CRONOLOGÍA

Impacto de las nuevas tecnologías en la ciberseguridad

The impact of new technologies on cybersecurity

M. Sc. Reniel Carvajal Alfonso[*], M. Sc. Dianelys Alvarez González[2]

Recibido: 11/2025| Aceptado: 11/2025| | Publicado: 12/2025

Resumen

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) ha posibilitado, junto al avance de las redes de comunicaciones 5G y 6G, la evolución del mercado de las *Fintech*. Dicho mercado facilita el intercambio de información, pero, a su vez, ha propiciado que ciberdelincuentes roben a los gobiernos y a los TELCOS información sensible con el objetivo de causar la inoperancia de estos y obtener, por medio de chantaje, financiamientos. Esta investigación analiza el creciente impacto de la ciberseguridad en el sector de las telecomunicaciones. El estudio describe amenazas específicas como los ataques de denegación de servicio distribuidos (DDoS), los troyanos bancarios, las vulnerabilidades *zero-day* y *malware* impulsado por inteligencia artificial. Como resultado se evidencia el impacto de las nuevas tecnologías como IA, Internet de las Cosas (IoT) y el comercio electrónico han incrementado la vulnerabilidad, así como la interrelación entre los organismos reguladores, empresas, gobiernos a través de marcos regulatorios y la capacitación constante de los usuarios como elemento crucial para hacer frente a estas amenazas.

[*] Empresa de Telecomunicaciones de Cuba S.A., ETECSA. La Habana 11300. Cuba. reniel.carvajal@etecsa.cu

[2] Empresa de Telecomunicaciones de Cuba S.A., ETECSA. La Habana 11300. Cuba. dianelys.alvarez@etecsa.cu

Palabras clave: inteligencia artificial, ciberataques, TELCOS, ciberseguridad, ciberdelincuentes

Abstract

Advances in Information and Communication Technologies (ICT) together with those of 5G and 6G communications networks have facilitated the exchange of information and enabled the evolution of the Fintech market. However, cybercriminals have also targeted these technologies with the firm determination to render TELCOs and governments inoperative and obtain financial gain through blackmails and the theft of sensitive information as a result of these cyberattacks. This study focuses on analyzing the increasing impact of cybersecurity on telecommunications industry. Threats such as Distributed Denial of Service (DDoS) attacks, banking Trojans, zero-day vulnerabilities, and AI-driven malware are described. As a result, it is clear that new technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and e-commerce have increased vulnerability and the interrelation between regulatory bodies, companies, and governments. This is evident through regulatory frameworks and the constant training of users, which are crucial elements in addressing these threats.

Keywords: *Artificial Intelligence, cyberattacks, TELCOs, cybersecurity, cybercriminals*

Introducción

La ciberseguridad emerge como una disciplina esencial, derivada del avance en infraestructura de red, *hardware*, *software* y del incremento en la interconexión y digitalización de servicios estratégicos como la Bancarización y las soluciones *Fintech*. Si bien estos procesos generan beneficios significativos, también exponen a las organizaciones a un creciente riesgo y las convierten en blancos potenciales de ataques maliciosos. El objetivo de tales ataques es el robo de información, el daño de activos digitales o la interrupción de la continuidad operativa, con el fin último de generar desestabilización, pérdidas económicas y deterioro de la confianza de los clientes.

La Oficina de las Naciones Unidas contra las Drogas y el Delito considera que la ciberdelincuencia es un concepto muy complejo

que engloba una variedad de actividades ilícitas. En este sentido, precisa que la *ciberdelincuencia* es un acto que infringe la ley y que se comete usando las TIC para atacar las redes, sistemas, datos, sitios web, entre otros (Ministerio de Relaciones Exteriores de Cuba, 2021). Varios autores defienden el ciberdelito, teniendo en cuenta lo anterior, como aquel delito que se comete mediante las Tecnología de la Información y las Comunicación (TIC), contra individuos, empresas o gobiernos. Por lo tanto, el ciberdelito constituye una acción antijurídica que está contemplada en el derecho penal (Benito, 2023).

De acuerdo a los expertos de la Asociación de Auditoría y Control de Sistemas de Información (ISACA), la ciberseguridad se define como una capa de protección para los archivos de información. También, para referirse a la ciberseguridad se utiliza el término seguridad informática o seguridad de la información electrónica (Infosecurity Mexico, 2025).

Es un hecho que la expansión de la conectividad conlleva una necesidad urgente de proteger no solo los datos personales de los usuarios, sino también la infraestructura crítica de las empresas. En este contexto, resulta imprescindible fomentar la interoperabilidad entre operadores de telecomunicaciones (TELCOS), agencias reguladoras y gobiernos. El objetivo es implementar estrategias conjuntas que permitan prevenir, detectar y mitigar ciberamenazas. Asimismo, es esencial fortalecer las capacidades institucionales y ciudadanas mediante la formación continua, esta medida garantiza una protección integral frente a los riesgos emergentes del entorno digital.

Materiales y métodos

Esta investigación adopta un enfoque metodológico de carácter mixto con preponderancia cualitativa. Se emplearon los métodos **inductivo-deductivo** y **analítico-sintético** para el examen de la información. La técnica de análisis documental fue fundamental para la selección y evaluación crítica de las fuentes bibliográficas, lo que permitió una profundización sistemática en el tema de estudio.

Panorama de la Ciberseguridad a nivel global

Según el Fondo Monetario Internacional (FMI) estima que la ciberdelincuencia costará a nivel global 23 billones de dólares para el año 2027. En la región de Latinoamérica se ha experimentado un aumento de 108 % de ciberataques a operadores de telecomunicaciones, respecto al año anterior, con más de 2,600 incidentes semanales por organización. México, Colombia y Brasil encabezan los reportes en volumen y sofisticación de amenazas. El costo promedio de violación de datos de 4,88 millones de dólares en 2024. Ese mismo año, el *ransomware* se consolidó como la principal amenaza, tanto a nivel global como en Latinoamérica y el Caribe, al representar un 38 % del total de todas las ciberamenazas registradas. Los principales sectores de ataque de esta amenaza se centraron en comercio mayorista y servicios, salud y construcción. Los principales *ransomware* con mayor impacto en el área de Latinoamérica fueron RansomHub, LockBit y Akira. En la Figura 1. se muestra un resumen del impacto global de esta amenaza.

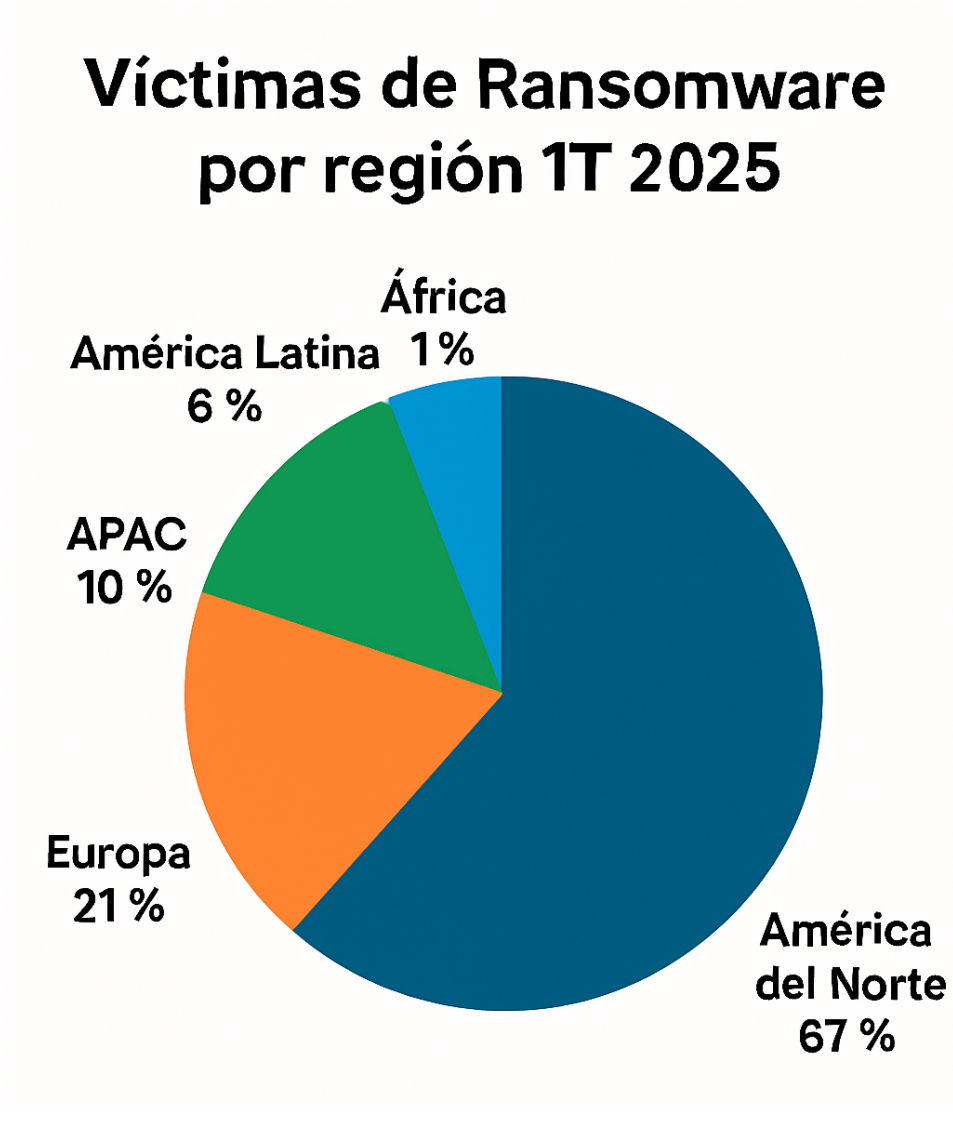

Figura 1. Víctimas de *ransomware* a nivel global. Fuente: Check Point, 2025

El espectro de las amenazas se ha expandido de forma considerable y sus operaciones se orientan hacia objetivos de alto impacto, como gobiernos, infraestructuras críticas y corporaciones de alto valor estratégico. El principal vector de ataque contra estos sectores

lo constituyen los grupos de Amenaza Persistente Avanzada (APT). Estas entidades suelen ser patrocinadas por Estados nación o por organizaciones criminales sofisticadas. Se especializan en ejecutar campañas de intrusión dirigidas y de larga duración, diseñadas para causar un impacto estratégico máximo. A diferencia de los cibercriminales convencionales, los grupos APT operan con un enfoque de largo plazo. Un ejemplo paradigmático de este tipo de grupos es Lazarus, una APT patrocinada por el estado de Corea del Norte. Atribuido a la Oficina General de Reconocimiento (OGR) (el principal órgano de inteligencia y operaciones especiales del país), el grupo es reconocido a nivel internacional por la magnitud y el impacto global de sus campañas de ciberataque. Se especializa en espionaje militar, operaciones clandestinas y actividades cibernéticas ofensivas.

En el año 2024 en el mundo se han producido ataques significativos de APT tales como:

• MirrorFace (Origen: Japón; alcance: Japón y Unión Europea), utiliza la herramienta HiddenFace. Emplea su línea de ataque a través de un correo electrónico de spear phishing donde MirrorFace incluye un enlace a un archivo ZIP. Dentro, con un LNK disfrazado como un documento de Word que una vez abierto, muestra un documento señuelo y ejecuta la versión 5.5.5 del *backdoor* ANEL.

• Gamaredon (Origen: Rusia, alcance: Ucrania, OTAN), emplea las herramientas: PteroGraphin, PteroPSDoor, PteroSig, su estrategia de ataque se basa en la realización de modificaciones a uno de sus *backdoors* escritos en PowerShell, conocido como PteroPSDoor. Estas mejoras incluyeron la incorporación de múltiples capas de ofuscación y el almacenamiento de componentes clave en el registro de Windows©, lo que aumentó de manera significativa su capacidad de operar de forma encubierta.

La «transformación digital» es el proceso mediante el cual las organizaciones utilizan tecnologías digitales para transformar de manera fundamental su forma de operar y de ofrecer valor a los clientes. Se trata de adoptar nuevas herramientas y métodos que puedan mejorar la eficiencia, optimizar la experiencia del cliente y crear nuevos modelos

de negocios. En conjunto con ello, se pueden mencionar desafíos, dentro de los cuales destaca la ciberseguridad. Las empresas, para lograr sortear esta amenaza, se deben apoyar en una plantilla detallada de informes de incidentes TI para garantizar una documentación exhaustiva y una respuesta rápida ante posibles brechas de seguridad.

Ataques ocurridos a sectores claves

• **Ataque de *ransomware* de la Corporación de Defensa Nacional: Fecha:** marzo de 2025, **Impacto:** 4,2 TB de datos confidenciales vulnerados. El grupo de Ransomware Interlock atacó a la National Defense Corporation (NDC) y a su filial AMTEC en marzo, exfiltrando 4,2 *terabytes* de datos que luego se filtraron en la *dark web*. **Aprendizaje clave:** Este incidente resalta la importancia de garantizar, el cumplimiento de las normas, de toda la cadena de suministro, incluidos proveedores internos y externos, además de los estándares de seguridad.

• **Ciberataque a WestJet: Fecha:** junio de 2025, **Impacto:** Interrupciones intermitentes en el sitio web y la aplicación móvil. En junio, la aerolínea canadiense WestJet reveló un incidente de ciberseguridad que interrumpió el acceso a su sitio web y aplicación móvil. **Aprendizaje clave:** Las organizaciones deben adoptar una defensa multicapa que incluya capacitación periódica en seguridad, especialmente en tácticas de ingeniería social. Capacitar a los empleados, especialmente a los equipos de TI y soporte, para que reconozcan los intentos de suplantación de identidad puede evitar que los atacantes se afiancen.

Tendencias de ataques cibernéticos

Los ataques cibernéticos se basan en el secuestro de datos. Hospitales, pequeñas y medianas empresas han sido las principales víctimas. A continuación, se relacionan una serie de ciberamenazas que, a nivel mundial se han evidenciado contra diferentes sectores y se prevé su aumento en los próximos años.

• **El ataque de denegación de servicio o DDoS:** consiste en provocar la caída de un servidor al sobrecargar su ancho de banda. Estas acciones fuerzan la interrupción de un sitio web. En el caso

del sistema financiero, los DDoS se utilizan para inundar con una gran cantidad de tráfico los servicios en línea de los bancos y de las plataformas de *trading*. De esa manera, el servidor colapsa y deja de funcionar.

• **Los troyanos bancarios:** otro *software* malicioso que en principio parecen inofensivos, sin embargo, no lo son y están tras los bancos. Los troyanos pueden instalarse en cualquier dispositivo por visitar un sitio web infectado, por descargar el anexo de un *email*, o incluso, por bajar una aplicación. Una vez este virus se instale en el celular detecta en qué momento se utilizan los servicios en línea de un banco y así capturar los datos personales y bancarios.

• **Vulnerabilidades *zero-day*:** los atacantes buscan fallos desconocidos en programas, dispositivos IoT o servicios *Cloud*. Estas brechas permiten el acceso a datos antes de que los desarrolladores tengan oportunidad de corregirlas.

• ***Malware* impulsado por IA:** la generación de código mediante inteligencia artificial (IA) ha democratizado y acelerado de manera significativa el desarrollo de *malware*. Los atacantes pueden generar, refinar y ofuscar variantes de *software* malicioso con una eficiencia sin precedentes, lo que facilita la evasión de mecanismos de detección basados en firmas y heurísticos.

• **Explotación de las API inseguras:** las interfaces de programación de aplicaciones (API) mal configuradas o sin la debida protección suponen una ventana para extraer datos, ya que muchas empresas se apoyan en servicios de terceros con controles de seguridad débiles.

• **Dispositivos IoT como puerta de entrada:** se pueden utilizar sensores, cámaras, periféricos y otros dispositivos conectados a la red corporativa como vectores de ataque para acceder a sistemas internos y extraer datos.

Blockchain, nube, teletrabajo

Blockchain

Las Tecnologías como *blockchain* aparecen como soluciones para mejorar la seguridad de datos y la confianza. Los ciberataques

dirigidos a la nube, *hardware* y sistemas de aprendizaje automático pueden crear brechas complejas, lo que dificulta a las empresas proteger sus datos. La tecnología *blockchain*, con sus libros digitales transparentes e inmutables, ofrece soluciones innovadoras para la ciberseguridad.

Las auditorías *blockchain* pueden abordar varios ataques y vulnerabilidades en contratos inteligentes. Para la gestión de respuesta a amenazas, *blockchain* permite la automatización y descentralización, lo que posibilita una rápida identificación, contención y mitigación de amenazas sin comprometer la seguridad de datos. Los contratos inteligentes pueden responder a ciberataques aislando las amenazas de forma automática y rápida. Desde la perspectiva de la ciberseguridad, la tecnología *blockchain* introduce avances transformadores: fortalece la resiliencia operativa, robustece los modelos de control de acceso y garantiza la integridad de los datos. Su arquitectura descentralizada mitiga el impacto de los ataques DDoS al eliminar puntos únicos de fallo, que dificulta de forma significativa la interrupción de servicios.

Al mismo tiempo, los principios de confianza cero (*Zero Trust*) se ven potenciados mediante mecanismos nativos de verificación de identidad y control de acceso granular, lo que reduce los riesgos de accesos no autorizados y amenazas internas. Además, el almacenamiento descentralizado de archivos (basado en la distribución de fragmentos cifrados a través de múltiples nodos) minimiza la exposición ante brechas de datos, mientras que la inherente inmutabilidad y replicación de la red aseguran la disponibilidad e integridad continua de la información, incluso durante incidentes de seguridad.

Nube

La seguridad en la nube es una disciplina de la ciberseguridad dedicada a asegurar los sistemas informáticos en la nube. Incluye mantener los datos privados y seguros a través de la infraestructura, las aplicaciones y las plataformas en línea. En su núcleo, la seguridad en la nube se compone de las siguientes categorías:

- Seguridad de los datos.
- Gestión de identidades y accesos (IAM).

- Gobernanza (políticas de prevención, detección y mitigación de amenazas).
- Planificación de la retención de datos (DR) y la continuidad del negocio (BC).
- Cumplimiento legal.

La seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos, las aplicaciones que se ejecutan y los datos almacenados en ella. La seguridad de los servicios comienza por comprender qué se está asegurando con exactitud, así como los aspectos del sistema que se deben administrar. El alcance total de la seguridad en la nube está diseñado para proteger lo siguiente:

- **Redes físicas:** enrutadores, energía eléctrica, cableado, controles de clima.
- **Almacenamiento de datos:** discos duros.
- **Servidores de datos:** *hardware* y *software* informáticos de la red central.
- **Plataformas de virtualización de equipos informáticos:** *software* de máquinas virtuales, máquinas anfitrionas y máquinas invitadas.
- **Sistemas operativos (OS):** *software* que soporta todas las funciones informáticas.
- **Middleware:** gestión de la interfaz de programación de aplicaciones (API).
- **Entornos de ejecución:** ejecución y mantenimiento de un programa en ejecución.
- **Datos:** toda la información almacenada, modificada y a la que se ha accedido.
- **Aplicaciones:** servicios tradicionales de *software* (correo electrónico, *software* de impuestos, paquetes de productividad.)
- ***Hardware* de usuario final:** ordenadores, dispositivos móviles, dispositivos de IoT.

Teletrabajo

El teletrabajo se consolidó como un pilar fundamental para la continuidad del negocio durante la pandemia, esto permitió

la operación de innumerables organizaciones. Sin embargo, esta modalidad ha expandido de forma crítica la superficie de ataque, transformando el acceso remoto de los empleados en un vector de amenaza frecuentemente explotado por actores maliciosos. Para enfrentar este panorama de riesgo, es imperativo la adopción inmediata de un conjunto de buenas prácticas de seguridad diseñadas para robustecer las defensas y minimizar la exposición a ciberataques, estas se describen a continuación:

- **Definir una política de seguridad para el teletrabajo:** siendo estrictamente necesario crear una política que defina los protocolos, orden y plan de crisis para cada uno de los escenarios en los que pueda verse involucrado el usuario.
- **Emplear modelo *Zero Trust*:** basado en las directrices, soluciones y políticas de seguridad para proteger el entorno de trabajo corporativo.
- **Gestionar la administración de dispositivos:** trabajar con un entorno de gestión basado en la Nube y aplicar las políticas adecuadas para su acceso.
- **Emplear una autenticación multifactorial (MFA):** contar con una base de identidad sólida que permite que los usuarios puedan acceder de forma segura a los recursos y aplicaciones allí donde quiera que se encuentren.
- **Trabajar en un entorno seguro:** acceder a recursos como servidores o conectarse los recursos de la empresa a través de VPN.
- **Implementar soluciones de seguridad integrada en la nube:** conectar todas las soluciones de identidad, aplicaciones y datos en un único ecosistema.
- **Realizar test de seguridad periódicos:** es necesario realizar periódicamente auditorías de seguridad.
- **Realizar copias de seguridad de manera automatizada:** realizar el *Backups* como medida de prevención y seguridad de la información para garantizar la continuidad ante cualquier incidencia que pueda afectar los sistemas.

Ciberseguridad en las redes 5G y 6G

La actual red 5G y su evolución hacia la 6G permiten una mayor velocidad de conexión, una menor latencia y nuevas posibilidades de interconexión masiva entre dispositivos IoT, así como el desarrollo de hologramas interactivos en tiempo real e internet sensorial, todo ello potenciado por la inteligencia artificial. Sin embargo, estas ventajas tecnológicas evidentes conllevan riesgos de seguridad paralelos. Por ello, todos los sectores de la sociedad deben prepararse para alcanzar la resiliencia necesaria ante las ciberamenazas y los ataques contra sus sistemas informáticos.

Dentro de los riesgos que implican el despliegue de esta se pueden citar:

1. Mayor superficie de ataque: la tecnología 6G promete la conectividad de más dispositivos, lo que se traduce en un aumento de posibles vulnerabilidades a ciberataques.

2. Compromiso de privacidad: esta tecnología incluye ajustes de localización y seguimiento en tiempo real de mayor precisión y esto compromete la seguridad de los usuarios.

3. Ataques más avanzados: las redes 6G necesitan de herramientas de IA para fortalecerse, pero, como ocurre con estas herramientas que se utilizan en la actualidad, pueden ser de ayuda para los ciberdelincuentes para llevar a cabo ataques más difíciles de detectar por los usuarios.

4. Vulnerabilidad de los dispositivos IoT: al incluir en su alcance a una gran cantidad de nuevos dispositivos IoT, si estos no cuentan con medidas de protección adecuadas, pueden ser objeto de ciberataques con más facilidad.

Estrategias generales ante los ciberataques

Los TELCOS y las empresas deben implementar medidas claves de ciberseguridad para proteger sus operaciones y la confianza de los clientes. A continuación, se relacionan algunas recomendaciones importantes a tener en cuenta:

- **Implementar sistemas de detección y respuesta avanzada:** detectar amenazas a tiempo es clave para prevenir daños mayores.

Los sistemas de detección y respuesta avanzada identifican patrones inusuales en el tráfico de red y responden de forma rápida a posibles ataques. Estas herramientas, basadas en IA y aprendizaje automático, son útiles para detectar amenazas desconocidas.

• **Adoptar la autenticación multifactor:** las contraseñas solas no bastan para proteger el acceso a sistemas sensibles. La autenticación multifactor agrega una capa extra de seguridad, lo que asegura que solo personal autorizado acceda a información crítica, algo esencial en el contexto de acceso remoto cada vez más común.

• **Capacitar a los empleados en prácticas de seguridad:** los ataques de ingeniería social, como el *phishing*, se aprovechan de la falta de conocimientos del equipo para acceder a sistemas y datos. Capacitar al personal en reconocer correos sospechosos y proteger contraseñas es clave para prevenir brechas de seguridad.

• **Actualizar y parchear con regularidad todos los sistemas y dispositivos:** uno de los errores más comunes es no mantener los sistemas actualizados. Las actualizaciones de *software* incluyen parches que corrigen vulnerabilidades conocidas. Es clave que las empresas de telecomunicaciones establezcan un calendario de mantenimiento regular para reducir el riesgo de ataques.

• **Implementar políticas de acceso y permisos estrictos:** limitar el acceso a sistemas y datos según el rol es una buena práctica de ciberseguridad. Las empresas deben asegurar que solo personal autorizado acceda a información confidencial y ajustar permisos según las funciones de cada empleado.

• **Realizar auditorías y evaluaciones de seguridad periódicas:** la ciberseguridad evoluciona y las amenazas cambian. Las auditorías y evaluaciones ayudan a identificar vulnerabilidades y ajustar medidas de seguridad, además de verificar la efectividad de las políticas y herramientas implementadas. La ciberseguridad es esencial en telecomunicaciones. En un entorno donde la conectividad y el intercambio de datos son clave, proteger la información y la infraestructura mantiene la confianza de los clientes y asegura el cumplimiento regulatorio. Medidas robustas y atención a nuevas amenazas fortalecen a cualquier empresa en el mercado.

Impacto de la IA en la ciberseguridad

La IA se ha consolidado como una herramienta poderosa que los defensores utilizan para anticipar, detectar, remediar y mitigar incidentes de seguridad con mayor eficacia. No obstante, los ciberdelincuentes también la emplean para automatizar la búsqueda de vulnerabilidades, generar *phishing* de mayor sofisticación y crear *malware*.

La convergencia de las tecnologías de *Fintech*; IoT con redes más rápidas, como la 5G, permitirá un volumen de tráfico muy superior al actual. Por ello, es necesario proyectar y emplear estas nuevas capacidades para defender los sistemas de ciberataques. A continuación, se relacionan los elementos clave que se deben considerar para el uso de la IA en este contexto.

Ataques más inteligentes y difíciles de detectar

- ***Phishing* hiperrealista:** con IA un atacante puede analizar perfiles sociales, correos electrónicos, imágenes y el lenguaje utilizado por una víctima para construir mensajes fraudulentos casi indistinguibles de los legítimos.
- **Automatización del reconocimiento de vulnerabilidades:** antes un ciberdelincuente examinaba de forma manual sistemas para encontrar vulnerabilidades. Ahora, con IA, puede analizar miles de componentes a gran escala y en tiempo récord para identificar vulnerabilidades y debilidades.

Recomendaciones

- **Herramientas de seguridad con IA integrada:** adoptar soluciones basadas en aprendizaje automático y análisis de comportamiento para detectar amenazas en tiempo real.
- **Supervisión humana indispensable:** los analistas con conocimientos sólidos y experiencia en ciberseguridad interpretan los resultados de la IA, identifican falsos positivos y negativos y toman decisiones informadas. La IA no es infalible y el factor humano sigue siendo imprescindible.
- **Trabajar con *partners* tecnológicos especializados:** muchas empresas optan por servicios gestionados de seguridad (MSSP) que utilizan IA para la monitorización y la respuesta a inciden-

tes aprovechando las capacidades y la experiencia de expertos especializados en ciberseguridad, sin necesidad de invertir en tecnología, formación e incorporación de un equipo interno.

Marco Normativo para la ciberseguridad

1) El Convenio de Budapest sobre la Ciberdelincuencia: este convenio es conocido formalmente como el Convenio sobre la Ciberdelincuencia del Consejo de Europa y se abrió a la firma el 23 de noviembre de 2001, como el primer tratado internacional que aborda los delitos cometidos a través de Internet y otras redes informáticas.

2) El Reglamento General de Protección de Datos (RGPD): este reglamento establece estándares estrictos para el procesamiento y almacenamiento de datos personales en la Unión Europea (UE).

3) Recomendación UIT-TX.1157 del 2015: describe las capacidades necesarias para el servicio de detección y respuesta al fraude de servicios basados en las TIC.

4) Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA): esta ley estadounidense entró en vigor en 1996 y tiene como objetivo proteger la privacidad y la seguridad de la información dentro del sector de la salud.

5) Estándar de Seguridad de Datos para la Industria de Tarjetas de pago (PCI DSS): se trata de un conjunto de normas y requisitos de seguridad diseñados para proteger la información de las tarjetas de pago y garantizar la seguridad de las transacciones con tarjeta de crédito y débito.

6) ISO 27001: se trata de una regla internacional que se centra en la seguridad de la información que proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

7) NIST Cybersecurity Framework: se trata de un conjunto de estándares, directrices y mejores prácticas diseñadas para ayudar a las organizaciones a gestionar y mejorar su postura de ciberseguridad. Se basa en tres principios fundamentales: gestión de riesgos, flexibilidad y escalabilidad, estructurado en cinco funciones:

- Identificar vulnerabilidades y brechas de seguridad de un sistema informático.
- Proteger los sistemas informáticos.
- Capacidad de detectar actividades maliciosas en un sistema informático.
- Saber cómo responder ante un incidente informático.
- Capacidad y recursos para recuperar la información ante un incidente informático.

8) Disposición Cubana sobre la Ciberseguridad: *Resolución* 105 Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad, es la implementación de lo establecido en el Decreto 360/2019, tiene carácter preventivo y alcance a toda la sociedad, al implementar un sistema de trabajo entre las entidades especializadas en seguridad de las TIC para el cumplimiento de sus funciones en el intercambio seguro de información relativa a vulnerabilidades e incidentes de ciberseguridad.

Inversión en ciberseguridad

Se han abordado diferentes factores que impactan y constituyen riesgos, tendencias, proyecciones en el contexto de la ciberseguridad. Los avances tecnológicos requieren la inversión en ciberseguridad en las empresas de telecomunicaciones, que no se trata solo de proteger los activos, sino también de garantizar la resistencia y la sostenibilidad, al centrarse en áreas clave como la evaluación de riesgos, la gestión de proveedores, la planificación de la continuidad del negocio, la respuesta a incidentes y las pruebas continuas. La inversión debe enfocarse en robustecer los servicios de trabajo en la nube, *blokchain*, la computación cuántica y el empleo de herramientas de IA que permitan proteger a las infraestructuras de telecomunicaciones de amenazas o ataques.

Casos registrados durante este año de ciberataques a TELCOS

Telefónica

En enero de 2025, Telefónica, sufrió un ciberataque significativo que resultó en la filtración de aproximadamente 2.3 *gigabytes* de

datos internos. El ataque se originó a través de una sofisticada campaña de *phishing* dirigida a empleados de Telefónica. Los ciberdelincuentes emplearon técnicas de ingeniería social para engañar a los empleados y obtener sus credenciales de acceso. Una vez dentro del sistema, accedieron al sistema interno de *ticketing* de la empresa, conocido como Jira, y extrajeron una cantidad significativa de datos.

Consecuencias del ciberataque

1. **Filtración de datos internos y de clientes corporativos:** más de 236.000 registros de clientes empresariales y alrededor de 469.000 registros de *tickets* internos quedaron expuestos, lo que generó preocupaciones sobre privacidad y seguridad.
2. **Daño reputacional:** la exposición de información sensible afectó la imagen de Telefónica y disminuyó la confianza de sus clientes y socios estratégicos.
3. **Potenciales sanciones legales:** la filtración de datos puede derivar en sanciones económicas debido a incumplimientos de normativas como el Reglamento General de Protección de Datos (RGPD).
4. **Aumento de intentos de fraude:** los ciberdelincuentes pueden utilizar la información filtrada para realizar ataques dirigidos a los clientes afectados.

Respuesta

Una vez detectado el ataque, Telefónica activó su protocolo de respuesta a incidentes y trabajó con su equipo de ciberseguridad para mitigar el impacto y evitar nuevas filtraciones.

1) Se identificaron y bloquearon los accesos comprometidos. Esta acción permitió aislar las cuentas utilizadas por los atacantes y reforzar los controles de acceso.

2) Se estableció la obligatoriedad del restablecimiento de credenciales para todos los empleados. Esta medida se acompañó de la implementación de mecanismos más estrictos de autenticación multifactor.

Al mismo tiempo, la Empresa llevó a cabo un análisis forense del ataque con el objetivo de determinar qué vulnerabilidades fueron

explotadas y cómo mejorar su infraestructura de seguridad. Como resultado de esta investigación, Telefónica decidió fortalecer sus defensas internas, implementar soluciones de detección de amenazas en tiempo real y reforzar la segmentación de redes para dificultar la movilidad de posibles atacantes dentro de sus sistemas.

Lecciones aprendidas y estrategias de prevención

El incidente destaca la importancia de adoptar un enfoque proactivo en ciberseguridad. Algunas estrategias clave para prevenir ataques similares incluyen:

- **Autenticación multifactor (MFA):** evitar que el robo de credenciales sea suficiente para comprometer sistemas críticos.
- **Concienciación en ciberseguridad:** entrenar a los empleados para detectar intentos de *phishing* y aplicar buenas prácticas de seguridad.
- **Monitorización avanzada:** utilizar inteligencia artificial y análisis de comportamiento para detectar accesos inusuales.
- **Gestión de accesos con privilegios mínimos:** limitar los permisos a lo estrictamente necesario para cada usuario.
- **Pruebas de penetración periódicas:** evaluar la seguridad de los sistemas mediante simulaciones de ataques reales.

Claro Argentina

El 4 de julio del 2025, atacantes sustrajeron la base de datos de usuarios de Claro, una de las tres principales compañías de telecomunicaciones de Argentina. La información robada está actualmente a la venta en la *dark web*.

Cómo se realizó el ataque

El ataque tenía como objetivo la app y el portal de Claro, desde donde los usuarios gestionan sus servicios y realizan compras. Esto significa que los ciberdelincuentes no accedieron a las líneas de telefonía celular en sí, pero sí a cuentas asociadas a esos servicios, desde las cuales es posible realizar compras de equipos, solicitar servicios y gestionar información personal.

La filtración incluye correos electrónicos, nombres completos, direcciones, DNI, y códigos postales, datos sensibles que ya están circulando en la *deep web* y que también fueron subidos a sitios

como BiteBlob.com, una plataforma que permite compartir archivos de forma anónima. En esos foros, los datos se venden al mejor postor o incluso se publican de manera gratuita, lo que pone en riesgo la privacidad de miles de personas.

Acciones por parte de Claro

Se activaron los protocolos internos de análisis tras detectar que se mencionaba a la empresa en foros donde suelen ofrecerse bases de datos robadas.

Recomendaciones

Los expertos en general recomiendan una serie de medidas a los usuarios, entre ellas se encuentran:

- Cambiar contraseñas con regularidad y no repetirlas entre servicios.
- Activar la verificación en dos pasos en todas las cuentas.
- Evitar ingresar datos personales en sitios no oficiales o sospechosos.
- Estar atentos a posibles correos *phishing* y no descargar archivos desconocidos.
- Verificar con las empresas si sus cuentas han sido vulneradas y seguir las indicaciones oficiales.

Bouygues Telecom

La tercera mayor operadora de telecomunicaciones en Francia, con una base de alrededor de 27 millones de usuarios, confirmó el 4 de agosto haber sido víctima de un ciberataque. El incidente resultó en una brecha de datos que comprometió la información personal de un aproximado de 6.4 millones de sus clientes, lo que equivale a casi una cuarta parte de su base total de usuarios en el país.

Consecuencias

Los atacantes pudieron obtener información de contacto, detalles del contrato y su número de cuenta bancaria internacional (IBAN), entre los afectados se encuentran clientes particulares y empresas. No obstante, parece que los datos más confidenciales, como contraseñas y números de tarjetas de crédito, no se vieron afectados por esta violación.

Acciones

La operadora presentó una denuncia ante las autoridades judiciales. En ella, señaló que el autor podría enfrentarse a una pena de hasta cinco años de prisión y una multa de 150.000 euros. La TELCO no ha explicado el tipo de ataque, ni la vulnerabilidad atacada en su red.

Orange Francia

La multinacional francesa de telecomunicaciones Orange ha confirmado que fue víctima de un ciberataque el pasado 25 de julio de 2025.

Acciones

El ataque ha obligado a su equipo de seguridad, en colaboración con Orange Cyberdefense, a tomar medidas de contención inmediatas. El incidente, que afectó a uno de sus sistemas de información, ha tenido consecuencias en diversos servicios para empresas y consumidores, especialmente en Francia.

Medidas

La compañía presentó una denuncia oficial el 28 de julio de 2025, mientras las autoridades ya están involucradas en la investigación. No menciona indicios de que se haya producido una exfiltración de datos internos o de clientes. Apenas fue identificado el ataque, los equipos técnicos de Orange se movilizaron para aislar los servicios que podrían haberse comprometido. Esta acción preventiva tuvo como efecto colateral la interrupción de algunas plataformas de gestión para clientes empresariales y ciertos servicios para usuarios particulares.

Resultados y discusión

Los resultados obtenidos evidencian una creciente vulnerabilidad del sector de telecomunicaciones frente a amenazas cibernéticas cada vez más sofisticadas. En América Latina, se ha registrado un incremento del 108 % en los incidentes semanales, siendo México, Colombia y Brasil los países más afectados. Este dato revela una tendencia alarmante que exige una revisión profunda de las políticas de seguridad digital en infraestructuras críticas.

Entre las amenazas más frecuentes, el *ransomware* destaca como el vector de ataque predominante, que representa el 38 % de los incidentes globales. Variantes como LockBit y Akira han demostrado una capacidad de penetración significativa, lo que afecta tanto a grandes

corporaciones como a proveedores regionales. Además, se observa un aumento en la actividad de grupos de APT, como Lazarus y MirrorFace, que operan con objetivos estratégicos y respaldo estatal, lo que añade una dimensión geopolítica al problema.

Se muestra con la investigación el papel de tecnologías emergentes como la IA en la evolución de los ataques. La IA está siendo utilizada para generar *malware* más evasivo y automatizar campañas de *phishing* hiperrealistas. A su vez, la expansión de redes 5G y 6G, junto con el crecimiento exponencial de dispositivos IoT, ha ampliado la superficie de ataque, lo que genera nuevas vulnerabilidades en APIs y sistemas de autenticación.

El análisis de casos reales de ataques a Telefónica, Claro Argentina y Bougyes Telegom ilustra cómo las brechas de seguridad pueden comprometer la privacidad de millones de usuarios y dañar la reputación corporativa. Las respuestas implementadas por estas empresas, como la autenticación multifactor (MFA), la segmentación de redes y el análisis forense, constituyen ejemplos valiosos de buenas prácticas que pueden replicarse en otros contextos.

En cuanto al marco normativo, se destaca la importancia de instrumentos como el Convenio de Budapest, el Reglamento General de Protección de Datos (RGPD), la norma ISO 27001 y la Resolución 105 en Cuba. La cooperación internacional y la interoperabilidad entre gobiernos, operadores de telecomunicaciones y organismos reguladores se perfilan como elementos clave para una defensa efectiva y coordinada. Además, se evidencia el papel dual de la IA en este escenario. Por un lado, permite detectar amenazas en tiempo real y optimizar la respuesta ante incidentes. Por otro, plantea riesgos éticos y operativos al facilitar los ataques automatizados. En este contexto, la supervisión humana sigue siendo indispensable para interpretar los datos y tomar decisiones estratégicas.

En conjunto, los resultados confirman que la ciberseguridad ha dejado de ser una cuestión meramente técnica para convertirse en un componente esencial de la estrategia empresarial y nacional. La investigación aporta una visión integral del panorama actual y sugiere que futuras investigaciones deberían enfocarse en el impacto

económico de los ciberataques y en la evaluación de soluciones basadas en IA desde una perspectiva ética y de sostenibilidad.

Conclusiones

La ciberseguridad se consolida como un eje estratégico en el sector de telecomunicaciones, impulsada por la rápida adopción de tecnologías emergentes como *Fintech*, IoT, inteligencia artificial (IA), computación cuántica y redes 5G. Este ecosistema digital, cada vez más interconectado, ha ampliado de forma significativa la superficie de ataque, que ha dado lugar a amenazas más sofisticadas y persistentes.

En este contexto, la IA desempeña un papel doble: por un lado, potencia las capacidades defensivas mediante análisis predictivo y automatización de respuestas; por otro, habilita nuevos vectores de ataque más adaptativos y difíciles de detectar. Ante este panorama, se vuelve imperativo fortalecer las capacidades técnicas de los operadores, fomentar la interoperabilidad entre los distintos actores del ecosistema digital y promover una cultura organizacional resiliente, capaz de anticipar y mitigar riesgos. La colaboración interinstitucional, junto con el desarrollo profesional continuo, se posiciona como un componente esencial para enfrentar un entorno de amenazas dinámico, distribuido y en constante evolución.

Referencias bibliográficas

AECC Consultoras. (2025). *La transición al 6G pone a prueba la ciberseguridad global*. https://aecconsultoras.com/noticias-sectoriales/la-transicion-al-6g-pone-a-prueba-la-ciberseguridad-global/.

Benito, M. (2023). *Ciberdelincuencia: ¿qué es y cómo combatirla? Blog de los Estudios de Derecho y Ciencia Política*, Universidad Abierta de Cataluña. https://blogs.uoc.edu/edcp/ciberdelincuencia-que-es-y-como-combatirla/.

BitLife Media. (2025, agosto). *Qué sabemos del ciberataque a Orange: cronología, servicios afectados y respuesta de la compañía*. https://bitlifemedia.com/2025/08/que-sabemos-del-ciberataque-a-orange-cronologia-servicios-afectados-y-respuesta-de-la-compania/.

Check Point Software. (2025). *Informe global sobre ciberataques del primer trimestre de 2025* [Blog: Blog Check Point]. https://blog-checkpoint-com.translate.goog/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc.

Djilp.org. (s.f.). *Marcos jurídicos internacionales sobre ciberseguridad y derecho de protección de datos*. Recuperado 18 de octubre de 2024, de https://djilp-org.translate.goog/international-legal-frameworks-on-cybersecurity-and-data-protection-law/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc.

El Siglo Web. (2025, julio 20). *Hackearon la base de datos de Claro y ya está a la venta en la dark web*. https://elsigloweb.com/2025/07/20/hackearon-la-base-de-datos-de-claro-y-ya-esta-a-la-venta-en-la-dark-web/.

Escudo Digital. (2025). *Un ciberataque a la tercera telco francesa expone los datos de 6 millones de clientes*. https://www.escudodigital.com/ciberseguridad/un-ciberataque-a-la-tercera-telco-francesa-expone-los-datos-de-6-millones-de-clientes.html.

Estrategias de Inversión. (2025). *Por qué invertir en ciberseguridad en 2025: claves, amenazas y oportunidades*. https://www.estrategiasdeinversion.com/fondos/por-que-invertir-en-ciberseguridad-en-2025-claves-n-818277.

Ministerio de Relaciones Exteriores de Cuba. (2021). *Cuba actualiza marco jurídico sobre telecomunicaciones y tipifica incidentes de ciberseguridad*. Misiones Cubaminrex. https://misiones.cubaminrex.cu/es/articulo/cuba-actualiza-marco-juridico-sobre-telecomunicaciones-y-tipifica-incidentes-de-0.

InfoSecurity México. (2025). *Una guía completa del concepto, tipos, amenazas y estrategias*. https://www.infosecuritymexico.com/es/ciberseguridad.html.

Kaspersky. (2025). *¿Qué es la seguridad en la nube?* Centro de Recursos. https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security.

Piranirisk. (2025). *Ciberseguridad: qué es, cómo funciona y su importancia*. Academia Piranirisk. https://www.piranirisk.com/es/academia/especiales/ciberseguridad-que-es-como-funciona-y-su-importancia.

Revista Tono. (2023). "Comportamiento del fraude internacional y su impacto en operadores de telecomunicaciones", (17), 1-15. https://www.revistatono.etecsa.cu/tono/article/view/392/711

Telefónica Tech. (2025). "Tendencias en ciberseguridad para 2025." https://telefonicatech.com/blog/tendencias-en-ciberseguridad-para-2025

Winforsystems. (2025). Caso práctico: Ciberataque a Telefónica. https://winforsystems.com/caso-practico-ciberataque-a-telefonica/