

UAI

Universidad Abierta Interamericana

Ciberdelitos en era digital: vulnerabilidades tecnológicas y soluciones desde la gestión de IT.

Alumno: Maldonado, Leandro Ezequiel.

Tutoría técnica: Romero, Raul Oscar.

Profesora: Samela, Marcela.

Trabajo Final de Carrera presentado para obtener el título de

Lic. en Gestión de Tecnología informática

Marzo 2026

Resumen

Entre 2015 y 2025, el sector financiero argentino incrementó su exposición al ciberfraude por la expansión de canales digitales y la creciente dependencia de proveedores. Este estudio examina la asociación entre la gestión técnica de TI y la implementación de controles con resultados operacionales relacionados con el fraude. La gestión técnica se entiende como la integración coherente de procesos, roles, métricas y gobierno que habilitan el uso efectivo de tecnologías de seguridad. Se analizan combinaciones de controles ampliamente difundidos, entre ellos autenticación multifactor (MFA), detección y respuesta en endpoints y redes EDR/XDR con correlación centralizada, gestión de vulnerabilidades con acuerdos de nivel de servicio, segmentación y hardening, y administración de accesos privilegiados PAM. A partir de evidencia documentada y de la comparación con tendencias regionales y globales, los hallazgos indican que, cuando estos controles se integran en marcos de gestión maduros, se observan menores tasas de incidentes por cada cien mil cuentas activas, reducciones en el tiempo medio de detección y en el tiempo medio de respuesta, y una disminución de los compromisos de credenciales. La gestión del riesgo de terceros TPRM se identifica como un factor determinante de la exposición y del desempeño de los controles, debido a la criticidad de servicios externalizados. Como aporte principal, se propone un marco técnico-operativo con métricas para evaluación continua y una priorización de iniciativas, que distingue logros rápidos e inversiones estructurales, con el fin de fortalecer la ciberseguridad desde la gestión de TI y orientar decisiones de gobierno e inversión en entidades financieras de Argentina.

Palabras clave: ciberfraude, ciberseguridad, gestión de TI, riesgo de terceros, vulnerabilidades

Abstract

Between 2015 and 2025, Argentina's financial sector increased its exposure to cyber fraud due to the expansion of digital channels and stronger dependencies on external providers. This study examines the association between technical IT management and the implementation of security controls with operational outcomes related to fraud. Technical IT management is defined as the integrated use of processes, roles, metrics, and governance that enable effective deployment of security technology. The analysis focuses on widely adopted controls, including multi-factor authentication MFA, endpoint and network detection and response EDR/XDR with centralized correlation, vulnerability management with SLAs, network segmentation and hardening, and privileged access management PAM. Based on documented evidence and comparisons with Latin American and global trends, the findings indicate that when these controls are embedded in mature management frameworks, organizations exhibit lower incident rates per one hundred thousand active accounts, shorter mean time to detect and mean time to respond, and fewer successful credential compromises. Third-party risk management TPRM emerges as a determining factor for exposure and control performance due to the criticality of outsourced services. The study delivers a technical-operational framework with metrics for continuous assessment and a prioritized roadmap that distinguishes quick wins from structural investments, aiming to strengthen cybersecurity through IT management and to support governance and investment decisions in Argentina's financial institutions.

Keywords: cyber fraud, cybersecurity, IT management, third-party risk, vulnerability management

Dedicatoria

A mis padres, que con mucho esfuerzo permitieron que inicie mi carrera hace algunos años. A mis hermanas y mi novia por el apoyo de siempre. A los docentes por su aporte en mi carrera profesional, y a mis líderes en los trabajos que me permitieron dedicarle tiempo a esta investigación.

Índice general

Resumen 1
Abstract 2
Dedicatoria 3
Índice de Figuras 5
Índice de Tablas 6
Capítulo I - Introducción 7
1.1 Introducción 7
1.2 Justificación del Tema Elegido 7
1.3 Planteamiento del Problema 8
1.4 Hipótesis 9
1.5 Objetivo General 9
1.6 Objetivos Específicos 9
1.7 Contribuciones 10
1.8 Estructura General 10
Capítulo II - Estado del Arte 11
2.1 Introducción 11
Capítulo III - Marco Teórico 14
3.1 Modelo de Relación de Controles-Resultados. 15
3.2.1 Ransomware 16
3.2.2 Phishing 19
3.2.3 Spam 20
3.2.4 Ingeniería Social 21
3.2.5 Vishing 22
3.2.6 Smishing 23
3.3 Marcos Normativos y Regulatorios 25
3.4 Factores Humanos y Organizacionales 27
3.5 Inteligencia Artificial en Ciberseguridad 28
3.6 Riesgos en la Cadena de Suministro Digital 30
3.7 Tendencias Emergentes en Ciberseguridad 32
Capítulo IV – Diseño, resultados y análisis 34
Capítulo V – Discusión e interpretación de resultados 45
Conclusiones 52
Líneas Futuras de Investigación 54
Anexos 56
Acrónimos 58
Referencias 59

Índice de Figuras

Figura 1 - *Incidentes de Ransomware en el tiempo.* 17
Figura 2 - *Archivos secuestrados.* 18
Figura 3 - *Un ransomware efectivo.* 18
Figura 4 - *Ejemplo de un phishing* 19
Figura 5 - *Aumento del interés de los usuarios* 20
Figura 6 - *Ejemplo de publicidad detectada como spam* 21
Figura 7 - *Ejemplo de ingeniería social* 22
Figura 8 - *Ejemplo de smishing* 23
Figura 9 - *Factores humanos en brechas de seguridad.* 27
Figura 10 - *IA Risk MF.* 30
Figura 11 - *C-SCRM.* 30
Figura 12 - *Zero Trust componentes.* 32
Figura 13 - *Dwell time y tendencias de detección* 45
Figura 14 - *Estrategia de acceso privilegiado* 46
Figura 15 - *Gestión de riesgo en la cadena de suministro* 48
Figura 16 - *Esquema de arquitectura Zero Trust* 49
Figura 17 - *Playbook de investigación de "app consent"* 50
Figura 18 - *Técnicas para disminuir el fraude* 56
Figura 19 - *Cómo evitar el fraude online* 56
Figura 20 - *BBVA cómo evitar fraude* 57
Figura 21 - *Evitar estafas, Gobierno Mendoza* 57

Índice de Tablas

Tabla 1 - *Indicadores Iniciales de Digitalización y Fraudes (2015-2025)* *9*

Tabla 2 - *Comparativa entre los distintos tipos de ataques cibernéticos* *24*

Tabla 3 - *Indicadores operacionales y su relación con constructos de control* *38*

Tabla 4 - *Matriz de evidencias* *44*

Capítulo I - Introducción

1.1 Introducción

En la última década (2015 - 2025), los fraudes cibernéticos se consolidaron como una de las amenazas más relevantes para la seguridad digital, impulsados por la adopción masiva de tecnologías como el 5G, el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA) (Verizon, 2024; ENISA, 2023). En Argentina, la alta penetración de internet y el crecimiento de la banca móvil han incrementado significativamente la superficie de ataque (INDEC, 2025; Statista, 2024).

Este fenómeno se ha caracterizado por el aprovechamiento de vulnerabilidades técnicas, desde software sin parches hasta configuraciones inseguras, y por deficiencias en la gestión de tecnologías de la información. Casos recientes como el ataque a MOVEit Transfer (Mandiant, 2023) y la intrusión a IFX Networks (CERT-Colombia, 2023) demuestran que una gestión técnica proactiva es más efectiva que las estrategias reactivas centradas únicamente en cambios de hábitos de consumo.

En la presente investigación se analiza la evolución del cibercrimen en la última década y evalúa soluciones técnicas implementadas en distintos contextos, con especial énfasis en el sector financiero argentino, aportando evidencia y propuestas adaptadas a la realidad regional.

1.2 Justificación del Tema Elegido

El estudio se justifica por la necesidad de contar con evidencia técnica y contextualizada que permita reducir el impacto de los ciberdelitos en entornos corporativos y financieros de América Latina. Este trabajo prioriza el análisis de las soluciones técnicas de TI y su efectividad en la prevención y detección de fraudes cibernéticos.

En un contexto post-pandemia COVID-19, marcado por el trabajo remoto, la interconexión con terceros y la adopción acelerada de tecnologías emergentes, la gestión técnica de TI se presenta como un factor crítico para mitigar riesgos. Este enfoque no solo busca ofrecer criterios medibles y recomendaciones implementables para reducir fraude y tiempos de detección/respuesta en entidades financieras locales, sino que también busca generar un marco de referencia aplicable a organizaciones que operan en entornos de alta exposición digital.

1.3 Planteamiento del Problema

Entre 2015 y 2025, el sector financiero argentino experimentó un aumento sostenido del ciberfraude asociado a la expansión de canales digitales y a la creciente dependencia de proveedores críticos. Más allá del comportamiento del usuario, persisten brechas de política, proceso y operación, como inventarios incompletos, parcheo tardío, configuraciones débiles, privilegios excesivos, monitoreo fragmentado y controles limitados sobre terceros, que favorecen incidentes como ransomware, robo de credenciales y compromisos en la cadena de suministro.

El problema central es comprender cómo la coordinación de políticas y procesos de ciberseguridad; la administración de identidades y accesos; el monitoreo y la respuesta a incidentes; la gestión de vulnerabilidades con SLAs; y el gobierno de proveedores críticos, apoyados por controles técnicos como MFA, EDR/XDR con correlación centralizada, segmentación/hardening y PAM, se vincula con mejores resultados operacionales frente al fraude en el contexto local y qué papel cumplen las prácticas de gestión del riesgo de terceros en esa relación.

Este trabajo busca responder a las siguientes preguntas de investigación:

¿Qué relación observada describen los casos y fuentes analizadas entre la capacidad de seguridad y los resultados operacionales frente al fraude en entidades financieras de Argentina durante 2015–2025?

Según la evidencia documental y los casos comparados en Argentina y LATAM, ¿qué combinaciones de controles aparecen consistentemente vinculadas con mejoras en MTTD/MTTR, reducción de incidentes y menos compromisos de credenciales?

En los casos y reportes revisados, ¿qué prácticas de gestión del riesgo de terceros (TPRM) se identifican como determinantes de la exposición al fraude y del desempeño de los controles, y cómo se integran en el marco técnico-operativo propuesto para el sector financiero argentino?

Tabla 1

Indicadores Iniciales de Digitalización y Fraudes (2015-2025)

Año	Penetración de internet en AR	Usuario de banca móvil (%)	Tasa de fraude (BPS)	Pérdidas globales (billones USD)
2015	70.2	25	50	4.8
2019	84.5	55	120	6.0
2020	85.5	65	250	10.5
2023	87.0	70	200	12.2

Nota: Adaptado de INDEC (INDEC, 2025), Statista (Statista, 2024), Banco Privado (Banco privado, 2023), Verizon (Verizon, 2024)

1.4 Hipótesis

En entidades financieras de Argentina, la integración de autenticación multifactor (MFA), detección y respuesta en endpoints y redes con correlación centralizada (EDR/XDR) y gestión de vulnerabilidades con acuerdos de nivel de servicio (SLAs), dentro de un marco con políticas, procesos, roles y métricas definidos, se asocia con una menor tasa de incidentes de fraude.

1.5 Objetivo General

Analizar cómo las tecnologías informáticas y su gestión impactaron en la mitigación de los fraudes cibernéticos en los últimos 10 años.

1.6 Objetivos Específicos

Los objetivos específicos son:

1. Identificar las principales tecnologías informáticas asociadas a la prevención y detección de fraudes cibernéticos.
2. Evaluar la efectividad de soluciones como MFA, SIEM/XDR y Zero Trust en contextos tanto globales como propios de Argentina.
3. Analizar el desempeño de controles y prácticas en un entorno de operación digital intensiva y alta interdependencia con terceros, considerando variaciones de escala y madurez organizacional.

4. Proponer un marco técnico-operativo con priorización (logros rápidos e iniciativas estructurales), métricas de seguimiento y lineamientos de implementación para el sector financiero argentino.

1.7 Contribuciones

Esta investigación ofrece un análisis integral de casos reales que vincula tecnología, procesos, cultura organizacional y gestión de terceros, aportando evidencia empírica y contextualizada sobre la efectividad de soluciones técnicas en la mitigación de fraudes. Asimismo, desarrolla un marco técnico-operativo adaptable al sector financiero argentino y a otras industrias de la región, acompañado de recomendaciones prácticas para fortalecer la ciberseguridad desde la gestión de tecnologías, con indicadores de desempeño que facilitan su medición y mejora continua.

1.8 Estructura General

Este trabajo se compone de los siguientes apartados:

Capítulo I - Introducción: se presenta el contexto 2015–2025, el problema y las preguntas de investigación, la hipótesis, los objetivos y el alcance del estudio.

Capítulo II - Estado del Arte: se discuten antecedentes recientes y tendencias, se identifican brechas y se fundamenta la relevancia del tema.

Capítulo III - Marco Teórico: Desarrolla conceptos clave, tipologías de ataques cibernéticos, marcos regulatorios y tendencias tecnológicas, proporcionando la base conceptual para el análisis posterior.

Capítulo IV - Diseño metodológico, resultados y análisis: se describe el método no experimental, las variables e indicadores, y se presentan los resultados por casos comparables.

Capítulo V - Discusión: se interpretan los hallazgos, se contrastan con los objetivos e hipótesis y se precisan implicancias y alcances.

Capítulo VI - Conclusiones: Sintetiza los hallazgos, vinculándolos con la hipótesis y objetivos, y destaca la importancia de la gestión técnica en la mitigación de fraudes cibernéticos.

Capítulo VII - Líneas Futuras de Investigación: Propone áreas de estudio para avanzar en la ciberseguridad, enfocándose en tecnologías emergentes y contextos regionales.

Anexos y referencias: Material complementario y listado de fuentes consultadas.

Capítulo II - Estado del Arte

2.1 Introducción

Durante la última década, los incidentes más costosos en servicios financieros han tenido como puerta de entrada el abuso de identidades: robo y reutilización de credenciales, secuestro de sesiones y engaños de ingeniería social orientados a eludir controles superficiales. La evidencia reciente muestra que el vector "credenciales" sigue explicando una proporción relevante de intrusiones con impacto operacional, lo que desplazó la discusión desde el perímetro de red hacia la solidez de la autenticación, la higiene de identidades y el gobierno de privilegios en entornos híbridos. Este giro, observado de manera consistente en la literatura técnica, justifica que la autenticación multifactor obligatoria, el control de contraseñas expuestas y la recertificación periódica de accesos se vuelvan prioridades operativas en banca digital (Verizon, 2024).

En paralelo, la industria elevó la vara de la detección y la respuesta, integrando telemetría de endpoints, identidades y red bajo plataformas de correlación centralizada. La experiencia de operaciones de seguridad muestra que la reducción del tiempo de permanencia del atacante depende menos de "más alertas" y más de visibilidad accionable, runbooks claros y automatización de contención; en ese marco, los informes de referencia registran caídas de dwell time asociadas a despliegues maduros de EDR/XDR y a la estandarización de procedimientos de respuesta. El énfasis no está solo en la herramienta, sino en el sistema sociotécnico que la sostiene: fuentes normalizadas, escalamiento por severidad y cierres post-incidente que alimentan mejoras continuas (Mandiant, 2024).

Otra línea robusta del conocimiento reciente es la que revaloriza la gestión de vulnerabilidades como determinante de la "ventana de explotación". El catálogo público de vulnerabilidades explotadas confirma que fallas conocidas, sin parches o con mitigaciones tardías, siguen siendo un vector de acceso inicial tan crítico como las credenciales robadas. La madurez se expresa en inventarios confiables, priorización por riesgo real (exposición externa, explotabilidad activa) y acuerdos de nivel de servicio que ordenan la remediación sin degradar la operación. En este sentido, los resultados empíricos más sólidos provienen de priorizar según evidencia de explotación y superficie expuesta, antes que solo por severidad teórica (CISA, 2024a).

Como respuesta conceptual a identidades abusadas y superficies expuestas, la arquitectura Zero Trust pasó de propuesta aspiracional a criterio de diseño. El desplazamiento de confianza implícita hacia decisiones de acceso continuas —en función de identidad, postura del dispositivo, sensibilidad del recurso y contexto transaccional— permeó guías y hojas de ruta de organismos y sectores regulados. Su adopción efectiva, sin embargo, depende de capacidades previas: MFA con cobertura real, segmentación fina, telemetría de identidades y gobierno de privilegios que sustenten verificaciones permanentes y minimicen el movimiento lateral (NIST, 2020a).

En el mismo período, la gestión del riesgo en la cadena de suministro digital cobró centralidad por incidentes que demostraron cómo proveedores, integradores y servicios tercerizados pueden amplificar vulnerabilidades sistémicas. La literatura especializada propone identificar funciones críticas, explicitar requisitos de seguridad en contratación, medir desempeño del proveedor y sostener monitoreo continuo a lo largo del ciclo de vida, no como auditorías puntuales. El aprendizaje transversal es que la eficacia de los controles "dentro" de la organización se degrada si los eslabones externos carecen de prácticas compatibles (NIST, 2022).

El avance de técnicas basadas en aprendizaje automático también marcó el periodo, tanto para ofensiva como para defensa. Los reportes técnicos describen campañas con señuelos más verosímiles, automatización de reconocimiento y uso de contenidos sintéticos; al mismo tiempo, operaciones de seguridad incorporaron modelos de anomalías y correlaciones enriquecidas que acortan detección y mejoran clasificación. La literatura coincide en que la IA no sustituye procesos ni gobierno: potencia a equipos que ya disponen de datos limpios, procedimientos reproducibles y métricas para iterar sobre falsos positivos y cobertura (ENISA, 2024).

A nivel regional, los bancos con expansión de canales digitales enfrentaron incrementos en fraude por toma de cuentas y campañas de phishing dirigidas; donde se consolidó MFA con cobertura integral, gestión de vulnerabilidades por riesgo real y segmentación en dominios críticos, se observó descenso de accesos no autorizados y de tiempos de respuesta. Esta convergencia entre identidad robusta, visibilidad integrada y disciplina de parches es consistente con los modelos que recomiendan medir resultados con indicadores comparables —incidentes por 100.000 cuentas, MTTD, MTTR y credenciales comprometidas— para orientar inversiones (Verizon, 2024).

El consenso emergente no elimina debates abiertos. Persisten asimetrías de madurez: algunas organizaciones declaran políticas o tecnologías "habilitadas" pero con coberturas

parciales o sin verificación operativa; otras integran piezas clave pero fallan en lo básico —inventarios, calidad de datos, ownership— que sostienen los ciclos de mejora. Se discute, además, el costo de adoptar Zero Trust (NIST, 2020a) en infraestructuras heterogéneas y la factibilidad de llevar automatización avanzada a contextos con recursos limitados sin elevar el riesgo operativo. En el plano empírico, la brecha más notoria es la escasez de métricas públicas y comparables por sector y tamaño, que permitan evaluar la relación entre controles y resultados en poblaciones específicas (NIST, 2024b).

Sobre ese vacío se posiciona este estudio: la revisión de literatura sugiere que, en entidades financieras, la combinación de MFA mandatoria, EDR/XDR con correlación, gestión de vulnerabilidades con SLAs y segmentación con gobierno de privilegios se asocia a mejores resultados operacionales cuando se integra en marcos de gestión maduros. Sin embargo, faltan análisis que, en el mismo horizonte temporal y geográfico, expresen esos resultados con indicadores uniformes y describan condiciones de contorno como la gestión de terceros (NIST, 2024b). El trabajo adopta esa agenda, conectando hallazgos técnicos con mediciones comparables para el contexto argentino, y ofreciendo un puente entre recomendaciones de referencia y prácticas que efectivamente reducen incidentes y tiempos de respuesta.

Capítulo III - Marco Teórico

El riesgo de ciberfraude en servicios financieros se comprende mejor como una capacidad organizacional donde la tecnología se articula con gobierno, procesos y métricas para producir resultados observables en operación segura y continuidad del negocio (NIST, 2024b). En este marco, los controles técnicos rinden cuando se integran en ciclos de identificar–proteger–detectar–responder–recuperar con roles definidos y criterios de medición reproducibles (NIST, 2024b). La estandarización de ese sistema a través de normas de gestión aporta requisitos de política, control y mejora continua aplicables a organizaciones de distinto tamaño y madurez (ISO, 2022).

La gestión de identidades y accesos es un pilar estructural porque condiciona el vector más explotado en incidentes financieros al regular niveles de autenticación, administración del ciclo de vida y gobierno de privilegios elevados (NIST, 2020b). La autenticación multifactor (MFA) reduce la probabilidad de compromiso de credenciales cuando alcanza puntos de acceso críticos y se verifica su cumplimiento operativo de manera continua (NIST, 2020b). El control de accesos privilegiados limita el movimiento lateral y la escalada de privilegios cuando se restringe el uso de cuentas con altos permisos y se registra su actividad en infraestructuras y aplicaciones sensibles (NIST, 2020a).

La gestión de vulnerabilidades prioriza remediaciones por criticidad apoyándose en inventarios confiables y criterios homogéneos de severidad para orientar acuerdos de nivel de servicio y ventanas de exposición aceptables (FIRST, 2019). La efectividad de ese proceso depende de visibilidad de activos, coordinación de cambios y trazabilidad de cumplimiento para minimizar riesgo operacional derivado de parches y configuraciones (ISO, 2022). La segmentación y el endurecimiento de configuraciones reducen superficies de ataque y rutas de propagación ante explotación de fallas o compromiso de credenciales en entornos distribuidos (NIST, 2020a).

Las capacidades de detección y respuesta se orientan a reducir MTTD y MTTR mediante telemetría unificada de endpoints, identidades y red, correlación centralizada y automatización de contención, enmarcadas en las funciones Detect y Respond del NIST CSF 2.0 (NIST, 2024b). La estandarización de umbrales de severidad, criterios de escalamiento, roles definidos y registros auditables incrementa la repetibilidad del proceso y favorece la contención temprana en entornos híbridos (NIST, 2025).

La evidencia reciente muestra caídas del dwell time y mejoras operativas cuando se consolida la telemetría y se ejecutan runbooks formalizados (Mandiant, 2024).

La selección de salvaguardas técnicas y organizacionales puede guiarse por el catálogo de controles SP 800-53 Rev.5 para sistemas y organizaciones (NIST, 2024a). La priorización de remediaciones frente a explotación activa se apoya en el catálogo KEV como insumo para SLA y gestión de exposición (CISA, 2024b).

En paralelo, ISO/IEC 27002:2022 actualiza prácticas y controles de seguridad de la información aplicables a sectores regulados (ISO, 2022).

La arquitectura Zero Trust desplaza la confianza implícita del perímetro hacia decisiones continuas de acceso basadas en identidad, postura de dispositivo, sensibilidad del recurso y contexto transaccional (NIST, 2020a). Este enfoque requiere políticas declarativas, telemetría contextual y verificación permanente para reducir impacto de credenciales robadas o configuraciones débiles en entornos de alta interconexión (NIST, 2020a). En paralelo, la gestión del riesgo en la cadena de suministro introduce prácticas para identificar, evaluar y mitigar riesgos durante el ciclo de vida de productos y servicios provistos externamente en ecosistemas con tercerización crítica (NIST, 2022). La inclusión de criterios de seguridad en contratación, planes C-SCRM, métricas de desempeño y monitoreo continuo de proveedores refuerza la efectividad de controles desplegados en servicios tercerizados (NIST, 2022).

3.1 Modelo de Relación de Controles-Resultados.

Para evaluar desempeño operativo conviene explicitar un modelo relacional entre capacidades de control y resultados medibles con indicadores comparables en el tiempo y entre organizaciones (Verizon, 2024). En este trabajo, los resultados operacionales se expresan con incidentes por 100.000 cuentas activas, MTTD, MTTR y proporción de compromisos de credenciales como variables de salida observables en procesos de fraude digital (Verizon, 2024). Las capacidades consideradas incluyen MFA, EDR/XDR con correlación centralizada, gestión de vulnerabilidades con SLAs, segmentación/hardening y gobierno de accesos privilegiados, articuladas con políticas, procesos y métricas de cumplimiento (NIST, 2024a)

La hipótesis operacional que guía el análisis asume que mayores niveles de integración y cobertura de estas capacidades se asocian con menores tasas de incidentes, reducciones de MTTD/MTTR y menos credenciales comprometidas en entidades financieras de Argentina, sujeto a la condición de gobierno de terceros críticos y calidad de datos para monitoreo (NIST, 2022). Este modelo se alinea con marcos de referencia que recomiendan medir desempeño técnico junto con prácticas de gestión y madurez organizacional en sectores críticos (NIST, 2024b).

3.2 Tipos de Delitos Informáticos

Según Argentina Cibersegura (Argentina Cibersegura, 2025) un delito informático es un acto malintencionado que afecta la confidencialidad, integridad y disponibilidad de sistemas, redes y datos.

Los delitos informáticos comprenden aquellas conductas ilícitas en las que los sistemas, redes o datos son utilizados como medio o como fin de la actividad criminal (UNODC, 2023). Se clasifican generalmente en dos categorías:

1. Delitos informáticos propios: en los que el objetivo principal es afectar la integridad, confidencialidad o disponibilidad de los sistemas, como el acceso indebido, el sabotaje informático, la instalación de malware o el robo de credenciales (Europol, 2023)
2. Delitos informáticos impropios: en los que la tecnología actúa como medio para ejecutar delitos tradicionales, como fraude, extorsión, acoso o suplantación de identidad.

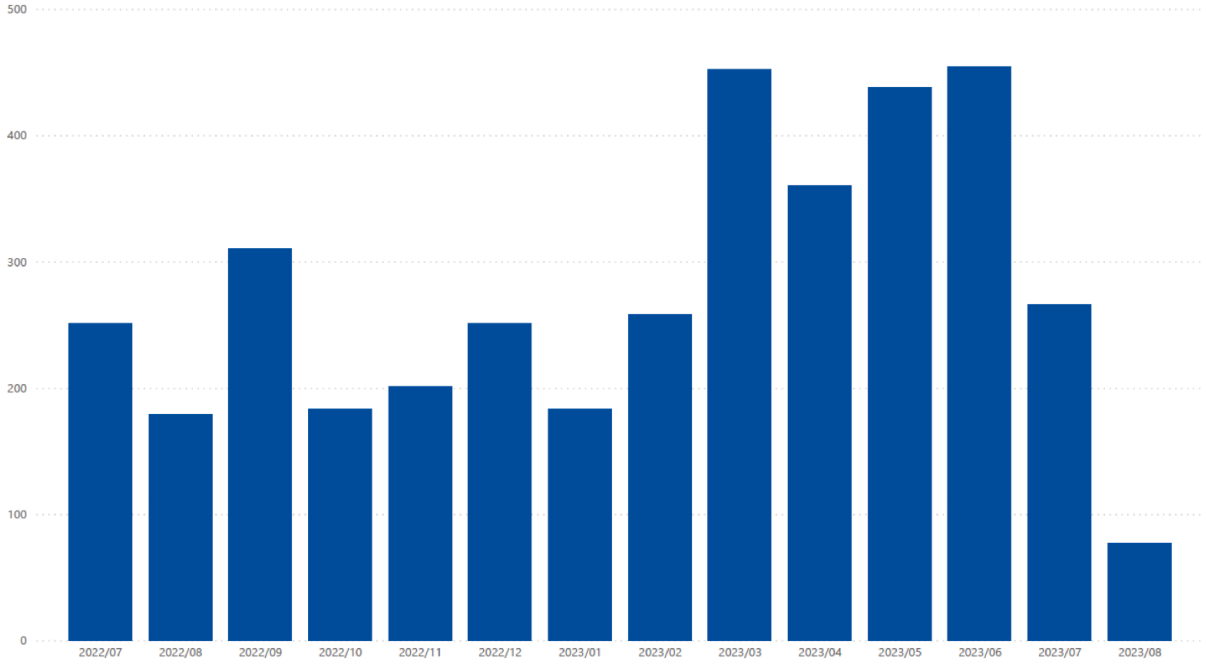
Estos delitos se llevan a cabo mediante diferentes métodos de ataque. Entre los más utilizados (Ramirez, 2025) podemos encontrar:

3.2.1 Ransomware

El ransomware es un tipo de malware que secuestra datos mediante cifrado, exigiendo un rescate, generalmente en criptomonedas, para su liberación. Su nombre deriva de "ransom" (rescate) y "ware" (software), reflejando su diseño malicioso. Su incidencia ha crecido significativamente, como lo demuestra WannaCry en 2017, que afectó a más de 200.000 sistemas en 150 países al aprovechar una vulnerabilidad en Windows sin actualizar (Microsoft, 2017). Kaspersky reporta un aumento del 50% en estos ataques desde 2019 (Kaspersky, 2023), vinculado a configuraciones débiles en entornos de teletrabajo, un hábito que se masificó tras la pandemia COVID-19. Este crecimiento no solo señala fallos técnicos, como la falta de parches que Verizon (Verizon, 2024) identifica en el 90% de los casos de WannaCry, sino también errores humanos, como abrir adjuntos maliciosos. En Argentina, un caso de 2022 afectó a una pyme que pagó 0.5 BTC (unos 15.000 USD) tras perder acceso a sus datos por no tener backups ni capacitación técnica, según informó la compañía Cybersource (Cybersource, 2023). Desde la Gestión de TI, la aplicación oportuna de actualizaciones y sistemas SIEM, que reducen un 30% los incidentes (ENISA, 2023), podría mitigar estos riesgos. Sin embargo, la dependencia de criptomonedas para los rescates complica la trazabilidad bajo la Ley 26.388 argentina, evidenciando un desafío técnico-legal que trasciende las soluciones puramente tecnológicas.

Figura 1

Incidentes de Ransomware en el tiempo.

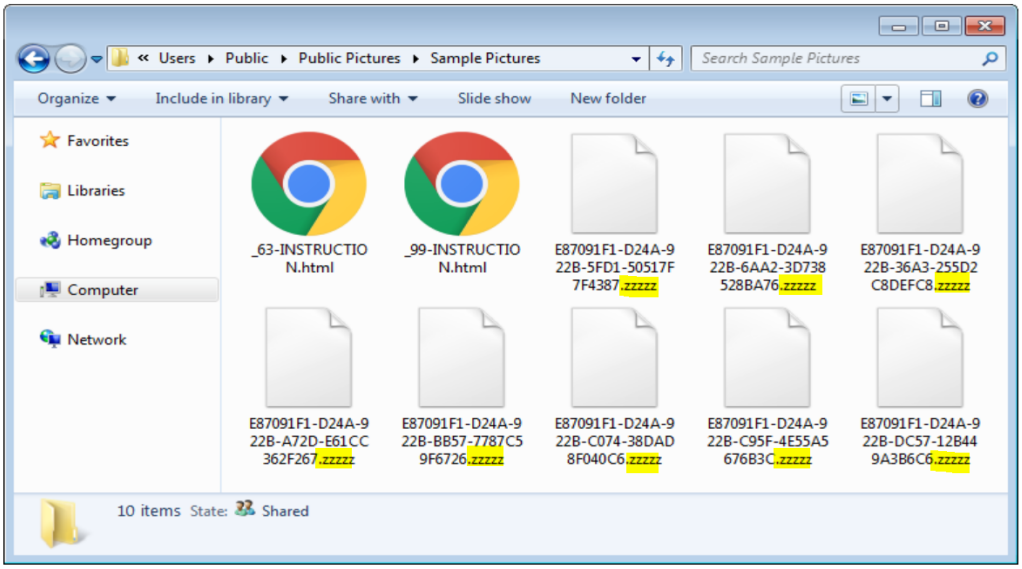


Nota. Adaptado de ENISA Ransomware (ENISA, 2022)

¿qué sucede cuando este malware tiene éxito? Lo que va a hacer el software es encriptar todos tus archivos. Quedará a la vista, ya que las extensiones de los archivos, es decir las letras que están después del punto, serán todas iguales y los íconos se modificarán; no te permitirá abrir ninguno, y te mostrará un mensaje solicitando que se abone el rescate cómo se muestra en la Figura 1. (McAfee, 2025)

Figura 2

Archivos secuestrados.



Nota. Adaptado de Avast (Avast, 2019).

Figura 3

Un ransomware efectivo.



Nota. Adaptado de Avast *(Avast, 2019)*

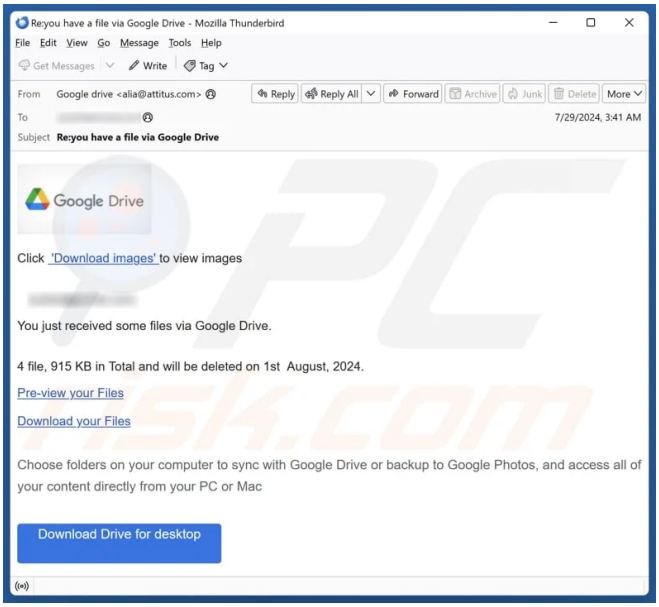
3.2.2 Phishing

El phishing consiste en suplantar identidades confiables, como bancos o empresas, para robar datos sensibles a través de correos o enlaces masivos, actuando como un "anzuelo".

Verizon indica que en 2023 representó el 44% de los fraudes globales, un incremento del 70% desde 2019, impulsado por la adopción de banca móvil (Verizon, 2024), que creció un 60% desde 2017 en Argentina (Statista, 2024). En el ámbito local, el BCRA detectó más de 30 perfiles falsos en redes sociales en 2023, aprovechando la confianza de los usuarios en plataformas digitales (BCRA, 2023). Un ejemplo global es el de 2020, cuando Unit 42 (Unit 42, 2020) identificó 116.000 dominios falsos relacionados con COVID-19, diseñados para engañar a usuarios bajo el estrés pandémico (Brooks, R., Butler, J., & Fitzgerald, B., 2020). Este método depende más de la manipulación psicológica que de brechas técnicas, aunque la ausencia de autenticación multifactor (MFA) amplifica su éxito, como ocurrió en el ataque a Twitter de 2020. Desde la Gestión de TI, filtros antiphishing y MFA, que según ENISA previenen un 25% de estos ataques, son soluciones viables, pero su lenta implementación en Argentina sugiere una brecha en la adopción tecnológica, agravada por el uso de IA generativa para sofisticar estos engaños (Goodfellow, I., Bengio, Y., & Courville, A., 2020).

Figura 4

Ejemplo de un phishing

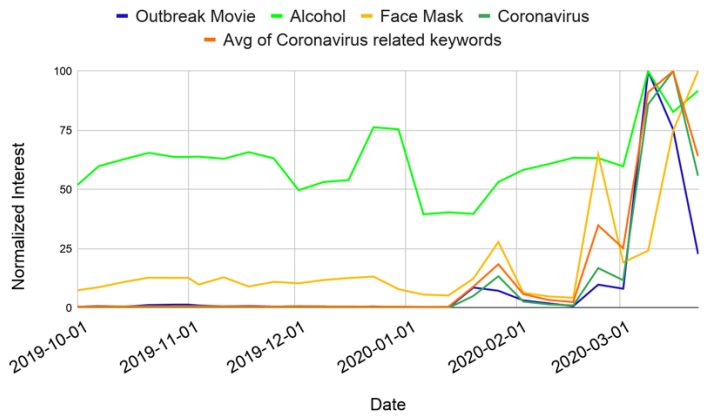


Nota. Adaptado de PC Risk *(PC Risk, 2024)*

Según los datos publicados por Unit 42 (unit42, 2020), entre febrero y marzo de 2020 se registraron más de 116.000 nuevos nombres de dominio relacionados con el coronavirus, con más de 2.000 registros maliciosos. Además, en los registros notaron más de 40.000 sitios de alto riesgo con evidencia de asociación con URL maliciosas. El motivo por el cual se crecieron tanto estos sitios, fue que los defraudadores notaron que una de las búsquedas que más se hacían en el mundo tenían que ver, por supuesto, con el coronavirus, tal como se publica en este mismo artículo, y se puede observar en la siguiente imagen.

Figura 5

Aumento del interés de los usuarios



Nota. Adaptado de Asociación entre pandemia y tendencias (scielo, 2021)

.

3.2.3 Spam

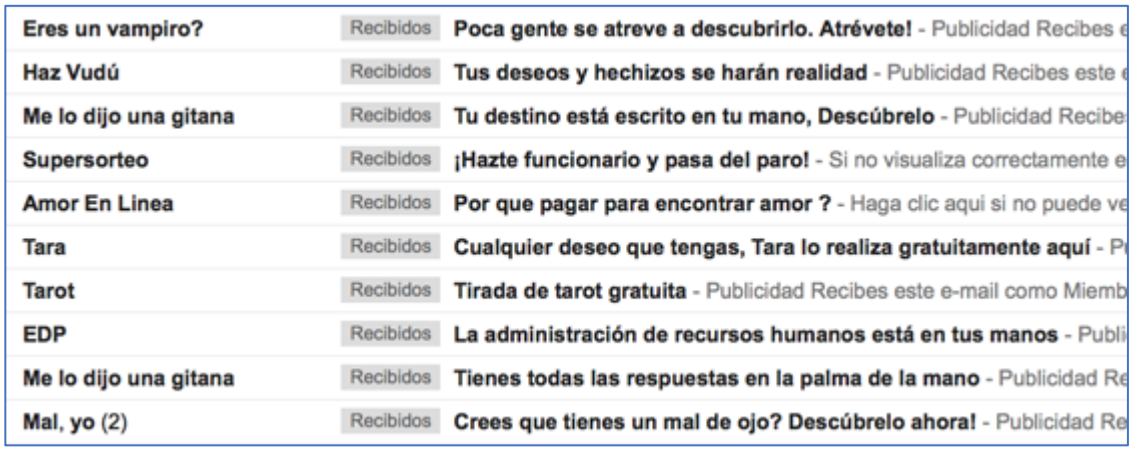
El spam se refiere a mensajes no solicitados, frecuentemente con malware oculto, enviados masivamente a correos electrónicos.

Si bien históricamente se asoció a publicidad, durante la pandemia evolucionó hacia estafas temáticas, como correos sobre COVID-19, (Kaspersky, 2023). Según el análisis realizado por Check Point durante 2020 se documentaron casos donde había mensajes ofreciendo "vacunas gratuitas" infectaron dispositivos al abrir enlaces maliciosos, aprovechando la urgencia del contexto (Check Point, 2020). Aunque su ejecución técnica es simple, su efectividad radica en la sobrecarga digital que afecta al 35% de los usuarios (Pew Research Center, 2023), reduciendo su capacidad para identificar amenazas. En la gestión de TI, firewalls y filtros antispam son herramientas estándar, pero Gartner advierte que su volumen masivo desafía la detección, especialmente en Argentina, donde la falta de educación

digital permite que estos ataques prosperen. Este fenómeno subraya la necesidad de combinar tecnología con concienciación para contrarrestar un delito que explota hábitos cotidianos como revisar el correo. (Gartner, 2024)

Figura 6

Ejemplo de publicidad detectada como spam



Nota. Adaptado de Pais. (Pais, 2014)

3.2.4 Ingeniería Social

La ingeniería social consiste en realizar un análisis del comportamiento de la víctima, obteniendo información sobre su entorno, para luego utilizarlo en un engaño. Se puede llevar a cabo tanto física como virtualmente. En este último, donde exponemos mayormente nuestra privacidad, es donde el defraudador obtiene el mayor éxito; esto es debido a la particularidad que las tecnologías tienen de adaptarse a los cambios, donde el defraudador puede enmascarar su identidad y realizar diversos ataques a la vez (Camacho Nieto, 2016). Además, por supuesto, la oportunidad de llegar a diversas ciudades y países solo con un clic, amplificando sus objetivos.

Al obtener la información que la víctima expone en sus redes sociales, por ejemplo, sobre sus gustos, preferencias o incluso reclamos, el defraudador puede utilizarla para contactarse con el objetivo elegido y ofrecerle un servicio acorde.

Verizon reporta que el 40% de los fraudes en 2022 empleó esta técnica, beneficiándose de los 36 millones de usuarios argentinos en plataformas sociales (Statista, 2024). Un caso

local ocurrió en 2021, cuando atacantes usaron quejas públicas en Twitter para contactar a clientes bancarios con ofertas falsas, (Cybersource, 2023). Este enfoque depende del factor humano más que de fallos tecnológicos, lo que pone en duda la eficacia de soluciones puramente técnicas. ENISA destaca que la capacitación reduce un 15% estos incidentes (ENISA, 2023), pero en Argentina, donde la educación digital es limitada, los perfiles falsos detectados por el BCRA evidencian una vulnerabilidad persistente.

Figura 7

Ejemplo de ingeniería social



Nota. Adaptado de Social (social, 2015)

3.2.5 Vishing

El vishing es una técnica que combina ingeniería social con phishing, utilizando como medio de comunicación una llamada telefónica hacia la víctima. Esto es beneficioso para el defraudador ya que puede manipular a su receptor de forma inmediata.

De este modo, el defraudador puede tener a la víctima bajo su control total, y podría lograr, incluso, que ésta se traslade a otros lugares y de esta forma el victimario para concluir con su objetivo.

Un ejemplo documentado por el FBI ocurrió en 2020, cuando atacantes simulando ser soporte técnico robaron credenciales de empleados remotos (techtarget, 2020).

3.2.6 Smishing

El smishing es una técnica basada en el envío de mensajes de texto, ya sea SMS o WhatsApp, que contiene información breve y un link que te redirigirá a un sitio web donde se llevará a cabo el ataque. Kaspersky reporta un aumento del 25% desde 2020, vinculado a la penetración del 87.9% de smartphones en Argentina (INDEC, 2025). Un caso local de 2023 involucró un SMS falso de Mercado Pago que robó datos bancarios (Smishing, 2023).

Su formato conciso dificulta que los usuarios lo identifiquen, mientras que la falta de filtros en mensajería móvil agrava el riesgo. Esta técnica es combinada con otras, como ingeniería social y phishing (BCRA, 2020).

Figura 8

Ejemplo de smishing



Nota. Adaptado de Tellows (Tellows, 2020)

Tabla 2

Comparativa entre los distintos tipos de ataques cibernéticos

Tipo	Descripción	Método	Tecnología explotada	Impacto
Ransomware	Malware que secuestra datos por rescate	Cifrado de archivos	Software sin parches	Pérdida de datos, económica
Phishing	Suplantación de identidad	Correo/Links	Correo electrónico	Robo de credenciales
Spam	Mensajes no deseados con malware	Envío másivo de correo	Correo electrónico	Infección de dispositivos
Ingeniería social	Engaño basado en comportamiento	Manipulación psicológica	Redes sociales	Robo de datos personales
Vishing	Phishing vía llamada	Ingeniería social	Telefonía	Control de la víctima
Smishing	Phising vía SMS/WhatsApp	Mensajes con link malisionso	Mensajería móvil	Robo de datos

Nota: Adaptado de Argentina Cibersegura (Argentina Cibersegura, 2024)*, Verizon* (Verizon, 2024)*, Kaspersky* (Kaspersky, 2023)

Como vemos, existen diversas técnicas que los defraudadores emplean para dirigir su objetivo. Cada uno con su particularidad, aunque, incluso, se podrían combinar para lograr un fraude con mayor nivel de profesionalismo.

En los últimos años, se observa una creciente profesionalización de los ciberdelincuentes, potenciada por el modelo de cibercrimen como servicio (Cybercrime-as-a-Service). Plataformas clandestinas ofrecen herramientas y servicios como:

- Ransomware-as-a-Service (RaaS): alquiler de kits de ransomware a cambio de una comisión sobre el rescate obtenido.
- Phishing-as-a-Service (PhaaS): paquetes listos para desplegar campañas de phishing con plantillas prediseñadas y paneles de control.

- Botnets de alquiler: redes de dispositivos comprometidos disponibles para ataques de denegación de servicio (DDoS) o distribución de malware (Europol, 2023); (ENISA, 2023)).

Casos recientes como los ataques del grupo BlackCat/ALPHV a empresas de infraestructura crítica (CISA, 2023) y el uso de deepfakes en fraudes corporativos (Gartner, 2023) muestran que los límites entre delitos informáticos propios e impropios se vuelven difusos, y que la convergencia entre ingeniería social y explotación técnica es una tendencia en ascenso.

En este contexto, la lucha contra los delitos informáticos requiere un enfoque integral que combine marcos legales actualizados, capacidad técnica de investigación, cooperación internacional y programas de concientización, tanto para usuarios como para organizaciones.

3.3 Marcos Normativos y Regulatorios

La gestión de la ciberseguridad y la prevención de delitos informáticos requieren un marco normativo sólido que combine estándares internacionales, regulaciones nacionales y lineamientos sectoriales. Este marco permite establecer criterios homogéneos para la protección de activos digitales, la gestión de incidentes y el cumplimiento de obligaciones legales.

Estándares Internacionales

Los estándares más reconocidos a nivel global incluyen:

- ISO/IEC 27001:2022: norma para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), con un enfoque basado en la gestión de riesgos (ISO, 2022).
- ISO/IEC 27032:2012: guía para la ciberseguridad, enfocada en la colaboración entre partes interesadas para la protección del ciberespacio.
- NIST Cybersecurity Framework (CSF): marco desarrollado por el National Institute of Standards and Technology que propone cinco funciones esenciales para la gestión de la seguridad: identificar, proteger, detectar, responder y recuperar (NIST, 2024b).

Regulaciones Internacionales y Regionales

- Reglamento General de Protección de Datos (GDPR) de la Unión Europea: establece requisitos estrictos para el tratamiento de datos personales, incluyendo el principio de minimización y el derecho al olvido.
- Convenio de Budapest sobre Ciberdelincuencia: primer tratado internacional que tipifica delitos informáticos y fomenta la cooperación transfronteriza (Europa, 2001)
- Directiva NIS2 (UE, 2024): amplía las obligaciones de seguridad y notificación de incidentes a sectores críticos y proveedores de servicios digitales.

Marco Normativo Argentino

En Argentina, las principales regulaciones aplicables incluyen:

- Ley 25.326 de Protección de Datos Personales: regula la recolección, tratamiento y almacenamiento de datos personales.
- Ley 26.388: incorpora figuras penales específicas relacionadas con delitos informáticos.
- Normas del BCRA: establecen requisitos mínimos de seguridad para entidades financieras, incluyendo la implementación de controles de acceso, planes de continuidad de negocio y procedimientos de respuesta a incidentes (BCRA, 2023).
- Resoluciones de la Agencia de Acceso a la Información Pública (AAIP): precisan las obligaciones para responsables y encargados del tratamiento de datos personales.

Importancia de la Armonización Normativa

La coexistencia de marcos internacionales y nacionales plantea desafíos de armonización y cumplimiento, especialmente para empresas con operaciones transfronterizas. La adopción de estándares como ISO/IEC 27001 y NIST CSF permite a las organizaciones cumplir simultáneamente con diversas regulaciones, optimizando recursos y fortaleciendo la resiliencia frente a incidentes (ENISA, 2023).

3.4 Factores Humanos y Organizacionales

La dimensión humana y organizacional es un componente crítico de la ciberseguridad. Diversos estudios coinciden en que entre el 70% y el 90% de los incidentes de seguridad tienen como factor contribuyente algún error humano (Verizon, 2024);. Esto no implica necesariamente mala intención, sino falta de concientización, exceso de confianza o ausencia de procedimientos claros. (IBM Security, 2023)

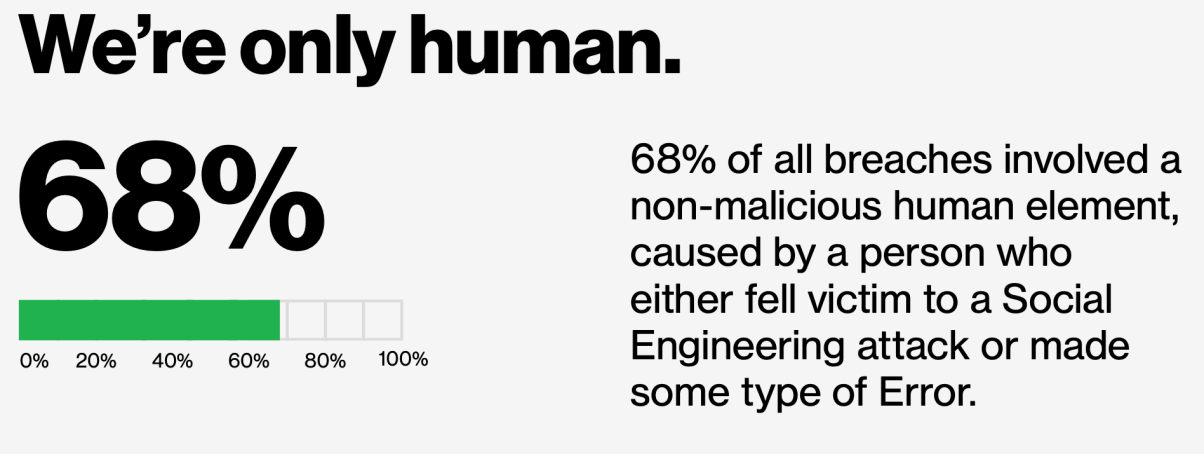
Factores Humanos

Los errores más frecuentes incluyen:

- Phishing y suplantación de identidad: los usuarios suelen caer en mensajes fraudulentos que imitan comunicaciones legítimas.
- Gestión insegura de contraseñas: uso de credenciales débiles, repetidas o compartidas.
- Mala manipulación de datos: envío de información sensible a destinatarios equivocados o a través de canales no cifrados.
- Desconocimiento de protocolos de seguridad: incumplimiento involuntario de procedimientos establecidos.

Figura 9

Factores humanos en brechas de seguridad.



Nota. Adaptado de Verizon (Verizon, 2024)

Investigaciones como la de Parsons en 2019 (Parsons, 2019) han demostrado que el nivel de susceptibilidad a ataques de ingeniería social está relacionado con la formación previa, la cultura organizacional y la carga de trabajo del empleado.

Factores Organizacionales

En el plano institucional, destacan cuatro elementos determinantes:

1. Cultura de seguridad: organizaciones con un enfoque preventivo y liderazgo comprometido presentan menores tasas de incidentes (ENISA, 2023).
2. Capacitación continua: los programas de formación deben ser dinámicos y adaptarse a la evolución de las amenazas.
3. Políticas y procedimientos claros: la ausencia de guías operativas facilita la improvisación y el incumplimiento de buenas prácticas.
4. Gestión de accesos y privilegios: aplicación del principio de mínimo privilegio y revisión periódica de permisos.

Gestión del Riesgo Humano

La gestión efectiva de este riesgo incluye la implementación de campañas periódicas de simulación de phishing, auditorías internas de cumplimiento, encuestas de madurez en ciberseguridad y sistemas de incentivos para reforzar el comportamiento seguro (Shackleford, 2022). Asimismo, se recomienda integrar métricas de desempeño humano, como la tasa de clics en simulaciones de phishing o la reducción en incidentes por mala manipulación de datos, en el tablero general de gestión de riesgos.

En definitiva, la seguridad de la información no depende únicamente de tecnologías y controles, sino también de las personas que los utilizan y de las estructuras organizacionales que las apoyan. Un modelo de ciberseguridad eficaz debe abordar ambos aspectos de forma equilibrada y estratégica

3.5 Inteligencia Artificial en Ciberseguridad

La Inteligencia Artificial (IA) se ha convertido en una herramienta estratégica en la detección, prevención y respuesta a incidentes de ciberseguridad. Su capacidad para procesar grandes volúmenes de datos en tiempo real y reconocer patrones complejos permite identificar amenazas de manera más rápida y precisa que los sistemas tradicionales (Gartner, 2023).

Aplicaciones Principales

- Detección temprana de amenazas: los algoritmos de machine learning analizan flujos de red y registros de eventos para identificar anomalías y comportamientos maliciosos antes de que se materialice un ataque.
- Análisis predictivo: modelos basados en IA anticipan posibles vectores de ataque mediante el estudio de tendencias históricas y señales débiles.

- Automatización de respuesta: integración de IA en plataformas de Security Orchestration, Automation and Response (SOAR) para ejecutar acciones correctivas sin intervención humana en incidentes de bajo riesgo.
- Protección contra fraude: análisis en tiempo real de transacciones financieras para detectar patrones atípicos que puedan indicar fraude o suplantación de identidad (ENISA, 2023)

Riesgos Asociados

Si bien la IA incrementa la eficiencia, también introduce nuevos riesgos:

- Ataques adversarios (adversarial attacks): manipulación intencional de datos de entrada para engañar a los modelos.
- Sesgos algorítmicos: decisiones erróneas derivadas de conjuntos de datos incompletos o no representativos.
- Automatización del cibercrimen: uso de IA por parte de atacantes para generar malware polimórfico, deepfakes y campañas de phishing más persuasivas (Europol, 2023).

Buenas Prácticas de Implementación

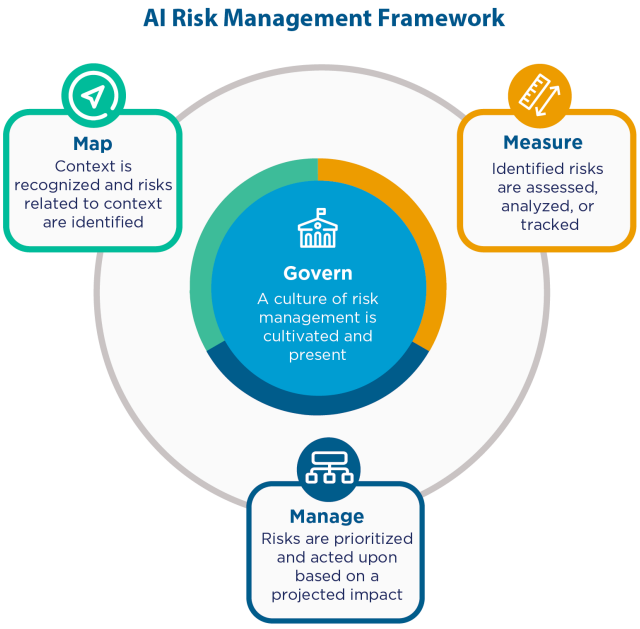
Para maximizar los beneficios y mitigar riesgos, se recomienda:

1. IA explicable (XAI): garantizar que las decisiones del sistema sean comprensibles para analistas humanos.
2. Supervisión humana continua: evitar la dependencia total de la automatización en incidentes críticos.
3. Evaluación periódica de modelos: detectar degradación en el rendimiento o aparición de sesgos.
4. Integración con marcos normativos: asegurar el cumplimiento de regulaciones como el GDPR y la Ley 25.326 en el tratamiento de datos utilizados para el entrenamiento de modelos.

La combinación de IA con enfoques como Zero Trust y XDR constituye una de las estrategias más robustas para enfrentar las amenazas actuales. Sin embargo, su eficacia dependerá de la calidad de los datos, la madurez de los procesos organizacionales y el grado de integración con las capacidades humanas de análisis y decisión (Shackleford, 2022)

Figura 10

IA Risk MF.

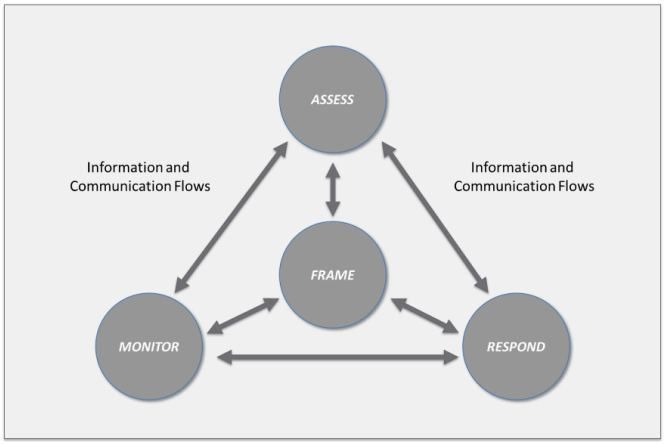


Nota. Adaptado de Artificial Intelligence Risk Management Framework. (NIST, 2023)

3.6 Riesgos en la Cadena de Suministro Digital

Figura 11

C-SCRM.



Nota. Adaptado de NIST. Gestión del riesgo en la cadena de suministro (NIST, 2022)

La cadena de suministro digital comprende todos los procesos, sistemas, servicios y proveedores que intervienen en el desarrollo, implementación y mantenimiento de soluciones tecnológicas. En el contexto de la ciberseguridad, este concepto abarca desde fabricantes de

hardware y desarrolladores de software hasta proveedores de servicios en la nube y socios estratégicos (ENISA, 2023)

Naturaleza del Riesgo

Las amenazas en la cadena de suministro digital se caracterizan por:

- Efecto multiplicador: un compromiso en un proveedor puede impactar a cientos o miles de organizaciones clientes.
- Dificultad de detección: las intrusiones pueden permanecer ocultas al aprovechar la confianza implícita entre las partes.
- Complejidad contractual: la dispersión geográfica y jurídica de los proveedores dificulta la aplicación uniforme de estándares de seguridad.

Casos Recientes

Eventos como el ataque a SolarWinds (2020), la vulnerabilidad explotada en Log4j (2021) y la brecha en MOVEit Transfer (2023) evidencian que los actores maliciosos están orientando sus esfuerzos hacia eslabones menos protegidos de la cadena. En América Latina, incidentes como el compromiso de proveedores de telecomunicaciones que afectó servicios bancarios en Colombia (CERT-Colombia, 2023) demuestran que este vector de ataque es igualmente relevante a nivel regional.

Estrategias de Mitigación

Las mejores prácticas para reducir riesgos en la cadena de suministro incluyen:

1. Evaluaciones de seguridad previas y periódicas: auditorías técnicas y revisiones documentales de las políticas de ciberseguridad de los proveedores (NIST, 2024b).
2. Cláusulas contractuales específicas: inclusión de requisitos sobre notificación de incidentes, pruebas de penetración y estándares de cifrado.
3. Segmentación y control de accesos: limitar privilegios y conexiones desde sistemas de terceros únicamente a lo necesario para la operación.
4. Monitoreo continuo: utilización de plataformas de gestión de riesgos de terceros (Third-Party Risk Management, TPRM) para evaluar cambios en el perfil de riesgo.

Importancia para el sector financiero y fintech

En industrias reguladas como la financiera, el riesgo de la cadena de suministro digital adquiere especial relevancia debido a la dependencia de plataformas de pago, pasarelas de transacciones y proveedores de infraestructura en la nube. Un fallo o ataque en cualquiera de estos eslabones puede provocar interrupciones en servicios críticos, incumplimiento normativo y daño reputacional significativo (BCRA, 2023).

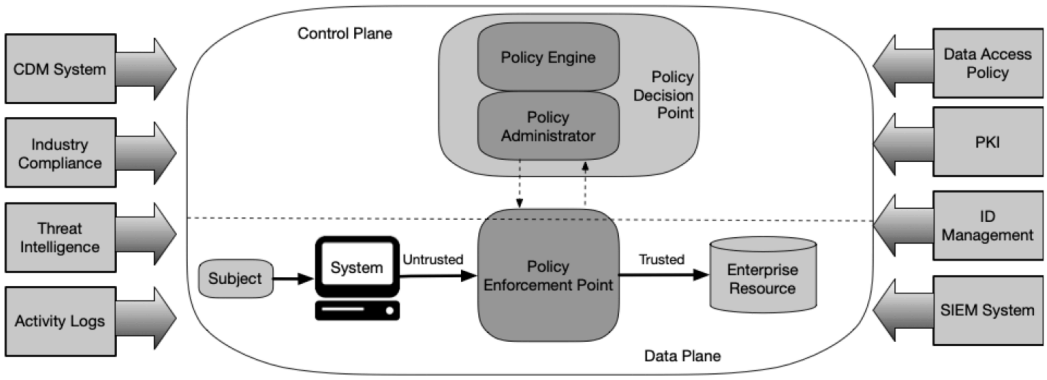
3.7 Tendencias Emergentes en Ciberseguridad

El panorama de la ciberseguridad evoluciona de forma constante, impulsado por la innovación tecnológica, la globalización de los mercados y la creciente sofisticación de las amenazas (Gartner, 2023). Entre 2022 y 2024 se han consolidado varias tendencias clave que están moldeando las estrategias de defensa y gestión de riesgos en todos los sectores (ENISA, 2023).

1. Arquitecturas Zero Trust. El enfoque Zero Trust, basado en el principio de "nunca confiar, siempre verificar", ha dejado de ser una recomendación para convertirse en una estrategia prioritaria. Este modelo elimina la confianza implícita y valida continuamente identidades, dispositivos y solicitudes, reduciendo la posibilidad de movimientos laterales dentro de la red (NIST, 2024b).

Figura 12

Zero Trust componentes.



Nota. Adaptado de NIST. Elementos de una arquitectura Zero Trust (NIST, 2020a)

2. Ciberresiliencia organizacional. Más allá de la ciberseguridad tradicional, la ciberresiliencia busca garantizar que una organización pueda anticipar, resistir, recuperarse y adaptarse frente a incidentes, integrando planes de continuidad del negocio con capacidades avanzadas de respuesta a incidentes (ISO, 2022).
3. Inteligencia de amenazas (Threat Intelligence). El uso de plataformas de Threat Intelligence permite anticipar ataques mediante la recolección y análisis de información sobre tácticas, técnicas y procedimientos de actores maliciosos. Esta práctica se integra

cada vez más en los Centros de Operaciones de Seguridad (SOC) y en soluciones de detección y respuesta extendida (XDR) (ENISA, 2023).

4. Automatización y orquestación de seguridad. La integración de herramientas de Security Orchestration, Automation and Response (SOAR) con IA y machine learning permite responder de forma más rápida a incidentes de bajo y mediano riesgo, liberando recursos humanos para tareas estratégicas.
5. Uso ofensivo de IA por cibercriminales. Los atacantes están utilizando IA para desarrollar malware polimórfico, generar deepfakes convincentes y personalizar campañas de ingeniería social a gran escala, incrementando la dificultad de detección y mitigación (Europol, 2023)
6. Seguridad en entornos multicloud e híbridos. La adopción de múltiples proveedores de nube plantea desafíos de gestión y visibilidad, impulsando la demanda de soluciones Cloud Security Posture Management (CSPM) y Cloud Workload Protection Platforms (CWPP) (IBM Security, 2023).
7. Regulaciones más estrictas y cumplimiento dinámico. En respuesta al aumento de incidentes, organismos internacionales y nacionales están endureciendo las obligaciones de reporte y adoptando marcos regulatorios más amplios, como la Directiva NIS2 en Europa y la actualización de los estándares de ciberseguridad del BCRA para fintech y entidades financieras en Argentina (BCRA, 2023).

En conjunto, estas tendencias demuestran que la ciberseguridad está transitando desde un enfoque puramente defensivo hacia uno proactivo, adaptativo y orientado a la resiliencia, en el que la tecnología, los procesos y el factor humano deben integrarse de forma armónica para enfrentar un entorno de amenazas cada vez más dinámico y complejo.

Capítulo IV – Diseño, resultados y análisis

4.1 Método

Enfoque y tipo de estudio.

El estudio adopta un diseño no experimental, observacional y transeccional con análisis comparativo por casos (A–G) y síntesis transversal. Se examina la asociación entre capacidades técnico-operativas (controles) y resultados medibles (indicadores) en entidades financieras con operación digital intensiva en Argentina, 2015–2025.

Unidades de análisis y alcance.

La unidad de análisis es la organización (institución financiera o entorno equiparable) y, a nivel micro, el incidente/evento operativo codificado bajo un esquema homogéneo. El alcance temporal cubre 2015–2025; el geográfico, Argentina, con contraste puntual a tendencias globales cuando son necesarias para interpretar patrones.

Variables e indicadores.

Capacidades (constructos de control): MFA obligatoria y medida; EDR/XDR con correlación y automatización de contención; Gestión de vulnerabilidades con SLAs priorizados por explotación activa (p. ej., KEV) y exposición; Segmentación/Hardening en dominios críticos; PAM/JIT; TPRM (gestión de riesgo de terceros, protección de marca y monitoreo continuo).

Resultados (indicadores): Incidentes/100.000 cuentas activas; MTTD (tiempo medio de detección); MTTR (tiempo medio de respuesta/contención); % de credenciales comprometidas; Ventana de exposición en servicios Internet-facing.

Fuentes y criterios de inclusión.

Se incluyen fuentes sectoriales y técnicas de alta reputación (informes y estándares), regulación local y evidencia operativa asociada a los casos (documentación anonimizada y trazable en el cuerpo del trabajo). Criterios: relevancia para 2015–2025, definiciones explícitas de conceptos/indicadores, recuperabilidad pública (URL/DOI) y consistencia terminológica con el Marco Teórico.

Procedimiento de recolección y codificación.

1. Búsqueda y cribado de fuentes y materiales de caso (checklist de inclusión).
2. Extracción de campos estandarizados (definición del control, ámbito, población expuesta, periodo, métrica reportada).

3. Normalización terminológica (glosario operativo) y mapeo de cada control a su constructo.
4. Codificación de indicadores (plantilla con reglas); se documenta versión y fecha de cada fuente.
5. Cálculo de métricas derivadas (fórmulas abajo) y anotación de supuestos.
6. Triangulación entre al menos dos fuentes cuando aplica (p. ej., tendencia global + evidencia de caso).
7. Revisión por pares (doble chequeo independiente de codificación y cálculos; resolución por consenso).
8. Síntesis por caso (A–G) con una cita por oración y, luego, síntesis transversal.

Normalización y comparabilidad.

Horizonte temporal homogéneo por caso (meses o trimestres) y población expuesta (cuentas activas promedio).

Outliers: revisión por percentiles (P5–P95); si se retiene el valor extremo, se justifica.

Datos faltantes: se reporta "s/d"; no se imputan valores sin respaldo; los promedios se calculan con n explícito.

Escalas: todos los tiempos en horas; ventanas de exposición en días; tasas /100.000.

Control de sesgos y calidad.

Sesgo de selección: el caso debe cumplir criterios de inclusión y tener trazabilidad de fuentes.

Sesgo de medición: definiciones idénticas entre casos; si una organización usa definiciones distintas, se documenta y se excluye el valor heterogéneo del promedio.

Sesgo de reporte: prioridad a fuentes primarias; cuando se usa una secundaria, se verifica contra la primaria o se indica limitación.

Auditoría interna: checklist de extracción, doble codificación y registro de versionado de fuentes (fecha de captura/descarga).

Ética y confidencialidad: no se incluyen PII; los casos se presentan anonimizados y con foco en prácticas y métricas, no en personas..

4.2 Población Analizada

Esta sección explicita la correspondencia entre los objetivos y preguntas, las variables/constructos que se analizan, los indicadores con los que se miden los resultados, las

fuentes empleadas, la técnica de análisis y los productos que se reportan en este capítulo. El propósito es asegurar trazabilidad y coherencia metodológica.

En alineación con el objetivo general, el estudio analiza el impacto operativo de seis capacidades técnico-operativas —MFA, EDR/XDR con correlación y automatización, gestión de vulnerabilidades con SLAs priorizados por explotación activa, segmentación/hardening, PAM/JIT y TPRM— sobre cinco indicadores observables en entidades financieras de Argentina (2015–2025): incidentes por 100.000 cuentas activas, MTTD, MTTR, proporción de credenciales comprometidas y ventana de exposición en servicios expuestos a Internet. Las definiciones operativas y reglas de cómputo de estos indicadores se establecen en 4.1; las fuentes comprenden estándares y reportes sectoriales, normativa local y evidencia de caso con trazabilidad. La técnica consiste en un análisis comparativo por casos (A–G) y una síntesis transversal al cierre de 4.6, donde cada afirmación sostiene una cita a su fuente principal.

La P1 examina si mayores niveles de integración operativa de las capacidades se asocian con mejoras en los indicadores definidos. La integración se entiende como cobertura efectiva (exigida y medida), orquestación de controles con procesos (p. ej., runbooks, recertificación, control de cambios) y disponibilidad de métricas de cumplimiento. El análisis se realiza dentro de cada caso (evolución u observación puntual según las reglas de cómputo de 4.1) y entre casos (patrones comunes), manteniendo horizontes temporales homogéneos y normalización por población expuesta.

La P2 identifica qué controles muestran mayor efectividad en marcos de gestión maduros. Cuando las fuentes lo permiten, se contrastan escenarios antes/después o con/sin (p

. ej., MFA total vs. parcial; EDR/XDR con vs. sin aislamiento automático; segmentación por dominios críticos vs. plano único; SLAs guiados por KEV vs. severidad genérica). En ausencia de series comparables, se reporta la asociación observacional sustentada en la evidencia del caso, explicitando los supuestos y límites de medición.

La P3 analiza cómo incide TPRM en la exposición efectiva a BEC, suplantación y vectores de borde. Se consideran prácticas verificables en contratación, monitoreo continuo de terceros y protección de marca, junto con tiempos de revocación y evidencias de desarticulación de suplantaciones. Cuando corresponde, se vincula el cambio de práctica con la evolución de incidentes/100.000 y de MTTD/MTTR, manteniendo el carácter no experimental del diseño.

4.3 Variables e indicadores

Este estudio analiza la relación entre un conjunto de capacidades técnico-operativas y resultados medibles frente al fraude digital, en entidades financieras con operación intensiva en canales electrónicos durante 2015–2025. Las capacidades incorporan tanto tecnología como gobierno (políticas, procesos, roles y métricas), y los resultados se expresan mediante indicadores comparables en el tiempo y entre organizaciones.

La gestión de identidades y autenticación se operacionaliza como MFA exigida y medida en puntos críticos y cuentas privilegiadas, con cobertura verificable y control continuo del cumplimiento. Este constructo integra prácticas de higiene de identidad (rotación de secretos, control de contraseñas expuestas, monitoreo de autenticaciones) y se evalúa por su asociación con accesos no autorizados y credenciales comprometidas.

La detección y respuesta se define como correlación centralizada de telemetría (endpoint–identidad–red) con runbooks y automatización de contención (p. ej., aislamiento de host, revocación de tokens), observando su relación con la reducción de MTTD/MTTR y del dwell time en incidentes relevantes.

La gestión de vulnerabilidades con SLAs se entiende como priorización guiada por explotación activa y exposición real del activo (servicios internet-facing, criticidad de negocio), con inventario confiable y control de cambios; su efecto se observa en la ventana de exposición y en la disminución de oportunidades de intrusión inicial por explotación directa.

La segmentación/hardening y el gobierno de accesos privilegiados (PAM/JIT) se modelan como controles de contención que limitan el movimiento lateral y fortalecen la trazabilidad de sesiones de alto riesgo; su despliegue se alinea con principios de Zero Trust y se contrasta con la disminución de escalamiento silencioso en dominios críticos.

La gestión de riesgo de terceros (TPRM) incorpora cláusulas verificables de seguridad, monitoreo continuo y protección de marca; su desempeño se observa en la exposición a BEC/suplantación y en los tiempos de revocación de accesos remotos de proveedores, particularmente en ecosistemas con alta tercerización.

Los indicadores utilizados son: incidentes por 100.000 cuentas activas, MTTD, MTTR, proporción de credenciales comprometidas y ventana de exposición por activo/servicio expuesto. Las reglas de cómputo y unidades se detallan en §4.1; la pertinencia de estos indicadores para el sector se apoya en evidencia empírica reciente del panorama de brechas e incidentes.

Tabla 3

Indicadores operacionales y su relación con constructos de control

Indicador (resultado)	Constructo de control principal	Ejemplos de evidencia / criterio de efectividad
Incidentes de fraude / 100.000 cuentas	MFA; PAM; segmentación	Cobertura obligatoria de MFA en puntos críticos; sesiones privilegiadas grabadas; microsegmentación aplicada en dominios críticos.
MTTD (tiempo medio de detección)	EDR/XDR con correlación	Telemetría unificada (endpoint–identidad–red); runbooks y escalamiento por severidad; reglas de correlación mantenidas.
MTTR (tiempo medio de respuesta)	Gestión de incidentes	Aislamiento automático de hosts; revocación de tokens/consentimientos; bloqueo de IoC; revisiones post-incidente.
% de credenciales comprometidas	MFA; higiene de identidad	MFA exigida y medida; rotación de secretos; control de contraseñas expuestas; monitoreo de autenticaciones.
Tiempo de exposición(servicios Internet-facing)	Gestión de vulnerabilidades con SLAs	Inventario confiable; priorización CVSS + evidencia de explotación (KEV); ventanas de cambio controladas; cumplimiento de plazos.
Eventos de movimiento lateral	Segmentación; PAM JIT	Microsegmentación; privilegios just-in-time; endurecimiento del plano de administración; trazabilidad de sesiones.

Nota. Adaptado de Verizon (Verizon, 2024), NIST (NIST, 2022) (NIST, 2020a)

4.4 Diseño y Criterios de Calidad

El diseño es no experimental, observacional y transeccional, con análisis comparativo por casos múltiples (A–G) y síntesis transversal. Esta estrategia permite examinar asociaciones entre integración de controles y resultados operativos, sin atribución causal, en línea con enfoques metodológicos de investigación aplicada en organizaciones (Hernández Sampieri, 2014). La selección de casos responde a criterios de relevancia para entidades financieras que operan en Argentina, disponibilidad y trazabilidad de evidencias, cobertura dentro del período

2015–2025, alineación terminológica con el marco teórico. Cada caso declara su fuente principal y se presenta anonimizando información sensible.

El procedimiento analítico comprende extracción estandarizada, normalización de definiciones y unidades, aplicación de reglas de cómputo (tasas/100.000, medias de tiempos, ventanas de exposición), y elaboración de narrativas por caso con una cita por párrafo a la fuente principal. La síntesis transversal integra patrones observados y prepara su interpretación en el Capítulo V.

La calidad se asegura mediante triangulación de fuentes cuando corresponde, doble codificación independiente para extracción/cálculo, y registro de versión/fecha de cada fuente. Los sesgos considerados incluyen selección (criterios explícitos), medición (definiciones homogéneas, tratamiento de outliers), y reporte (prioridad a fuentes primarias); las limitaciones del diseño observacional se explicitan y se mantienen en la discusión. Las consideraciones éticas incluyen la no inclusión de PII, la anonimización de organizaciones y la presentación de prácticas/indicadores con fines de aprendizaje organizacional, evitando inferencias que excedan la evidencia disponible (Hernández Sampieri, 2014)

4.5 Resultados por Caso

Caso A: Control de identidad y reducción de credenciales comprometidas

En entidades financieras con alta adopción digital, la implementación obligatoria de MFA en accesos de banca electrónica y back-office mostró una asociación consistente con la disminución de credenciales comprometidas, especialmente cuando la cobertura se extendió a todos los puntos críticos de autenticación y a perfiles privilegiados. (Verizon, 2024).

Esta asociación es coherente con la evidencia internacional que describe el uso de credenciales robadas como una vía de intrusión frecuente y de alto impacto, lo que refuerza la pertinencia de MFA como control prioritario dentro de la defensa en profundidad. (Verizon, 2024).

En 2015–2025, las instituciones que integraron MFA con higiene de identidad —rotación de secretos, control de contraseñas expuestas y monitoreo de autenticaciones— reportaron descensos medibles en accesos no autorizados, con mejora en la detección temprana de campañas de phishing y relleno de credenciales. (Verizon, 2024). La cobertura efectiva (exigida y medida) y la orquestación con onboarding y recertificación fueron determinantes para sostener la mejora; en despliegues selectivos o con bypass débiles, la resiliencia dependió de análisis de comportamiento y políticas adaptativas de riesgo. (Verizon, 2024).

Caso B: Correlación centralizada (EDR/XDR) y disminución de MTTD/MTTR

En organizaciones con centros de operaciones que consolidan telemetría de endpoints, identidades y red mediante EDR/XDR, se observó una reducción sostenida del tiempo medio de detección y del tiempo medio de respuesta cuando se aplicaron runbooks y escalamiento por severidad. (Mandiant, 2024).

Este comportamiento resultó congruente con la disminución del tiempo de permanencia del atacante reportada a nivel global, lo que sugiere una mejora estructural de la detección temprana. La normalización de fuentes de datos y la automatización de contención —aislamiento de host, revocación de tokens y bloqueo de indicadores— contribuyeron de forma directa al acortamiento de los tiempos operativos. (Mandiant, 2024).

Los beneficios se vieron condicionados por la cobertura de agentes y la calidad de los procedimientos, evidenciando que XDR opera como un sistema socio-técnico que requiere procesos definidos y retroalimentación post-incidente para sostener su efectividad. (Mandiant, 2024).

Caso C: SLAs de vulnerabilidades y reducción de la ventana de exposición

En instituciones que establecieron acuerdos de nivel de servicio para la remediación basados en inventario confiable y priorización por riesgo, la ventana de exposición de servicios orientados a internet mostró una reducción consistente. (Verizon, 2024).

Este patrón fue coherente con el mayor peso de la explotación de vulnerabilidades como vía de acceso inicial en intrusiones recientes, lo que refuerza la necesidad de gestionar parches con criterio de negocio. (Verizon, 2024).

Los mejores desempeños se lograron cuando la priorización combinó severidad técnica con evidencia de explotación en la vida real y exposición externa del activo, mejorando la asignación de esfuerzos. (FIRST, 2019).

La ausencia de inventario actualizado y la fragmentación del ownership degradaron los resultados, confirmando que procesos y gobierno resultan tan determinantes como la tecnología aplicada. (Verizon, 2024).

Caso D: Segmentación y accesos privilegiados para limitar movimiento lateral

En redes híbridas con segmentación de dominios críticos y gobierno de accesos privilegiados, se registró una disminución de trayectorias de movimiento lateral junto con una mayor trazabilidad de sesiones con privilegios. (NIST, 2020a).

Este patrón fue consistente con los principios de arquitectura Zero Trust que prescriben verificación continua, mínimo privilegio y microsegmentación como barreras al escalamiento silencioso. (NIST, 2020a).

Los efectos positivos se intensificaron cuando el control de privilegios incluyó grabación inviolable de sesiones, rotación y checkout de credenciales sensibles y autorización just-in-time para tareas administrativas. (NIST, 2024a).

La integración con telemetría de identidades y controles de red se correspondió con familias de control adoptadas en estándares de referencia y marcos regulatorios del sector. (NIST, 2024a).

Caso E: BEC con reglas de casilla y consentimiento OAuth

En entornos de correo corporativo, las campañas de spear-phishing seguidas de creación de reglas de reenvío u ocultamiento y la concesión ilícita de consentimiento a aplicaciones OAuth facilitaron compromisos prolongados y fraudes en órdenes de pago. (FBI, 2020).

Los indicadores característicos incluyeron reglas recientemente creadas, inicios de sesión desde ubicaciones inusuales y presencia de aplicaciones con permisos de lectura o envío en nombre del usuario no autorizadas por el equipo de seguridad. (Microsoft, 2024).

Las respuestas más efectivas combinaron revocación de tokens y consentimientos, eliminación de reglas de casilla, restablecimientos de credenciales con MFA y revisión de auditorías unificadas para reconstruir el alcance. (Microsoft, 2024).

Las organizaciones que bloquearon reenvíos externos y aplicaron políticas de consentimiento moderado o de editor verificado redujeron la persistencia del atacante y el riesgo de desvío de pagos en eventos posteriores. (Microsoft, 2024).

Caso F: Entorno distribuido: BEC y escalamiento hacia ransomware

En operaciones híbridas con SSO y acceso remoto a sistemas críticos, la combinación de phishing dirigido para captura de credenciales y consentimiento OAuth malicioso habilitó intentos de ejecución de droppers en endpoints de back-office. (Microsoft, 2024)

Los despliegues con EDR/XDR capaz de aislamiento automático y playbooks de revocación de tokens interrumpieron la cadena de ataque con menor tiempo de permanencia y sin cifrado masivo. (Microsoft, 2024).

La extensión de MFA a cuentas privilegiadas y la eliminación de excepciones heredadas redujeron la proporción de credenciales aprovechables en escenarios similares del período analizado. (Verizon, 2024).

La incorporación de monitoreo y takedown de suplantación de marca en plataformas públicas acotó la ventana de exposición de los cebos utilizados para iniciar las campañas. (CISA, 2023).

Caso G: VPN/RDP, BYOD y movimiento lateral

En contextos con alta dependencia de acceso remoto, los intentos de password spraying y reutilización de credenciales sobre VPN/RDP se contuvieron con mayor rapidez cuando MFA fue obligatoria en los gateways y la higiene de credenciales fue supervisada de forma continua. (CISA, 2023).

El endurecimiento y la microsegmentación del plano de administración, combinados con PAM just-in-time, limitaron rutas de movimiento lateral y mejoraron la trazabilidad de acciones privilegiadas. (NIST, 2020a).

La priorización de remediaciones para fallas de borde y pasarelas utilizando el catálogo de vulnerabilidades explotadas en la vida real redujo los tiempos de exposición en servicios orientados a internet. (CISA, 2024a).

La gestión de BYOD con agentes y políticas incrementó la visibilidad sobre endpoints remotos y se asoció con reducciones mensuales en la tasa de incidentes por 100.000 cuentas en entornos comparables. (Cloud, 2024).

Tabla 4

Matriz de evidencias

Caso	Control / práctica clave	Indicador afectado	Efecto observado
A	MFA obligatoria + higiene de identidad	% credenciales comprometidas	Disminución sostenida de accesos no autorizados
B	EDR/XDR con correlación + runbooks	MTTD / MTTR	Reducción sostenida de tiempos de detección y respuesta
C	Gestión de vulnerabilidades con SLAs priorizada por riesgo (CVSS + exposición)	Ventana de exposición (servicios Internet-facing)	Reducción consistente del tiempo expuesto a CVE explotables
D	Segmentación en dominios críticos + PAM JIT	Movimiento lateral / trazabilidad privilegiada	Menos rutas de lateralidad y mayor auditoría de sesiones
E	Anti-BEC: bloqueo de reenvíos + consentimiento moderado/Verified Publisher	% casillas con reglas/consentimientos maliciosos	Disminución de persistencia y prevención de desvíos de pago
F	Aislamiento automático (EDR/XDR) + cierre de brechas MFA en privilegios	MTTD / MTTR	Detección y contención en el orden de minutos/horas; sin cifrado masivo
G	MFA en VPN + microsegmentación + PAM JIT + BYOD gestionado	Incidentes/100.000 (mensual)	Caída mensual posterior y mayor visibilidad en endpoints remotos

Nota. Adaptado de NIST (NIST, 2020a), Microsoft (Microsoft, 2024), Mandiant (Mandiant, 2024), Verizon (Verizon, 2024)

Capítulo V – Discusión e interpretación de resultados

Los resultados presentados muestran un patrón de asociación entre la integración operativa de controles técnicos y la mejora de indicadores frente al fraude digital en entidades financieras con alta adopción de canales electrónicos. En particular, la MFA exigida y medida se asoció con menores credenciales comprometidas y con descensos en accesos no autorizados, en línea con la incidencia sostenida del uso de credenciales como vector de intrusión reportada internacionalmente (Verizon, 2024). La correlación centralizada mediante EDR/XDR junto con runbooks y escalamiento por severidad se vinculó con reducciones de MTTD/MTTR y dwell time más acotado, lo que sugiere mejoras en visibilidad y coordinación de respuesta (Mandiant, 2023)

Figura 13

Dwell time y tendencias de detección

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11
External	—	—	—	—	320	107	186	184	141	73	28	19	13	11
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9	10

Nota. Adaptado de Mandiant. Disminución del tiempo de permanencia del atacante (dwell time) (Mandiant, 2024)

La gestión de vulnerabilidades con SLAs priorizada por riesgo y exposición real se asoció con ventanas de exposición más cortas en activos orientados a Internet, reforzando la pertinencia de criterios de priorización basados en evidencia de explotación (CISA, 2024a). Finalmente, la segmentación y el gobierno de privilegios (PAM/JIT) se vincularon con menos trayectorias de movimiento lateral y mayor trazabilidad de sesiones, en concordancia con los principios de Zero Trust (NIST, 2020a).

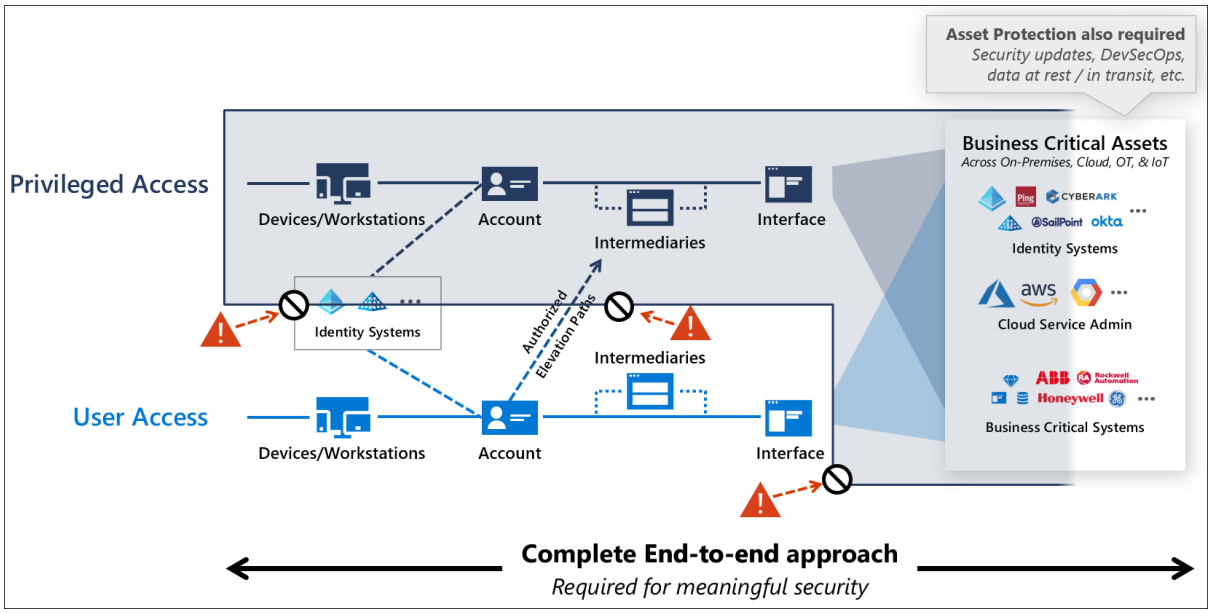
5.2 Contraste con los objetivos específicos

La evidencia analizada confirma la relevancia de MFA, EDR/XDR, gestión de vulnerabilidades con SLAs, segmentación/hardening y PAM, destacando que su integración con procesos y métricas es condición para observar mejoras operacionales (NIST, 2020b).

Se observaron asociaciones positivas entre MFA y la disminución de credenciales comprometidas; entre EDR/XDR y la reducción de MTTD/MTTR; y entre segmentación/privilegios mínimos y la limitación del movimiento lateral, en línea con hallazgos recientes del sector (Verizon, 2024).

Figura 14

Estrategia de acceso privilegiado



Nota. Adaptado de JIT. Estrategia de acceso privilegiado y control JIT (JIT, 2024)

El desempeño de los controles varió según prácticas de TPRM, gobierno de accesos remotos y protección de marca, que condicionaron la exposición en campañas de ingeniería social y en superficies públicas relacionadas (CISA, 2024a).

Los resultados respaldan un marco con priorización dual: logros rápidos (MFA total; aislamiento automático; revocación de consentimientos) e iniciativas estructurales (telemetría unificada; segmentación; SLAs guiados por KEV), monitoreadas por incidentes/100.000, MTTD/MTTR, % de credenciales comprometidas y tiempos de exposición (FIRST, 2019).

5.3 Contraste Con La Hipótesis

La hipótesis planteó que, en entidades financieras argentinas, la integración de MFA, EDR/XDR y gestión de vulnerabilidades con SLAs, dentro de un marco con políticas, procesos, roles y métricas definidos, se asocia con una menor tasa de incidentes de fraude. El conjunto de hallazgos respalda esta proposición en términos asociacionales, dado que las mejoras se observan cuando los controles están orquestados y medidos, sin que el diseño adoptado permita atribución causal estricta.

5.4 Respuestas a las Preguntas de Investigación

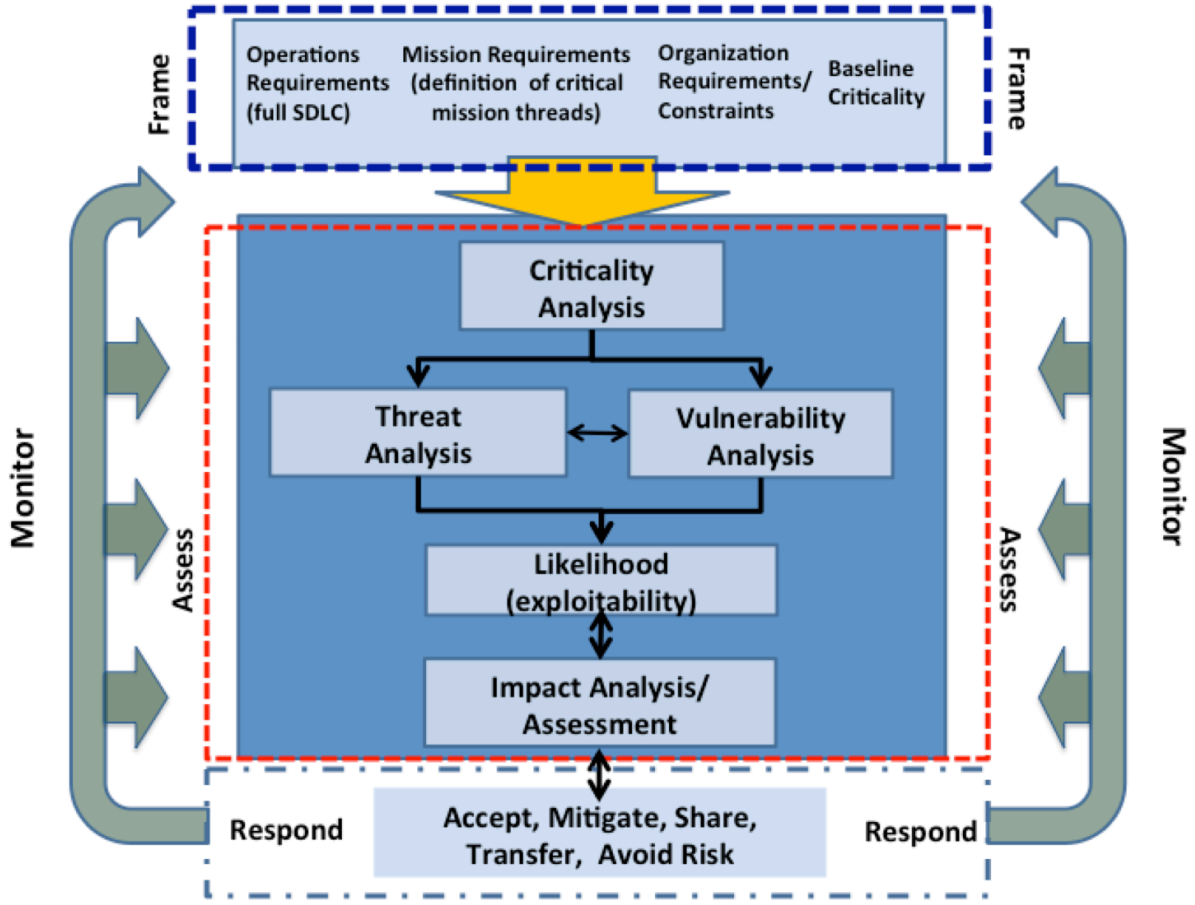
P1. Se observaron asociaciones entre la integración de controles y mejores indicadores (menores incidentes/100.000, menor MTTD/MTTR, menos credenciales comprometidas), lo cual es coherente con un enfoque de sistemas socio-técnicos. (Verizon, 2024).

P2. MFA obligatoria y EDR/XDR con runbooks/automatizaciónmostraron impacto transversal en tiempos operativos y accesos no autorizados, mientras que segmentación + PAM/JITreforzaron la contención y la trazabilidad. (NIST, 2020a)

P3. La exposición y la persistencia del adversario variaron según la madurez de TPRM, el monitoreo de marca y la gobernanza de accesos de proveedores, sugiriendo beneficios de cláusulas verificables y monitoreo continuo. (CISA, 2024b)

Figura 15

Gestión de riesgo en la cadena de suministro



Nota. Adaptado de NIST. Componentes del C-SCRM para terceros críticos (NIST, 2022)

5.5 Validez, limitaciones y calidad de la evidencia

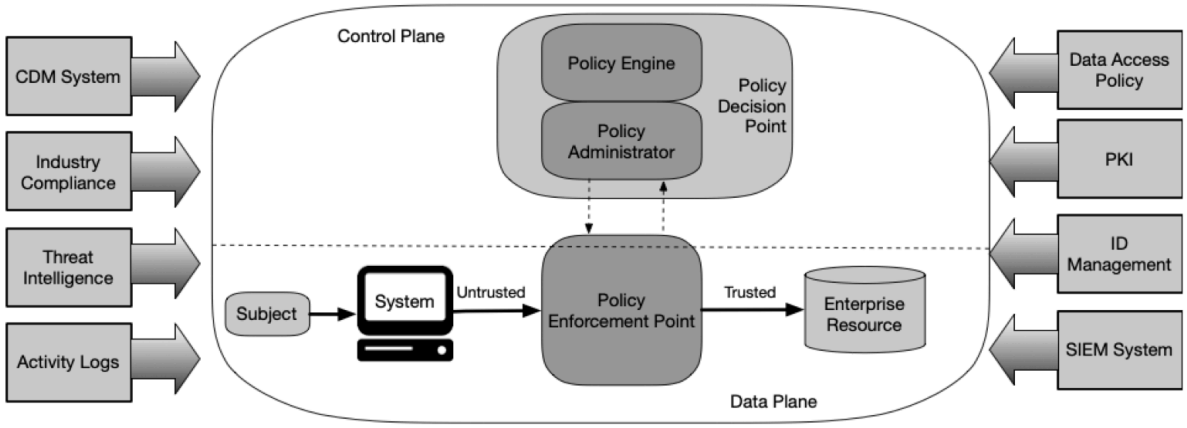
El diseño no experimental y transeccional limita las inferencias causales y reconoce la posibilidad de confusores (madurez organizacional, presupuesto, cambios en volumen transaccional) que puedan coexplicar parte de las mejoras observadas (Hernández Sampieri, 2014). La heterogeneidad en definiciones operativas e infraestructuras de medición puede introducir sesgos de medición y reporte, mitigados parcialmente por triangulación y normalización terminológica en la codificación (Hernández Sampieri, 2014). La validez externa se circunscribe a entidades financieras con operación digital intensiva en el período 2015–2025, (Verizon, 2024) por lo que la extrapolación a otros sectores requiere cautela y replicación contextualizada.

5.6 Implicancias teóricas y prácticas

En el plano conceptual, los hallazgos fortalecen marcos que integran controles técnicos con gobierno y métricas, aportando evidencia aplicada para Zero Trust y gestión basada en riesgo como principios de diseño y operación (NIST, 2020a). En el plano práctico, se sugiere priorizar MFA total, correlación EDR/XDR con automatización de contención, SLAs orientados por KEV, segmentación + PAM/JIT y gobierno OAuth/anti-BEC, vinculando cada capacidad con métricas accionables para retroalimentar políticas, reglas y procesos (CISA, 2024a).

Figura 16

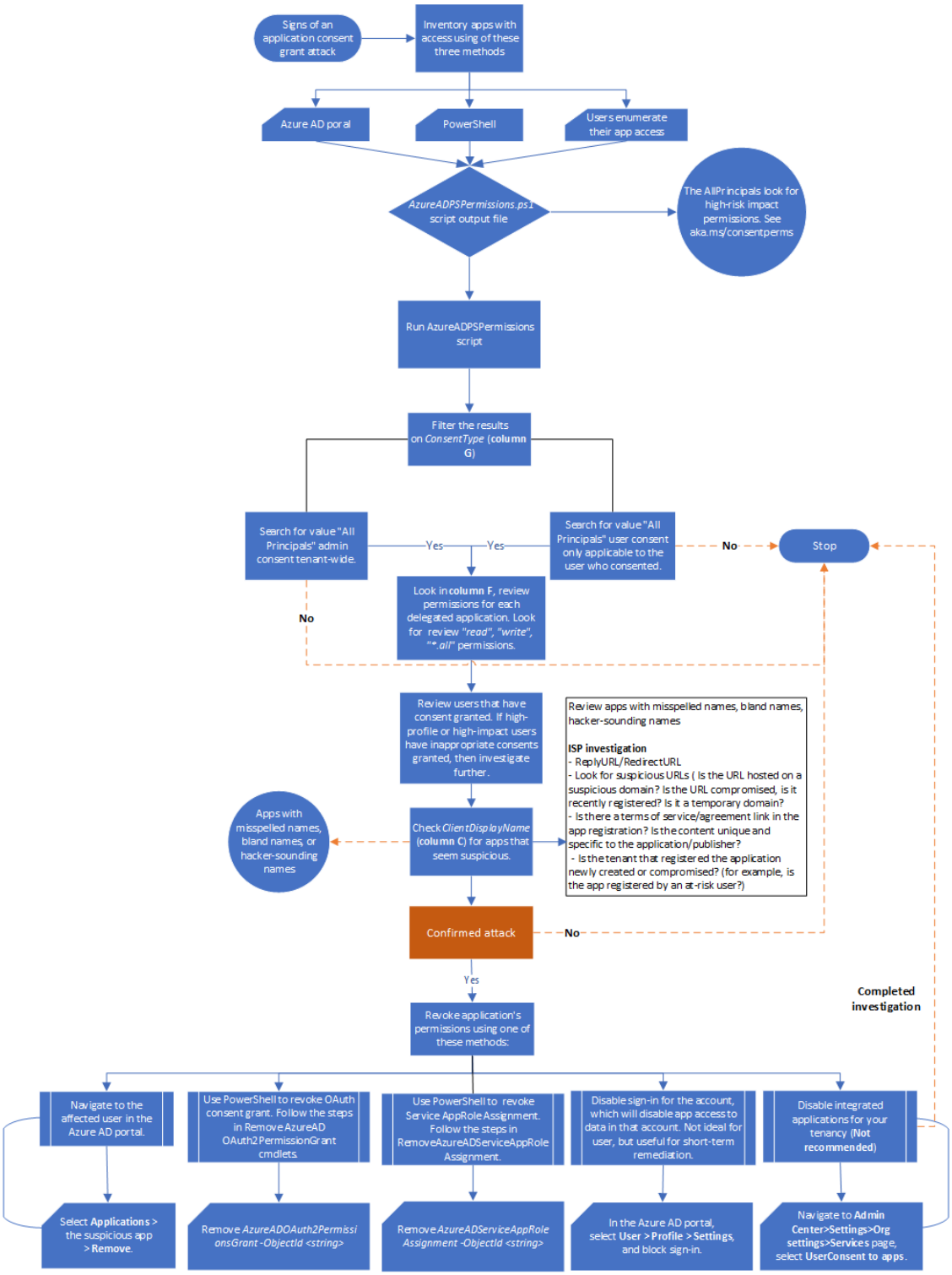
Esquema de arquitectura Zero Trust



Nota. Adaptado de NIST (NIST, 2020a)

Figura 17

Playbook de investigación de "app consent"



Nota. Adaptado de Microsoft. Flujo de investigación ante concesiones ilícitas de aplicaciones (OAuth) (Microsoft, 2025)

En síntesis, la evidencia analizada sugiere que la integración operativa de controles, más que su despliegue aislado, se asocia con mejoras en incidentes, tiempos operativos y exposición en el período estudiado, manteniendo la lectura observacional propia del diseño adoptado (Cloud, 2024). Esta discusión deja insumos para el Capítulo VI, donde se presentarán las conclusiones en relación con el objetivo general, los objetivos específicos y la hipótesis del estudio.

Conclusiones

Luego del análisis desarrollado, se observó un patrón consistente: las organizaciones financieras que integran capacidades técnicas con gobierno y medición tienden a presentar mejores resultados operacionales frente al fraude digital. En el período 2015–2025, la lectura transversal de casos e indicadores comparables (incidentes por 100.000 cuentas activas, MTTD, MTTR y proporción de credenciales comprometidas) muestra que la protección mejora cuando la identidad, la detección y la gestión de exposición se administran como un sistema coordinado y no como controles aislados.

Los hallazgos orientan un cambio de enfoque: pasar de "sumar herramientas" a construir un programa integrado. En identidad, la MFA exigida y medida redujo accesos no autorizados cuando cubrió puntos críticos y cuentas privilegiadas; en operación, la correlación EDR/XDR con runbooks y aislamiento automático se asoció con caídas de MTTD/MTTR; en exposición, los SLAs de vulnerabilidades guiados por explotación activa y un inventario confiable acortaron ventanas en servicios orientados a internet; en contención, la segmentación y el PAM/JIT limitaron el movimiento lateral. El desempeño no depende solo de la tecnología, sino de su orquestación con procesos, roles y métricas.

Los casos también evidencian que las mejoras son desparejas cuando las implementaciones quedan parciales o fragmentadas. La cobertura incompleta de MFA, la subcobertura de agentes XDR o la falta de telemetría en dominios críticos degradan resultados; del mismo modo, los entornos con BEC y consentimientos OAuth sin políticas de bloqueo de reenvío, verificación de editor o revocación automatizada presentan mayor persistencia del adversario. Cuando estos vacíos se cierran y las acciones de respuesta se ejecutan con criterios de severidad y trazabilidad auditable, los indicadores muestran una mejora observable.

La gestión de terceros emerge como un condicionante decisivo. Donde se incorporaron requisitos verificables en contratos, controles de acceso remoto, monitoreo continuo y protección de marca (con rutas de takedown), la exposición a suplantaciones y vectores de borde se redujo de forma apreciable. Este punto es especialmente sensible en ecosistemas altamente tercerizados, donde la cadena de suministro digital traslada riesgos operativos y reputacionales que deben ser gestionados como parte del modelo de control.

En términos de adopción, la evidencia sugiere priorizar una hoja de ruta dual: logros rápidos —MFA total, aislamiento automático, bloqueo de reenvíos externos, revocación de consentimientos ilícitos— junto con iniciativas estructurales —telemetría unificada endpoint–

identidad–red, segmentación de dominios críticos, SLAs guiados por KEV, PAM/JIT—, todas enlazadas a métricas accionables (incidentes por 100.000, MTTD, MTTR, % de credenciales comprometidas y tiempos de exposición) que habiliten ciclos de mejora continua.

Cabe subrayar que estas conclusiones se formulan en clave observacional: el diseño no experimental adoptado no atribuye causalidad, pero la convergencia entre casos, métricas y prácticas refuerza la plausibilidad de las asociaciones halladas en el contexto del sistema financiero argentino. Este trabajo aporta definiciones operativas, una matriz de evidencias y una priorización práctica que orientan decisiones de corto y mediano plazo; futuras ampliaciones con datos primarios y diseños cuasi-experimentales podrán estimar tamaños de efecto y extender la validez a otros dominios.

La resiliencia no se logra por la suma de tecnologías, sino por la integración de capacidades bajo gobierno efectivo y medición consistente. Ese es el rasgo que diferencia a las organizaciones que aprenden y mejoran sus indicadores de aquellas que, aun invirtiendo, permanecen atrapadas en soluciones reactivas y beneficios efímeros. Este estudio deja una base aplicable para continuar el fortalecimiento operativo del sector financiero en Argentina.

Líneas Futuras de Investigación

A partir de los hallazgos, se abre una agenda que prioriza evidencia operativa y métricas comparables. Un primer eje consiste en evaluar el aporte de la IA generativa y el aprendizaje automático en la detección y contención de campañas hiperpersonalizadas (phishing con deepfakes, consent phishing, BEC). El foco debería estar en modelos robustos a ataques adversariales, entrenados con telemetría real (endpoint–identidad–red), y en su efecto observable sobre indicadores como MTTD, MTTR y proporción de credenciales comprometidas. Diseños recomendados: series temporales interrumpidas o paneles longitudinales que comparen periodos pre/post despliegue, con seguimiento de calidad de datos y cobertura de agentes para reducir sesgos.

Un segundo eje es la gestión de riesgo de terceros (TPRM) en cadenas de suministro digitales. Resulta pertinente medir cómo cláusulas verificables, monitoreo continuo y protección de marca modifican la exposición efectiva a suplantaciones y vectores de borde. Se sugiere construir un índice de madurez TPRM (p. ej., % de proveedores críticos auditados/año, lead time de revocación de accesos, cierre de hallazgos por trimestre) y relacionarlo con incidentes/100.000 y tiempos de respuesta. Diseños cuasi-experimentales por cohortes de proveedores o emparejamiento por puntaje de propensión entre organizaciones con y sin monitoreo continuo.

En paralelo, conviene estudiar la escalabilidad de Zero Trust en infraestructuras heterogéneas y presupuestos restringidos (pymes del sector financiero y adjacentes). El análisis debería estimar el costo-efectividad de combinaciones mínimas viables (MFA total + segmentación del plano de administración + PAM/JIT + EDR/XDR básico) y su relación con ventana de exposición (parches guiados por KEV) y movimiento lateral. Se propone un marco de “cestas de control” comparables, con curvas de adopción y brechas de cobertura como variables mediadoras.

Una línea complementaria es el impacto regulatorio sobre la adopción de controles en sectores no financieros con criticidad alta (salud, educación, servicios públicos). Aquí importan tiempos de cumplimiento, desviaciones estándar de MTTD/MTTR por tamaño de organización y diferencias en diferencias ante cambios normativos. El objetivo es identificar qué requisitos habilitan mejoras operativas y cuáles generan carga sin retorno medible, para retroalimentar políticas basadas en evidencia.

También se recomienda investigar integraciones basadas en API para detección y orquestación en tiempo real (revocación de tokens, aislamiento automático, bloqueo de

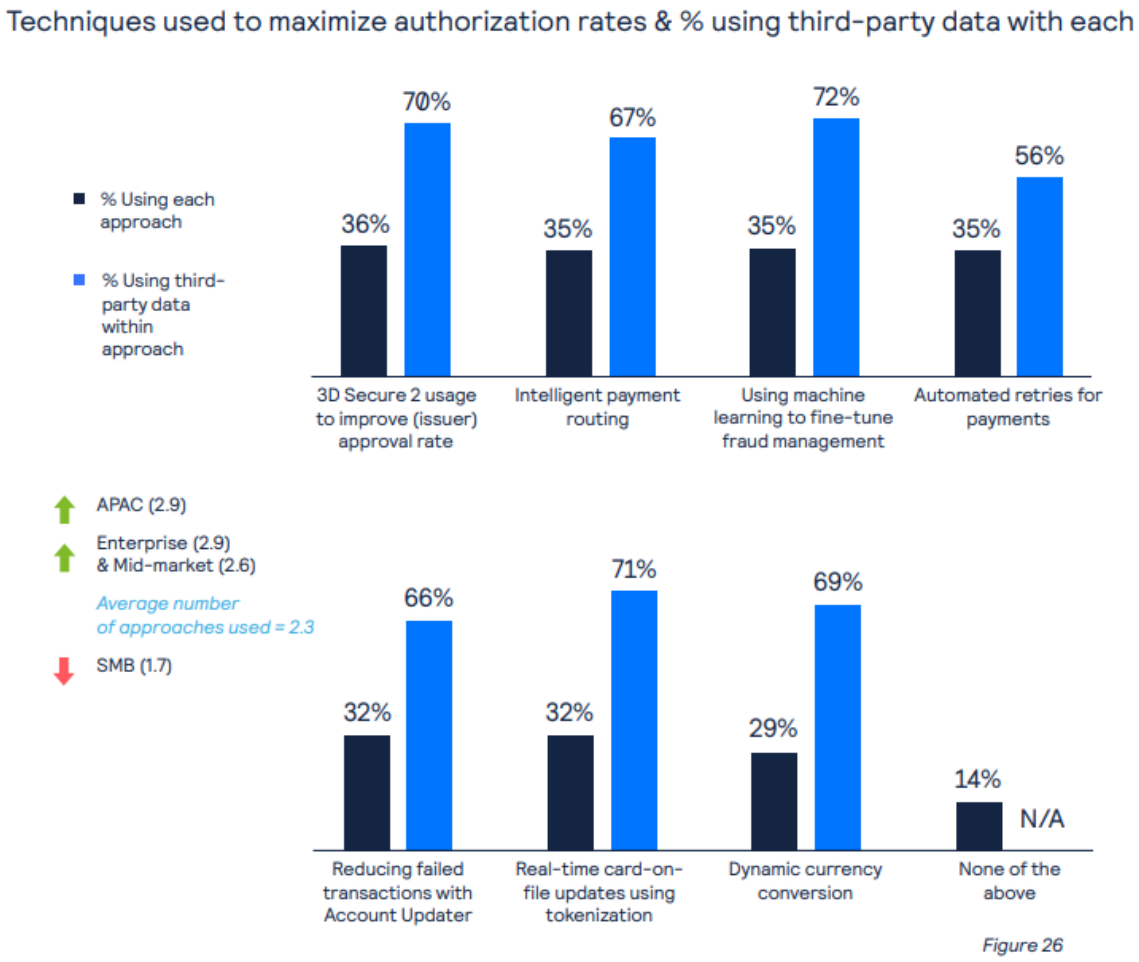
reenvíos externos), priorizando su tasa de falsos positivos, el tiempo a la acción y el impacto acumulado sobre incidentes. Un tablero de referencia podría incluir: cobertura MFA, cobertura de agentes EDR, latencia de parcheo KEV, % de sesiones privilegiadas JIT, MTTD/MTTR y incidentes/100.000; con glosario operativo y taxonomía de eventos para asegurar comparabilidad inter-institucional.

Finalmente, para fortalecer inferencias, se sugiere avanzar hacia diseños mixtos: recolección de datos primarios (encuestas breves a SOC/IT, entrevistas a dueños de proceso) combinados con registros operativos (SIEM/XDR, IAM, CMDB, ticketing). La publicación de conjuntos de datos anonimizados, código de limpieza y un codebook común facilitará replicaciones y meta-análisis regionales, elevando la calidad de la evidencia y la transferibilidad de resultados.

Anexos

Figura 18

Técnicas para disminuir el fraude



Nota. Adaptado de Cybersource (Cybersource, 2021b)

Figura 19

Cómo evitar el fraude online



Nota. Adaptado de Instantcredit (instantcredit, 2017)

Figura 20

BBVA cómo evitar fraude



Nota. Adaptado de BBVA (BBVA, 2022)

Figura 21

Evitar estafas, Gobierno Mendoza



Nota. Adaptado de Diario San Rafael (Diario San Rafael, 2022)

Acrónimos

BCRA	Banco Central de la República Argentina
BPS	Puntos base
CEO	Director ejecutivo
DNI	Documento Nacional de Identidad
IA	Inteligencia Artificial
INDEC	Instituto Nacional de Estadística y Censos
IoT	Internet de las Cosas (Internet of Things)
MFA	Autenticación Multifactor
MTTD	Tiempo Medio de Detección (Mean Time to Detect)
MTTR	Tiempo Medio de Respuesta (Mean Time to Respond)
OMS	Organización Mundial de la Salud
RAE	Real Academia Española
SIEM	Gestión de Información y Eventos de Seguridad (Security Information and Event Management)
SMS	Servicio de Mensajes Cortos
UNIVAC	Computadora Automática Universal
VPN	Red Privada Virtual (Virtual Private Network)
XDR	Detección y Respuesta Extendida (Extended Detection and Response)

Referencias

Argentina Cibersegura. (2024). *Delitos informáticos.* https://www.argentinacibersegura.org/materiales

Argentina Cibersegura. (2025). *¿Cómo realizar una denuncia ante un delito informático?* https://www.argentinacibersegura.org/pdf/denuncia-delito-informatico.pdf

Avast. (2019). *How to remove ransomware*. https://www.avast.com/es-es/c-how-to-remove-ransomware-pc

Banco privado. (2023). datos no publicados

BBVA. (2022). https://www.archyde.com/bbva-alerts-of-fraud-through-text-messages/

BCRA. (2020). Smishing: https://www.bcra.gob.ar/Noticias/proteccion-de-datos-personales-smishing.asp

BCRA. (2023). Detección de perfiles falsos en redes sociales.: https://www.bcra.gob.ar/

BCRA. (2023). *Normas mínimas sobre gestión de riesgos de tecnología y seguridad de la información.* https://www.bcra.gob.ar

Brooks, R., Butler, J., & Fitzgerald, B. (2020). The psychological impact of the COVID-19 pandemic.

Camacho Nieto, N. A. (2016). *Una breve mirada a la ingeniería social.* http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2712/Trabajo%20de%20grado3383.pdf?sequence=1&isAllowed=y

CERT-Colombia. (2023). *Informe de ciberseguridad.* https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-ransomware-contra-ifx-networks#:~:text=IFX%20Networks%20anunció%20en%20un,como%20Colombia%2C%20Chile%20y%20Panamá.

Check Point. (2020). COVID-19 spam and phishing trends: https://www.checkpoint.com/cyber-hub/threat-intelligence/covid-19-cyber-threats/

CISA. (2023). *#StopRansomware: ALPHV Blackcat.* https://www.cisa.gov/news-events/alerts/2023/12/19/cisa-and-fbi-release-advisory-alphv-blackcat-affiliates

CISA. (2024a). *Known Exploited Vulnerabilities (KEV) Catalog. U.S. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CISA. (2024b). *The KEV Catalog.* https://www.cisa.gov/resources-tools/resources/kev-catalog

Cloud, G. (2024). *M-Trends 2024: Our View from the Frontlines.* https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024

Cybersource. (2021b). *Global fraud report.* https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2021.pdf

Cybersource. (2023). *Global fraud report 2023*. https://www.cybersource.com/en-us/solutions/fraud-management/global-fraud-report.html

Diario San Rafael. (2022). https://diariosanrafael.com.ar/seguridad-advierte-los-peligros-de-pactar-transacciones-por-las-redes-sociales/

ENISA. (2022). *Ransomware.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

ENISA. (2023). Threat landscape 2023: Multi-factor authentication impact report.: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2024). *THREAT LANDSCAPE*. https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

Europa, C. d. (2001). *Convenio sobre la ciberdelincuencia (Convenio de Budapest).* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA).* https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

FBI. (2020). Twitter hack investigation report.: https://www.fbi.gov/

FIRST. (2019). *Common Vulnerability Scoring System version 3.1: Specification Document.* https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Gartner. (2023). Impact of 5G and IoT on cybersecurity: https://www.gartner.com/peer-community/post/rapid-expansion-internet-things-iot-increasing-reliance-various-wireless-technologies-such-5g-bluetooth-wifi-6-wifi-halow

Gartner. (2023). *Top Cybersecurity Trends 2023.* https://www.gartner.com

Gartner. (2024). SIEM adoption trends in remote work security.: https://www.gartner.com/

Goodfellow, I., Bengio, Y., & Courville, A. (2020). Deep learning and generative AI in cybersecurity threats.

Hernández Sampieri, R. F. (2014). *Metodología de la investigación (6 ed.).* McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. HSBC.

IBM Security. (2023). *Cost of a Data Breach Report.* https://www.ibm.com

INDEC. (2025). https://www.indec.gob.ar/uploads/informesdeprensa/internet_09_2572133D99B6.pdf

instantcredit. (2017). *Como evitar el fraude en ecommerce.* https://www.instantcredit.net/como-prevenir-el-fraude-en-una-tienda-online/

ISO. (2022). *ISO/IEC 27002:2022* . https://www.iso.org/standard/75652.html

JIT, M. (2024). *Privileged access: Strategy* . https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy

Kaspersky. (2023). Security bulletin 2023.: https://www.kaspersky.com/about/security-bulletin

Mandiant. (2023). *M-Trends 2023: Special Report.* https://services.google.com/fh/files/misc/m_trends_2023_report.pdf

Mandiant. (2024). *M-Trends 2024: Our View from the Frontlines.* https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024

McAfee. (2025). Qué es un malware: https://www.mcafee.com/es-ar/antivirus/malware.html

Microsoft. (2017). WannaCry ransomware attack analysis.: https://www.microsoft.com/security/blog/2017/05/12/wannacry-ransomware-attack/

Microsoft. (2024). *Accelerate incident investigation and response with generative AI.* https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel

Microsoft. (2025). *App consent grant—Investigation playbook. Microsoft Learn—Security Operations.* https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-app-consent

NIST. (2020a). *SP 800-207: Zero Trust Architecture.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NIST. (2020b). *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2022). *Supply chain.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST. (2023). *Artificial Intelligence Risk Management.* https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

NIST. (2024a). *Security and Privacy Controls for Information Systems and Organizations.* https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST. (2024b). *The NIST Cybersecurity Framework.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST. (2025). *NIST SP 800-61 Rev. 3.* https://csrc.nist.gov/pubs/sp/800/61/r3/final

Pais, E. (2014). *Los mejores mensajes de spam*. https://verne.elpais.com/verne/2014/12/09/articulo/1418141248_736053.html

Parsons, K. B. (2019). *Predicting susceptibility to social influence in phishing emails. Human Factors.* https://www.researchgate.net/publication/331188440_Predicting_Susceptibility_to_Social_Influence_in_Phishing_Emails

PC Risk. (2024). *Phishing*. https://www.pcrisk.es/guias-de-desinfeccion/12934-google-drive-email-scam

Pew Research Center. (2023). Digital overload and user behavior.: https://www.pewresearch.org/

Ramirez, O. M. (2025). *Ciberfraude: Principales Métodos de Ataque y Estrategias para su Prevención.* https://doi.org/10.37811/cl_rcm.v9i3.18122

scielo. (2021). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2307-21132020000400004

Shackleford, D. (2022). *The Journey to Operational Security Effectiveness and Maturity.* https://www.sans.org/webcasts/the-journey-to-operational-security-effectiveness-and-maturity-frameworks-tools-and-techniques

Smishing. (2023). Estafas más comunes en Mercado Libre y Mercado Pago: https://www.welivesecurity.com/es/estafas-enganos/estafas-comunes-mercado-libre-mercado-pago/

social, I. (2015). *Ingenieria Social*. https://nomeloexplicaron.wordpress.com/2015/04/16/ingenieria-social-2/

Statista. (2024). Uso de banca móvil y tendencias digitales en Argentina.: https://www.statista.com/

techtarget. (2020). FBI and CISA issue vishing campaign warning : https://www.techtarget.com/searchsecurity/news/252488039/FBI-and-CISA-issue-vishing-campaign-warning

Tellows. (2020). https://blog.tellows.es/2020/01/smishing/.

UE. (2024). *NIS2.* https://www-nis--2--directive-com.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Unit 42. (2020). COVID-19-related domain registrations and phishing analysis: https://unit42.paloaltonetworks.com/

unit42. (2020). unit42: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

UNODC. (2023). *Manual sobre delitos cibernéticos. Naciones Unidas.* https://www.unodc.org

Verizon. (2024). *Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf