Revista Brasileira de Engenharias

ISSN 3085-8089 vol. 1, n. 2, 2025

ARTIGO 1

Data de Aceite: 02/12/2025

SEGURIDAD DE LA INFORMACIÓN Y RIESGOS CIBERNÉTICOS: TENDENCIAS Y DESAFÍOS

Andrés David Dávila Bernal

Resumen: El presente artículo tiene como objetivo proporcionar un análisis sobre los riesgos cibernéticos que afectan a diversas industrias, destacando las tendencias emergentes y los desafíos en el ámbito de la ciberseguridad dentro de un entorno dinámico y en constante evolución. Para ello, se ha llevado a cabo una revisión de la literatura disponible, incluyendo investigaciones académicas, opiniones de expertos, informes de fabricantes de tecnologías de ciberseguridad y medios de comunicación confiables. Este análisis busca identificar y contextualizar las circunstancias que, principalmente en el ámbito corporativo, están moldeando los escenarios de ciberseguridad actuales.

Palabras clave: Ransomware, ciber resiliencia, malware, phishing, vishing, smishing, ransomware.

Introducción

En la era digital contemporánea, la seguridad de la información se ha consolidado como un pilar fundamental para la protección de activos, procesos y datos en organizaciones públicas y privadas. El crecimiento exponencial de las tecnologías de la información y la comunicación (TIC), junto con la adopción masiva de servicios en la nube, dispositivos inteligentes y sistemas interconectados, ha generado un entorno altamente dinámico pero también vulnerable. En este contexto, los riesgos cibernéticos han evolucionado en complejidad, frecuencia y alcance, afectando no solo la infraestructura tecnológica, sino también la confianza de los usuarios y la estabilidad de los ecosistemas digitales.

Actualmente, se destacan tendencias como el modelo de arquitectura Zero Trust, la ciberresiliencia organizacional, el uso de inteligencia artificial en ciberdefensa, y el incremento de ataques sofisticados como el ransomware dirigido y el phishing avanzado. Estas dinámicas exigen una revisión crítica de los enfoques tradicionales de seguridad, así como la adopción de estrategias proactivas y adaptativas que respondan a los desafíos emergentes. Además, el marco normativo internacional y las políticas de gobernanza digital juegan un papel clave en la articulación de respuestas coordinadas frente a amenazas transnacionales.

Este artículo tiene como objetivo analizar las principales tendencias en seguridad de la información y riesgos cibernéticos, así como los desafíos que enfrentan las organizaciones en su implementación, con el fin de aportar una visión integral que contribuya al fortalecimiento de la protección digital en un entorno cada vez más complejo y exigente.

Importancia de la Seguridad de la Información Dentro de las Organizaciones

Riesgos Actuales

El presente contexto empresarial y personal refleja una creciente digitalización, la cual genera grandes posibilidades para el desarrollo de negocios, la eficiencia de procesos y comodidad de los individuos: Trayendo como consecuencia alta dependencia tecnológica, hiper conectividad, expansión de dispositivos y sin duda alguna el crecimiento de los riesgos inherentes a este contexto. Por lo tanto, aspectos como la pérdida o robo de información, fraude digital, secuestro de datos o afectaciones a la disponibilidad de los servicios, deben

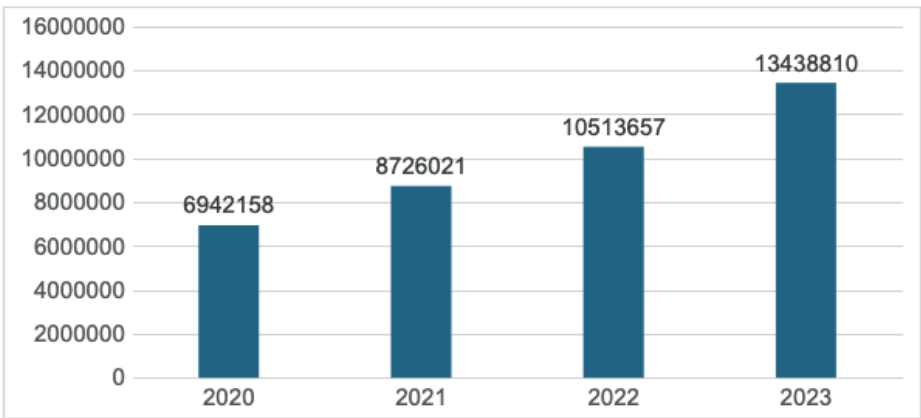
ser gestionados, con el objetivo de mitigar su impacto y la probabilidad y que en esta línea las compañías puedan comprometer su estabilidad financiera, reputación o su misma continuidad. A continuación, serán desarrollados aspectos que en términos de seguridad de información y ciberseguridad están marcado tendencia.

Protección de los datos

La información se ha convertido en un elemento fundamental para la operación y el desarrollo de oportunidades para los negocios, en muchas situaciones puede verse como su materia prima, por lo tanto, la importancia de ella es fundamental. Dentro del contexto colombiano leyes como la 1581 - Protección de Datos Personales establece lineamientos y condiciones que la industria debe seguir en miras de dar un manejo apropiado de este recurso, más sin embargo dado el valor que representa, se ha convertido en un objetivo de los ciber criminales, quienes a través de diversas técnicas buscan su compromiso con diversos fines criminales, en este sentido serán citadas algunas técnicas aplicadas por los ciber delincuentes, alguna de ellas ya conocidas, pero en la actualidad mucho más evolucionadas y que junto con otras que están emergiendo a consecuencia de la aparición de nuevas tecnologías como la inteligencia artificial, representan riesgos de ciberseguridad.

Phishing

Esta técnica Presente desde hace al menos 20 años comúnmente utilizada y lejos de caer en obsolescencia, evoluciona consistentemente, según Anti Phishing World Group en su reporte del segundo semestre de 2024 señala crecimiento tanto en el número de ataques como compañías objeto de estos. En el segundo trimestre de 2024, OpSec Security, miembro fundador de APWG, descubrió que las plataformas de redes sociales volvieron a ser el sector más atacado, representando el 32,9 por ciento de todos los ataques de phishing. El phishing contra el segmento de instituciones financieras (banca) se mantuvo mayoritariamente estable en



Note. Adaptado de Bolster Research Phishing in Focus 2024 Mid-Year Report, 2024, https://bolster.ai/2024-mid-year-phishing-report

Figura 1. Crecimiento del phishing.

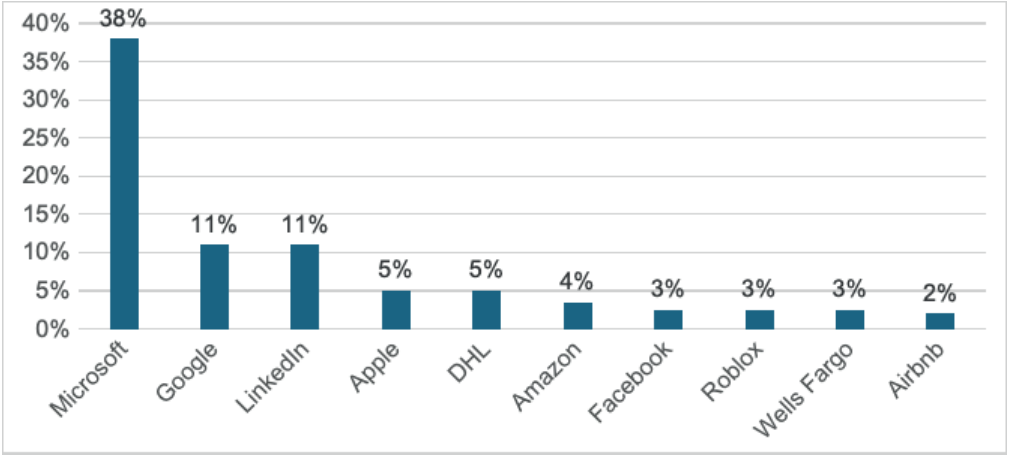
un 10 por ciento, frente al 24,9 por ciento de todos los ataques en el tercer trimestre de 2023 y el 14 por ciento en el cuarto trimestre de 2023. Los ataques contra servicios de pago en línea (como PayPal, Venmo, Stripe y empresas similares) también se mantuvieron estables, con otro 7,5 por ciento de todos los ataques.

El Ministerio de las telecomunicaciones de Colombia señala que el phishing es el método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima, la siguiente figura ilustra respecto a su crecimiento.

Dentro del ámbito latinoamericano Según Colombia Fintech en publicación realizada en septiembre e 2024 (https://colombiafintech.co/lineaDeTiempo/articulo/phishing-la-modalidad-de-mayor-estafa-en-latam), menciona que el 85% de empresas han sufrido ataques de phishing, indicando que distintos informes llevados a cabo de forma reciente muestran cómo los ataques de phishing incrementaron en los últimos años, generando pérdidas de miles de millones de dólares. Países como México, Brasil, Colombia y Argentina reportaron un aumento de este tipo de delitos desde el 2022, siendo los sectores más afectados el comercio electrónico y el sector financiero.

En la actualidad son utilizadas diferentes técnicas para desarrollar ataques de phishing las cuales prometen permanecer en el tiempo, así como evolucionar alcanzados ataques más sofisticados en el futuro debido a la combinación de nuevas técnicas disponibles. (Salloum, et. al., 2022), la figura 2 señala cuales son las marcas o compañías de mayor uso para ciber atacantes que usan el phishing.

De acuerdo con lo descrito surgen recomendaciones encaminadas a mitigar el riesgo, algunas de ellas enfocadas en controles técnicos y otras orientadas a la sen-



Nota: Adaptado de The SSL Store. (s.f.). Phishing statistics. The SSL Store Blog. https://www.thesslstore.com/blog/phishing-statistics/

Figura 2. Top de las marcas más utilizadas para phishing

sibilización de las personas. Los ataques de phishing hacen un mal uso del desconocimiento de los usuarios humanos, que no pueden abordarse simplemente con métodos técnicos y pueden requerir intervenciones humanas como capacitación y concienciación humana (Dou et. al., 2017), por tal razón la generación de conciencia es pieza fundamental de la prevención y así lo identifican las organizaciones. En el escenario actual, las organizaciones deben brindar a sus empleados conciencia y soluciones factibles para detectar e informar ataques de phishing de manera proactiva y rápida antes de que causen algún daño (Basit et. al. 2020)

Si bien el phishing se ejecuta más comúnmente a través de correos electrónicos, también se puede realizar a través de otros canales, incluidas llamadas telefónicas (vishing) y SMS (smishing). El smishing, específicamente, implica el uso de mensajes de texto SMS para hacerse pasar por organizaciones acreditadas, como bancos, agencias gubernamentales o proveedores de servicios, para incitar a los destinatarios a tomar medidas inmediatas, como hacer clic en un enlace o llamar a un número de teléfono. Los mensajes a menudo transmiten una sensación de urgencia, explotando la naturaleza inmediata y personal de los SMS para dificultar que los usuarios reconozcan la estafa. La siguiente figura indica el crecimiento del comportamiento de smishing en estados unidos a manera de ejemplo.

Los ataques de vishing generalmente involucran a estafadores que hacen llamadas telefónicas a personas desprevenidas (Jones, et al., 2021), con base en pretextos y suplantando a entidades legítimas para manipular y engañarlas a sus víctimas para que revelen información confidencial (Interpol, 2022 & Europol, 2022). Los ataques de vishing modernos a menudo emplean tecnología VoIP (Voz IP), lo que permite a los atacantes falsi-

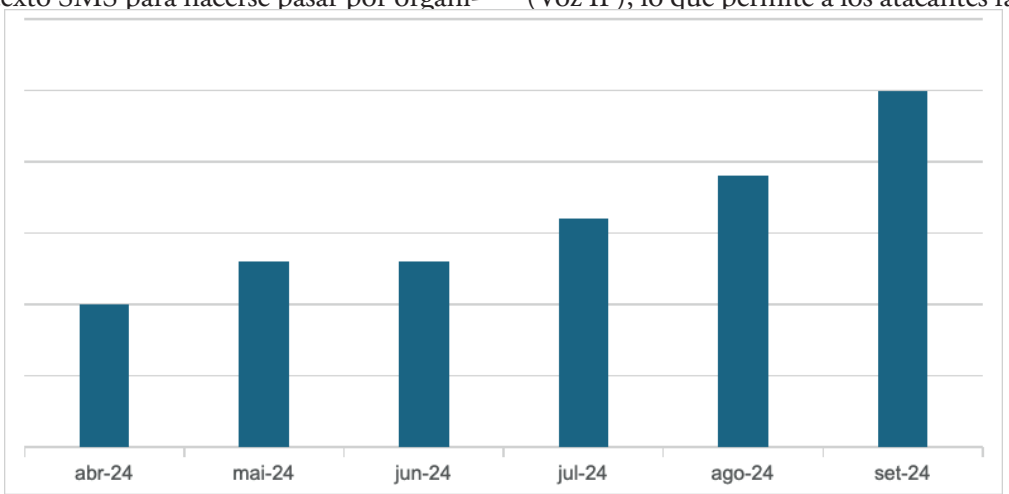


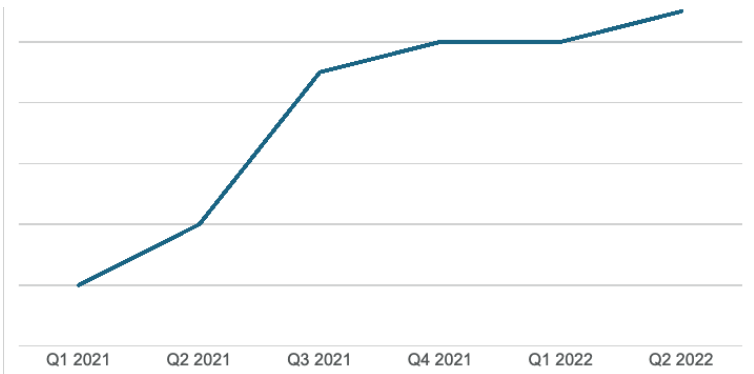
Figura 3. Tendencia del crecimiento del smishing en Estados Unidos.

Nota. Adaptado de Mobile Political Spam Volume Continues Rapid Growth in the Lead Up to the U.S. November Elections, W. Stuart Jones and Adam McNeil, 2024, https://www.proofpoint.com/uk/blog/email-and-cloud-threats/spam-text-messages-dos-donts

ficar la información del identificador de llamadas y llegar a una audiencia global con un costo y esfuerzo mínimos en comparación con la telefonía tradicional. La integración del vishing con otras técnicas de ciberataque, como los correos electrónicos de phishing que incitan a las víctimas a llamar a un número fraudulento se ha generalizado (Hashmi, 2023). El cibercrimen organizado opera desde call centers (Interpol, 2022), y con frecuencia se dirige a las víctimas con haciéndoles creer que han sido demandados por algún incumplimiento o infracción, también utilizan el fraudes simulando soportes técnicos sobre algún servicio contratado o bajo la disculpa de alertas de seguridad bancaria, esto con el fin de extraer información personal y financiera confidencial o incitar a las víctimas a realizar pagos con falsos pretextos. La figura 4 muestra como la técnica de vishing ha incrementado su uso.

Ransomware

Uno de los objetivos que persigue el phishing es abrirle paso a una infección de ransomware, el cual es un tipo de malware que impide o limita el acceso de los usuarios a su sistema y/o datos hasta que se pague un rescate (Kirda, 2016). Activo por más de 30



Nota. Adaptado de Callback phishing attacks see massive 625% growth since Q1 2021. Bleeping Computer, B. Toulas, 2022, https://www.bleepingcomputer.com/news/security/callback-phishing-attacks-see-massive-625-percent-growth-since-q1-2021/

Figura 4. Tendencia de crecimiento del vishing.

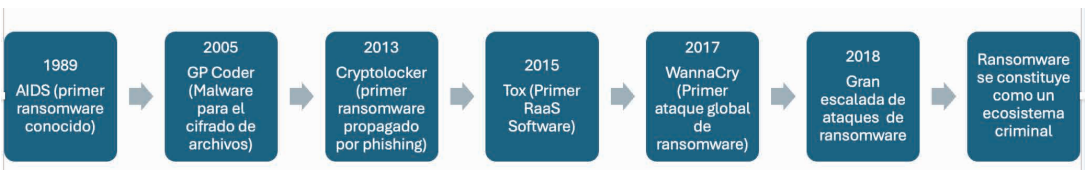


Figura 5. Evolución del ransomware

Nota. Adaptado de Evolution of Ransomware: So Far and Hereafter, SOC Radar Research, 2022, https://socradar.io/evolution-of-ransomware-so-far-and-hereafter/

años, ha evolucionado durante este tiempo, la figura 5 ilustra respecto a algunos hitos relacionados a este proceso.

Con el paso del tiempo las compañías también han evolucionado sus esquemas de defensa, mejorando sus mecanismos de respaldo, por tal razón dentro de la evolución del ataque, los hackers, una vez han logrado llegar hasta los datos de su víctima, como primera medida intentan extraer sus datos de tal manera que si al cifrarlos posteriormente la víctima se niega a pagar porque quizás tiene copias limpias de su información, el atacante opta por amenazar con la divulgación de sus datos que en muchos casos son confidenciales en sitios como la *dark web.* Los nuevos ransomware prefieren la exfiltración de datos al cifrado de archivos, y los ataques son más selectivos, operados por humanos y sigilosos. Podrá cifrar o extraer datos del almacenamiento en la nube o de bases de datos, sin afectar las actividades del sistema de archivos local (Mcintosh et. al, 2024).

Según el World Economic Forum en su reporte relacionado a las tendencias de ciberseguridad para 2025 indica que el Ransomware sigue siendo el principal riesgo cibernético organizacional respecto a los últimos años, dentro de su exploración han identificado que un 45% de los líderes, refiriéndose a gerentes generales y responsables específicos de ciberseguridad indican que es el riesgo que más les preocupa, considerando que se deben esperar innovaciones significativas en los ataques de este tipo. Esto se ve agravado por la aparición de la figura de *Ransomware-as-a-Service* (RaaS), que conso-

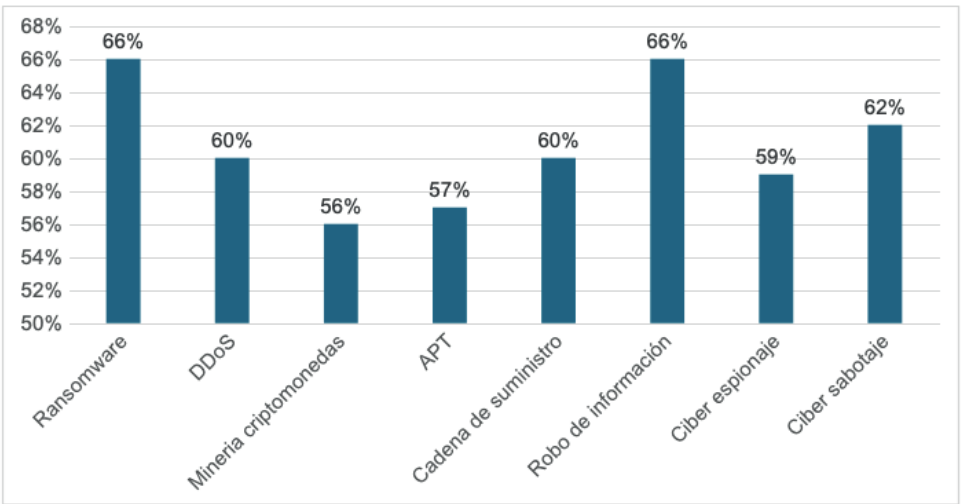


Figura 6. Nivel de probabilidad de ocurrencia para diferentes tipos de amenazas.

Nota. Adaptado de Newswit: Emerging threats and mitigating risks in 2024, 2024,https://www.newswit.com/en/if9yfqirlpp0c847uxb9cocjjv2pbbu0

lida la comercialización de esta modalidad criminal. La siguiente figura indica los tipos de amenaza y su probabilidad de ocurrencia.

El impacto de los ataques de ransomware son de tal importancia que las organizaciones hacen evidente el esfuerzo que están haciendo para fortalecer las medidas de control y recuperación a través de inversiones en su infraestructura, personal y procesos, así como en la búsqueda de colaboración por parte de compañías expertas en la gestión de este tipo de incidentes como en las entidades de gobierno que combaten este tipo de amenazas, ejemplo de ello el ColCert en Colombia, estando integrado a otras organizaciones en el plano internacional.

El objetivo de gestionar el riesgo de ransomware como parte de la gestión general de los riesgos de ciberseguridad, está orientado a minimizar el impacto y la probabilidad de infección. identificando oportunamente comportamientos asociados a sus procesos de infección, evaluándolos y priorizándolos, así como implementando medidas de mitigación adecuadas. También es importante señalar que la gestión de riesgos de ciberseguridad, incluyendo el ransomware no es una actividad única, sino un proceso continuo (Mcintosh et. al, 2024).

El crecimiento de la tecnología y la digitalización de prácticamente todos los sectores empresariales han transformado la forma de trabajo, alejando los procesos manuales. Las nuevas innovaciones continúan mejorando los productos y servicios a un ritmo vertiginoso.

Si bien disfrutamos de los beneficios que aporta la tecnología, una gran oportunidad conlleva un gran riesgo. La Asociación Alemana de Economía Digital (Bitkom), en su informe del 5 de agosto de 2021 (https://distologystudios.com/blog/exponential-growth-in-cybercrime-s-bitkom-study-2021), revela un aumento dramático de los ciberataques entre 2020 y 2021 para las organizaciones alemanas. calculó que los delitos cibernéticos causan más de 220 mil millones de euros cada año y están en continuo aumento, esto señalando comportamientos para países desarrollados que si bien cuentan con mayor digitalización que aquellos países en vía de desarrollo, también su madurez en términos de protección es mayor.

Ataques a la Cadena de Suministro

En las economías modernas, las complejas cadenas de suministro son parte integral de la producción de casi todos los bienes y servicios, desde automóviles hasta alimentos y servicios médicos. Cada vez más, las cadenas de suministro son globales y vinculan la producción en los países menos desarrollados con el consumo en los países desarrollados (Nicita et. al., 2013). Conscientes de ellos los atacantes han identificado el esfuerzo que las grandes compañías están realizando con el objetivo de proteger su infraestructura tecnológica y procesos críticos dependientes de ella, por tal razón en su búsqueda de eslabones débiles han identificado que algunos proveedores de estas organizaciones carecen de controles y por ende representan la posibilidad de materializar sus actividades criminales.

El informe Global Cybersecurity Outlook 2024 reveló una importante inequidad cibernética, exponiendo marcadas diferencias en aspectos de resiliencia comparando organizaciones pequeñas y grandes. El Informe Global Risks 2024 del Foro Económico Mundial concluyó que la inseguridad cibernética es un riesgo global en múltiples

escenarios, con riesgos cibernéticos como malware, deepfakes y desinformación que amenazan las cadenas de suministro, la estabilidad financiera y los sistemas democráticos. Por otre parte, el evento de Chief Risk Officers Outlook de octubre de 2024 clasificó el riesgo cibernético entre las tres principales amenazas que afectan gravemente a las organizaciones. Un sorprendente 71% de los directores de riesgos anticiparon graves interrupciones organizacionales debido a los riesgos cibernéticos y la actividad delictiva. Particularmente 2024, reflejó la mayor interrupción de TI de la historia, afectando a aerolíneas, bancos, emisoras, sistemas de salud, sistemas de pago minorista y cajeros automáticos a nivel mundial, causando pérdidas estimadas en 5 mil millones de dólares. Este escenario alerta respecto a las vulnerabilidades derivadas de la dependencia de un número limitado de proveedores críticos. Adicionalmente las ciberamenazas siguieron aumentando, La encuesta reveló además que los delitos cibernéticos aumentaron tanto en frecuencia como en sofisticación, marcados por ataques de ransomware, tácticas mejoradas con inteligencia artificial (como phishing, vishing y deepfakes) y un notable aumento de los ataques a la cadena de suministro.

Uno de los casos de mayor impacto en Colombia y otros países latinoamericanos ocurrido recientemente, ha sido el incidente sobre IFX Networks, un proveedor tecnológico destacado por los servicios de telecomunicaciones, quienes sufrieron un ataque de ransomware por medio del malware RansomHouse, comprometiendo alrededor de 700 servidores, impactando el servicio de al menos 46 entidades del estado, dentro de ellas algunas que soportan el sistema de salud (García, 2023).

Respecto a las posibles estrategias de defensa. Cartwright y Cartwright (2023) señalan dos consideraciones clave:

- Las cadenas de suministro deben verse de manera integral y no fragmentada cuando se defiende contra ataques cibernéticos. Esto debe ir más allá de que una empresa se interese simplemente por la seguridad cibernética de sus proveedores. En particular, podría implicar que una empresa invierta activamente en la seguridad cibernética de sus proveedores. Esta inversión tiene sentido financiero si protege a la empresa de un ataque de ransomware a través de debilidades en la cadena de suministro. Ataques de ransomware que afectaron a Apple, Toyota y JSB ilustran los peligros de no invertir en la seguridad de la cadena de suministro.
- La cadena de suministro debe diseñarse para aumentar la resistencia al ataque de ransomware. Apoyados en la literatura sobre la resiliencia de la red que contribuye a configurar un diseño óptimo de la red. Ejemplo de ello es diversificar y desacoplar los riesgos en la cadena de suministro. Esto puede limitar el daño que puede causar cualquier infracción cibernética.

Ciber Resiliencia

La dinámica relacionada a la creciente cantidad de ataques cibernéticos que involucra diversos tipo de industria, países y compañías con ampla experiencia tecnológica prevé que un incidente de ransomware no está solamente reservado a compañías que

pudiesen considerarse débiles en términos de su ambiente de control, por el contrario aquellas compañías de alto renombre son objeto de múltiples ataques que en caso de materializar el riesgo impactan considerablemente la operación, llegando a afectar la reputación y finanzas de la empresa. Ante la presente situación múltiples organizaciones sin dejar de lado las tareas de prevención de un incidente de Ransomware o similar, también están enfocados en la manera de reaccionar adecuadamente, enmarcados en el concepto de ciber resiliencia, CertPro quienes son una firma de auditoría y consultoría norteamericana expertos en ciberseguridad, han compartido los que según su experiencia han sido las principales amenazas para 2024 como lo muestra la figura 2, al revisar la tipología se puede deducir que la materialidad de la mayoría de ellos puede traer como consecuencia indisponibilidad de los servicios de alguna organización, en ese sentido las organizaciones deben prepararse para hacer frente a situaciones de este tipo, la figura 7 resalta las situaciones o amenazas de mayor ocurrencia.

La definición dada por el Disaster Recovery Institute International (DRII, 2019) respecto al concepto de Ciber resiliencia es "a capacidad de una entidad para entregar

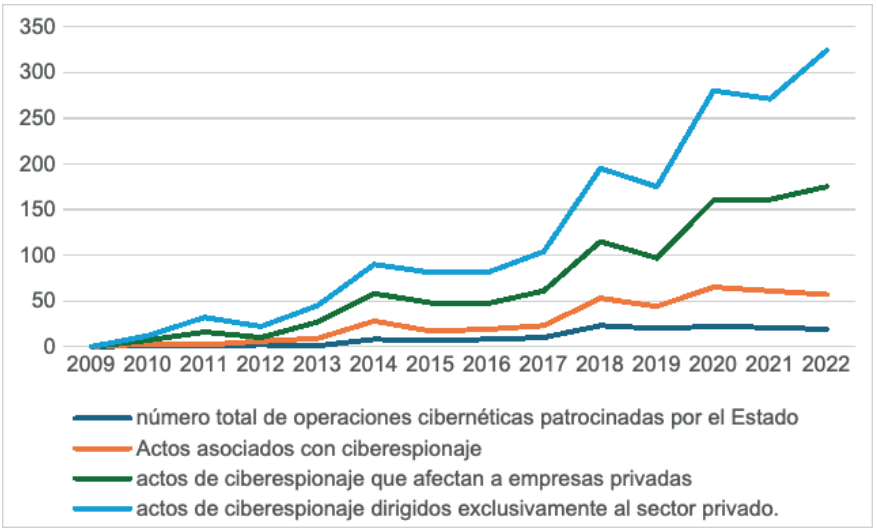


Figura 7. Top de ciber amenazas para 2024.

Nota. Adaptado de Top 10 Cybersecurity Threats in 2025, Patil, A. 2024, https://certpro.com/cybersecurity-threats/

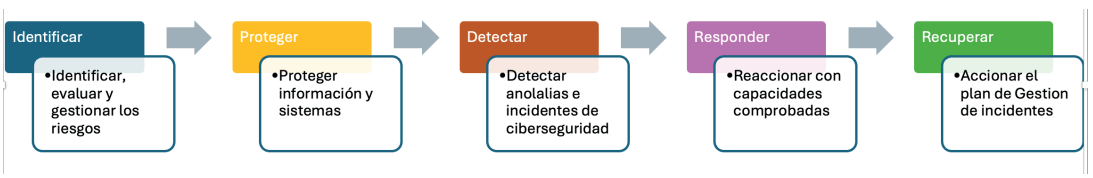


Figura 8. Descripción general de elementos del modelo NIST CSF 2.0

continuamente el resultado previsto a pesar de los eventos cibernéticos adversos". En este mismo sentido el National Institute of Standards and Technology (NIST) en su modelo de Ciber resiliencia lo plantea en al menos 5 grandes pasos como es señalado en la figura 8.

Este modelo refleja la fusión de la gestión de ciberseguridad respecto a las primeras etapas planteadas asociadas a identificar, proteger y detectar. Considerando las dos últimas etapas de responder y recuperar hacen parte de la continuidad de negocio haciendo parte de este, de acuerdo con el momento se incorporan riesgos de ciber ataques. (Ramírez, 2021)

De acuerdo con el reporte 2024 de Ciberseguriad generado por el World Economic Forum, la percepción de los lideres encuestados respecto a la madurez de los procesos de ciber resiliencia, encontrando que en las regiones desarrolladas como son Europa, Norteamérica, Asia y Oceanía, la preocupación oscila entre un 15% y 20%, mientras que en África y Latinoamérica esta preocupación aumenta al 36% y 42% respectivamente. Por otra parte, El 71% de los ciber lideres encuestados cree que las pequeñas organizaciones ya han alcanzado un punto de inflexión crítico en el que ya no pueden protegerse adecuadamente contra la creciente complejidad de los riesgos cibernéticos, lo anterior enfatiza el riesgo que este tipo de compañías incorporan en las cadenas de suministro.

Ciber espionaje – Ciber Guerra

Garcia (2021) define que las actuales condiciones de interconexión global en el plano cibernético en donde intervienen muchos actores internacionales e incluyendo a la propia sociedad, representa tantos beneficios a raíz de esta cercanía, pero también han provocado ataques cibernéticos por parte de los mismos actores quienes la utilizan día a día. La reincidencia de estos acontecimientos refleja una realidad en la que el espionaje se mantiene como uno de los medios favoritos para alcanzar objetivos dentro de las estrategias de algunos actores. Lo anterior a pesar del surgimiento de métodos para recolectar y procesar información de maneras cada vez más eficientes e innovadoras. El espionaje se ha reinventado para adaptarse a las plataformas virtuales. Algo en lo que concuerda Candau (2019) quien lo cataloga como un método relativamente económico, rápido y que implica menos riesgos que el espionaje tradicional, porque dada la dificultad de atribución de la autoría, siempre cabe la posibilidad de negar su uso. Por ello, es importante reconocer al ciber-espionaje como parte de las implicaciones negativas que trajo consigo la globalización tecnológica y entender de qué manera su uso, repercute a los derechos humanos en materia de seguridad y privacidad, así como también en el derecho a la no intervención y en la soberanía de los Estados.

"Estados Unidos es uno de los pioneros de las estrategias de ciber-espionaje y utilizará cualquier otro medio con fines políticos. Además, se cree que es uno de los países que más indaga sobre la información de las personas" (Yancey, 2017). Yancey (2017) también menciona el caso del mayor ataque de espionaje cibernético que tuvo lugar cuando China se infiltró en el Pentágono. Así como el establecimiento militar de la India y robó documentos confidenciales, o el incidente de espionaje de China para robar el avión Lockheed Martin F-35. Aunque China aún no ha producido tecnología militar estadou-

nidense o india, se hace de las herramientas y de sus habilidades en el ciberespacio para hostigar su rivalidad regional con Estados Unidos y la India.

En relación con el reciente conflicto entre Rusia y Ucrania, esta situación ha puesto de manifiesto que el ciberespacio se ha convertido en el nuevo campo de batalla.

Desde el año 2015 Ucrania ha sido objetivo de diversos ataques a su infraestructura, empezando por la interrupción del servicio eléctrico que a través del malware BlackEnergy quiso sabotear los sistemas de control de suministro de energia, impactando a 1,5 millones de habitantes de Ivano-Frankivsk, pero esta no fue la primera aparición de esta amenaza pues hay reseñas de su uso desde 2007 orientadas a ataques de denegación de servicio (DoS), robo y destrucción de información (Santos, 2024).

Posteriormente casos como el de Industroyer otro software malicioso generó un ataque del mismo tipo, pero ahora sobre Kiev, seguido en 2017 por Petya direccionado a destruir programas contables propios de Ucrania, propagándose a nivel mundial, generando cuantiosas perdidas (Santos, 2024)

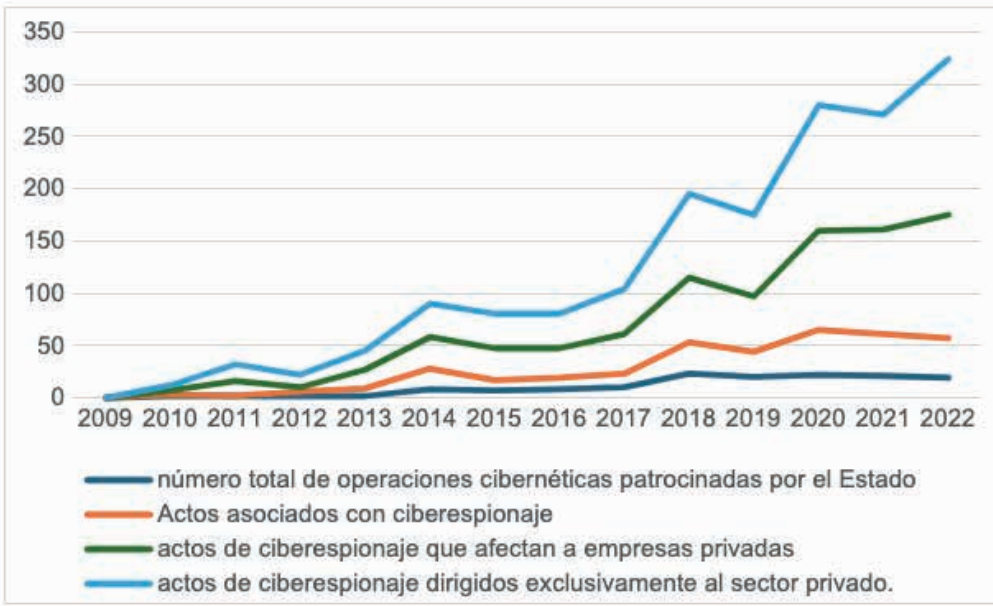
Durante 2024 se ha suscitado bastante preocupación debido a la posible compra del software espía Pegasus por el Estado colombiano, pegasus es un poderoso software malicioso dirigido principalmente a dispositivos móviles, lo anterior a dejando bastantes dudas y preocupaciones tanto en el uso como en la forma como pudo ser adquirido pues se involucra a unidades de la policía colombiana como es la DIPOL. Algunas, ONG de derechos humanos que le ha seguido la pista a Pegasus, ha advertido que mediante este dispositivo se ha vulnerado la información de, por lo menos, 50.000 personas en el mundo, incluyendo políticos, periodistas, defensores de derechos humanos y activistas (Parada, 2024).

La cada vez menor utilización de documentos impresos dando paso a las opciones digitales, obliga a tomar las medidas necesarias en relación a su protección. El mundo digital no tiene fronteras y practicar espionaje es cada vez más fácil, recursos como keyloggers en línea, a disposición de cualquier persona, siendo de fácil uso, señalan la necesidad de estar protegidos desde la parte legal y técnica (Soltero, 2019).

Machín Nieva, (2016) Cataloga los tipos de espionaje que realizan las empresas, como espionaje industrial y espionaje comercial. A la vez, menciona cómo las empresas como agentes económicos son de los actores principales en generar ciberataques. La figura 9 pretende ilustrar respecto al crecimiento de estos casos de ciber espionaje han crecido principalmente en el sector privado o la industria.

Deep Fake

La combinación deep fake de aprendizaje profundo y contenidos falsos es un proceso que implica el intercambio de una cara de una persona a una persona objetivo en un video y hacer que la expresión de la cara sea similar a la de la persona objetivo y actuar como si la persona objetivo estuviera diciendo las palabras que realmente dijo otra persona (Mahmud et al., 2021). Aunque todos conocen la creación de contenido falso, pero Deepfake es algo que va más allá de los pensamientos de alguien, lo que hace que estas técnicas sean más poderosas y casi reales utilizando Machine Learning e Inteligencia Artificial para manipular el contenido origi-



Nota. Adaptado de Combating the cyber heists that are costing the global economy, 2023, Seth, S., & Priyandita, G., https://www.aspistrategist.org.au/combating-the-cyber-heists-that-are-costing-the-global-economy/

Figura 9. Número de incidentes notificados de operaciones cibernéticas gestionados por el Estado, 2009 a 2022

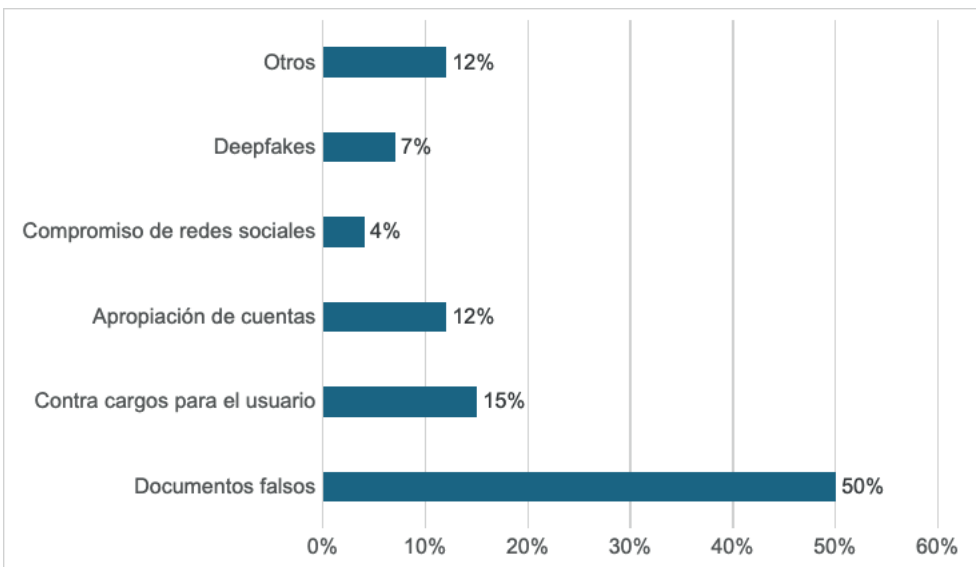


Figura 10. Top de fraudes relacionados a identidad en 2024.

Nota. Adaptado de Identity Fraud Report 2024, Sum and Substance Ltd., 2024, https://static.poder360.com.br/2025/02/Sumsub-Fraude-Digital-2024-Poder360.pdf

nal y convertirlo en fraude (Schwartz, 2020 & Clark, 2019). Deepfake tiene una amplia gama de usos, como crear pornografía falsa de celebridades conocidas, difundir noticias falsas, voces falsas de políticos, fraude financiero y muchos más (Banks, 2018 & Abhimanyu, 2018). Aunque la técnica de intercambio de caras es bien conocida en la industria cinematográfica, donde se crean varias voces o videos falsos como requisito, pero eso requiere mucho tiempo y cierto nivel de experiencia. Pero a través de técnicas de aprendizaje profundo, cualquiera que tenga sólidos conocimientos informáticos y una computadora GPU de alta configuración puede crear videos o imágenes falsos confiables, la figura 10 resalta aquellos comportamientos que impactan la identidad de los ciudadanos, indicando la tendencia de acuerdo con el tipo de ataque.

Una tendencia de las organizaciones sin importar su segmento es migrar sus tecnologías tradicionalmente localizadas en centros de cómputo propios o rentados (on premise) a infraestructuras en nube, buscando entre otros ahorros, flexibilidad de crecimiento y delegación de riesgos y responsabilidades de operación. La migración a la nube puede ahorrar costos debido a que los proveedores de servicios en la nube cuentan con la infraestructura suficiente para poder gestionar eficientemente la provisión de recursos (Ren et al., 2012).

Soewito (2020) expone razones claras para que las empresas migren a la nube como son:

- Los servicios de computación en la nube tienen escalabilidad, lo que significa que pueden satisfacer las necesidades de recursos de tecnología de la información de acuerdo con las necesidades de las empresas.
- El proveedor de la nube proporciona ajustes tanto para la configuración del hardware como para las actualizaciones de software o configuración de los servidores y demás elementos de su infraestructura al servicio de sus clientes, de modo que las empresas, como usuarios de servicios en la nube, estén más enfocadas en sus negocios desarrollando mejores productos innovadores.
- El proveedor de la nube al ser especializado en este tipo de servicios tiene centros de datos que brindan servicios informáticos rápidos y eficientes, por lo que esto tendrá un efecto en el alto rendimiento en la nube en comparación con los centros de datos propiedad del común de las empresas.
- En este mismo sentido, Hussein (2020) resalta estos otros aspectos.
- Integrar unidades de negocio dentro de la organización, conduciendo a cambios de proceso, incorporando agilidad.
- Mejorar la eficiencia, el rendimiento y la escalabilidad del conjunto de aplicaciones del negocio.
- Adaptar nuevas alternativas en términos de tecnología, prácticas de mercado, eficiencia operativa, requisitos regulatorios para conducir a un mejor servicio al cliente.
- Reducir el costo operativo y mejorar la eficiencia, simplificando y eliminando cuellos de botella en el

proceso de requerimientos al reunir diferentes centros de datos a una sola ubicación.

- El crecimiento respecto a la adopción de tecnologías de nube es una realidad, la figura 11 muestra una realidad y proyección al respecto.

El proceso de migración a la nube promete seguir creciendo de manera consistente, a pesar de involucrar riesgos como los identificados por Soewito (2020), como es representado en la figura siguiente.

La seguridad del sistema en la nube es un gran desafío, ya que es una combinación de políticas, tecnologías, controles, datos, servicios e infraestructura. Por tanto, las vulnerabilidades aumentan debido a esta combinación (Kaufman, 2009). Los datos en la nube están siendo delegados a proveedores de servicios algunos de ellos pueden no confiables pudiendo comprometer la privacidad de sus clientes (Qadiree, 2017).

Como resultado de una encuesta a expertos en ciberseguridad, se determinaron algunas de las amenazas más comunes, siendo priorizaron en función de su importancia. A ellas se asignaron a los elementos de modelado de amenazas STRIDE (Meier, 2003). STRIDE significa suplantación de identidad, manipulación, reputación, divulgación de información, denegación de servicio y elevación de privilegios, con sus siglas en ingles. Las principales amenazas fundadas son:

- Denegación de servicio. Realizar ataques de denegación de servicio (DoS) a proveedores de servicios en la nube puede provocar que los usuarios no tengan acceso a sus cuentas. Los ataques DoS se pueden llevar a cabo saturando el servidor con varias solicitudes para agotar todos los recursos disponibles del dispositivo, enviando datos maliciosos al servidor que bloquean un procedimiento de aplicación, insertando repetidamente contraseñas incorrectas para bloquear la cuenta del usuario. (Paxton, 2016)
- Acceso no autorizado y secuestro de cuenta. El entorno de nube abre la posibilidad a los atacantes acceder a los datos de otros usuarios. Si un intruso logra robar las cuentas de un cliente (secuestrar la cuenta), es posible que pueda acceder a sus recursos en la nube, monitorear sus acciones, explotar sus registros y transferir usuarios a sitios web no autorizados, lo que podría causar daños a la reputación y pérdidas financieras (Qadri, 2018).
- Fuga de datos. Las empresas son susceptibles a ataques cuando los datos no están seguros, ya sea que estén en tránsito o en reposo. Sin embargo, si los datos se encuentran en movimiento de carga o descarga, estarán expuestos a un mayor riesgo (Al Nafea & Almaiah, 2021).
- Intrusos maliciosos en proveedores de nube. Las amenazas internas maliciosas son un grave problema de seguridad, especialmente en el entorno de la nube, donde el sistema de la nube se comparte con entidades desconocidas, sumando al acceso desde la Internet pública las organizaciones no tienen todo el control de sus sistemas.

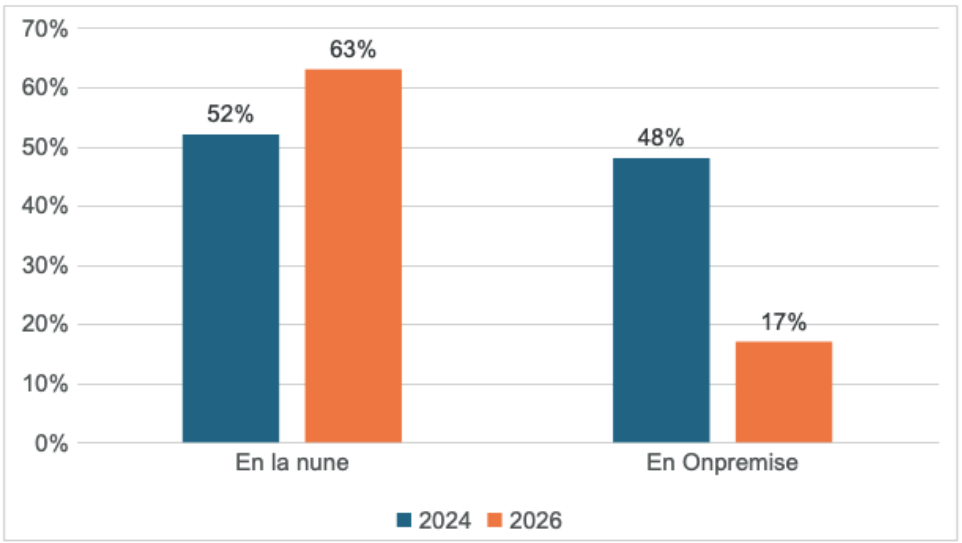


Figura 11. Comportamiento de la migración de infraestructura a la nube.

Nota. Adaptado de 15 Cloud Migration Statistics and Trends for 2024. Krook, D., 2024, https://www.auvik.com/franklyit/blog/cloud-migration-statistics/

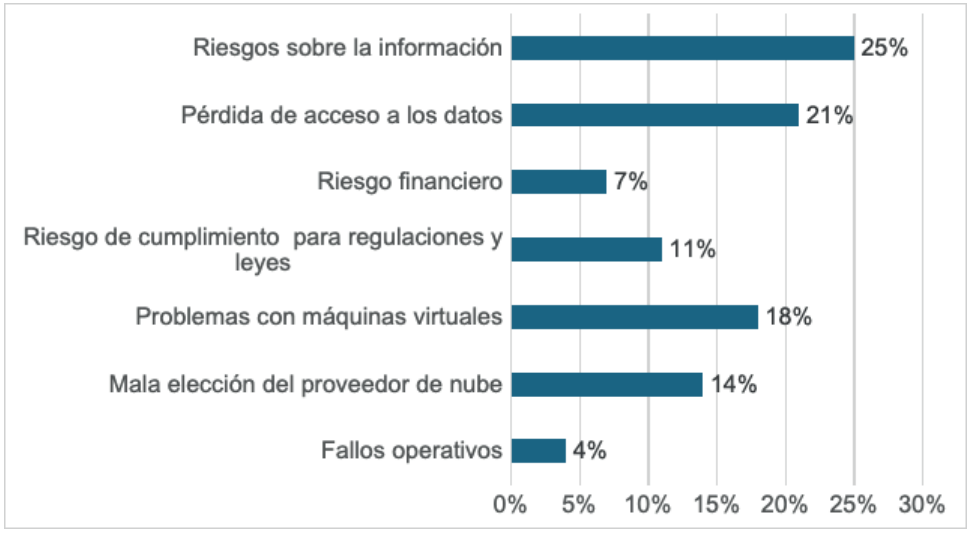


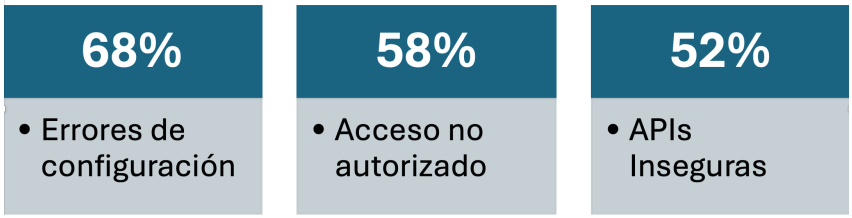
Figura 12. Tendencia por tipo de Riesgo.

Nota. Adaptado de A systematic literature Review: Risk analysis in cloud migration, Soewito, B., Gaol, F. L., & Abdurachman, E., 2022, https://doi.org/10.1016/j.jksuci.2021.01.008

En conclusión la fuerte acogida en la adopción de servicios de nube representa un crecimiento importante en los riesgos que estas tecnologías representan, sin lugar a dudas los grande jugadores de estas tecnologías como son entre otros AWS, Microsoft y Google ofrecen opciones de protección muy robustas, así como tecnologías que se integran a ellos, es fundamental que se sigan buenas prácticas en las implementaciones y su operación, siguiendo recomendaciones como las dadas por CSA (Cloud Security Alliance). El World Economic Forum en 2021 señala como uno de los principales causantes de los incidentes de seguridad es la no aplicación correcta de configuraciones, como lo señala la siguiente figura.

Zero Trust

Los puntos anteriormente señalados reflejan riesgos importantes dentro del actual contexto tecnológico cada vez más di-



Nota. Adaptado de Five ways to ensure the cloud doesn't cast a shadow over your cybersecurity, Kretchmer, R., & Gonen, T., 2021, https://www.weforum.org/stories/2021/04/cloud-cybersecurity/

Figura 13. Problemáticas comunes en la migración a la nube

Nota. Adaptado de Zero Trust Architecture, NIST Special Publication 800-207, Rose, S. , Borchert, O., Mitchell, S. and Connelly, S., 2020, https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Figura 14. Requerimientos fundamentales para alcanzar un entorno zero trust.

gital, involucrando muchos más elementos conectados como lo muestra las tecnologías IoT y sobre todo más abierto a diversas ubicaciones como lo implican las tecnologías en nube, conduciendo en muchos escenarios a ambientes multi-nube, en donde se involucran más de un proveedor de este tipo de servicios y ambientes híbridos para aquellos casos en donde las organizaciones aún mantienen tecnologías *on premise* y servicios contratados en nube.

Dentro de los conceptos y tecnologías que surgen con el objetivo de proteger las infraestructuras esta Zero Trust (Cero Confianza), según Akamai quien ofrece servicios en internet incluidos elementos de protección de ciberseguridad, define Zero Trust de la siguiente manera "*Una estrategia de seguridad de red basado en la filosofía de que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso para conectarse a sistemas o cargas de TI hasta que se considere explícitamente necesario. En resumen, significa cero confianza implícita*".

Los cuatro fundamentos esenciales de Zero Trust son el control de acceso y la autenticación, el cifrado, la micro segmentación de redes y la automatización e integración de sistemas de protección (Sied, 2022)

NIST (National Institute of Standards and Technology) define los siete principios básicos para una ZTA (Zero Trust Architecture) (Rose, 2020) que tienen como fin lograr una implementación optima de ZTA (con la opción de implementar selectivamente algunos principios y no otros, de acuerdo con la necesidad percibida).

- Recurso. Cualquier fuente de datos o servicio informático.
- Seguridad de la comunicación. La comunicación está asegurada independientemente de la ubicación.
- Seguridad de sesión. El acceso a los recursos se otorga por sesión, y la autenticación y autorización para un recurso no pueden extender los privilegios a otros.
- Control de acceso. El acceso a los recursos está determinado por una política dinámica, incluido el estado observable de la identidad del cliente, la aplicación y el activo solicitante.
- Postura de seguridad mínima. La empresa debe garantizar que todos los dispositivos propios y terceros se encuentren en el estado más seguro posible y debe monitorearlos permanentemente para garantizarlo.
- Autenticación continua. Toda la autenticación y autorización de recursos es dinámica y se aplica estrictamente. Una empresa que pretende implementar ZTA debe tener un sistema de gestión de identidad, credenciales y acceso, así como autenticación multifactor (MFA) para mayor seguridad. Pudiendo ser útil una inspección continua durante la interacción del usuario con los sistemas con la posibilidad de requerir una nueva autenticación/autorización sin generar fricciones.
- Registro de información. La empresa debe recopilar tanta información como sea posible sobre el estado actual de la infraestructura de la red y las comunicaciones, y utiliza esta información para mejorar su postura de seguridad.

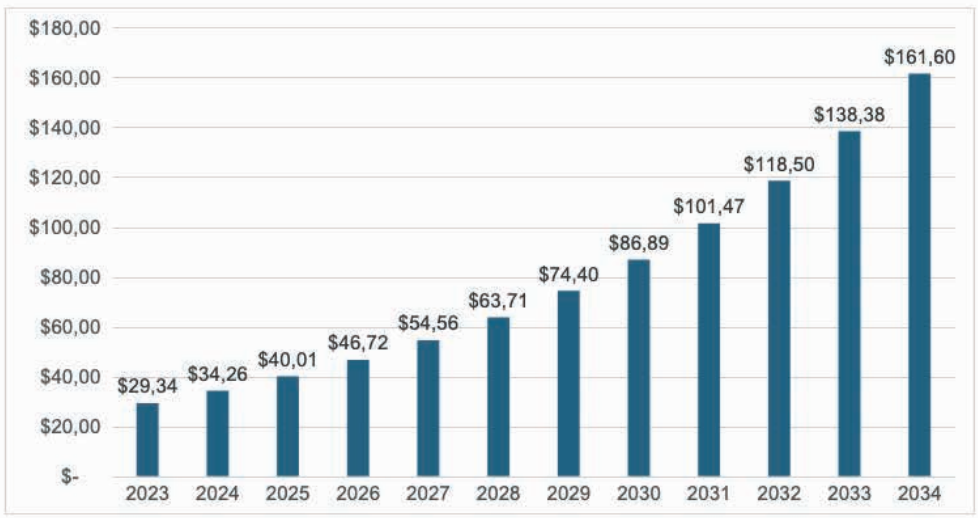


Figura 15. Mercado para tecnologías zero trust proyectado para 2023 hasta 2034 (valores expresados en miles).

Nota. Adaptado de Zero Trust Security Market Growth Driven by Rising Cyber Threats and Compliance Regulations, Precedence Research, 2025, https://www.precedenceresearch.com/zero-trust-security-market

De acuerdo con las características anteriormente planteadas, la adopción de Zero Trust viene en aumento durante los últimos años y seguramente será uno de los mecanismos de mayor consideración en miras de proteger los ecosistemas informáticos. La siguiente imagen muestra lo que pudiese ser un crecimiento proyectado en estas tecnologías hasta el año 2034.

Conclusiones

El análisis de las tendencias y desafíos en materia de seguridad de la información y riesgos cibernéticos evidencia un panorama dinámico y cada vez más complejo. Amenazas como el phishing y sus variantes, los ataques de ransomware y las compromisos en la cadena de suministro continúan evolucionando, aprovechando vulnerabilidades en los ecosistemas organizacionales. La acelerada migración hacia entornos en la nube introduce nuevos retos de seguridad que requieren gobernanza sólida y monitoreo continuo para mitigar riesgos. Asimismo, fenómenos emergentes como las tecnologías deepfake amplifican los riesgos asociados al fraude de identidad y la desinformación, mientras que el ciberespionaje resalta la dimensión estratégica de la ciberseguridad en ámbitos corporativos y geopolíticos.

En este contexto, la ciberresiliencia se posiciona como una capacidad crítica que permite a las organizaciones no solo prevenir y detectar incidentes, sino también recuperarse y adaptarse frente a ataques persistentes y sofisticados. Los hallazgos subrayan la necesidad de enfoques integrales que combinen soluciones tecnológicas, cumplimiento normativo y factores humanos, fomentando una cultura de seguridad y gestión proactiva del riesgo. Las investigaciones futuras deberían orientarse hacia el desarrollo de marcos adaptativos que aborden la convergencia entre amenazas tradicionales y riesgos emergentes, garantizando que las organizaciones mantengan su

resiliencia en un entorno caracterizado por el cambio tecnológico acelerado y la creciente sofisticación de los ciberataques.

Referencias

Abhimanyu, G., (7 de febrero de 2018). Twitter, Pornhub and other platforms ban AI-generated celebrity porn. The Next Web. https://thenextweb.com/insider/2018/02/07/twitter-pornhub-and-other-platforms-ban-ai-generated-celebrity- porn/

Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779–786). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491638

Ali, M.M.; Mohd Zaharon, N.F. (2024). Phishing—A cyber fraud: The types, implications and governance. International Journal of Educational Reform, 33(1), 101–121. https://doi.org/10.1177/10567879221082966

Akamai Technologies. (n.d.). What is Zero Trust? Zero Trust security model. https://www.akamai.com/glossary/what-is-zero-trust

Amaral, A. C. (2014). La Amenaza Cibernética para la Seguridad y Defensa de Brasil. Visión Conjunta(10), 19-22. Obtenido de http://cefadigital.edu.ar/bitstream/1847939/32/3/VC%2010-2014%20AMARAL.pdf

Banks, A., (20 de febrero de 2018). Deepfakes & Why the Future of Porn is Terrifying. Highsnobiety. https://www.highsnobiety.com/p/what-are-deepfakes-ai- porn/

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Bolster AI. (2024). 2024 mid-year phishing report. Bolster AI. https://bolster.ai/2024-mid-year-phishing-report

Candau, J. (2019). Ciberespionaje, una amenaza al desarrollo económico y la defensa. Seguritecnia 460. Revista decana independiente de seguridad (460), 70-72. Obtenido de https://www.seguritecnia.es/revistas/seg/460/index.html

Cartwright, A., & Cartwright, E. (2023). The economics of ransomware attacks on integrated supply chain networks. Digital Threats: Research and Practice, 4(4), 1–14. https://doi.org/10.1145/3579647

Clarke, Y., (2019) H.R.3230 - 116th Congress (2019-2020): DEEP FAKES Accountability Act. (2019, junio 28). https://www.congress.gov/bill/116th-congress/house-bill/3230

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of knowledge (SoK): A systematic review of software-based web phishing detection. IEEE Communications Surveys & Tutorials, 19(4), 2797–2819. https://doi.org/10.1109/COMST.2017.2752087

E. Kirda. 2016. Most Ransomware isn't as Complex as You Might Think. https://privacy-pc.com/articles/mostransomware- isnt-as-complex-as-you-might-think.htm. [Online; accessed 13-October-2020].

Europol, https://www.europol.europa.eu/media-press/newsroo m/news/europol-and-eurojust-support-czech-and-ukrainian-police-in-taking-down-multi-million-euro-voice-phishing-gang, 2022, accessed: 2024-06-06

García, J. (2023). Así enfrenta Colombia su primer caso de 'megasecuestro digital'; ¿qué está pasando?. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-detalles-del-ataque-a-ifx-networks-806778

Hashmi, S. I., George, N., Saqib, E., Ali, F., Siddique, N., Kashif, S., ... & Javed, M. (2023, April). Training Users to Recognize Persuasion Techniques in Vishing Calls. In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-8). Interpol, https://www.interpol.int/en/News-and-Events/News/2 022/Cyber-enabled-financial-crime-USD-130-million-interce pted-in-global-INTERPOL-police-operation, 2022, accessed: 2024-06-06.

Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4), 61–64. https://doi.org/10.1109/MSP.2009.87

Kretchmer, R., & Gonen, T. (2021, abril 20). Five ways to ensure cybersecurity while using the cloud. World Economic Forum. https://www.weforum.org/stories/2021/04/cloud-cybersecurity/

Krook, D. (2024, agosto 13). 15 Cloud Migration Statistics and Trends for 2024. Auvik Blog. https://www.auvik.com/franklyit/blog/cloud-migration-statistics/

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. Information & Computer Security, 29(2), 314–331. https://doi.org/10.1108/ICS-07-2020-0113

Jones, W. S., & McNeil, A. (2024, octubre 17). Spam text messages: Dos and don'ts. Proofpoint Blog. https://www.proofpoint.com/uk/blog/email-and-cloud-threats/spam-text-messages-dos-donts

Machín Nieva, G. (2016). La Ciberseguridad como factor crítico en la seguridad de la Unión Europea. Revista UNISCI, (42), 47–68. https://doi.org/10.5209/RUNI.53786

Mahmud, B. U., & Sharmin, A. (2021). Deep insights of deepfake technology: A review. arXiv preprint arXiv:2105.00192. https://doi.org/10.48550/arXiv.2105.00192

Meier, J. D. (2003). Improving web application security: Threats and countermeasures. Microsoft Press. ISBN: 978-0-7356-1842-8

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). Phishing. Recuperado de https://www.mintic.gov.co/portal/inicio/5683:Phishing

Newswit. (2024). Kaspersky: Emerging threats and mitigating risks in 2024. Newswit. https://www.newswit.com/en/if9yfqirlp-p0c847uxb9cocjjv2pbbu0

Patil, A. (2024, julio 10). The 10 biggest cybersecurity threats of 2025. CertPro. https://certpro.com/cybersecurity-threats/

Parada, V. (2024). Pegasus en Colombia: las claves para entender la denuncia de Petro. El Pais. https://elpais.com/america-colombia/2024-09-06/pegasus-en-colombia-las-claves-para-entender-la-denuncia-de-petro.html

Paxton, N. C. (2016, November). Cloud security: A review of current issues and proposed solutions. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC) (pp. 452–455). IEEE. https://doi.org/10.1109/CIC.2016.073 [researchr.org]

Precedence Research. (2025, July 25). Zero trust security market size to hit USD 161.60 billion by 2034. https://www.precedenceresearch.com/zero-trust-security-market

Qadiree, J., Prasad, N., & Gautam, P. (2017). Security and privacy approach of cloud computing environment. International Journal of Advanced Research in Computer Science, 8(7), 648–651. https://doi.org/10.26483/ijarcs.v8i7.4355

Qadri, M. N., & Quadri, S. M. K. (2018). Mapping cloud computing in university e-governance system. International Journal of Intelligent Computing and Cybernetics, 11(1), 141–162. https://doi.org/10.1108/IJICC-11-2016-0048

Ramírez, N. A. (2021). Ciberresiliencia. Revista Sistemas, (159), 96–110. https://doi.org/10.29236/sistemas.n159a7

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69–73. https://doi.org/10.1109/MIC.2012.14

Román Soltero, A. R. (2019). Análisis ético de la información en el escándalo Pegasus. Revista de Investigación en Tecnologías de la Información, 7(14), 22–37. https://doi.org/10.36825/RITI.07.14

Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420 (Accessed February 16, 2025)

Santos Barón, M. A. (2024). El conflicto entre Rusia y Ucrania: una guerra de quinta generación. Revista Opera, (35), 37–61. https://doi.org/10.18601/16578651.n35.03 [redalyc.org]

Seth, S., & Priyandita, G. (2023, junio 8). Combating the cyber heists that are costing the global economy. The Strategist. https://www.aspistrategist.org.au/combating-the-cyber-heists-that-are-costing-the-global-economy/

SOCRadar Research. (2024, noviembre 1). Evolution of ransomware: So far and hereafter. SOCRadar. https://socradar.io/evolution-of-ransomware-so-far-and-hereafter/

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

Soewito, B., Gaol, F. L., & Abdurachman, E. (2022). A systematic literature Review: Risk analysis in cloud migration. Journal of King Saud University-Computer and Information Sciences, 34(6), 3111-3120. https://doi.org/10.1016/j.jksuci.2021.01.008

Schwartz, O. (2018, December 12). You thought fake news was bad? Deep fakes are where truth goes to die. The Guardian. https://www.theguardian.com/technology/2018/dec/12/deep-fakes-fake-news-truth

Sum and Substance Ltd. (2024). Fraude digital 2024. Poder360. https://static.poder360.com.br/2025/02/Sumsub-Fraude-Digital-2024-Poder360.pdf

The SSL Store. (s.f.). Phishing statistics. The SSL Store Blog. https://www.thesslstore.com/blog/phishing-statistics/

Toulas, B. (15 de agosto de 2022). Callback phishing attacks see massive 625% growth since Q1 2021. Bleeping Computer. https://www.bleepingcomputer.com/news/security/callback-phishing-attacks-see-massive-625-percent-growth-since-q1-2021/

Yancey, J. (Abril de2017). Los ataques cibernéticos y sus repercusiones políticos globales. Obtenido de https://repositorio.utdt.edu/bitstream/handle/utdt/6596/MEI_2017_Yancey.pdf?sequenc e=1

Waldman, D. H. G., Téllez, G. D. O., & Sánchez, P. G. S. (2021). El ciber-espionaje como herramienta estratégica de los actores internacionales en la era digital: una revisión desde la literatura. Sapienza: International Journal of Interdisciplinary Studies, 2(4), 136–153. https://doi.org/10.47697/sapienza.v2i4.136-153