión de terceros, la gestión de incidentes, la cadena de suministro, la seguridad de la información, y la continuidad de negocio para crear un marco general.

Estas iniciativas las regulan sectores de la Unión Europea catalogados como críticos en la Directiva NIS2 como las energéticas, el transporte, la banca o el sector sanitario.

Mientras que el Reglamento DORA homologa la gestión del riesgo TIC en los seguros, en el mercado de capitales y en la banca. Mediante controles de seguridad definidos y los estándares técnicos se está logrando armonizar las herramientas, los métodos, los procesos y las políticas de las organizaciones.

Todos estos cambios están incrementando el nivel de exigencia de las empresas y, como consecuencia, un aumento de los costes para cumplir con las normativas. Según IDC, el gasto en ciberseguridad encadena dos años de incremento en dobles dígitos 10,6% en 2023 y 12,3% en 2024, respectivamente.

Se prevé una senda cercana al doble dígito hacia 2026, con el mercado europeo rondando los 71.000 M$. En paralelo, el presupuesto de TI que las organizaciones reservan a seguridad ya asciende al 9,0%, según ENISA en el informe emitido para el 2024. Como termómetro de intención a 12 meses, el Trends Report 2025 de Infosecurity Europe detecta un aumento medio previsto del 31% en los presupuestos entre los encuestados.

El incremento de los costes se traduce en una mejora en las medidas de seguridad de las organizaciones. Dicho progreso se da tanto en los controles preventivos como en los reactivos. Existe una concienciación en la mejora de medidas de seguridad para evitar incidentes.

El aumento exponencial de ataques año tras año confirma la importancia de llevar a cabo tanto controles reactivos como los planes de contingencia ante incidentes o la manera en la que se reportan. El plan de la Unión Europea unifica con la Directiva NIS2 y el Reglamento DORA el gobierno de la ciberseguridad en la manera de reportar los incidentes en tiempo y forma.

NIS2 obliga a extender el gobierno más allá del perímetro, con la evaluación continua de proveedores, cláusulas contractuales que llegan a los controles y planes de continuidad compartidos. DORA añade la pieza operativa en el sector financiero: en la vigilancia específica sobre proveedores TIC críticos, en los escenarios de concentración, en las pruebas de resiliencia y en el reporte sobre incidentes coordinados.

El resultado final se evidencia en un único catálogo de requisitos para terceros, una matriz de criticidad viva y evidencias homogéneas para auditoría. Se gestiona de igual modo que lo propio, con *due diligence real:* los ejercicios de crisis con proveedores prioritarios, las métricas de salud (con sus correspondientes tiempos de notificación, cobertura contractual y porcentaje de planes probados) y decisiones informadas sobre dependencia. El resultado de su implementación se certifica con menos imprevistos y más resiliencia medible.

Europa ha elegido el modelo a seguir y es la convergencia regulatoria para elevar el listón y medir el impacto con rigor. NIS2 y DORA se complementan. La factura sube, pero el retorno también. Supone un menor tiempo fuera de servicio, de riesgo legal y más confianza del cliente. Todo ello se traslada en un solo marco de gobierno NIS2–DORA, un catálogo único de controles para negocio, TI y terceros, y un reporte de incidentes cronometrado que cierra el círculo. Se pasa entonces de cumplir por obligación a demostrar resiliencia con datos. Si bien antes se realizaba un marcado de casillas para demostrar el cumplimiento, ahora se protege la continuidad.

Carlos Chavarría
Cybersecurity Senior Consultant

El *ransomware* no se ha ido de vacaciones

Cibercrónica por Antonio Melo y Alejandro Ignacio García

El verano de 2025 ha vuelto a demostrar que el ciberespacio no para de inquietar y seguir avanzando. Mientras millones de personas se desconectaban, los grupos de ciberdelincuentes y los equipos de seguridad han mantenido ese pulso silencioso e ininterrumpido. El mes de septiembre ha dado por cerrada la temporada estival trayendo unas conclusiones que realmente son preocupantes, pues se mezclan ataques de alto impacto, vulnerabilidades críticas y ha empezado un intenso debate sobre la resiliencia de infraestructuras críticas y una visión de la ciberseguridad con la inteligencia artificial.

Los ataques de *ransomware* han mantenido su hegemonía durante los meses estivales. Volvemos a encontrar en el sector sanitario y la administración pública los preferidos de los ataques con *ransomware*.

Países europeos como Irlanda, Suiza o Alemania, han vuelto a vivir el secuestro de sistemas que ha llevado a algunos hospitales a suspender citas o aplazar operaciones.

El nivel de sofisticación de esas campañas demuestra la forma como los grupos criminales modifican sus preferencias en las tácticas híbridas, como la extorsión doble, el robo de información sensible y las filtraciones públicas para presionar a sus víctimas.

Zero-days y vulnerabilidades críticas

El verano ha hecho llegar varios avisos urgentes de los fabricantes. Vulnerabilidades críticas de sistemas de virtualización o de *software* implantado de forma masiva en entornos corporativos han hecho que las tareas de los equipos de seguridad tuvieran que aplicar parches en pleno agosto.

La ventana de exposición ha sido de nuevo reducida al extremo, recordando que el ciclo de parches no se mide ya en semanas, sino en horas.

Geopolítica digital en tensión

Las tensiones internacionales también han sido cuantificadas en el ámbito cibernético.

Este tipo de investigaciones en seguridad han detectado un aumento notable de las campañas de espionaje de infraestructuras energéticas y de transporte en Europa del Este vinculadas a agentes estatales cuyo objetivo es la recolección de inteligencia estratégica en un momento dominado por la incerteza geopolítica.

El auge ofensivo y defensivo de la IA

El mes de septiembre consolidó un tema debatido: el papel de la IA en ciberseguridad. A medida que las organizaciones empiezan a experimentar con algoritmos que son capaces de detectar anomalías o incluso de automatizar la respuesta a incidentes, los atacantes no se quedan a la zaga: se han documentado campañas de *phishing* que emplean mensajes generados por IA que son prácticamente indistinguibles de la comunicación legítima, lo cual eleva la peligrosidad para usuarios y empresas.

Balance: un verano que certifica la tendencia

La cibercrónica de este verano y de septiembre apunta a un patrón claro: la profesionalización del delito digital avanza más rápido que la capacidad de adaptación de muchas organizaciones.

El *ransomware*, los *zero-days*, las campañas de espionaje... forman un cóctel en el que CISOs y equipos de seguridad deben reforzar su capacidad de anticipación. El otoño se perfila como un nuevo capítulo en un tablero en el que solo es constante la presión permanente.

Antonio Melo Leon
Cybersecurity Analyst

Alejandro Ignacio García
Cybersecurity Lead Analyst

GRC: el pilar estratégico de la seguridad y la sostenibilidad organizacional

Artículo por Eduardo Fernando Alves

En un panorama digital cada vez más complejo, las organizaciones enfrentan una multitud de riesgos que van mucho más allá de las amenazas tecnológicas. La interconexión entre sistemas, la dependencia de los datos y la constante evolución de la legislación exigen un enfoque integrado de gestión empresarial. Este es el escenario donde surge el concepto de GRC (Gobernanza, Riesgo y Cumplimiento). Se trata de un marco que permite a las organizaciones alinear los objetivos estratégicos, gestionar eficazmente los riesgos y garantizar que las operaciones cumplan con normas y regulaciones.

Más que un conjunto de procesos administrativos, GRC representa una filosofía de gestión que combina visión estratégica, disciplina operativa y cultura organizacional. Cuando se implementa correctamente, se convierte en un verdadero diferenciador competitivo, fomentando la resiliencia, la transparencia y la confianza entre todas las partes interesadas.

Qué es GRC y por qué es esencial

Gobernanza, Riesgo y Cumplimiento (GRC) forman un triángulo inseparable dentro de las buenas prácticas corporativas.

La gobernanza define cómo se dirige la organización, incluyendo la estructura de toma de decisiones, la definición de responsabilidades y la alineación con los objetivos estratégicos.

La gestión del riesgo busca identificar, evaluar y mitigar las amenazas que podrían comprometer la continuidad del negocio, ya sean de naturaleza financiera, operativa, tecnológica o reputacional.

El cumplimiento garantiza que todas las actividades organizacionales se ajusten a las leyes, regulaciones, políticas internas y principios éticos.

Integrar estas tres dimensiones es vital para asegurar que la empresa opere de manera responsable, transparente y sostenible. Cuando el GRC se aborda de forma fragmentada, se crea un entorno propenso a la ineficiencia, la duplicación de esfuerzos y los fallos que pueden derivar en pérdidas financieras, daños reputacionales y sanciones legales.

El papel fundamental del GRC en la ciberseguridad

La ciberseguridad ha trascendido el ámbito técnico; hoy es una prioridad estratégica que impregna toda la estructura organizacional.

Un programa eficaz de Gobernanza, Riesgo y Cumplimiento (GRC) fortalece la seguridad digital al establecer políticas claras, definir responsabilidades y fomentar una cultura de vigilancia continua.

Con GRC, la empresa puede identificar con rapidez los riesgos cibernéticos críticos, evaluar el impacto potencial de los incidentes y desplegar mecanismos sólidos de respuesta y recuperación.

Esta alineación con la estrategia corporativa garantiza que las decisiones se tomen en función de riesgos reales, y no de percepciones.

Además, GRC asegura que los controles de seguridad no operen de manera aislada, sino integrados con la auditoría, el cumplimiento normativo y la gestión de la continuidad del negocio. Es esta visión holística la que diferencia a las organizaciones preparadas para el futuro de aquellas que simplemente reaccionan ante las crisis.

Cultura y liderazgo: los cimientos de un GRC eficaz

Ningún programa de GRC será efectivo sin la participación de la alta dirección y el compromiso de toda la organización.

La cultura del riesgo debe fomentarse desde arriba, promoviendo el comportamiento ético, la toma de decisiones basadas en evidencias y la responsabilidad individual. Más que documentos y políticas, el GRC se sostiene en las personas y sus actitudes.

La comunicación interna también es un factor determinante. Cuando los empleados comprenden el valor de la gestión del riesgo y reconocen su papel dentro de ese marco, el GRC deja de percibirse como un conjunto de obligaciones burocráticas y pasa a verse como una herramienta que apoya la toma de decisiones informadas.

La formación y la concienciación continuas son igualmente esenciales. En la era de la transformación digital, los riesgos evolucionan a diario, lo que exige que los equipos estén preparados para responder con agilidad y criterio.

Los beneficios de un enfoque integrado

Implementar un modelo maduro de GRC aporta beneficios significativos a la organización como:

- Mejor toma de decisiones, basada en información consolidada sobre riesgos y controles.
- Reducción de costos y duplicidades mediante la integración de procesos y sistemas de monitorización.
- Mayor confianza de inversores, clientes y reguladores gracias a la transparencia en la gestión.
- Mayor resiliencia operativa y capacidad de respuesta ante incidentes críticos.
- Consolidación de la reputación organizacional como entidad ética, responsable y predecible.

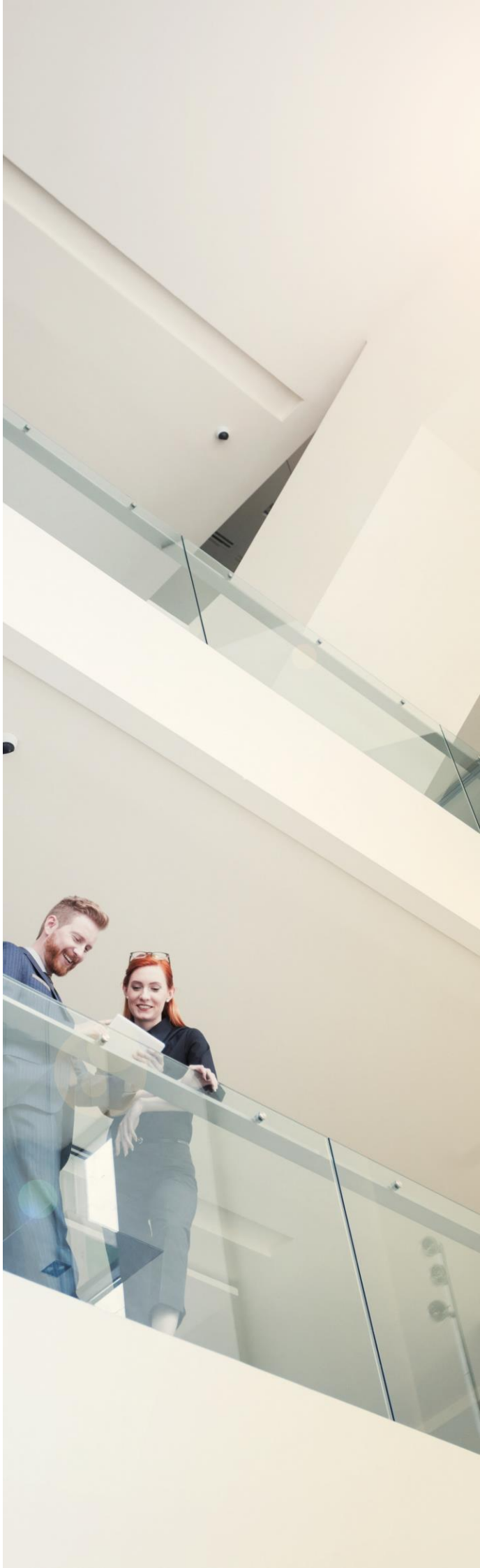
Más allá de estos beneficios tangibles, GRC promueve la innovación responsable. Al comprender sus riesgos y operar de manera controlada, la empresa puede explorar nuevas oportunidades de forma segura, sin comprometer el cumplimiento ni la confianza del mercado.

Los verdaderos desafíos detrás de los fracasos en la implementación del GRC

A pesar de sus promesas, un número considerable de programas de GRC no prospera. ¿La causa principal? Rara vez es técnica. Con mayor frecuencia, el problema radica en enfoques desconectados o, peor aún, en la falta de compromiso genuino de la alta dirección.

Otra trampa común es la burocracia asfixiante. Algunas organizaciones caen en el error de adoptar marcos de GRC excesivamente complejos. En lugar de simplificar las operaciones, terminan generando una resistencia interna generalizada, convirtiendo el cumplimiento en un obstáculo.

La clave de un GRC verdaderamente eficaz reside en la simplificación radical. Es esencial centrarse en el riesgo real, asegurando que los mecanismos de control sean proporcionales y perfectamente adaptados a la realidad de la empresa. La tecnología es una herramienta poderosa: puede centralizar datos, automatizar informes y proporcionar trazabilidad.



Sin embargo, no se debe confundir la herramienta con el objetivo: la tecnología siempre debe estar al servicio de la estrategia, nunca al revés.

El futuro del GRC

Con el avance de la inteligencia artificial, la automatización y el análisis predictivo, el GRC está entrando en una nueva era.

Las herramientas inteligentes son capaces de identificar patrones de riesgo, predecir incidentes, preparar evaluaciones de seguridad y apoyar la toma de decisiones en tiempo real.

La tendencia es que el GRC evolucione de una función de control reactiva a un sistema dinámico, basado en datos, que anticipe amenazas y guíe proactivamente el negocio.

Sin embargo, a medida que las herramientas se vuelven más sofisticadas, también aumentan la responsabilidad ética y regulatoria. El futuro del GRC requerirá profesionales capaces de equilibrar tecnología, estrategia y valores humanos, manteniendo siempre el foco en la integridad y la confianza.

La diferencia entre reaccionar y liderar

La Gobernanza, el Riesgo y el Cumplimiento (GRC) no son simples obligaciones corporativas. Son, en realidad, los cimientos que garantizan la credibilidad, la seguridad y la longevidad de cualquier organización moderna. Vivimos en una era en la que las amenazas cibernéticas están interconectadas y la presión regulatoria es cada vez mayor.

En este escenario complejo, el GRC actúa como una guía esencial que orienta el liderazgo hacia una gestión responsable y predecible.

Hoy, la madurez en GRC es el verdadero indicador de resiliencia. Las empresas que adoptan este principio con rigor y visión estratégica no solo evitan sanciones; construyen activamente una base sólida para un crecimiento sostenible y, lo más importante, ganan la confianza del futuro.

Eduardo Fernando Alves
Cybersecurity Expert Engineer

Resiliencia operativa digital: riesgo tecnológico, continuidad del negocio y riesgo de terceros

Artículo por Fernando Valles Barbudo

La resiliencia operativa digital es una tendencia dentro de la gestión de los riesgos operativos de toda empresa. En el ámbito financiero (banca y seguros) ha entrado en vigor este año el Reglamento DORA (Digital Operational Resilience Act, por sus siglas en inglés), lo que supone una vuelta de tuerca más en la gestión y control de los riesgos no financieros. Además, puede concebirse como un compendio de mejores prácticas de aplicación en empresas no financieras que, si bien no están obligadas a su cumplimiento, sí quieran repensar su modelo de gestión y cultura de riesgos.

Riesgo tecnológico

La tecnología se ha convertido en una parte muy relevante de las **estrategias empresariales**, dejando atrás su percepción como un simple medio.

Su uso conlleva implícitamente la asunción de los **riesgos** afectos a la misma, por lo que es necesario disponer de un **marco de gestión** adecuado y un apetito al riesgo establecido por la Alta Dirección. De hecho, los riesgos de las tecnologías de la información y las comunicaciones (TIC) pueden tornarse cruciales para la **supervivencia y resiliencia** de las empresas.

Y no solo se considera el riesgo implícito en las infraestructuras IT propias de las entidades, sino que el ecosistema de impacto es mucho mayor. La tendencia de externalización de infraestructuras en servicios proporcionados por *hyperscalers*, y su posición cada vez más extendida en toda la actividad empresarial, como proveedores para el almacenamiento y procesamiento de las operaciones (en la nube), hace que empresas no consideradas como entidades financieras sean *de facto* parte del flujo de análisis de riesgo.

Orígenes del riesgo tecnológico

Los orígenes del riesgo tecnológico son variados, pero generalmente se utiliza la siguiente clasificación:

- **Riesgo de Disponibilidad y Continuidad de Sistemas**: derivado de que el desarrollo y disponibilidad de sistemas y datos TIC se vea adversamente afectado. Esto incluye la incapacidad de la recuperación a su debido tiempo de los servicios de la entidad, por un fallo en los componentes de *software* o *hardware*.
- **Riesgo de Seguridad de la información:** derivado del acceso no autorizado a los sistemas y datos TIC desde dentro o fuera de la institución.
- **Riesgo de Cambio en Sistemas:** derivado de la incapacidad de la institución para gestionar cambios en sus sistemas TIC en un tiempo adecuado y de forma controlada.
- **Riesgo de Integridad de Datos:** derivado de que los datos almacenados y procesados sean incompletos, inexactos o inconsistentes en diferentes sistemas, lo que perjudica la capacidad de la institución para proveer servicios y gestionar la información en tiempo y de forma adecuada.
- **Riesgo de *Outsourcing*:** derivado de la externalización de actividades y sistemas. Nótese la importancia de *outsourcing cloud*.

Los eventos de cualquiera de estos orígenes pueden poner en jaque la continuidad del negocio.

El riesgo tecnológico como parte del riesgo operacional

El riesgo operacional se define como el riesgo de **pérdidas (económicas)** derivadas de, entre otras causas, (i).- incidencias en el negocio y fallos en los sistemas; (ii).- fallos en la ejecución, entrega y gestión de procesos; (iii).- daños a activos materiales; o (iv).- fraude (interno o externo).

Por tanto, los eventos que generan riesgo tecnológico deben ser clasificados y considerados como parte de la gestión del riesgo operacional. Disponer de una **gestión integrada** no es un tema técnico, sino de gobierno: un único **apetito de riesgo**, una **taxonomía** común y **prioridades** alineadas con el valor del proceso y del **negocio**, no únicamente con el componente tecnológico "*per-se*".

El trinomio proceso-riesgo-control se extiende a servicio/activo/plataforma/aplicación/ vulnerabilidad... siendo de aplicación igualmente la determinación del riesgo inherente y residual.

Los perfiles de gestión de ambos tipos de riesgo son cualitativamente diferentes, pero necesarios.

En el caso del sector bancario, estos podrían incorporarse en la estimación del consumo de capital regulatorio por riesgo operacional.

Procesos críticos o esenciales

Identificar procesos críticos es el primer paso para cualquier estrategia de resiliencia. Son aquellos cuya interrupción supera la **tolerancia al impacto** del negocio. El análisis de impacto en negocio (BIA) debe cuantificar ventanas máximas de interrupción (MTPD), Recovery Time Objective/ Recovery Point Objective (RTO/RPO) y dependencias: personas, datos, aplicaciones, infraestructura y terceros.

Disponer de un **catálogo vivo** de procesos esenciales, con su mapa proceso–activo–dato–proveedor y riesgos asociados cuantificados con o sin mitigantes (riesgos inherentes y residuales). Ese catálogo ordena **prioridades**, dirige las **pruebas de resiliencia** y alinea todos los **equipos** involucrados.

Además, este mapa de procesos debe mapearse de manera bidireccional con aquellos componentes IT que dan soporte en la operación para una identificación y prevención de riesgos: sistemas/procesos comprometidos antes ataques, vulnerabilidades, fallos varios, etc.

Los procesos catalogados como críticos deberán ser **monitorizados** con mayor celo, máxime si se cuenta con un tercero en la cadena de valor.

Continuidad del negocio y pruebas de resiliencia

No todo en continuidad es la ISO 22301. En banca, la regulación DORA también amplia aspectos relativos para la **continuidad del negocio**.

Además de las estrategias proporcionales a partir de los RTO/RPO del BIA y del ciclo de mejora continua PDCA (*plan-do-check-act*) para el SGCN (Sistema de Gestión de Continuidad de Negocio) en DORA se establecen varias tipologías de **pruebas de resiliencia**:

- Evaluaciones y escaneos de vulnerabilidades.
- Análisis de "*open source*".
- Evaluaciones de seguridad de red.
- Análisis de brechas (*gap analysis*).
- Revisiones de seguridad física.
- Cuestionarios y soluciones de escaneo automatizado.
- Revisiones de código fuente (cuando sea viable).
- Pruebas basadas en escenarios.
- Pruebas de compatibilidad y de rendimiento.
- Pruebas "*end-to-end*".
- Pruebas de penetración (*pentesting*).

Riesgo de terceros

Los proveedores son parte real de la cadena operativa y digital. Muchos de los problemas tienen su origen en la **externalización** a terceros, y en toda la **cadena de subcontratación**. Por ello, una buena gestión de terceros es esencial (TPRM, *third-party risk management*) y constituye uno de los pilares esenciales de DORA.

En términos simples, la gestión de proveedores debe realizarse en todo su **ciclo de vida**: (i).- homologación del proveedor; (ii).- evaluación del binomio proveedor-servicio; (iii).- prestación del servicio y (iv).- estrategia de salida.

Los **marcos de control y auditoría** sobre las operaciones están evolucionando, poniendo los **procesos en el centro** y revisándolos/auditándolos en su conjunto sin importar quien los opera, e incluyendo en las actuaciones a todos los equipos implicados, ya sean internos o externos.

Llegados a este punto, cabe plantearse unas **preguntas**: ¿cuántos recursos humanos y técnicos se dedican a la ciberseguridad y cuántos al riesgo de terceros?, ¿cuánto riesgo real o potencial tiene su origen en la ciberseguridad y cuánto en el riesgo de terceros?, ¿es la inversión dedicada a ambos bloques adecuada, proporcional y equilibrada en relación con el riesgo que emana de cada uno?, ¿es suficiente granular el marco de apetito al riesgo de las compañías para establecer un adecuado nivel de tolerancia e identificar aquellos riesgos inaceptables que deban de ser mitigados?

Fernando Valles Barbudo
Business Consulting Director – Finance, Risk & Compliance

Internet cuántico

Espacio cuántico
por María Gutiérrez

El “internet cuántico” es una nueva generación de red de comunicaciones que utiliza las leyes de la mecánica cuántica para transmitir información.

Si la internet actual se basa en copiar y transmitir información, el Internet cuántico se fundamenta en algo mucho más radical: la imposibilidad de copiarla. Esa idea, que puede parecer una paradoja en plena era de la réplica digital, es precisamente su mayor fortaleza. La base física que lo sostiene es el teorema de no clonación, una de las piedras angulares de la mecánica cuántica. Este principio, formulado en los años ochenta, establece que no se puede crear una copia exacta de un estado cuántico desconocido. Dicho de otro modo, si una partícula porta información codificada en su estado cuántico, por ejemplo, la polarización de un fotón, cualquier intento de duplicarla o medirla altera ese estado irremediablemente. Esta imposibilidad de copiar hace que la comunicación cuántica sea, en teoría, invulnerable a la interceptación.

Hoy, el internet cuántico es una realidad en construcción. Existen prototipos funcionales y redes experimentales en distintas partes del mundo. Aunque el concepto parece abstracto, los avances son reales. En 2017, el satélite chino Micius demostró por primera vez la distribución cuántica de claves entre estaciones terrestres separadas por 1.200 kilómetros. En Europa, el proyecto EuroQCI está construyendo una red de comunicaciones cuánticas seguras que enlazará los Estados miembros mediante enlaces terrestres y satelitales. España participa en esta iniciativa a través del programa Quantum Spain, coordinado por el Instituto de Ciencias Fotónicas (ICFO), el Instituto de Física Teórica (IFT) y el Centro Criptológico Nacional (CCN), que trabaja en la adaptación del Esquema Nacional de Seguridad al futuro escenario postcuántico.

A pesar de los progresos, el camino hacia un internet cuántico global está lleno de desafíos. El primero es tecnológico: los cúbits son extremadamente frágiles y pierden su coherencia con facilidad, lo que limita la distancia de transmisión. Para solventarlo se trabaja en los llamados repetidores cuánticos, que permitirían extender la red sin destruir la información. El segundo gran reto es de infraestructura, las redes cuánticas no reemplazarán a las actuales, sino que coexistirán con ellas, lo que exige protocolos híbridos capaces de integrar comunicaciones clásicas y cuánticas de forma eficiente.

Finalmente, existe un reto estratégico y geopolítico, las comunicaciones cuánticas tienen implicaciones directas para la seguridad nacional y la soberanía tecnológica. Los países que dominen estas redes podrán garantizar la confidencialidad de sus datos y proteger sus infraestructuras críticas frente a futuros ataques de ordenadores cuánticos.

El internet cuántico no llegará de golpe, sino por fases. Primero veremos redes cuánticas metropolitanas para entornos financieros o gubernamentales, seguidas de una expansión nacional y, finalmente, una interconexión global. Es posible que, dentro de una o dos décadas, el tráfico de información más sensible, desde datos médicos hasta comunicaciones diplomáticas, circule por canales cuánticos.

Lo fascinante de esta revolución es que, cuando se consolide, no será visible para el usuario común, navegaremos igual, pero bajo la superficie existirá una arquitectura completamente nueva, diseñada no solo para transmitir información, sino para preservarla con un nivel de seguridad que hoy solo podemos imaginar.

El internet cuántico no pretende sustituir al actual, sino complementarlo. Mientras las redes tradicionales se apoyan en el electromagnetismo clásico y en la criptografía matemática, la red cuántica se sustenta en las leyes fundamentales de la naturaleza, no será solo una evolución tecnológica, sino una nueva forma de entender la comunicación, donde la protección de los datos deje de depender de algoritmos y pase a estar escrita en las propias leyes de la física.

Gestión de riesgos de terceros

Tendencias por Antonio Chavarría

En 2025, el 89% de las brechas de seguridad tienen su origen en vulnerabilidades de terceros, según el último informe de Verizon Data Breach Investigations Report. Esta estadística no es solo un número: representa la realidad de que el perímetro de seguridad tradicional ha desaparecido. Las organizaciones modernas operan en ecosistemas digitales complejos donde la media de proveedores críticos por empresa ha crecido un 340% en los últimos tres años, transformando la gestión de riesgos de terceros (TPRM) de una función administrativa a un imperativo estratégico de supervivencia empresarial.

La convergencia de inteligencia artificial, regulaciones como NIS2 y DORA, y la profesionalización de grupos como Scattered Spider han creado un panorama donde los métodos tradicionales de evaluación de proveedores son tan efectivos como una armadura medieval contra un ciberataque moderno.

Revolución de la monitorización continua

El paradigma de evaluaciones anuales o semestrales ha colapsado ante la velocidad exponencial de evolución de las amenazas. Grupos como APT40 y Lazarus pueden comprometer un proveedor y pivotar hacia objetivos secundarios en menos de 72 horas, mientras que las evaluaciones tradicionales tardan entre 45 y 90 días en completarse.

Las organizaciones líderes han adoptado sistemas de monitoruzación continua 24/7 que combinan:

- External Attack Surface Management (EASM): Plataformas como Recorded Future y RiskIQ escanean automáticamente activos externos de proveedores, identificando:
  - Vulnerabilidades críticas en menos de 4 horas desde su publicación.
  - Certificados SSL expuestos o mal configurados.
  - Servicios shadow IT no documentados.
  - Exposición accidental de bases de datos (más de 23,000 bases de datos MongoDB fueron encontradas expuestas en 2024).

- Inteligencia de Threat Intelligence Contextualizada: integración con *feeds* de Mandiant, CrowdStrike y Microsoft Defender que alertan sobre:
  - Menciones de proveedores en foros de *ransomware* como LockBit 3.0.
  - Actividad sospechosa en la *dark web* relacionada con credenciales corporativas.
  - Campañas de *phishing* dirigidas específicamente a ecosistemas de proveedores.

- Behavioral Analytics con IA: Algoritmos de *machine learning* que establecen líneas base comportamentales para cada proveedor, detectando desviaciones como:
  - Patrones de acceso anómalos a sistemas críticos
  - Cambios no documentados en infraestructura de red
  - Incrementos súbitos en transferencia de datos.

Inteligencia Artificial, motor de la transformación TPRM.

La inteligencia artificial está revolucionando cada aspecto del ciclo de vida TPRM. Los sistemas de IA generativa pueden analizar contratos de proveedores, informes SOC 2 y documentación técnica en minutos (en lugar de horas). El procesamiento de lenguaje natural identifica automáticamente cláusulas de riesgo, *gaps* de responsabilidad y obligaciones de cumplimiento.

Las capacidades más avanzadas incluyen:

- Generación Automática de Cuestionarios: sistemas que crean evaluaciones personalizadas basadas en el perfil de riesgo específico de cada proveedor, el tipo de servicios proporcionados y las regulaciones aplicables.
- *Análisis Predictivo de Riesgos: modelos de machine learning* que combinan datos históricos, tendencias de la industria e inteligencia de amenazas para predecir la probabilidad de incidentes de seguridad.
- Automatización de Respuestas: agentes de IA que pueden generar borradores de planes de remediación, correspondencia con proveedores e informes ejecutivos basados en hallazgos de evaluaciones.

Cumplimiento Dinámico y Adaptativo

La tecnología regulatoria (RegTech) está transformando cómo las organizaciones gestionan el cumplimiento normativo en sus relaciones con terceros.

Los sistemas RegTech pueden rastrear cambios regulatorios en tiempo real y evaluar automáticamente su impacto en cada relación de proveedor, aportando así:

- Monitorización Regulatoria Continua: sistemas que rastrean automáticamente cambios en regulaciones como GDPR, DORA, NIS2 y evalúan el impacto en contratos y procesos existentes.
- Evaluaciones KYC/AML Automatizadas: procesos completamente automatizados para verificación de identidad, detección de lavado de dinero y *screening* de listas de sanciones.
- Generación Automática de Informes de Cumplimiento: herramientas que crean automáticamente informes regulatorios con validación de datos integrados y formateo conforme a estándares específicos.

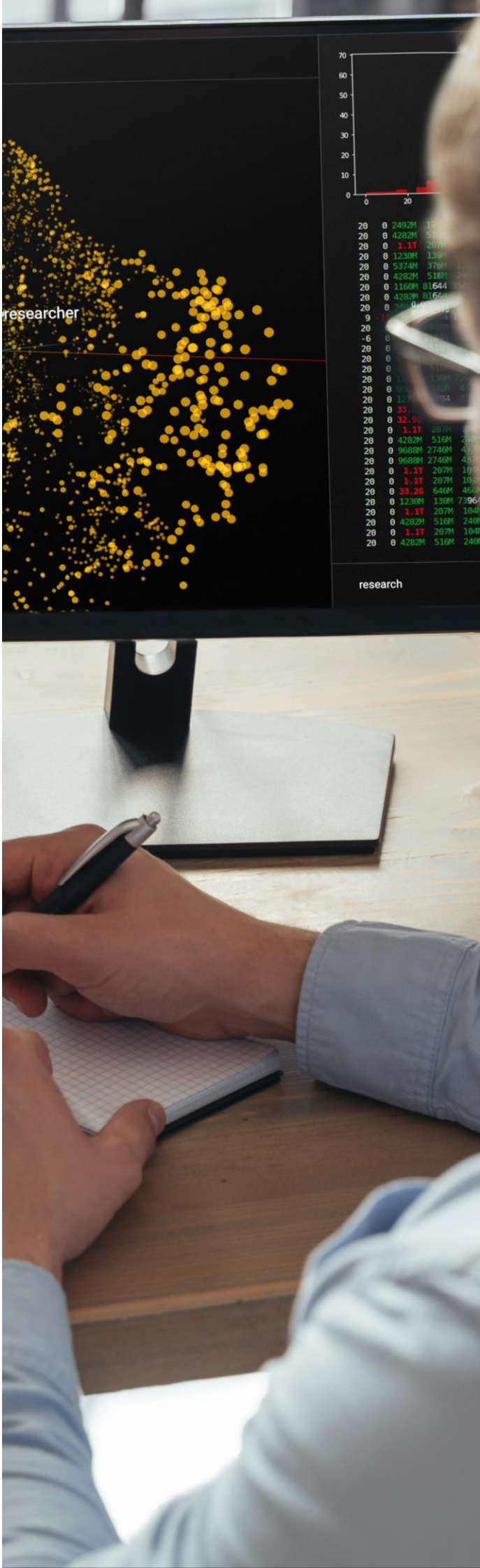
Futuro del TPRM

La gestión de riesgos de terceros está evolucionando hacia ecosistemas inteligentes que combinan IA, automatización y análisis predictivo para crear capacidades de gestión de riesgos sin precedentes. Las organizaciones que adopten estas tecnologías emergentes no solo mejorarán su postura de seguridad, sino que obtendrán ventajas competitivas significativas en un mundo cada vez más interconectado.

El éxito en esta transformación requiere más que implementación tecnológica: demanda un cambio cultural hacia la colaboración proactiva con proveedores, inversión en capacidades analíticas avanzadas y compromiso ejecutivo con la excelencia en gestión de riesgos.

Las organizaciones que lideren esta evolución definirán el futuro de los ecosistemas empresariales digitales.

Antonio Chavarría
Cybersecurity Senior Consultant



APP *Scams* en el Reino Unido y sus requisitos de reembolso obligatorio

Artículo por Octavio Sánchez Blanco

Reino Unido se ha adelantado en su cruzada contra las estafas y hace unos meses ha aprobado una normativa bajo la que, en determinadas circunstancias, los proveedores de servicios de pagos van a verse obligados al reembolso del dinero estafado. En este artículo analizamos cuales son las implicaciones de esta normativa.

Cada año, miles de personas y empresas son víctimas de estafas. En este artículo abordamos aquellas que preocupan especialmente al sector bancario por su alto coste reputacional y el incremento, tanto en número como en cantidad, observado en estos últimos años. Se trata de las estafas de pagos autorizados o Authorised Push Payment scams, en inglés (APP, en adelante).

Este tipo de estafa se produce cuando la víctima es engañada para que envíe dinero a un estafador que se hace pasar por un beneficiario genuino.

Existen multitud de *modus operandi* que utilizan los defraudadores para engañar a sus víctimas, pero los podemos resumir en dos grandes grupos: "beneficiario malicioso" y "redireccionamiento malicioso".

En el primer caso, se engaña a la víctima para comprar un bien y servicio que no existe o que nunca recibirá; en el segundo caso, un estafador se hace pasar por personal del banco o servicio técnico (gas, agua, empresa tecnológica) para que la víctima transfiera fondos de su cuenta bancaria a una controlada por el estafador.

Reino Unido se adelantó hace unos meses en su cruzada con un reglamento contra este tipo de estafas, siendo pionero en la aprobación de requisitos de reembolso obligatorio para estafas de pagos push autorizados (APP), el cual entró en vigor el 7 de octubre de 2024.

Anunciadas por el Regulador de Servicios de Pago (PSR) el 7 de junio de 2023, las nuevas reglas requieren que los proveedores de servicios de pago del Reino Unido estén obligados a reembolsar a todos los clientes que sean víctimas de APP Scam, salvo excepciones limitadas.

En Reino Unido, el valor del fraude de pagos autorizados ascendió a 459,7 millones de libras en 2023, con un total de casos de 232.429. El reembolso total a las víctimas contabilizó 287,3 millones de libras lo que supuso el 62% del total de las pérdidas reportadas (gráfico a pie de página).

- Cases (Casos): número de casos confirmados reportados. Un caso equivale a una cuenta, no a un individuo.
- Payments (Pagos): número total de pagos identificados como fraudulentos en relación con los casos reportados.
- Value (Valor): valor total de los pagos reportados.
- Returned to victim (Devuelto a la víctima): importe total devuelto a la víctima, bien sea porque el banco ha realizado la devolución directamente o bien porque se han recuperados los fondos de la cuenta beneficiaria.

		2020	2021	2022	2023	CHANGE
CASES	PERSONAL	145,207	188,964	200,643	224,694	12%
	NON-PERSONAL	9,407	7,032	6,729	7,735	15%
	TOTAL	154,614	195,996	207,372	232,429	12%
PAYMENTS	PERSONAL	228,946	333,751	361,761	405,095	12%
	NON-PERSONAL	15,625	11,386	10,505	12,364	18%
	TOTAL	244,571	354,137	372,266	417,459	12%
VALUE	PERSONAL	£347.4m	£505.9m	£408.2m	£376.4m	-8%
	NON-PERSONAL	£73.3m	£77.4m	£77.0m	£83.3m	8%
	TOTAL	£420.7m	£583.2m	£485.2m	£459.7m	-5%
RETURNED TO VICTIM	PERSONAL	£163.4m	£246.8m	£254.1m	£256.4m	1%
	NON-PERSONAL	£27.4m	£24.4m	£31.5m	£30.8m	-2%
	TOTAL	£190.8m	£271.2m	£285.6m	£287.3m	1%

Fuente: Annual Fraud Report 2024. UK Finance

En términos generales, los objetivos de esta implementación en el Reino Unido son:

- Incentivar la inversión de la industria en la prevención del fraude de extremo a extremo.
- Mejorar la protección del cliente y la confianza en el ecosistema de pagos.
- Perseguir el objetivo a largo plazo del PSR de que el organismo de normalización de los sistemas de pagos interbancarios del Reino Unido (Pay.UK) asuma un papel más amplio y mejore activamente las normas sobre pagos más rápidos.

Los nuevos requisitos provocarán un cambio radical en la cultura de pagos para mejorar la prevención del fraude y centrar el esfuerzo de todas las empresas en proteger a los clientes.

Aspectos acordados

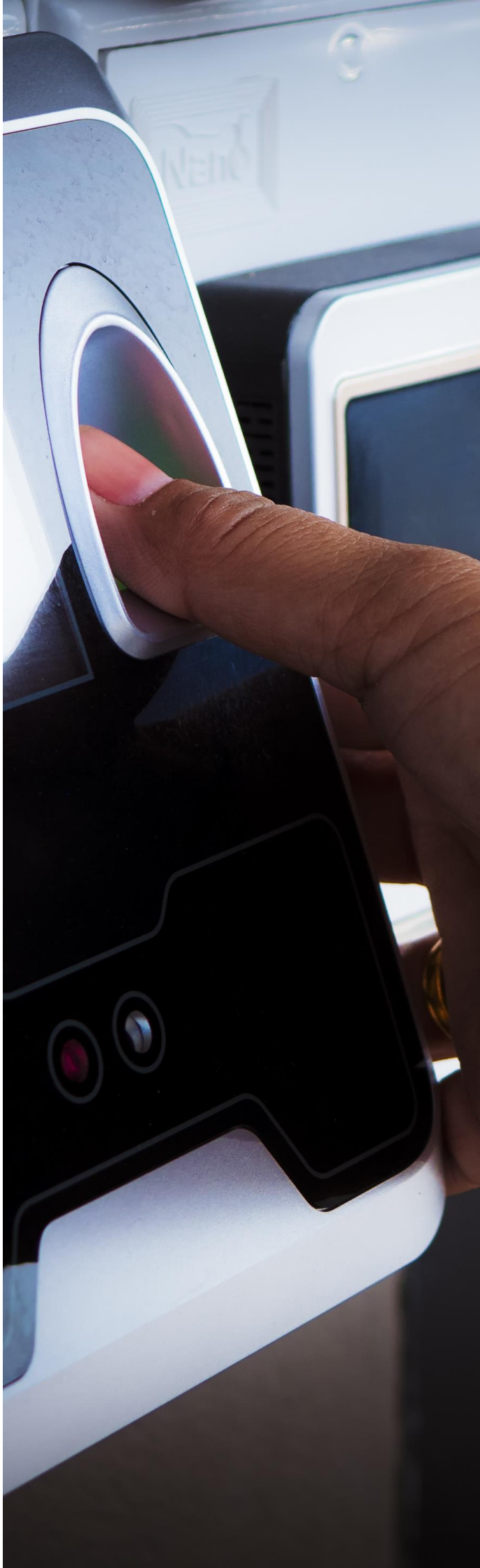
Estas reglas son obligatorias para todos los proveedores de servicios de pago (PSP, en adelante) que utilizan el sistema *Faster Payments* (sistema de pagos inmediatos), cubriendo prácticamente la totalidad de los APP scams.

Las decisiones sobre el reembolso las toma exclusivamente el PSP emisor. Sin embargo, el mismo puede reclamar la devolución del 50 % de cualquier reembolso al proveedor de servicios de pago destinatario.

El PSP debe realizar el reembolso en un plazo de cinco días hábiles, aunque puede ampliar ese plazo si requiere realizar investigaciones (hasta un máximo de 35 días).

Inicialmente se planteó un nivel máximo de reembolso de 415.000 £, pero se redujo a 85.000 £ justo antes de la fecha del inicio de estas medidas. Por parte del regulador se justificó este cambio como un ajuste práctico para evitar posibles abusos del sistema, y resaltando que este nuevo límite cubriría más del 99 % de los casos de fraude.

Los nuevos requisitos introducen el “estándar de precaución del consumidor”, donde se establecen excepciones a esta obligación general de reembolso: cuando el consumidor que solicita el reembolso haya actuado de manera fraudulenta y/o con negligencia grave. Por supuesto, el “estándar de precaución del consumidor” no se aplicaría a los consumidores que son identificados como vulnerables a una estafa de APP.



El reembolso sólo se puede rechazar si el cliente no ha cumplido con el "estándar de precaución del consumidor" por las casuísticas antes expuestas, y solo si el cliente no es considerado vulnerable. Adicionalmente, el Regulador de pagos del Reino Unido (PSR) se compromete a:

- Publicar periódicamente sobre el grado de protección de las empresas a sus clientes.
- Establecer la "Confirmación de beneficiario" (VoP, sistema de verificación de nombres en los pagos para ayudar a prevenir estafas y pagos mal dirigidos).
- Fomentar un mejor intercambio de inteligencia entre las empresas de pagos para detectar transacciones fraudulentas y evitar que se produzcan.

Existe un plazo de 13 meses para las reclamaciones (aunque los PSP pueden optar voluntariamente por conceder reembolsos para reclamaciones posteriores).

En resumen, Reino Unido está tomando medidas para asegurar la protección de los consumidores ante la creciente amenaza de las estafas de pagos autorizados (APP Scams) adaptándose a la implantación de la PSD3, en cuyo borrador se solicita hacer foco en aquellos clientes que pueden ser especialmente vulnerables.

Asegurando el reembolso de este tipo de casos de estafa, el regulador británico (PSR) pretende forzar a las entidades a tomar la iniciativa para prevenir este tipo de técnicas ilícitas. La colaboración entre entidades y con las empresas de telecomunicaciones se hace imprescindible, así como la inclusión de nuevas tecnologías tales como la biometría comportamental para conseguir mejorar la detección y la mitigación de estas estafas que tanto daño reputacional están causando.

Reino Unido ha sido pionero con esta nueva normativa. Las organizaciones del resto de territorios tendrán que prestar atención a la influencia que dicha normativa tenga en sus reguladores nacionales.

El regulador tiene previsto la publicación de un informe para el segundo trimestre de 2026. Dicho documento reflejará el resultado de una evaluación por parte de un organismo independiente del impacto de las políticas aplicadas con respecto a los APP scams, incluyendo las reglas de reembolso que se han tratado en el presente artículo. Para ello, se revisará la efectividad y cumplimiento de cada una de las políticas, así como el tratamiento de casos de estafa a clientes vulnerables.

Octavio Sánchez Blanco
FRC FinCrime Leader

Fuentes:
Sitio web del regulador británico donde se resume todo el trabajo del organismo en relación con los APP Scams (https://www.psr.org.uk/our-work/app-scams/)
Documento redactado por el regulador británico (PSR) sobre el concepto "estándar de precaución del consumidor". (https://www.psr.org.uk/media/as3a0xan/ sr1-consumer-standard-of-caution-guidance-dec-2023.pdf)
Documento redactado por el regulador británico (PSR) sobre políticas para la lucha contra las estafas de pagos push autorizados (APP scams). (https://www.psr.org.uk/ media/kwlgyzti/ps23-4-app-scams-policy-statement- dec-2023.pdf)

Estafas, ¿qué son y cuáles son las tipologías más comunes?

Artículo por Diego José de Benito

El crecimiento de las estafas se ha intensificado en los últimos años creando una sensación de inseguridad en toda la población que se siente vulnerable frente a los cibercriminales. En este artículo, introduciremos el concepto de qué es una estafa, las tipologías que más comunes y la evolución previsible de las mismas.

Una estafa es un acto fraudulento mediante el que una persona engaña a otra con la intención de obtener beneficio, principalmente económico. Por lo general, cuando se realiza una estafa, se utiliza información falsa con el propósito de manipular a la víctima y hacerla tomar decisiones que de otra forma no plantearía. Se puede estafar de muy diversas formas y métodos, pudiendo encontrar desde engaños sencillos hasta complejos y elaborados esquemas.

Es importante diferenciar entre estafa y fraude. Mientras que, en el segundo, es el defraudador el que empleando diversas técnicas obtiene los datos necesarios para su propósito (dolo económico), en la estafa es la propia víctima la que realiza la transacción. Cabe destacar que, en el caso de estafa, la víctima sufre un menor grado de protección.

Tipologías más comunes

Estafas de caridad, lotería o premios

Los estafadores fingen representar a una organización benéfica (legítima o falsa) y solicitan donaciones en momentos en los que se ha producido algún tipo de catástrofe natural o algún otro tipo de emergencia como las que sobrevienen cuando hay una guerra en marcha.

En otras ocasiones, los estafadores informan a la víctima que ganó un premio de lotería o un sorteo solicitando un pago anticipado que cubra las tarifas o impuestos de la supuesta recompensa que van a recibir. En la era digital, los avances tecnológicos y el uso y dependencia de la tecnología han hecho que las estafas hayan evolucionado y se hayan diversificado, convirtiendo tanto a individuos particulares, como a grandes organizaciones en claros objetivos.

En España, las estafas online son el tipo de delito que más ha crecido incrementándose un 509,1% entre 2016-2023. En el primer trimestre de 2024, 1 delito de cada siete se engloba en esta categoría.

Estafas de falso empleo

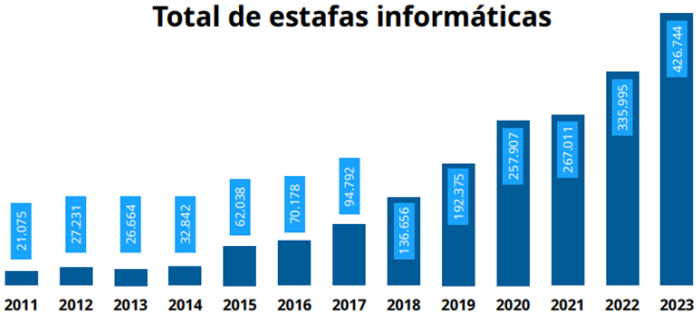
Hoy en día son excesivamente comunes los intentos de estafas de empleo a través de WhatsApp o de la red LinkedIn, relacionadas con oportunidades de empleo en las que el estafador finge trabajar en el departamento de nóminas o de administración de alguna empresa o sociedad bien conocida. Suelen ofrecer teletrabajo, empleo de no mucho esfuerzo y tiempo, con mucha flexibilidad y buen sueldo.

Después, piden unos gastos de gestión para enviar un equipo de trabajo o alguna otra excusa para que la víctima realice algún pago adelantado por la remuneración del trabajo que se vaya a realizar.

Estafas de inversión

Las estafas de inversión son una de las más comunes hoy en día, debido al auge de las redes sociales y de plataformas o apps de inversión en línea, en donde los estafadores han encontrado nuevas formas de llegar a un gran número de posibles víctimas con promesas de hacerse rico al momento o de altos rendimientos de las inversiones.

Los estafadores utilizan diferentes estrategias, además de prometer grandes beneficios como el empleo de esquemas Ponzi, en el que los estafadores pagan rendimientos a los inversores anteriores con el dinero de los nuevos, o esquemas piramidales, incitando a reclutar a más personas para mantener el flujo de ganancias y en el que no reclutar implica el no retorno de la inversión.



Balance de Criminalidad del Ministerio del Interior

En ocasiones, solicitan a la víctima instalar en sus dispositivos alguna aplicación de control remoto, como puede ser AnyDesk, con la excusa de enseñarles a realizar las operaciones de inversión, y acaban controlando esos dispositivos y realizando operaciones fraudulentas sin el conocimiento de esta. Para perfiles de inversión específicos, las estafas relacionadas con esquemas de bombeo y vertido (inflado artificial del precio de una acción o activo mediante información falsa o engañosa), inversiones binarias, micro capitalización o seminarios de inversión están a la orden del día.

TOP 5 ESTAFAS DE INVERSIÓN

- Esquema Ponzi
- Esquemas de bombeo y vertido
- Esquemas piramidales
- Fraude de tarifas anticipadas
- Estafas en opciones

Mención aparte, por su crecimiento exponencial, merece la inversión en criptomoneda o estafas por grupos de afinidad (ej. Inversión en Forex).

Estafas de soporte técnico

También conocida como estafa Microsoft, aprovecha el desconocimiento tecnológico de determinados sectores de la población. Se efectúa por los estafadores a través de llamadas o correos electrónicos, alertando de un problema de seguridad en el dispositivo que requiere intervención inmediata para evitar mayores problemas, solicitando información personal y sensible de la víctima a través de ingeniería social para dar acceso remoto al mismo dispositivo.

Estafas comerciales

Son una de las estafas más antiguas que existen, prácticamente desde que existen transacciones comerciales de cualquier tipo. Hoy en día pueden producirse a través de comercios electrónicos no seguros, webs de subastas, son muy comunes en redes sociales y, sobre todo, en los últimos tiempos, en aplicaciones online de venta de artículos como pueden ser Wallapop o Vinted.

Se tratan de anuncios falsos con los que la víctima realiza pagos de manera anticipada por bienes o servicios que nunca van a recibir o que no existen. Los productos y/o servicios para este tipo de estafa son de lo más variados y pueden cambiar según la época del año.

Desde estafas de viviendas de alquiler vacacional a estafas en la compra de pellets (combustible para sistemas de calefacción), automóviles, en la adopción de mascotas, etc.

Estafas románticas

Los estafadores utilizan plataformas como redes sociales o aplicaciones/webs de citas para crear perfiles atractivos utilizando fotos y biografías falsas para atraer a posibles víctimas. En ocasiones, incluso “suplantan” a artistas conocidos o personas de renombre. Es muy habitual que se hagan pasar por personal militar en el extranjero.

Es un tipo de estafa que suele alargarse bastante en el tiempo, consiguiendo establecer con la víctima una conexión emocional fuerte a base de comunicación frecuente, muestras de cariño e interés “genuino” por su vida.

Una vez que han ganado la plena confianza de la víctima suelen alegar algún tipo de problema de salud, una urgencia financiera, costes de viaje o problemas con visados para poder conocerse personalmente. Siempre tratan de presionar con contextos de emergencia falsa que hacen que la víctima, emocionalmente involucrada, no se planteé la naturaleza de la situación.

Es alarmante como algunas víctimas pueden llegar a perder grandes cantidades de dinero, en ocasiones los ahorros de toda la vida, además de sufrir una fuerte angustia emocional, vergüenza y humillación, aumentando la soledad y el aislamiento.

Estafas de Suplantación de un Organismo Oficial o Empresas de Servicios

El estafador se hace pasar por una de estas organizaciones mediante llamadas, correos electrónicos o SMS alertando de una supuesta deuda con Hacienda, con la compañía amenazando de un corte inmediato de luz, agua, paquete que no va a ser entregado... y solicitando movimientos directos por parte de la víctima.

Estafas de manipulación de IBAN/Fraude Factura

Es un tipo de estafa dirigido más habitualmente a empresas, aunque también pueden ser víctimas personas particulares. Los estafadores consiguen a través de técnicas de ingeniería social los datos o el correo electrónico de un proveedor habitual de la empresa, o de una empresa de servicios, interceptan o manipulan una factura digital o física para cambiar la información de la cuenta y garantizar que el próximo movimiento bancario se dirija a sus propias cuentas.

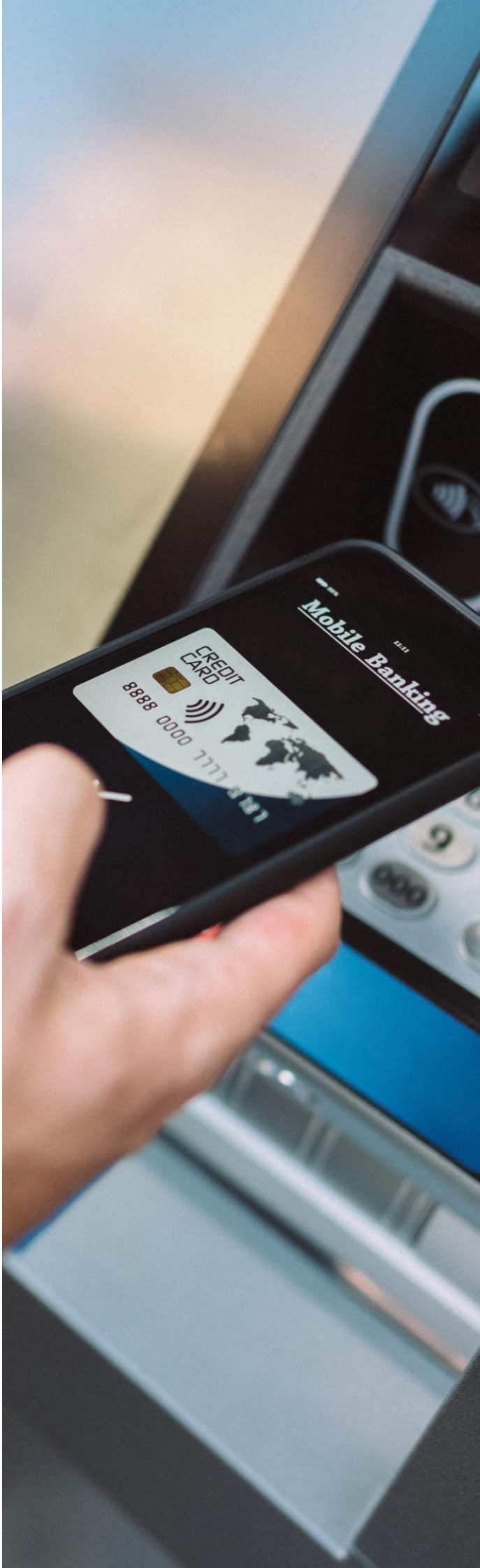
Normalmente la cuantía y el plazo concuerda con anteriores transacciones previas a la empresa que ha sido suplantada.

Estafas de Suplantación de Entidad Bancaria

La suplantación de un trabajador de una entidad bancaria es un tipo de estafa al auge. Suelen contactar por teléfono, pudiendo tener ya de antemano algún dato de la víctima, obtenido con otras estrategias de ingeniería social.

Se presentan como gestores o como miembros de los departamentos de seguridad como lo haría un empleado real. Informan a la víctima de algún tipo de actividad sospechosa en sus cuentas o de alguna transacción que el cliente no ha autorizado, generando ansiedad, urgencia y preocupación en la víctima. Con la premisa de tomar medidas inmediatas para proteger su dinero les acaban de convencer ya sea para entregar datos de acceso a la banca online, compartir información de doble autenticación para confirmar operaciones o para realizar algún movimiento directamente a la cuenta del estafador.

Se suelen usar técnicas conocidas como *spoofing* para que las llamadas parezcan venir de números de teléfono oficiales de dichas entidades, como los de Atención al Cliente.



Estafas de Suplantación de un familiar

Muy habitual a través de WhatsApp, este tipo de estafa se ha disparado en los últimos años. Suelen plantearse como, por ejemplo, un hijo que estudia en el extranjero o que está de viaje en el momento y cuenta una situación de emergencia repentina que les hace escribir desde un número desconocido. En ocasiones usan información específica sobre el hijo de la víctima que pueden encontrar en redes sociales.

Apelando a la preocupación del familiar, no dejan de insistir en la criticidad de la situación y en que una demora en la cantidad que solicitan tendrá graves consecuencias para ellos. Suelen pedir movimientos de dinero inmediatos que son imposibles de parar cuando la víctima se acaba percatando del engaño.

Estafa de Captación de Mulas

Comienzan de formas parecidas a los casos de estafas de falso empleo. Los estafadores anuncian trabajos legítimos o contactan directamente con personas a través de redes sociales, con la diferencia de convencerlas para que actúen como agente, es decir, creen una cuenta bancaria con este propósito o utilicen la propia, para transferir dinero que ellos creen legítimo. En muchas ocasiones, las víctimas no son conscientes del delito que están cometiendo.

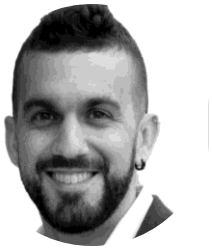
La red de mulas facilitará el blanqueo de fondos provenientes de otras estafas o fraudes a través de pagos en tiempo real, transfiriendo rápidamente los fondos entre varias cuentas.

Fraude al CEO

En este tipo de estafa, un delincuente o un grupo de ellos, mediante diferentes técnicas de ingeniería social, consigue suplantar la identidad del CEO de una organización. El *modus operandi* consiste en convencer a una persona encargada de las cuentas o de las transacciones de dicha organización de realizar movimientos urgentes a la cuenta del estafador.

Es un tipo de estafa que afecta habitualmente a empresas y suele cometerse a través de canales como WhatsApp, SMS o chats que utilice la organización como por ejemplo Microsoft Teams.

Tal y como hemos podido observar, el rango de tipologías de estafas es muy amplio y en constante evolución. Debido a ello, el reto que supone este crecimiento exponencial, tanto en tipología como en número de ataques, obliga a realizar una inversión constante en recursos que faciliten una protección de los consumidores. Además, también conlleva una gestión de la prevención del fraude adecuada y mitiguen las penalizaciones que puedan surgir debido a la regulación.

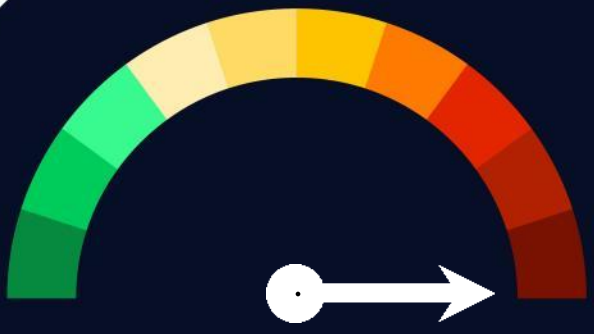


Diego José de Benito
FinCrime Analyst
Financial Risk &
Compliance (FRC)

Vulnerabilidades

Vulnerabilidad crítica en Redis

Fecha: 3 de octubre de 2025
CVE: CVE-2025-49844



CVSS: 9.9

CRÍTICA

Descripción

La vulnerabilidad **CVE-2025-49844** (apodada "**RediShell**") representa una amenaza crítica, ya que permite a los atacantes obtener la ejecución remota de código en miles de instancias vulnerables.

Se trata de un fallo de tipo *use-after-free* (CWE-416), presente desde hace más de una década en el código fuente de Redis. En este sentido, un atacante con credenciales válidas, podría usar un *script* especialmente manipulado en Lua (característica habilitada por defecto) para evadir el entorno seguro ("*sandbox*"), provocar el error de memoria, establecer una conexión inversa persistente (*reverse shell*) y, finalmente, ejecutar código remoto en el sistema afectado.

Solución

Redis recomienda **actualizar a la versión 8.2.2**, especialmente en instancias que son accesibles desde Internet:

- Una **solución alternativa adicional** para mitigar el problema sin parchear el ejecutable de redis-server es evitar que los usuarios ejecuten *scripts* de Lua. Esto se puede hacer usando ACL para restringir los comandos EVAL y EVALSHA.

Productos afectados

Esta vulnerabilidad crítica afecta a las **versiones 8.2.1 y anteriores**, que permiten a un usuario autenticado usar un *script* Lua especialmente diseñado para manipular el recolector de basura, desencadenar un uso después de la liberación y potencialmente conducir a la ejecución remota de código.

Referencias

- nvd.nist.gov
- bleepingcomputer.com

Vulnerabilidades

Vulnerabilidad crítica en Flag Forge

Fecha: 10 de octubre de 2025
CVE: CVE-2025-617777

CVSS: 9.4

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica en Flag Forge, una plataforma utilizada para competencias Capture The Flag (CTF).

El fallo se encuentra en los *endpoints* administrativos */api/admin/badge-templates* (GET) y */api/admin/badge-templates/create* (POST), los cuales permitían acceso sin autenticación ni autorización.

Esta vulnerabilidad, con una puntuación CVSS de 9.4, podía ser explotada por un atacante remoto no autenticado para obtener todas las plantillas de insignias con datos sensibles, además de crear plantillas arbitrarias directamente en la base de datos.

Solución

Se recomienda actualizar de inmediato a la versión 2.3.2, en la cual la vulnerabilidad ya ha sido corregida.

Productos afectados

La vulnerabilidad afecta a los siguientes productos:

- Forge CTF Platform: versión 2.0.0 a 2.3.1

Referencias

- incibe.es
- github.com

Oracle corrige una vulnerabilidad *zero-day* de Oracle E-Business Suite

Fecha: 5 de octubre de 2025
CVE: CVE-2025-61882

Crítica

Descripción

Oracle ha publicado un parche urgente para una vulnerabilidad *zero-day* en su suite E-Business (EBS), identificada como **CVE-2025-61882**, que ha sido usada activamente por el grupo Clop en ataques de robo de datos.

Según Oracle, esta debilidad reside en el componente "*BI Publisher Integration*" del módulo "*Concurrent Processing*" de EBS.

Lo más grave es que no requiere autenticación: un atacante puede ejecutarla a través de la red sin necesidad de usuario o contraseña, lo que le permite ejecutar código de forma remota si la explotación tiene éxito.

La vulnerabilidad tiene un puntaje base de CVSS **9.8**, reflejando su criticidad, dada la facilidad con la que puede ser aprovechada y su impacto potencial.

Productos afectados

Oracle ha confirmado que la vulnerabilidad *zero-day* afecta al producto Oracle E-Business Suite, desde la versión 12.2.3 hasta la versión 12.2.14.

Solución

Oracle ha lanzado una actualización de emergencia para abordar la falla, aunque para poder instalar el parche de emergencia contra CVE-2025-61882, primero se debe haber aplicado el *Critical Patch Update* de octubre de 2023.

Referencias

- nvd.nist.gov
- bleepingcomputer.com

IBM corrige vulnerabilidades que permiten escalada de privilegios

Fecha: 9 de octubre de 2025
CVE: CVE-2025-36356 y 2 más

Crítica

Descripción

IBM ha publicado un boletín de seguridad para corregir varias vulnerabilidades en los productos IBM Security Verify Access y IBM Verify Identity Access.

La más grave (CVE-2025-36356) permitía que un usuario autenticado localmente elevase sus privilegios hasta el nivel *root*, debido a una ejecución con más permisos de los necesarios. Esta vulnerabilidad presenta una puntuación CVSS de 9.3.

Además, se han corregido otros fallos que podían permitir la ejecución de comandos no autorizados o la inclusión de código desde entornos externos.

Productos afectados

Los productos afectados por la actualización son los siguientes:

- IBM Security Verify Access (Docker y Appliance): versiones 10.0.0.0 a 10.0.9.0-IF2
- IBM Verify Identity Access (Docker y Appliance): versiones 11.0.0.0 a 11.0.1.0

Solución

IBM recomienda actualizar de los productos afectados a las versiones corregidas:

- IBM Security Verify Access: aplicar Fixpack 10.0.9.0-IF3
- IBM Verify Identity Access: aplicar Fixpack 11.0.1.0-IF1

Referencias

- ibm.com
- incibe.es

Eventos

XIX Jornadas STIC CCN-CERT | VII Jornadas de Ciberdefensa ESPDEF-CERT | Congreso RootedCON

24 - 27 de noviembre

El mayor evento nacional de ciberseguridad se celebrará en los cines Kinépolis Ciudad de la Imagen de Madrid bajo el lema "Un escudo digital para una España interconectada". Por primera vez, el Centro Criptológico Nacional (CCN), el Mando Conjunto del Ciberespacio (MCCE) y RootedCON unen fuerzas para crear un programa integrado que reunirá a más de 7.000 profesionales.

El evento comenzará el 24 de noviembre con una edición especial del Congreso RootedCON centrada en sesiones formativas y prácticas. Del 25 al 27 de noviembre se desarrollarán las jornadas principales con las últimas investigaciones, políticas y tecnologías de protección cibernética.

Enlace

IT & Cybersecurity Meetings Marbella

18 – 20 de noviembre

Una innovadora feria one-to-one dedicada a redes, nube, movilidad, ciberseguridad y soluciones de IA se celebrará en el Palacio de Congresos de Marbella (Málaga). El evento utiliza un concepto único de reuniones de negocio de 15 minutos previamente programadas entre tomadores de decisiones cualificados de Francia, Italia, Alemania y Suiza, y expositores internacionales.

La feria reunirá a más de 80 expositores y 150 tomadores de decisiones con *networking* a través de cócteles-cena que permiten continuar el desarrollo de negocio en un ambiente distendido.

Enlace

ISMS Forum Spain

13 de noviembre

La vigesimoséptima edición de las Jornadas Internacionales de Seguridad de la Información tendrá lugar en el Estadio Cívitas, organizadas por ISMS Forum. Se centra en la gestión de sistemas de información y normativas de seguridad.

Enlace

Ciberseguridad en tiempo real: de la alerta a la acción

20 de noviembre

Ayesa organiza este evento especializado de 10:00 a 14:00h en Madrid, enfocado en la respuesta inmediata ante amenazas y la transición de la detección a la acción correctiva.

Enlace

Recursos

➢ Check Point Infinity AI Security Services: detección inteligente de amenazas

Check Point Infinity ha sido reconocida como la mejor plataforma de ciberseguridad impulsada por IA según el informe 2025 de Miercom. Esta arquitectura unificada proporciona protección integral para redes, nube, *endpoints* y dispositivos móviles, utilizando 50 motores de IA que analizan *big data* de millones de dispositivos conectados.

Su sistema ThreatCloud integra inteligencia de amenazas avanzada con capacidades *Zero Trust* y *Secure Access Service Edge* (SASE), ofreciendo facilidad de uso y gestión centralizada de seguridad.

Enlace

➢ AccuKnox AI CoPilot: asistente de seguridad para entornos *cloud*

Una nueva herramienta diseñada específicamente para proteger aplicaciones *serverless*, contenedores y Kubernetes mediante IA generativa. AccuKnox utiliza tecnología eBPF para monitorización profunda del sistema, identificando riesgos, desarrollando políticas de seguridad y gestionando crisis de manera eficiente.

Esta plataforma destaca por su enfoque en la seguridad nativa de la nube sin comprometer las operaciones existentes, ofreciendo detección temprana de amenazas y respuesta automatizada.

Enlace

➢ Darktrace ActiveAI Security Platform: detección autónoma de amenazas

Darktrace ha evolucionado su plataforma para detectar amenazas mediante el aprendizaje del comportamiento normal de la red, sin depender de firmas de ataques conocidas. Su capacidad de respuesta autónoma Antigena puede contener ataques de manera dirigida sin interrumpir las operaciones comerciales.
La plataforma utiliza análisis comportamental para identificar anomalías de alto riesgo, incluyendo amenazas sofisticadas impulsadas por IA, estableciendo modelos únicos para cada entorno digital empresarial.

Enlace

➢ SentinelOne Singularity: Protección unificada con IA comportamental

SentinelOne Singularity integra protección, detección y respuesta unificada para *endpoints*, cargas de trabajo en la nube e identidades. Su IA comportamental puede detener *ransomware*, amenazas de día cero y ataques activos mediante modelos estáticos y comportamentales que operan en sistemas operativos y entornos *cloud*.

La plataforma incluye Purple AI para búsqueda de amenazas en lenguaje natural, generación automática de resúmenes y aceleración de investigaciones, junto con respuesta automatizada basada en políticas.

Enlace

NTT DATA Technology Foresight 2025

5 tendencias que se convertirán en realidades empresariales.

Descarga el informe: **es.nttdata.com/ntt-data-technology-foresight-2025**

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com