



Informe de tendencias tecnológicas en ciberseguridad

Contenido

Introducción	2
Objetivo general	2
Alcance	3
Tecnología en doble filo: amenazas emergentes y cómo el sector financiero debe responder	4
Tecnologías que amplían la capacidad ofensiva	5
SEaaS (Ingeniería Social como Servicio): hacia una manipulación industrializada	5
Malware polimórfico con IA: la amenaza que aprende, muta y evade en tiempo real	7
Tecnologías que transforman la infraestructura y la confianza digital.....	10
Computación cuántica: prepararse hoy para la criptografía del mañana	10
Procedencia Digital: el nuevo escudo de autenticidad contra deepfakes, fraude y desinformación.....	12
Cloud 3.0: una oportunidad tecnológica que también amplía la superficie de riesgo	14
Matriz de priorización	17
Referencias	19



Introducción

La transformación digital del sector financiero ha impulsado una rápida adopción de tecnologías que optimizan la eficiencia operativa, fortalecen la experiencia del cliente y permiten el desarrollo de nuevos modelos de negocio. Sin embargo, este mismo avance tecnológico ha incrementado la complejidad del panorama de riesgos cibernéticos, donde las capacidades ofensivas de los actores maliciosos evolucionan al mismo ritmo que las herramientas de protección.

Actualmente, tecnologías como la inteligencia artificial generativa, la computación cuántica, la computación en la nube de nueva generación y los mecanismos de autenticidad digital están redefiniendo el ecosistema de la ciberseguridad. Mientras algunas de estas innovaciones representan oportunidades para fortalecer la resiliencia y la confianza digital, otras están siendo utilizadas para sofisticar ataques como la ingeniería social automatizada, el malware adaptativo, los fraudes mediante contenido sintético (deepfakes) y nuevas técnicas para evadir los controles de seguridad tradicionales.

En este contexto, las entidades del sector financiero enfrentan el desafío de comprender cómo estas tendencias tecnológicas modifican tanto las capacidades defensivas como las ofensivas del entorno digital. La gestión del riesgo ya no puede limitarse a responder incidentes, sino que debe incorporar una visión prospectiva que permita anticipar amenazas emergentes, fortalecer la resiliencia organizacional y preparar la infraestructura tecnológica para escenarios futuros.



Objetivo general

Analizar las principales tendencias tecnológicas que están transformando el panorama de la ciberseguridad y la confianza digital en el sector financiero, evaluando su impacto sobre las capacidades ofensivas y defensivas de las organizaciones, con el propósito de identificar riesgos emergentes, oportunidades de fortalecimiento tecnológico y lineamientos estratégicos que apoyen la toma de decisiones, la gestión integral del riesgo y la construcción de una mayor resiliencia frente a las amenazas actuales y futuras.



Alcance

El presente informe comprende el análisis de las tendencias tecnológicas con mayor impacto potencial en la seguridad digital del sector financiero, abordando tanto aquellas que incrementan la capacidad ofensiva de los actores maliciosos como las que transforman la infraestructura tecnológica y los mecanismos de confianza digital.

En el ámbito de las amenazas emergentes, se examinan tecnologías como la Ingeniería Social como Servicio (SEaaS) y el malware polimórfico impulsado por inteligencia artificial, evaluando su funcionamiento, evolución, nivel de sofisticación e implicaciones para las estrategias de prevención, detección y respuesta.

Asimismo, el informe analiza tecnologías con impacto estructural en la arquitectura de seguridad, incluyendo la computación cuántica y sus implicaciones para la criptografía, la procedencia digital como mecanismo para fortalecer la autenticidad de la información frente a deepfakes y campañas de desinformación, y la evolución hacia entornos Cloud 3.0, considerando tanto las oportunidades de innovación como los nuevos riesgos derivados de la expansión de la superficie de ataque.

Finalmente, el documento presenta un enfoque estratégico orientado a identificar implicaciones para la gestión del riesgo cibernético, la resiliencia operacional y la planificación tecnológica de las entidades financieras, proporcionando insumos para la definición de estrategias de ciberseguridad alineadas con la evolución del entorno tecnológico y las amenazas emergentes.

○●○ Tecnología en doble filo: amenazas emergentes y cómo el sector financiero debe responder

El panorama tecnológico avanza hoy a una velocidad que pocas organizaciones logran seguir de cerca. Lo que hace apenas un par de años parecía un horizonte lejano (computadores cuánticos, contenido sintético indistinguible del real, ataques completamente automatizados) es ya parte del análisis de riesgo cotidiano de cualquier sector estratégico, y la banca no es la excepción.

Las principales tendencias de este 2026 son distintas entre sí, con orígenes, plazos y actores muy diferentes. Algunas ya operan como vectores de ataque activos: la ingeniería social se ha industrializado hasta convertirse en un servicio criminal que imita voces, rostros y estilos de escritura con un realismo antes impensable, y el malware polimórfico reescribe su propio código en cada ejecución para evadir la detección.

Otras son transformaciones más estructurales que están redefiniendo el terreno de juego: la adopción de arquitecturas multicloud y de Edge computing multiplica los puntos de entrada que una compañía debe vigilar, la computación cuántica obliga a repensar desde ya la vigencia de la criptografía actual, y la procedencia digital surge como respuesta a un problema que la propia inteligencia artificial generativa ha creado. La IA, de hecho, aparece de forma transversal en varias de estas tendencias, aunque no todas responden a la misma lógica ni a la misma ventana temporal.

Para Colombia, este conjunto de tendencias tiene una traducción directa en riesgo local. La digitalización acelerada de servicios públicos, financieros y de infraestructuras críticas amplía la superficie de exposición del país frente a cada uno de estos fenómenos, ya sea por la multiplicación de puntos de entrada en entornos cloud, por la necesidad de anticipar una transición criptográfica que llevará años, o por el aumento de fraudes cada vez más sofisticados y difícilmente detectables.

Entender estas tendencias, y sobre todo el papel específico que juega la IA en cada una, ya no es un ejercicio técnico opcional: es una condición para tomar decisiones de seguridad informadas en un entorno que cambia más rápido que la capacidad de respuesta tradicional.

○●○ Tecnologías que amplían la capacidad ofensiva

SEaaS (Ingeniería Social como Servicio): hacia una manipulación industrializada

La "Ingeniería Social como Servicio" (Social Engineering as a Service, SEaaS) representa una evolución del modelo Cybercrime-as-a-Service, basada en la comercialización y automatización de ataques que manipulan a las personas.

Servicio	Cliente criminal recibe
Phishing-as-a-Service	Correos y páginas falsas listas para usar
Voice-as-a-Service	Voces clonadas y scripts de llamada
Deepfake-as-a-Service	Videos falsos de ejecutivos
Recon-as-a-Service	Información detallada de las víctimas
Credential Harvesting-as-a-Service	Robo automatizado de credenciales

Los ciberdelincuentes están desarrollando plataformas integradas que comercializan diferentes fases de la ingeniería social como un único servicio. Un ejemplo es ATHR, una plataforma identificada en 2026 que combina plantillas de phishing, envío de correos fraudulentos, agentes de voz basados en IA, telefonía gestionada desde el navegador y paneles para capturar credenciales en tiempo real.

Estas plataformas reducen considerablemente los conocimientos técnicos y los recursos necesarios para ejecutar ataques sofisticados.

En los entornos digitales, la identidad se está convirtiendo en una de las principales superficies de ataque. Los atacantes pueden sustituir o complementar la explotación técnica mediante la manipulación de procesos legítimos de autenticación, recuperación de cuentas y autorización.

Los modelos emergentes de inteligencia artificial están multiplicando la escala de la ingeniería social tradicional. Hace años, errores gramaticales, remitentes sospechosos y mensajes genéricos podían alertar a los usuarios de que algo no estaba bien. Ahora, la IA generativa permite crear mensajes hiperrealistas en cualquier idioma, imitando el estilo de escritura de

una empresa, jefe o familiar y personalizarlos a escala, de manera simultánea. La credibilidad sobre este tipo de mensajes aumenta y, con ella, sus probabilidades de éxito.

La peligrosidad realmente reside en la capacidad que tiene la IA de comprender el contexto, el tono y adaptar el contenido durante una interacción, lo que contribuye a dotar de un realismo extremo a las campañas de manipulación:

- o Imitación natural de determinados estilos de comunicación.
- o Análisis de fuentes abiertas para personalizar los mensajes.
- o Adaptación de los mensajes en tiempo real.
- o Automatización de los ataques sin afectar a su calidad.

Frente a este modelo de ataque, las medidas técnicas tradicionales resultan insuficientes.

El SEaaS está diseñado precisamente para eludir los controles perimetrales explotando el único elemento que no se puede parchear, las personas.

Las organizaciones están respondiendo con tres líneas de actuación:

1. Formación continua y actualizada con simulaciones reales adaptadas al rol de cada colaborador.
2. Múltiple verificación de identidad: ante cualquier solicitud urgente, el protocolo debe exigir confirmación por vías alternativas a la que inició la comunicación.
3. Inteligencia de amenazas aplicada: monitorización proactiva a través de un servicio de vigilancia digital que permita analizar la exposición de la compañía y sus trabajadores: datos filtrados, dominios similares, menciones en foros, con el fin de establecer mecanismos de alerta sobre cualquier nuevo vector de ataque.

La Ingeniería Social como Servicio ha industrializado la manipulación al democratizar las herramientas sofisticadas, transformando capacidades técnicas avanzadas en servicios accesibles y escalables.



Imagen 1. Ingeniería social como servicio. CSIRT Financiero.

Malware polimórfico con IA: la amenaza que aprende, muta y evade en tiempo real

El malware polimórfico impulsado por inteligencia artificial representa una de las amenazas más sofisticadas y desafiantes en el panorama actual de la ciberseguridad. Tradicionalmente, el malware polimórfico se define como un tipo de programa malicioso capaz de cambiar o transformar continuamente su propio código mientras mantiene intacta su funcionalidad original. El propósito de esta mutación es evadir las soluciones antivirus convencionales, las cuales suelen basarse en la detección de firmas, es decir, en la identificación de patrones estáticos de amenazas ya conocidas. Sin embargo, la integración de tecnologías de inteligencia artificial ha elevado esta capacidad de evasión a un nivel superior.

Al incorporar motores de IA, este tipo de malware ya no depende únicamente de algoritmos preprogramados para alterar su apariencia, sino que adquiere la capacidad de aprender, adaptarse y tomar decisiones de forma autónoma una vez se ha introducido en el entorno de la víctima. Mientras que el polimorfismo clásico se basaba en técnicas como la permutación de procesos o la sustitución de instrucciones, las variantes impulsadas por IA llevan a cabo una modificación de comportamiento profunda y adaptada. Esto significa que el código malicioso puede analizar activamente las medidas de seguridad del sistema en tiempo real, alterar sus patrones de ejecución y camuflarse simulando ser un proceso normal del sistema operativo para pasar completamente desapercibido.

El auge de este malware inteligente plantea nuevos retos, especialmente en el ámbito de las campañas de espionaje y el robo de información confidencial persistentes. Al ser capaz de reescribirse a sí mismo basándose en el análisis del entorno defensivo que encuentra, los métodos tradicionales de análisis de malware o los entornos aislados resultan muchas veces ineficaces, ya que la amenaza puede decidir permanecer inactiva al detectar que está siendo analizada. Este nivel de sofisticación ha facilitado la creación de agentes maliciosos autónomos que pueden cambiar dinámicamente sus tácticas de infiltración y exfiltración de datos, adaptándose a las respuestas del equipo de seguridad de la organización afectada.

La evolución reciente del malware polimórfico impulsado por inteligencia artificial ha dejado varios ejemplos que ilustran su rápida sofisticación¹:

o **PROMPTFLUX**. Se trata de una familia de malware basada en VBScript, la cual consulta de forma recurrente a la API de Gemini para generar variantes polimórficas únicas. En cada ejecución, el código fuente se reescribe al solicitar al modelo de lenguaje que actúe como un ofuscador experto. Esto le permite modificar dinámicamente las librerías, cabeceras, firmas y tamaños, logrando crear mutaciones cada quince minutos. Estas variantes resultan funcionalmente idénticas, pero imposibles de rastrear mediante herramientas de seguridad clásicas.

o **PROMPTSTEAL**. Vinculada a grupos de amenazas persistentes avanzadas (APT) rusos, emplea una táctica de adaptación extrema al consultar el modelo Qwen2.5-Coder para generar comandos de Windows bajo demanda. En lugar de llevar el código malicioso preprogramado de forma rígida, este malware solicita a la IA que genere las instrucciones en tiempo real, adaptándose con precisión al contexto y a las defensas del sistema en el que se acaba de infiltrar.

Para hacer frente a esta nueva generación de amenazas mutantes, las tecnologías de defensa cibernética están obligadas a evolucionar drásticamente. Las herramientas de Endpoint Detection and Response (EDR) y su evolución, Extended Detection and Response (XDR), son la primera línea de defensa de cualquier compañía. A diferencia de un antivirus que escanea archivos estáticos, estas herramientas monitorizan continuamente la actividad de los dispositivos (endpoints). La clave contra el malware polimórfico es la implementación del análisis de comportamiento en los EDR o XDR, en busca de acciones anómalas. Por

¹ <https://ciberso.com/blog/concienciacion-sobre-ciberseguridad/auge-malware-impulsado-ia/>

ejemplo, si un programa aparentemente inofensivo como Microsoft Word intenta repentinamente modificar claves del registro del sistema o comunicarse con un servidor externo desconocido, el EDR bloquea la acción. Algunas soluciones de seguridad como Sentinel One o CrowdStrike integran la inteligencia artificial en sus productos de EDR para llevar a cabo el análisis de comportamiento.



Imagen 2. Malware polimórfico impulsado por IA. CSIRT Financiero.

○ ○ ○ Tecnologías que transforman la infraestructura y la confianza digital

Computación cuántica: prepararse hoy para la criptografía del mañana

La computación cuántica representa una de las tecnologías emergentes con mayor potencial disruptivo para la ciberseguridad. A diferencia de los ordenadores clásicos, que procesan información mediante bits binarios, los sistemas cuánticos emplean qubits capaces de representar múltiples estados simultáneamente gracias a fenómenos como la superposición y el entrelazamiento cuántico. Aunque esta tecnología aún se encuentra en una fase temprana de madurez, los avances alcanzados durante los últimos años indican que su impacto podría ser comparable al que supuso la aparición de Internet o de la inteligencia artificial.

Se estima que la computación cuántica tenga el siguiente impacto en la sociedad:

- o Ruptura de la criptografía asimétrica utilizada en Internet, banca, administración electrónica y certificados digitales.
- o Mayor protección de la información a largo plazo, priorizando datos con ciclos de vida superiores a 10-20 años.
- o Migración hacia criptografía poscuántica (PQC) como nuevo estándar de protección.
- o Actualización masiva de infraestructuras: dispositivos IoT, sistemas industriales, VPN, PKI y servicios cloud deberán adaptarse.
- o Aumento de la inversión en investigación, talento especializado y capacidades nacionales de computación cuántica.

Desde la perspectiva de la seguridad, la principal preocupación radica en la capacidad que tendrán futuros ordenadores cuánticos para romper buena parte de los algoritmos criptográficos actualmente utilizados para proteger comunicaciones, infraestructuras críticas y servicios digitales. Algoritmos como RSA, Diffie-Hellman o la criptografía de curva elíptica, ampliamente empleados en protocolos TLS, VPN, certificados digitales o firmas electrónicas, podrían dejar de ofrecer garantías de confidencialidad e integridad frente a un adversario con capacidades cuánticas suficientemente avanzadas.

Aunque todavía no existen ordenadores cuánticos capaces de ejecutar ataques criptográficos a gran escala, ya se considera una amenaza real el denominado "harvest now, decrypt later". Esta estrategia consiste en interceptar y almacenar hoy comunicaciones cifradas para descifrarlas en el futuro cuando la tecnología cuántica lo

permita. Por ello, la información que debe mantenerse confidencial durante largos periodos de tiempo como información gubernamental, datos bancarios, datos sanitarios, propiedad intelectual o documentación de defensa comienza a requerir medidas de protección adaptadas a este nuevo escenario.

Como respuesta, gobiernos y organismos internacionales están impulsando la adopción de algoritmos de criptografía poscuántica, diseñados para resistir tanto ataques clásicos como cuánticos. La transición hacia estos nuevos estándares supondrá uno de los mayores procesos de actualización criptográfica de las próximas décadas, afectando a infraestructuras críticas, sistemas financieros, redes de telecomunicaciones y dispositivos conectados.

Para Colombia, esta tendencia implica la necesidad de comenzar una planificación temprana de la migración hacia criptografía resistente a ataques cuánticos, especialmente en sectores estratégicos como el financiero, la administración pública, la defensa, la energía o las telecomunicaciones. Del mismo modo, será necesario impulsar capacidades nacionales de investigación, formación de especialistas y cooperación internacional para evitar que la futura brecha tecnológica en computación cuántica se traduzca también en una brecha en materia de ciberseguridad. Si bien el riesgo inmediato sigue siendo limitado, la preparación debe iniciarse antes de que la amenaza se materialice, dado que la transición criptográfica requerirá varios años y afectará a una parte significativa de la infraestructura digital del país.



Imagen 3. Computación cuántica hacia la criptografía poscuántica. CSIRT Financiero.

Procedencia Digital: el nuevo escudo de autenticidad contra deepfakes, fraude y desinformación

La procedencia digital (o data provenance) es un conjunto de tecnologías y prácticas que permite rastrear, verificar y documentar el origen, la creación, las modificaciones y la cadena de custodia de cualquier contenido o dato digital. Funciona como un certificado de autenticidad inmutable que detalla quién creó la información, cuándo lo hizo y qué transformaciones ha sufrido a lo largo de su ciclo de vida.

En la era actual, marcada por la proliferación de la inteligencia artificial generativa y los deepfakes, distinguir el contenido real del falso a simple vista es cada vez más difícil. La procedencia digital actúa como un escudo fundamental: en lugar de intentar detectar qué contenido es falso (una carrera armamentística sin fin), incrusta una "prueba criptográfica de autenticidad" en el contenido real. De esta forma, cualquier usuario puede comprobar la integridad de un archivo (fotos, vídeos, documentos), limitando drásticamente el impacto de las campañas de desinformación.

La procedencia digital puede establecer fuertes mecanismos de defensa frente a actividades fraudulentas en múltiples sectores, incluido el financiero:

- Suplantación de identidad: puede evitar que un deepfake de voz o facial supere la verificación de identidad y realice operaciones en nombre de otra persona.
- Fraude del CEO mediante clonación de voz: previene que un empleado de la compañía autorice transacciones urgentes creyendo estar recibiendo instrucciones de un directivo real.
- Alta fraudulenta de usuarios nuevos: evita que identidades sintéticas logren abrir cuentas que posteriormente se utilizarán para fines fraudulentos (lavado de activos, etc.).
- Documentación falsificada en solicitudes de crédito: permite verificar comprobantes de ingresos, certificaciones laborales o cualquier otra documentación alterada con IA generativa.

Su aplicación también es transversal a otros ámbitos:

- Periodismo y Medios: verificación de fotografías y vídeos provenientes de zonas de conflicto para asegurar que no han sido alterados.
- Sector Sanitario y Farmacéutico: trazabilidad de datos en ensayos clínicos y protección en el manejo del historial médico de los pacientes.
- Gobiernos y Administración: emisión de licencias, pasaportes o contratos públicos certificados, reduciendo el fraude documental.
- Comercio Electrónico y Cadenas de Suministro: rastrear el origen ético y las certificaciones de calidad de un producto desde la fábrica hasta el consumidor.
- Propiedad Intelectual y NFTs: registro inmutable de la propiedad de activos digitales en la Web3.

No obstante, la arquitectura detrás de la procedencia digital es compleja y depende de varios componentes interconectados.

En primer lugar, destacan los estándares abiertos como el C2PA, un protocolo impulsado por la Coalition for Content Provenance and Authenticity y respaldado por entidades como Adobe, Microsoft o la BBC. Este sistema añade metadatos criptográficos directamente al contenido, de manera que, al publicarse, se genera un hash único firmado digitalmente con la identidad verificada del creador.

Para soportar esto, se emplean tecnologías subyacentes robustas, como los sistemas de contabilidad distribuida (Blockchain o DLT) que crean registros inmutables. Estas tecnologías suelen combinarse con módulos a nivel de sistema operativo, como los Linux Provenance Modules, y modelos estructurados como el Open Provenance Model.

A pesar de su evidente madurez técnica, la adopción masiva de la procedencia digital todavía se enfrenta a diversos obstáculos. Uno de los principales es lograr la estandarización, lo cual exige que tanto los grandes fabricantes de hardware (como cámaras y móviles), como los desarrolladores de software y las redes sociales utilicen los mismos parámetros en sus productos.

A esto se suma la tensión constante entre la privacidad y la transparencia, ya que resulta complicado verificar el origen de una información sin comprometer el anonimato vital para ciertas fuentes, como denunciantes o disidentes políticos.

Por otro lado, los costes de implementación representan un freno importante; modificar la infraestructura de datos para recopilar, almacenar y asegurar tal cantidad de metadatos supone una barrera de entrada muy elevada para las organizaciones pequeñas.

Finalmente, existe el reto de la seguridad de los propios metadatos, puesto que, paradójicamente, la información que certifica la procedencia debe estar blindada para evitar que actores maliciosos puedan manipularla o alterarla desde su origen.



Imagen 4. Procedencia digital. CSIRT Financiero.

Cloud 3.0: una oportunidad tecnológica que también amplía la superficie de riesgo

Cloud 3.0 promete infraestructuras más dinámicas, híbridas, multicloud y adaptativas, capaces de ubicar cada carga de trabajo en el entorno más adecuado según coste, latencia, resiliencia, cumplimiento o soberanía del dato. Sin embargo, para el sector financiero, esta evolución también representa una amenaza si avanza más rápido que la capacidad de gobierno, seguridad y supervisión de las entidades.

El riesgo es especialmente relevante porque la digitalización financiera en Colombia ya es estructural. Según la Superintendencia Financiera de Colombia, en 2025 el 81% de los establecimientos de crédito utilizaban inteligencia artificial en sus procesos, y una proporción significativa de bancos, compañías de financiamiento y SEDPE ya operan como entidades

nativas digitales². En este contexto, Cloud 3.0 no solo habilita nuevos servicios financieros: también amplía la dependencia de proveedores tecnológicos, API, identidades digitales, modelos de IA y entornos distribuidos.

Uno de los principales desafíos de seguridad de Cloud 3.0 es mantener la visibilidad y el control sobre este tipo de arquitecturas. Los entornos híbridos y multicloud pueden mejorar la continuidad del negocio, pero también multiplican los puntos de exposición: configuraciones erróneas, permisos excesivos, interfaces inseguras, recursos de terceros y fallos de observabilidad. Estos riesgos coinciden con las principales amenazas cloud identificadas por Cloud Security Alliance en 2024, entre ellas la mala configuración, la gestión deficiente de identidades y accesos, las API inseguras, los recursos de terceros y la visibilidad limitada.

La incorporación de inteligencia artificial a la infraestructura aumenta aún más la exposición. Los modelos de IA financiera pueden requerir datos sensibles de clientes, transacciones, comportamiento crediticio, señales antifraude o información biométrica. Si estos datos se procesan en entornos cloud mal gobernados, el impacto potencial incluye fuga de información, uso indebido de datos, decisiones automatizadas difíciles de auditar, dependencia de proveedores externos y fallos de cumplimiento.

Por ello, Cloud 3.0 debe ser tratado como una oportunidad tecnológica, pero también como un vector de riesgo estratégico. Para el sector financiero colombiano, el desafío no es solo migrar a modelos híbridos o multicloud, sino mantener control efectivo sobre dónde están los datos, quién accede a ellos, qué proveedor los procesa, bajo qué jurisdicción operan y cómo se responde ante un incidente.

La SFC publica indicadores de seguridad de la información y ciberseguridad del sector bancario, incluyendo gestión de incidentes, vulnerabilidades detectadas y costes asumidos por incidentes que afectaron a clientes, lo que evidencia la importancia de medir y supervisar este riesgo de forma continua.

En resumen, Cloud 3.0 puede acelerar la innovación financiera en Colombia, pero también puede ampliar la superficie de ataque si no se acompaña de gobierno cloud, gestión estricta de identidades, monitoreo continuo, control de proveedores, clasificación de datos, cifrado, trazabilidad y planes de resiliencia. En un sector basado en la confianza, la amenaza no está en usar la nube, sino en perder el control sobre ella.

² <https://www.superfinanciera.gov.co/publicaciones/10116043/sistema-financiero-acelera-implementacion-de-canales-digitales/>



Imagen 5. Características clave del modelo Cloud 3.0. CSIRT Financiero.

Matriz de priorización

Tendencia	Ventana temporal	Nivel de urgencia	Impacto principal	Respuesta organizacional
SEaaS	Inmediato	Muy alto	Fraude y suplantaciones de identidad	Verificación multicanal ante solicitudes inusuales, servicio de vigilancia digital con monitorización continua
Malware polimórfico	Inmediato	Alto	Continuidad operativa, dificultades de detección	Migrar de antivirus por firmas a EDR/XDR con análisis de comportamiento, complementado con threat hunting proactivo
Computación cuántica	Medio - largo plazo	Medio - Alto	Caducidad de protección criptográfica actual	Inventario criptográfico y priorización de migración a los estándares NIST ya publicados (FIPS 203, 204 y 205) para los sistemas con datos de vida larga
Procedencia digital	Corto - medio plazo	Medio - alto	Confianza en el contenido, fraude por deepfake	Verificación biométrica con prueba de vida certificada contra ataques con IA (estándar ISO/IEC 30107-3 nivel 2), reforzada con estándares de procedencia como C2PA

Cloud 3.0	Corto plazo	Medio	Superficie de ataque ampliada, identidades fragmentadas	Gobernanza de identidades centralizada (IAM/CIEM) bajo Zero Trust, con inventario y control específico de identidades no humanas (API, bots, cuentas de servicio)
-----------	-------------	-------	---	---

Referencias

BASE4 Security. (2025, 11 de diciembre). *Malware IA polimórfico y campañas de espionaje: Ficción vs. realidad*. LinkedIn.

<https://www.linkedin.com/pulse/malware-ia-polim%C3%B3rfico-y-campa%C3%B1as-de-espionaje-ficci%C3%B3n-ezqyc/>

Bentley, J. (2026, 10 de febrero). *AI-assisted hacking group hits targets with a complicated 'social engineering' scam that involves deepfaked CEOs, spoofed Zoom calls and a malicious troubleshooting program*. PC Gamer. <https://www.pcgamer.com/software/ai/ai-assisted-hacking-group-hits-targets-with-a-complicated-social-engineering-scam-that-involves-deepfaked-ceos-spoofed-zoom-calls-and-a-malicious-troubleshooting-program/>

Bollero, D. (2025, 25 de octubre). *La procedencia digital pone en jaque a las organizaciones*. Público.

<https://www.publico.es/opinion/columnas/procedencia-digital-pone-jaque-organizaciones.html>

Ciberso. (2026, 10 de febrero). *El auge del malware impulsado por IA*.

<https://ciberso.com/blog/concienciacion-sobre-ciberseguridad/auge-malware-impulsado-ia/>

Cloud Security Alliance. (2024). *Top threats to cloud computing 2024*.

<https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024>

Coalition for Content Provenance and Authenticity. (2021). *C2PA founding press release*. C2PA. <https://c2pa.org/c2pa-founding-press-release/>

Coalition for Content Provenance and Authenticity. (2025). *C2PA technical specification*. C2PA. <https://spec.c2pa.org/specifications/>

Cybersecurity and Infrastructure Security Agency. (2023). *Quantum-readiness: Migration to post-quantum cryptography*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf

Cybersecurity and Infrastructure Security Agency. (s. f.). *Post-quantum considerations for operational technology*. U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology>

European Banking Authority, European Insurance and Occupational Pensions Authority, & European Securities and Markets Authority. (2025). *Joint Committee update on risks and vulnerabilities in the EU financial system: Spring 2025*. European Banking Authority. <https://eba.europa.eu/sites/default/files/2025-03/c9723ef6-82b0-4232-b0f7-37cbf9cb78a9/Joint%20Committee%20Update%20on%20risks%20and%20vulnerabilities%20in%20the%20EU%20financial%20system%20-%20Spring%202025.pdf.pdf?>

Federal Bureau of Investigation. (2026). *2025 Internet crime report*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Federal Bureau of Investigation. (2025, 15 de mayo). *Senior US officials impersonated in malicious messaging campaign*. Internet Crime Complaint Center. <https://www.ic3.gov/PSA/2025/PSA250515>

Mauko, E., Johnson, S. D., & Mariconti, E. (2026). *Cybercrime as a service: A scoping review* [Prepublicación]. arXiv. <https://doi.org/10.48550/arXiv.2604.00063>

Ministerio de Ciencia, Tecnología e Innovación de Colombia. (s. f.). *Lista de programas académicos relacionados con inteligencia artificial, ciencia y tecnologías cuánticas, industria 4.0 y TIC*. Minciencias. https://minciencias.gov.co/sites/default/files/upload/convocatoria/anejo_9_lista_programas_academicos_relacionados_con_ia_ciencia_y_tecnologias_cuanticas_industria_4.0_y_tic.pdf

Mucci, T. (2024, 23 de julio). *¿Qué es la procedencia de los datos?* IBM. <https://www.ibm.com/es-es/think/topics/data-provenance>

National Cyber Security Centre. (2025, 7 de mayo). *Impact of AI on cyber threat from now to 2027*. <https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027>

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). U.S. Department of Commerce.

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>

National Institute of Standards and Technology. (s. f.). *Post-quantum cryptography*. U.S. Department of Commerce. <https://www.nist.gov/pqc>

National Institute of Standards and Technology. (s. f.). *What is post-quantum cryptography?* U.S. Department of Commerce.

<https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography>

National Institute of Standards and Technology. (2026). *Quantum computers may put internet traffic at risk. NIST is safeguarding computers with new encryption standards*. U.S. Department of Commerce.

<https://www.nist.gov/blogs/taking-measure/quantum-computers-may-put-internet-traffic-risk-nist-safeguarding-computers-new>

Orchard, A., Baron, C., & Wojtyla, P. (2026, 16 de abril). *AI meets voice phishing: How ATHR automates the full TOAD attack chain*. Abnormal Security. <https://www.abnormal.ai/blog/athr-ai-voice-phishing-toad-attacks>

Panenkov, D. (2026, March 21). *Cloud 3.0: The future of intent-driven multi-cloud*. TechRadar. <https://www.techradar.com/pro/cloud-3-0-the-future-of-intent-driven-multi-cloud>

SentinelOne. (2025, 20 de agosto). *¿Qué es el malware polimórfico? Ejemplos y retos*. <https://www.sentinelone.com/es/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/>

Superintendencia Financiera de Colombia. (s. f.). *Indicadores de seguridad de la información y ciberseguridad*.

<https://www.superfinanciera.gov.co/publicaciones/10110733/informes-y-cifrasinformesindicadores-de-seguridad-de-la-informacion-y-ciberseguridad-10110733/>

Superintendencia Financiera de Colombia. (2026). *Sistema financiero acelera implementación de canales digitales*.

<https://www.superfinanciera.gov.co/publicaciones/10116043/sistema-financiero-acelera-implementacion-de-canales-digitales/>

TECSID. (2026, 25 de enero). *Procedencia digital: El escudo contra la desinformación en 2026*. <https://blog.tecsid.com/procedencia-digital-escudo-desinformacion-2026>

ThreatScene. (2026, 2 de julio). *Social engineering 2026: Why most breaches still start with a conversation*. <https://threatscene.com/blog-update/social-engineering-2025-the-hidden-breach-behind-every-breach/>

Trend Micro. (2025, 25 de noviembre). *Trend Micro predicts 2026 as the year cybercrime becomes fully industrialized* [Comunicado de prensa]. <https://newsroom.trendmicro.com/2025-11-25-Trend-Micro-Predicts-2026-as-the-Year-Cybercrime-Becomes-Fully-Industrialized>

World Economic Forum. (2026). *Global cybersecurity outlook 2026*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf