

# LA CIBERSEGURIDAD EN EL ÁMBITO EDUCATIVO



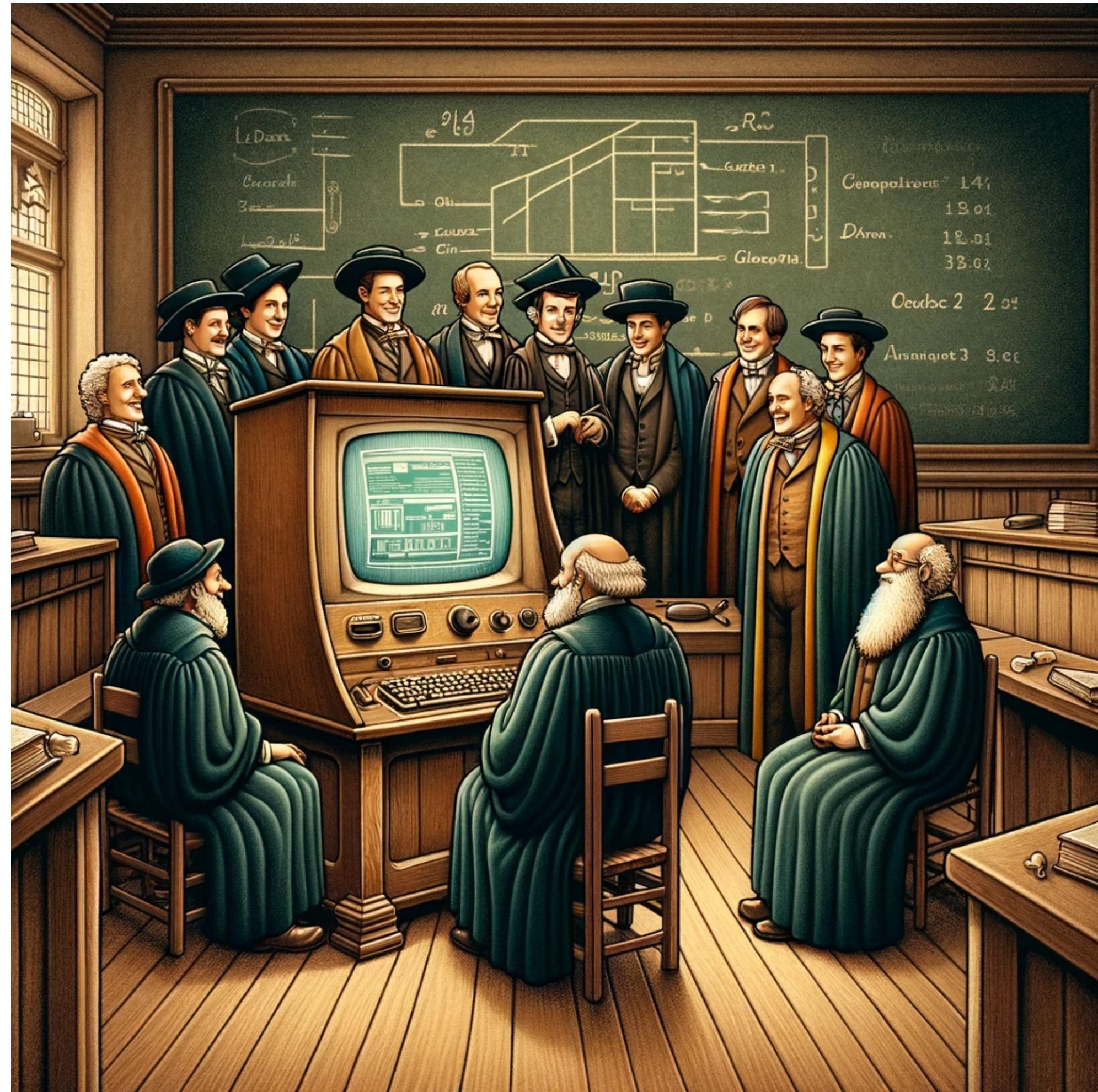
# INTRODUCCIÓN A LA CIBERSEGURIDAD



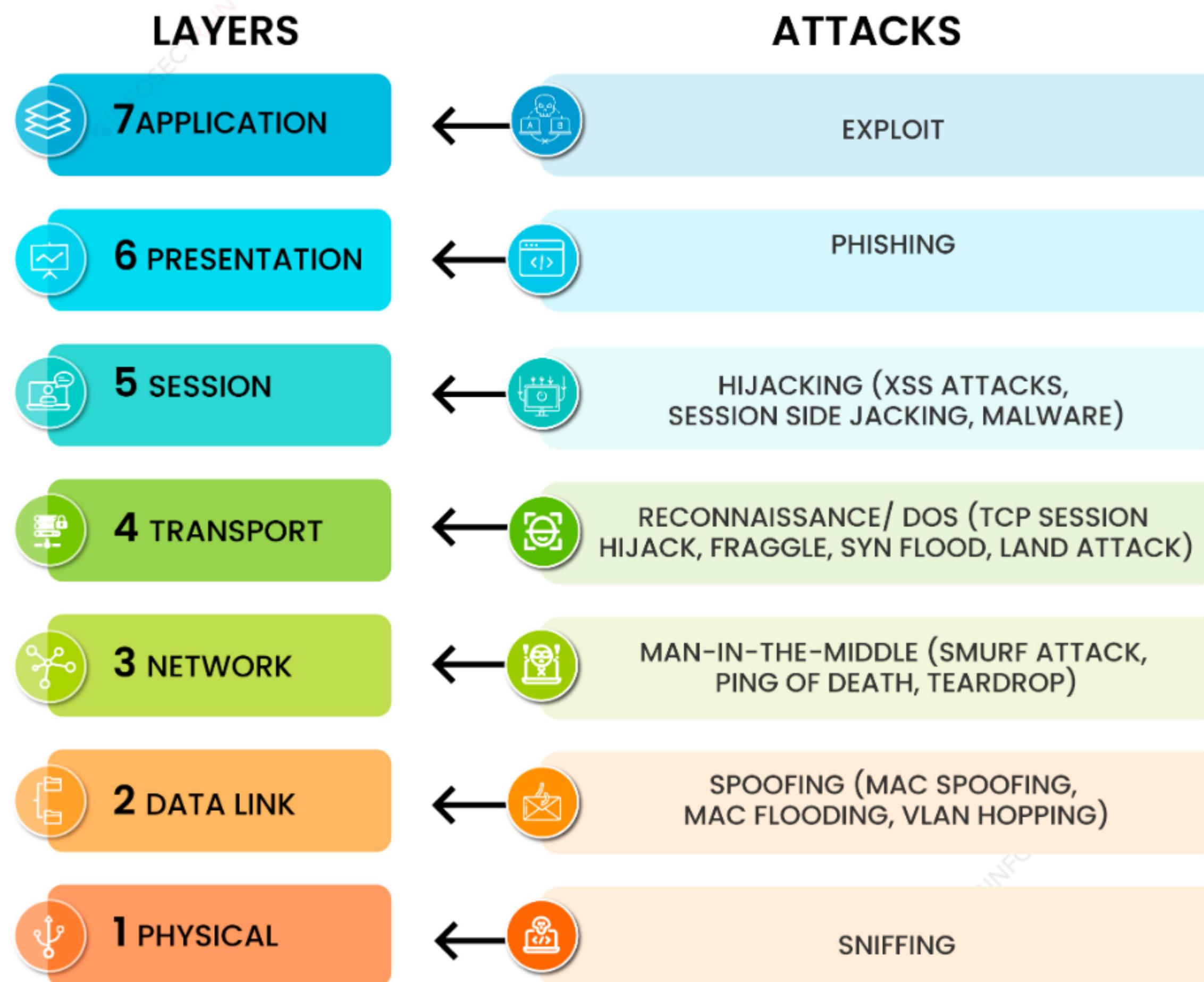
# TRIADA CIA



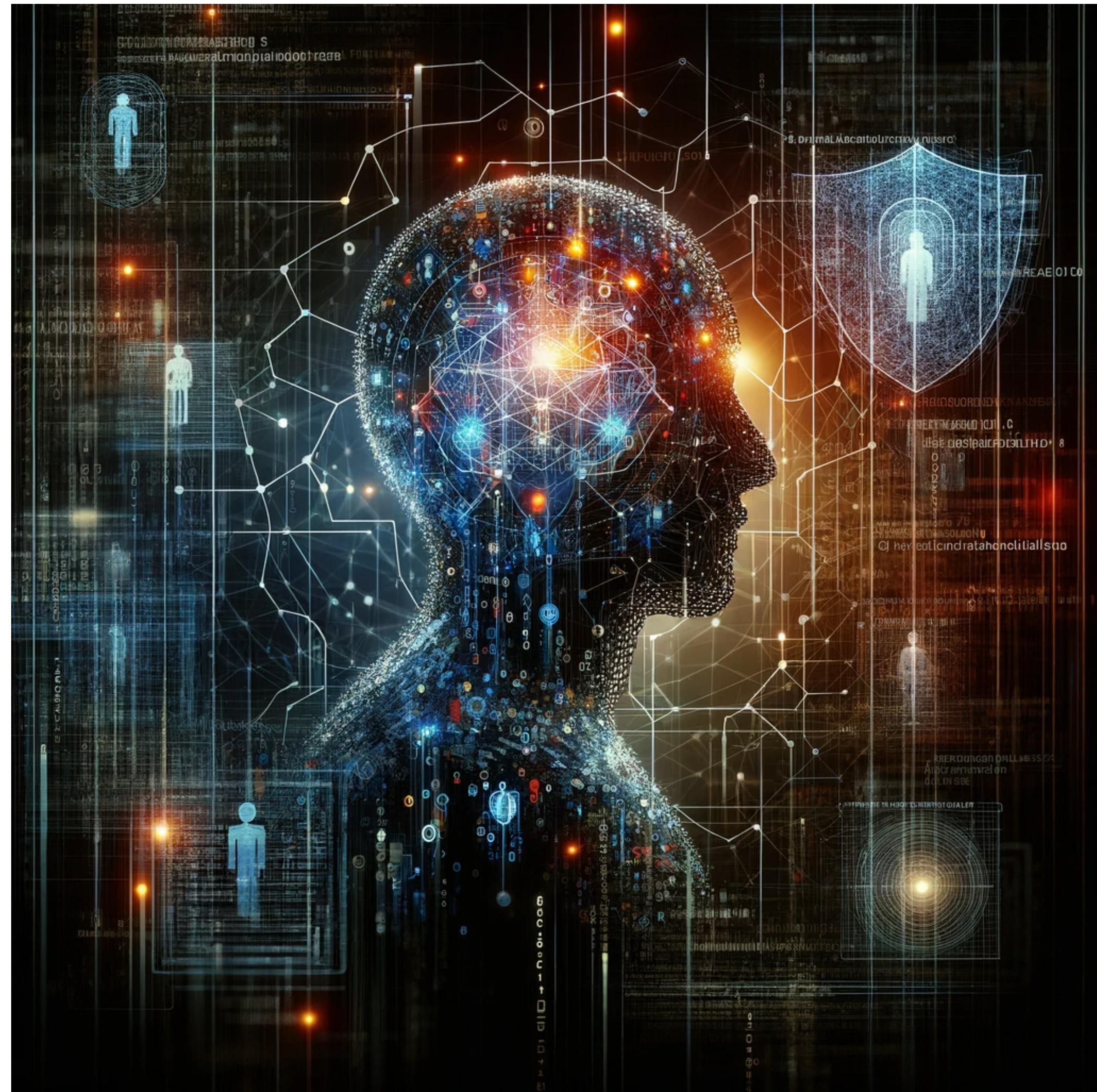
# INTERNET FUE DISEÑADA POR CABALLEROS Y PARA CABALLEROS



# ATAQUES COMUNES EN LAS CAPAS DEL MODELO OSI



# EL DESAFÍO DE CAPA 8



Capa 8: El Escollo Humano.

Psicología: Punto de Ataque.

Sin Solución Única.

Fortaleciendo Defensas.

## **PELIGROS MÁS COMUNES**

Robo de credenciales

Engaños y suplantaciones de identidad (phishing)

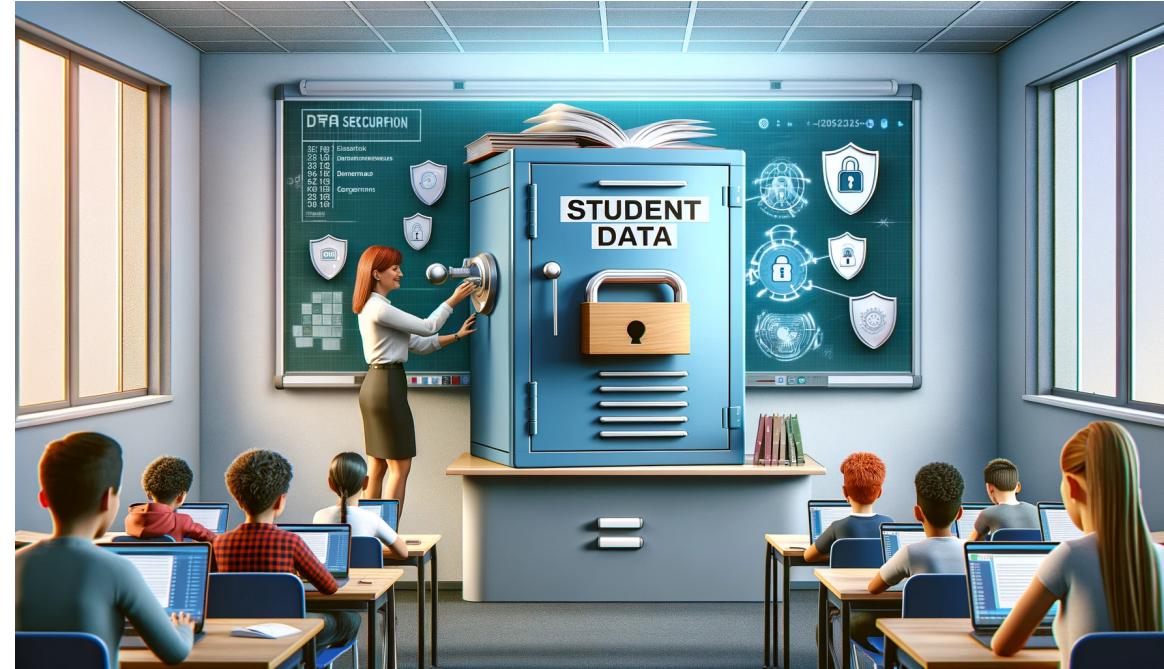
Pérdida o filtrado de información

Medios falibles

# MIS DATOS, MI TESORO



# SUS DATOS, TU RESPONSABILIDAD



Deshabilitar la función de autoarranque de dispositivos USB

¿Dónde están los datos de mi alumnado?

¿Puedo usar cualquier aplicación libremente?

¿Quién tiene la responsabilidad?

# ESTRATEGIA DE DEFENSA EN PROFUNDIDAD



Múltiples Capas de Seguridad.

Prevención y Detección Combinadas.

Reducción de Riesgos.

Adaptabilidad y Resiliencia.

# GUÍA DE SUPERVIVENCIA: NAVEGANDO CON SEGURIDAD



Crear juntos una guía práctica y realista.

Aprenderemos a protegernos en el mundo digital.

No hay que temer, ¡estamos preparados!

# RESGUARDANDO TU PRIVACIDAD



# CUANDO LOS USB SE VUELVEN CONTRA NOSOTROS



Daño físico: "USBs pueden quemar equipos".

Malware oculto: "Riesgo de virus y spyware".

Robo de datos: "Extracción silenciosa de info".

Acceso no autorizado: "Permiten hackeos remotos".

Infiltración de red: "Puerta trasera a sistemas".

# EL PATO EN ACCIÓN: DEMOSTRANDO LA SEGURIDAD USB"



Desconfiar y no conectar a nuestros equipos dispositivos encontrados en espacios públicos o de origen desconocido.

Disponer de un antivirus activo y debidamente actualizado.

# DESHABILITAR LA FUNCIÓN DE AUTOARRANQUE DE DISPOSITIVOS USB

The screenshot shows the Windows Settings interface. On the left, a sidebar lists various device categories: Inicio, Buscar una configuración, Dispositivos, Bluetooth y otros dispositivos, Impresoras y escáneres, Mouse, Panel táctil, Escritura, Lápiz y Windows Ink, Reproducción automática (which is selected and highlighted in orange), and USB. A large hand cursor icon is positioned over the USB item. At the bottom, there's a search bar with the placeholder "Escribe aquí para buscar".

**Reproducción automática**

Usar la reproducción automática para todos los medios y dispositivos

Desactivado

Elegir valores predeterminados de reproducción automática

Unidad extraible: Elegir un valor predeterminado

Tarjeta de memoria: Elegir un valor predeterminado

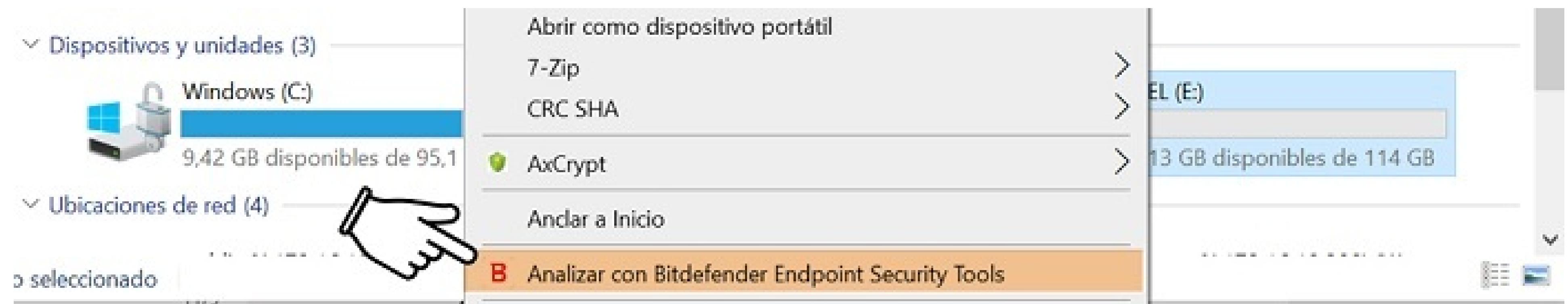
Opciones de configuración relacionadas: Configuración de aplicaciones predeterminadas

¿Tienes alguna pregunta? Obtener ayuda

Ayúdanos a mejorar Windows Envíanos tus comentarios

Una vez conectado, haremos clic derecho sobre él.

Luego, haremos clic sobre “Analizar con...”



# EL PODER DEL CIFRADO: PROTEGIENDO NUESTROS DATOS



Cifrado de archivos y carpetas.

Cifrado de un disco duro.

Cifrado de un dispositivos USB.

Cifrado de un dispositivo Android.

# DEMO



# EL RIESGO DEL SÍNDROME DE DIÓGENES DIGITAL



Evitar instalaciones innecesarias: seguridad y eficiencia.

Cada app extra es un riesgo potencial.

Priorizar herramientas esenciales.

Revisión periódica de aplicaciones en uso.

# ACTUALIZACIONES: ESCUDO DIGITAL



Actualizar = Proteger.

Evitar **vulnerabilidades conocidas**.

# LA REGLA 3, 2, 1: PLAN DE RESPALDO INFALIBLE



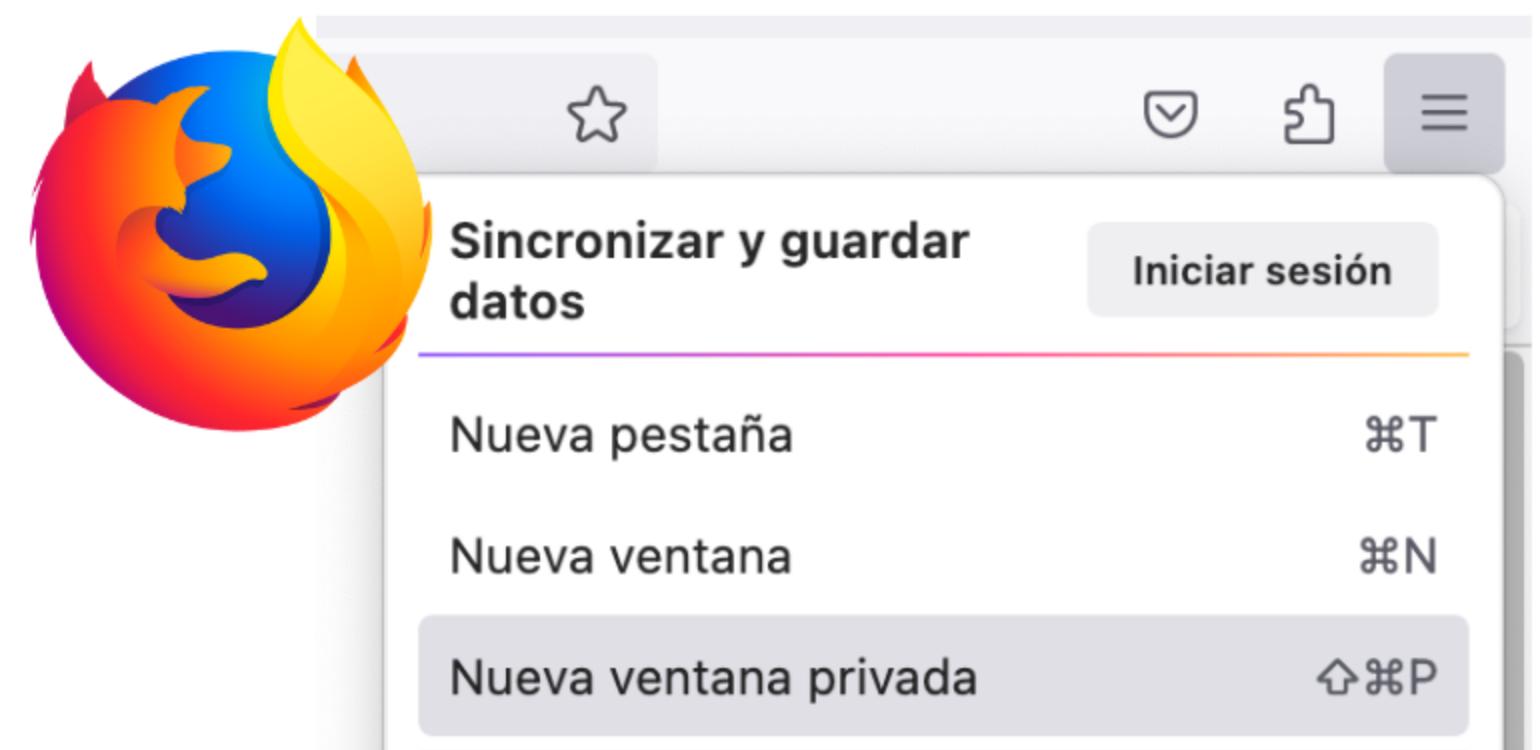
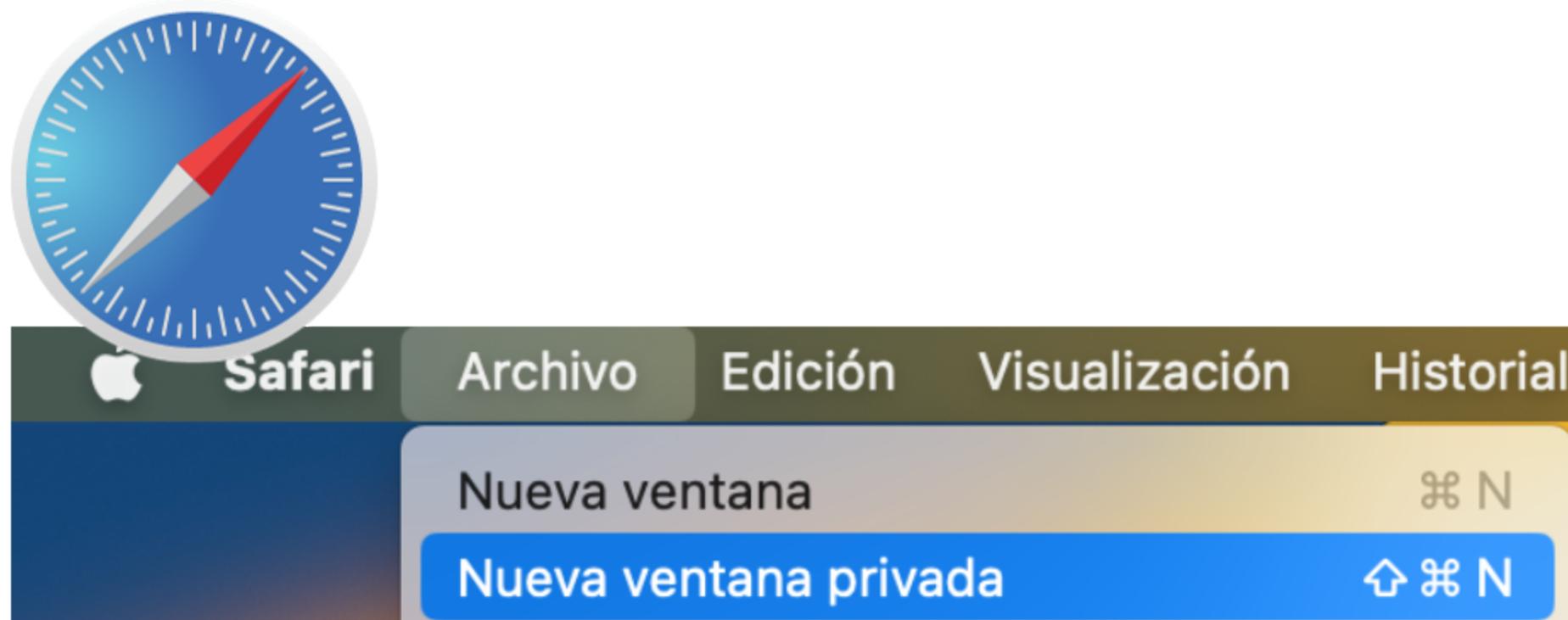
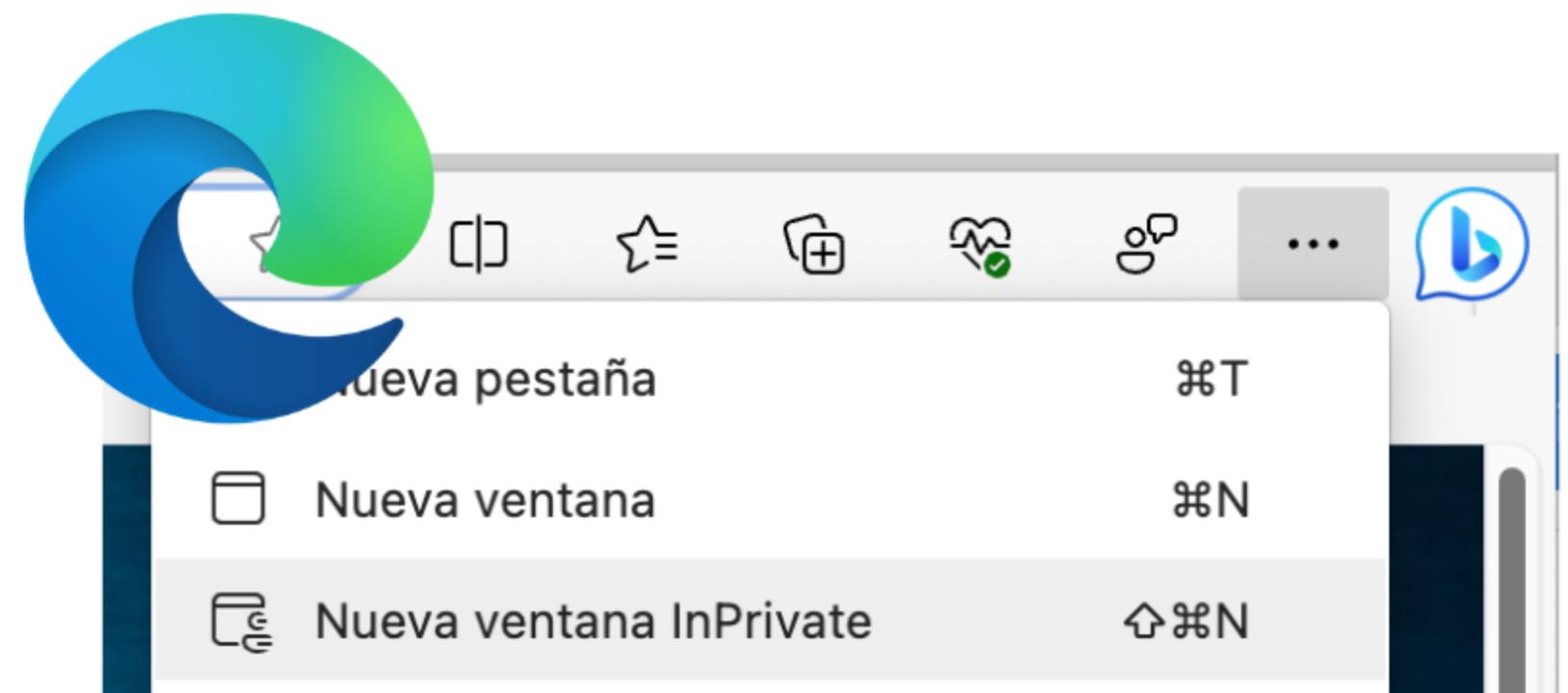
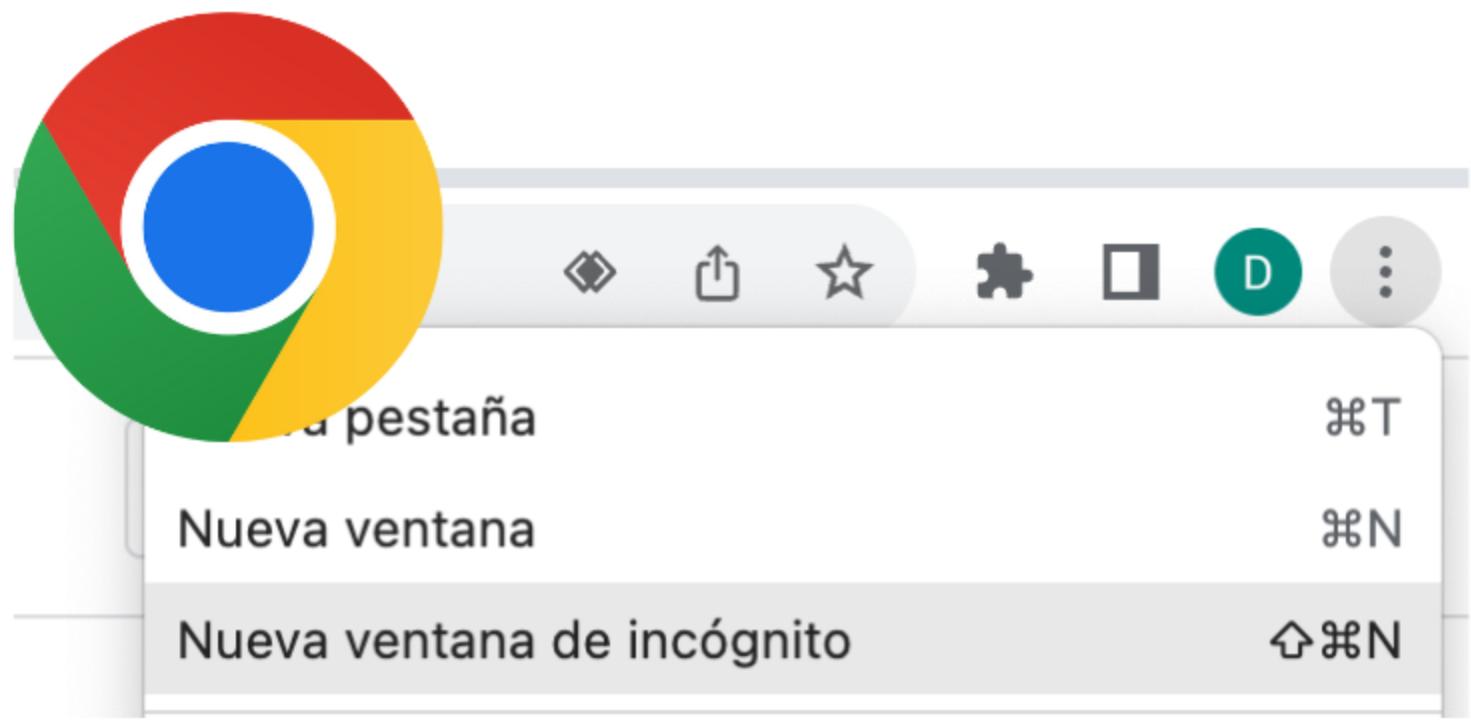
# NAVEGACIÓN PRIVADA



Evita dejar huellas digitales en PCs compartidos.

Protege tus credenciales en navegación pública.

La navegación privada no guarda historial ni  
cookies.



# GUARDIANES DE CONTRASEÑAS SEGURAS



# LA PRIMERA LÍNEA DE DEFENSA



Esenciales para la seguridad en línea.

Protegen información personal y profesional.

Son la clave de acceso a nuestros datos.

# CONSTRUYENDO MUROS ROBUSTOS



Criterios: Larga, compleja, única.

El riesgo de lo predecible

La regla de oro: diversificar

Herramientas para crear contraseñas seguras.

# TU COFRE FORTE DIGITAL



La paradoja de la complejidad.

¿Qué es un gestor de contraseñas?.

Demostración práctica de uso.

Recomendaciones de gestores populares.

# MÁS ALLÁ DE LA CONTRASEÑA

Importancia del MFA.

Cambiar contraseñas regularmente.

# COMUNICACIÓN SEGURA: CORREO ELECTRÓNICO



# BLINDANDO TU BUZÓN: FILTROS ANTISPAM



# DETECTIVE DIGITAL: IDENTIFICANDO PHISHING



# FORTALEZA DE CIFRADO: SEGURIDAD EN CORREOS



El poder del cifrado de correos electrónicos.

Cómo y por qué cifrar tus comunicaciones.

Herramientas prácticas para cifrado.

Para añadir una capa adicional de privacidad y asegurar que solo tú y el destinatario pueden leer el contenido de tus correos electrónicos:

Pretty Good Privacy (PGP).

Servicios de Correo Electrónico con Cifrado de Extremo a Extremo: ProtonMail.

# DOBLE BARRERA: AUTENTICACIÓN DE DOS FACTORES



# ¿DUDAS?

