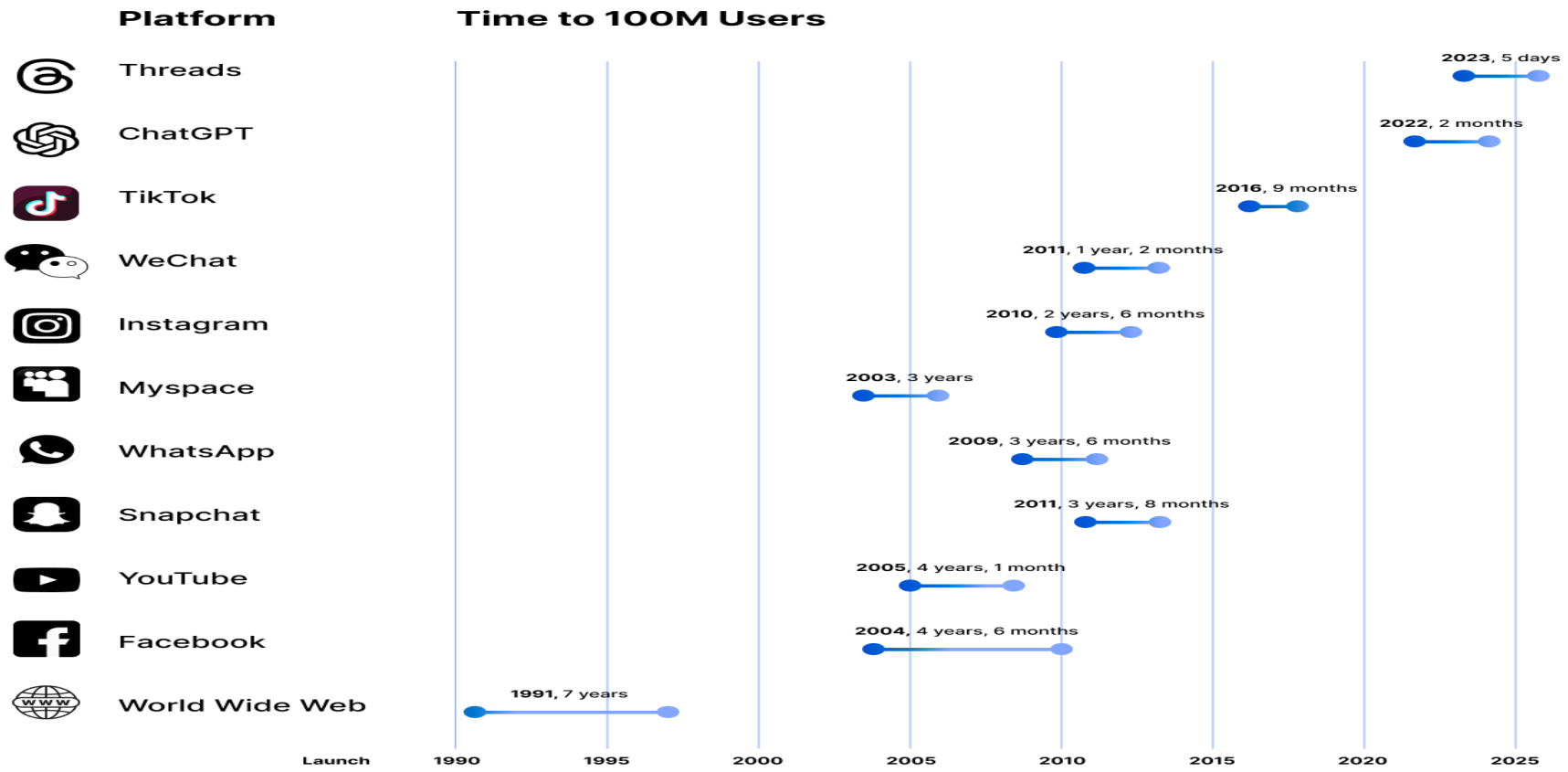
Introducción a la Ciberseguridad

Teoría: Javier Díaz
jdiaz@unlp.edu.ar
Práctica: Soledad Gomez
Ulises Cabrera

Estamos en la Era Exponencial

- “Exponencial” caracteriza a la aceleración de los avances tecnológicos actual.
- El libro: la Era Exponencial (Azeem Azar, 2021) Los cambios radicales ya no se llevan adelante en siglos o décadas, sino en años y hasta en meses.
- Ejemplo: ChatGPT alcanzó los cien millones de usuarios en tres meses, más rápido que TikTok, logrando dicho hito en nueve meses, mientras que Instagram lo hizo en dos años y medio. (30/11/2022)
- Mientras el cambio tecnológico se acelera rápidamente, la sociedad evoluciona a un ritmo más gradual e incremental. Se está produciendo una brecha entre la tecnología y la sociedad; ***“brecha exponencial”***

Top Apps and Websites: The Journey to 100 Million Users



Techopedia

Crece el uso de la IA

- Muchas personas utilizan la IA en el trabajo en Europa. En Dinamarca (enero 2024) el 65 % de los profesionales del marketing, el 64 % de los periodistas y el 30 % de los abogados, usan IA en el trabajo. https://bfi.uchicago.edu/insights/the-adoption-of-chatgpt/
- Un tercio de los trabajadores estadounidenses usaron IA generativa en el trabajo durante la última semana de agosto 2024

https://static1.squarespace.com/static/60832ecef615231cedd30911/t/66f0c3fbabdc0a173e1e697e/1727054844024/BBD_GenAI_NBER_Sept2024.pdf

Crece el uso de la IA

- El estudio de Dinamarca descubrió que los usuarios pensaban que la IA reducía a la mitad su tiempo de trabajo para el 41% de las tareas que realizan en el trabajo.
- En EEUU tres experimentos , 4.867 desarrolladores de software, se revela un aumento del 26,08 % en la cantidad de tareas completadas entre los desarrolladores que utilizan la herramienta de IA.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4945566

Uso de IA en Universidades

- Inglaterra: encuesta 1,047 estudiantes de 166 IES, flash survey sobre IA generative en Educacion Superior, realizada en Julio 2025
- La mayoria de los estudutiantes**, 85 por ciento**, dijeron que usarin IA generatva el ultimo año. Los tres usos principalesThe top three uses from a long list of options are:
  - brainstorming (55 %),
  - Usandolo y preguntandole como un tutor (50 %)
  - Estudiando para examenes o quizzes (46 %).
  - Usandolo como un motor de busqueda avanzado tambien es un uso destacado
- https://www.insidehighered.com/news/students/academics/2025/08/29/survey-college-students-views-ai

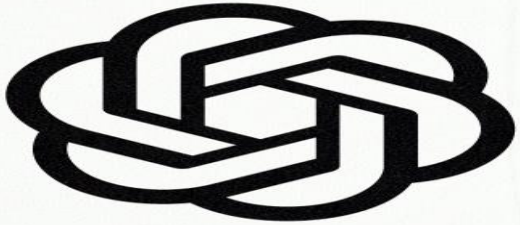
Crece el uso de la IA agosto 2025

- ***OpenAI (ChatGPT)***
  - **Semanal**: aproximadamente **700 millones** de usuarios activos por semana en agosto de 2025 (SQ Magazine).
  - **Mensual estimado**: entre **900 millones y 1,4 mil millones**, según extrapolaciones basadas en su actividad semanal (SQ Magazine, CNBC).
- ***Google Gemini***
  - **Marzo 2025**: cerca de **350 millones** de usuarios activos mensuales (PYMNTS.com).
  - **Mayo 2025**: ya superaba los **400 millones de usuarios activos mensuales** (TechCrunch).
  - **Julio 2025**: alcanzó los **450 millones de MAU**, según datos compartidos por ejecutivo de Google (The Economic Times, The Times of India).

Crece el uso de la IA opensurce

- *Perplexity AI:* Según varias fuentes, se estima que tiene entre **15 y 22 millones** de usuarios activos mensuales:
  - **15 millones** (estimación de principios de 2025) (Exploding Topics, Wikipedia).
  - **22 millones** (proyección para el primer semestre de 2025) (Wikipedia, Views4You, DemandSage).
- *DeepSeek:* Según informes internos, en **enero 2025** tenía aproximadamente **33,7 millones** de usuarios activos mensuales y cerca de **22,15 millones** diarios (withoutlimitsai.com).
  - Otras estimaciones (monitorizadas via Reddit) mencionan cifras combinadas (web + app) de hasta **117 millones** de usuarios (Reddit).

THE MOST POPULAR AI CHATBOTS IN 2025



ChatGPT
46.6B

ChatGPT hit **5 billion** average monthly visits for the first time ever in 2025

Meta AI
130.4M

Grok
686.9M

Claude
1.2B

Perplexity
1.5B

DeepSeek
2.7B

Gemini
1.7B

Microsoft Copilot
957.2M

Poe
378.1M

Mistral
101.39M

Annual global web visits from August 2024 to July 2025

Source: Onelittleweb

VISUAL CAPITALIST

Seguridad de la información

- ¿Qué se debe asegurar?

  La información: La nuestra y la de la organización donde trabajamos.

- ¿Cuál es el lugar que ocupa la información?

  La información constituye un **activo muy importante para la organización**, ya que tiene un rol fundamental a la hora de cumplir sus objetivos.

  Debemos proteger la información adecuadamente garantizando su seguridad y privacidad.

Seguridad de la información

Definamos más formalmente:

- ACTIVO: un activo de TI es hardware, sistemas de software o información que tienen valor para una organización
- VULNERABILIDAD: Es una **DEBILIDAD** en un activo
- AMENAZA: Es el problema que potencialmente puede ocurrir si se **aprovecha una debilidad/vulnerabilidad.**
- INCIDENTE: Se produce cuando **la amenaza se concreta** y atenta contra la seguridad de la información.

Principios básicos (CIA Triad)

- Confidencialidad: Garantiza que la información sólo sea accesible por las personas autorizadas. En otras palabras: proteger la información contra accesos no autorizados.
- Integridad: Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo. En otras palabras: proteger la información contra accesos no autorizados.
- Disponibilidad: Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.

Ejemplo: banca online → datos cifrados (C), registros contables no alterados (I), plataforma siempre operativa (A).

Historia de la Ciberseguridad

- Década 1960–70: seguridad centrada en acceso físico y control de usuarios en mainframes.
- Década 1980–90: primeras redes y virus → aparición de antivirus y firewalls.
  - 1995 surge Internet comercial
- Década 2000–10: cibercrimen organizado, botnets, ataques DDoS y auge del comercio electrónico.
- Década 2010–20: amenazas avanzadas persistentes (APT), ransomware global, seguridad en cloud e IoT.

Historia de la Ciberseguridad

- 2020 en adelante:
  - Explotación de vulnerabilidades como servicio (VaaS) → venta y alquiler de exploits y kits de ransomware.
  - Hacktivismo como actor global (Anonymous, ataques vinculados a conflictos geopolíticos como Rusia–Ucrania).
  - Grandes corporaciones de hackers y ransomware gangs (ej. Conti, REvil, LockBit) operando como empresas con estructura, servicio al cliente y programas de afiliados.
  - Crecimiento del mercado negro digital en dark web y profesionalización del cibercrimen.
  - Tendencias actuales: IA en ciberataques, ataques a la cadena de suministro (ej. SolarWinds), guerra cibernética y ciberespionaje estatal.

Ciberataque a Costa Rica

- Primer ataque 17/4/22 a los servidores del Ministerio de Hacienda de Costa Rica, inutilizo la Administración Tributaria Virtual (ATV) y el Sistema de Información Aduanera (TICA). Dos días después, el sitio web del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones fue hackeado. Horas más tarde, Conti atacó un servidor de correo electrónico del Instituto Meteorológico Nacional robando la información contenida en el mismo. Pidieron 20Musd
- El Grupo Hive 31/5/22 ataco la Caja Costarricense de Seguro Social y obligo a cerrar todos sus sistemas críticos, Historia Única Digital de Salud y el Sistema Centralizado de Recaudación. Pidieron 5Musd.efectos hasta junio inclusive

https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#:~:text=The%20Conti%20Group%2C%20which%20claimed,companies%20operating%20in%20Costa%20Rica

Incremento Ciberataques

- **38%** es el porcentaje de incremento de los ciberataques en el año 2022 respecto del año anterior .
  https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/
- **30 %** aumento interanual de los ciberataques en el segundo trimestre de 2024, alcanzando 1636 ataques por organización por semana.
- Sectores más atacadas: Educación/Investigación (3.341 ataques por semana), Gobierno/Militar (2.084) y Salud (1.999).
- América Latina (+53%), África (+37%) y Europa (+35%) mostraron los mayores aumentos en ataques cibernéticos en el segundo trimestre de 2024, en comparación interanual.

Es noticia! Les pasa a las Universidades ...

https://www.ull.es/portal/noticias/2022/universidades-exponen-casos-de-ciber-ataques/

Un ciberataque dejará a la UAB sin servicios informáticos durante toda la semana

• Todos los portales están desconectados y sólo se pueden hacer las clases presenciales que no requieran el uso de un ordenador

Campus de la Universidad Autónoma de Barcelona (UAB) / UAB

Los 'piratas' de la UAB amenazan con filtrar los datos robados en 24 horas

Los ciberdelincuentes de PYSA publican un ultimátum en la 'deep web' un mes después de secuestrar los servidores de la institución

Hackeo a Universidad Autonoma de Barcelona

En los rankings la UAB figura entre las 200 mejores del mundo.
https://www.uab.cat/web/conoce-la-uab/la-uab/la-uab-en-los-rankings-1345670592413.html

El ataque ransomware a la UAB habría afectado hasta 650.000 archivos Datos personales. Pidieron 3.5 Millones de Euros. https://blog.elhacker.net/2021/10/el-ataque-ransomware-la-uab-universidad-barcelona-pysa.html

El ataque afecto todos los servicios informáticos (hasta la red de WIFI) y estuvo sin servicio por mas de 5 meses. Tuvo que buscar empleados jubilados que conocieran como eran los circuitos en papel para funcionar durante la emergencia. Según palabras del rector volvieron retrocedieron tres décadas.

Vectores de ataque con IA

- Operaciones de Influencia
  - Engaños con imágenes generadas por IA y deepfakes
- Ingeniería Social
  - Phishing
  - Vishing: Voice Cloning-as-a-Service (VCaaS)
- Servicios y colaboración en la Deep Web con IA-como-Servicio
  - Herramientas maliciosas de IA para identificando vulnerabilidades para explotarlas
  - Participantes en estos foros han anunciado chatbots personalizados con IA, diseñados para crear programas maliciosos.

Vectores de ataque con IA

- Engaños con imágenes generadas por IA y deepfakes
  - Caso de uso 1: Actores de amenazas patrocinados por el estado usan imágenes generadas por IA para difundir propaganda en redes sociales.
  - Caso de uso 2: Actores de amenazas utilizan videos deepfake en vivo haciéndose pasar por un ejecutivo para engañar a un empleado de finanzas y hacer que transfiera millones a una cuenta maliciosa.
  - Caso de uso 3: Imágenes generadas por IA aumentan la interacción de los empleados en campañas de phishing.

IA y deepfakes

- Finance worker pays out $25 million after video call with deepfake CFO ‘chief financial officer’, 2/feb/24

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

- Deepfake fraud directed at banks on the rise (june 2024)

https://www.thebanker.com/Deepfake-fraud-directed-at-banks-on-the-rise-1718178559

- How I used deepfakes to bypass security verifications in a bank.

"Deepfake Offensive Toolkit"

https://github.com/sensity-ai/dot

¿Qué es la Criptografía?

- Ciencia de proteger información mediante técnicas matemáticas.
- Cifrado: proceso especifico de codificar la información

Tipos de Criptografía

- Simétrica (clave secreta): AES, 3DES (ejemplo obsoleto).
- Asimétrica (clave pública/privada): RSA, ECC.
- Hashing: SHA, MD5 (ejemplo de obsoleto).

Tipos de criptografia

Criptografía Simétrica (clave secreta)

- Una sola clave compartida entre emisor y receptor. Muy rápida, usada en cifrado de grandes volúmenes de datos.
- DES (Estándar de Cifrado de Datos) desde 1977, 56 bits, obsoleto en los 90
- 3DES (triple DES) NIST estableció obsolescencia en 2023, 112 o 168 bits

- Ejemplos: AES(Advanced Encryption Standard)
  - Longitudes de clave: 128, 192 o 256 bits
  - NIST FIPS 197 (AES).
  - NIST SP 800-57 (Key Management).
- Desafío: distribución segura de la clave

Tipos de criptografia

Criptografía Asimétrica (clave pública/privada)

Par de claves:

- pública para cifrar,
- privada para descifrar
- viceversa en firmas.

Más lenta que la simétrica, resuelve el problema de la distribución de claves.
Ejemplos: RSA, ECC (Elliptic Curve Cryptography).
Ejemplo práctico: intercambio de claves en TLS/HTTPS.

PGP (Pretty Good Privacy).: combina criptografía asimétrica (para intercambio de claves) y simétrica (para cifrar datos), usado en correo electrónico seguro y firma digital.

Tipos de criptografia

Funciones Hash (código de huella digital)

- **MD5 (Message Digest 5), 1992, Ronald Rivest, fue ampliamente utilizado para generar hashes criptográficos.**
- **Sin embargo, actualmente se considera inseguro porque es vulnerable a:**
  - **Colisiones: es posible generar dos entradas diferentes que producen el mismo hash. Esto compromete su uso en firmas digitales, certificados y validación de integridad.**
  - **Ataques de preimagen: aunque más costosos, también se han demostrado factibles, debilitando su resistencia teórica.**
  - **Velocidad de cómputo: su rapidez lo hace inadecuado para almacenamiento de contraseñas, ya que facilita ataques de fuerza bruta y rainbow tables.**
- https://eprint.iacr.org/2004/199

Tipos de criptografia

Funciones Hash (código de huella digital)

Transformación unidireccional de datos en un valor de longitud fija.
Útil para verificar integridad (no para cifrar).

El Instituto Nacional de Estándares y Tecnología (NIST) desaconsejó formalmente el uso de SHA-1 en 2011
En 2017, los principales navegadores web dejaron de aceptar certificados SSL basados en SHA-1

Ejemplos actuales: SHA-2 (SHA-256, SHA-384, SHA-512) o SHA-3

Protocolos Criptográficos en Ciberseguridad

- **TLS/SSL (HTTPS)**

Protege la comunicación entre navegador y servidor.
Combina criptografía asimétrica (para intercambio inicial) y simétrica (para el canal seguro).
Certificados digitales → garantizan la identidad del sitio.

- **VPNs (Redes Privadas Virtuales)**

Túneles seguros sobre Internet.
Usan cifrado simétrico (AES) y autenticación con certificados o credenciales.
Garantizan confidencialidad y privacidad en redes públicas.

Protocolos Criptográficos en Ciberseguridad

- **Firma Digital y PKI**

Basada en criptografía asimétrica.
Garantiza integridad, autenticidad y no repudio.
Ejemplo: firma de documentos PDF, trámites gubernamentales.

- **Autenticación Multifactor (2FA/MFA)**

Combinación de criptografía y protocolos (ej. TOTP/HOTP para códigos temporales).
Mejora la seguridad frente a robo de contraseñas.

Autenticación Multifactor (MFA)

- Método de autenticación que requiere dos o más factores independientes para verificar la identidad del usuario.
- Factores principales:
  - Algo que sabes → contraseña, PIN.
  - Algo que tienes → token, tarjeta inteligente, app móvil.
  - Algo que eres → huella dactilar, reconocimiento facial, iris.

- Objetivo: aumentar la seguridad reduciendo el riesgo de accesos indebidos si una credencial es comprometida.

Técnicas comunes de MFA

- **Contraseña + OTP (One-Time Password):**
  - Código temporal de un solo uso.
  - Puede recibirse por SMS,
  - correo electrónico
  - app autenticadora.
  - Ejemplo: Google Authenticator, Authy.
- **Tokens físicos o llaves de seguridad:**
  - Dispositivos como YubiKey o tarjetas inteligentes (Smart Cards).
  - Usan estándares como FIDO2 / U2F.
- **Push Notifications:**
  - Confirmación desde una app móvil (ej. Microsoft Authenticator, Duo Security)
  - Más simple para el usuario, menos dependiente de SMS.

U2F (Universal 2nd Factor)

- Estándar abierto creado por FIDO Alliance y Google/Yubico (2014) para implementar un segundo factor de autenticación.
- Cómo funciona:
  - El usuario se autentica con su contraseña.S
  - e conecta un dispositivo físico (ej. llave USB o NFC).
  - Usa criptografía de clave pública para validar la identidad.
- Ventajas:
  - Muy resistente a phishing y robo de credenciales.
  - Compatible con navegadores y servicios principales (Google, GitHub).

- Ejemplo: Usuario → contraseña + llave de seguridad (ej. YubiKey).

FIDO2

- Evolución de U2F lanzada en 2018 por FIDO Alliance y W3C.
- Componentes:
  - WebAuthn (Web Authentication API): estándar web que permite a navegadores usar autenticación sin contraseña.
  - CTAP2 (Client to Authenticator Protocol 2): protocolo que permite a llaves de seguridad y dispositivos (ej. smartphones) actuar como autenticadores.
- Características:
- Passwordless: acceso sin necesidad de contraseñas.
  - Uso de biometría, PIN o llaves físicas.
  - Mayor integración en sistemas operativos y navegadores modernos.
- Ejemplo: Iniciar sesión en un sitio → confirmar con huella en el celular o con una llave de seguridad.

Métodos avanzados de MFA

- **Biometría:**
  - Huella dactilar, reconocimiento facial, voz, iris.
  - Combinado con otro factor, aumenta la seguridad.
- **Basado en ubicación o contexto:**
  - Verificación de la geolocalización, dirección IP o dispositivo.
  - Ejemplo: acceso bloqueado si se detecta desde país inusual.
- **Códigos TOTP/HOTP:**
  - TOTP (Time-based One-Time Password): caducan cada 30–60 segundos.
  - HOTO (HMAC-based One-Time Password): cambia con un contador de eventos.
- **Autenticación adaptativa o de riesgo:**
  - El sistema ajusta el nivel de verificación según el riesgo detectado (ej. acceso desde dispositivo nuevo → pide MFA adicional).

Autenticación con OTP

- **HOTP (HMAC-based One-Time Password)**
  - Genera un código único usando un contador (event-based).
  - Cada vez que el usuario solicita acceso, el contador avanza y produce un nuevo código.
  - Ejemplo: tokens físicos clásicos (RSA SecurID).
- **TOTP (Time-based One-Time Password)Variante de HOTP basada en tiempo.**
  - El código cambia automáticamente cada 30 o 60 segundos.
  - Usado por apps como Google Authenticator, Authy, Microsoft Authenticator.
- **Características comunes**
  - Basados en criptografía (HMAC-SHA1/SHA256).
  - Requieren clave compartida (seed) entre el servidor y el generador de códigos.
  - Refuerzan el 2FA/MFA → incluso si la contraseña se filtra, el atacante necesita el OTP.

Criptografia en la vida cotidiana

- **Mensajería (WhatsApp, Signal).**
- **Banca online.**
- **Comercio electrónico.**
- **Blockchain y criptomonedas.**

Criptografia: vulnerabilidades y Ataques

- Fuerza bruta.
- Criptoanálisis (diferencial, lineal).
- Ataques a implementaciones (side-channel, time-based).
- Importancia de usar algoritmos actualizados.

Criptografia: tendencias actuales

- **Criptografía poscuántica**
  - Conjunto de algoritmos criptográficos diseñados para resistir ataques de computadores cuánticos, basados en problemas matemáticos distintos a factorización o logaritmos discretos.
  - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
  - https://ui.adsabs.harvard.edu/abs/2025arXiv250102292H/abstract

- **Homomorphic encryption.**
  - Técnica criptográfica que permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos, preservando la confidencialidad durante el procesamiento.
  - https://dl.acm.org/doi/10.1145/1536414.1536440
  - https://csrc.nist.gov/csrc/media/presentations/2023/stppa6-fhe/images-media/20230725-stppa6-he-fhe--kurt-rohloff.pdf

Criptografia: tendencias actuales

- **Zero-knowledge proofs (ZKP).**
  - Protocolos criptográficos que permiten a un usuario demostrar que posee cierta información sin revelar la información en sí.
  - https://epubs.siam.org/doi/10.1137/0218012
  - **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), key features:
  - izero-knowledge (privacy-preserving),
  - succinct (produces short proofs),
  - non-interactive (no back-and-forth between the prover and verifier), and
  - a form of argument of knowledge.
  - These cryptographic tools are used in applications like the **Zcash cryptocurrency** for private transactions and in **Ethereum's zk-Rollups** for increased scalability.
  - https://isef.net/project/math003-enhancing-ethereums-security-with-lumen
- **Estándares NIST en evolución.**

Criptografia: tendencias actuales

- **Estándares NIST en evolución: incorporación del algoritmo HQC**
- **Em marzo de 2025, el NIST seleccionó el algoritmo HQC (Hamming Quasi-Cyclic) como un mecanismo de encapsulación de clave (KEM) de respaldo para la criptografía post-cuántica, basado en códigos correctores de errores, como alternativa al algoritmo principal ML-KEM (derivado de CRYSTALS-Kyber) NIST+1. Este paso expande el portafolio de algoritmos estándar, incrementando la resiliencia mediante diversidad matemática. El NIST publicara un borrador del estándar HQC para comentarios públicos en 2026, con una versión final proyectada para 2027.**
- **https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption?utm_source=chatgpt.com**

Tipos de Amenazas

- **Malware**: software malicioso diseñado para dañar o acceder sin autorización.
  - *Tipos*: virus, gusanos, troyanos, spyware, adware, rootkits.
  - *Ejemplo*: Stuxnet (2010), malware industrial.
  - Los rootkits se instalan en bajo nivel (sistema operativo o firmware) para ocultar procesos o accesos no autorizados, permitiendo al atacante control persistente y difícil de detectar.
  - ZeroAccess Rootkit (activo entre 2011–2014), que infectaba sistemas Windows para crear **botnets** usadas en minería de criptomonedas y fraudes de clics.
- **Ransomware**: cifra archivos/sistemas y exige rescate en criptomonedas.
  - Evolución a *Ransomware-as-a-Service (RaaS)*.
  - *Ejemplo*: WannaCry (2017), Conti (2021), LockBit (2023).
- **Impacto**: interrupción de servicios críticos (salud, transporte, educación).

Tipos de Amenazas

- **Phishing**: correos o mensajes falsos que buscan credenciales o dinero.
  - Variantes: spear phishing (dirigido), vishing (voz), smishing (SMS).
  - *Ejemplo*: campañas masivas durante COVID-19.
- **Ingeniería Social**: manipulación psicológica para que usuarios entreguen acceso.
  - Estrategias: urgencia, autoridad, curiosidad.
  - *Ejemplo*: ataques al soporte técnico de Twitter (2020).
- **Impacto**: robo de identidad, fraude financiero, acceso inicial en ataques complejos.

Tipos de Amenazas

- **APT (Advanced Persistent Threats)**: grupos estatales o corporativos, ataques prolongados y sofisticados.
  - *Ejemplo*: APT29 (Rusia) en caso SolarWinds (2020).
- **Hacktivismo**: uso político o social de ataques digitales.
  - *Ejemplo*: Anonymous, ataques en contexto Rusia–Ucrania.
- **Cibercrimen organizado**: ransomware gangs, explotación de vulnerabilidades como servicio (**VaaS**).
- **Tendencias recientes**:
  - Uso de **IA generativa** para ataques más creíbles.
  - Ataques a **cadena de suministro**.
  - Ciberespionaje y ciberarmas en conflictos internacionales.

Vulnerabilidades en software y hardware

Software: errores de programación

- **Buffer Overflow → escribir fuera de los límites de memoria; puede ejecutar código arbitrario.**
  - Ejemplo: gusano Morris (1988), exploit de Blaster (2003).
- **Inyecciones SQL → manipulación de consultas a bases de datos mediante entradas no validadas.**
  - Ejemplo: robo masivo de datos en Heartland Payment Systems (2009).
  - https://www.infoteknico.com/heartland/
- **Cross-Site Scripting (XSS) → inyección de scripts en páginas web para robar cookies o credenciales.**
  - Ejemplo: vulnerabilidades recurrentes en foros y CMS.

Vulnerabilidades en hardware

- **Meltdown (2018):** procesadores Intel (y algunos ARM) que permitía a un programa leer memoria del kernel u otros procesos.
  - Cómo funciona: Aprovecha la ejecución especulativa y la falta de aislamiento estricto entre memoria de usuario y memoria privilegiada.
  - Impacto: Filtración de contraseñas, claves de cifrado o cualquier dato sensible almacenado en memoria.
  - Mitigación: Actualizaciones de microcódigo, parches en sistemas operativos (kernel page table isolation – KPTI).
- **Spectre (2018):** más general, afecta procesadores Intel, AMD y ARM.
  - Cómo funciona: Engaña al predictor de saltos de la CPU para ejecutar instrucciones especulativas que acceden a memoria no autorizada.
  - Impacto: Exposición de datos entre procesos aislados → rompe la idea de “sandboxing” en navegadores y máquinas virtuales.
  - Mitigación: Cambios en compiladores (inserción de retpolines), actualizaciones de microcódigo y rediseño en hardware.