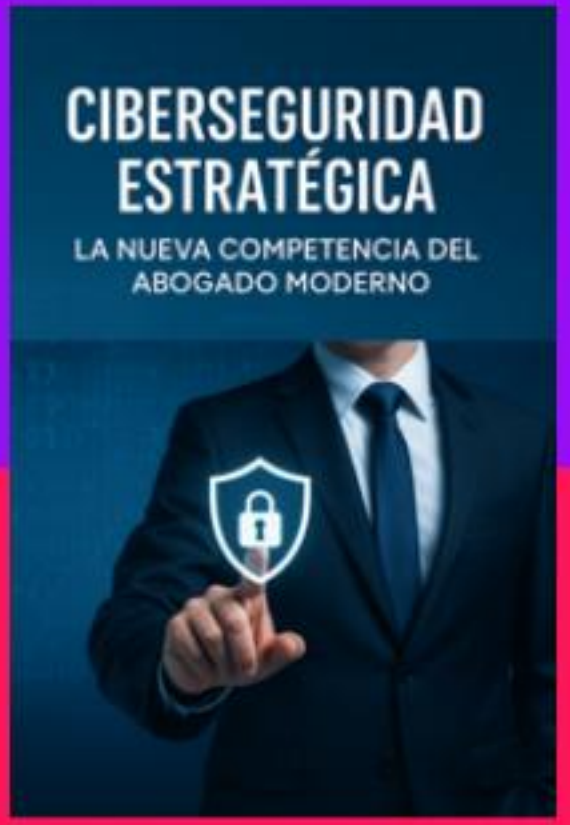
CIBERSO

AEF
ASOCIACIÓN ESPAÑOLA DE LA FRANQUICIA

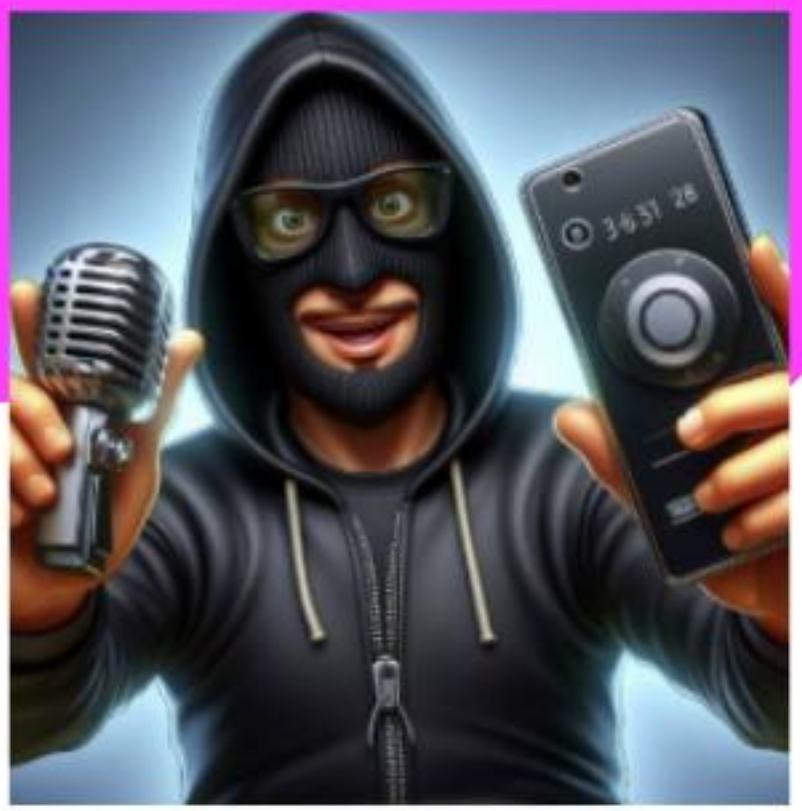
Ciber Newsletter - JUNIO 2025



🗓️ 26 de Junio de 2025
⏰ De 12:00 a 14:00 horas
📍 Espacio CIBERSO (Santa Leonor 65, Edificio C, Planta 4, 28037 Madrid)

📍 **Formato:** Charlas profesionales + debate + aperitivo. Presencial/online
🎯 **Dirigido a:** Socios de despachos, abogados de empresa, asesores de cumplimiento y responsables de relaciones con clientes.

🧠 Concienciación



⚠️¿Qué es el Voice Hacking y cómo protegerte?

La piratería de voz o voice hacking es una técnica donde atacantes imitan tu voz (con grabaciones o inteligencia artificial) para suplantar tu identidad. Esto puede usarse para fraudes, manipular asistentes virtuales o vulnerar sistemas de autenticación.🔐 7 Consejos para proteger tu voz:

1️⃣ Evita la autenticación por voz en servicios sensibles

Usa autenticación multifactor (MFA): combina algo que tienes (token, app) y algo que sabes (contraseña), no solo lo que eres (voz).

2️⃣ Controla lo que compartes públicamente

Limita la cantidad de audios/videos con tu voz en redes. Pueden ser usados para clonar tu voz con IA.

3️⃣ Usa frases aleatorias para autenticarte

Evita frases fijas como “Mi voz es mi contraseña”. Prefiere frases dinámicas y únicas para hacer más difícil la suplantación.

4️⃣ Activa alertas de actividad sospechosa

Configura notificaciones en servicios bancarios, apps o correos electrónicos para detectar movimientos inusuales.

5️⃣ Cuida tu entorno físico

Asistentes como Alexa o Google Assistant no deberían estar siempre activos ni al alcance de cualquiera.

6️⃣ Utiliza software anti-deepfake de voz

Algunas soluciones de ciberseguridad ya detectan voces sintéticas con análisis acústico avanzado.

7️⃣ Educa a tu entorno cercano

Familia y colegas deben estar alertas a posibles fraudes por voz clonada. Ejemplo típico: “Mamá, necesito dinero urgentemente...”

🔐 Prevención

📶 SIMULACRO PROTOCOLO CIMA

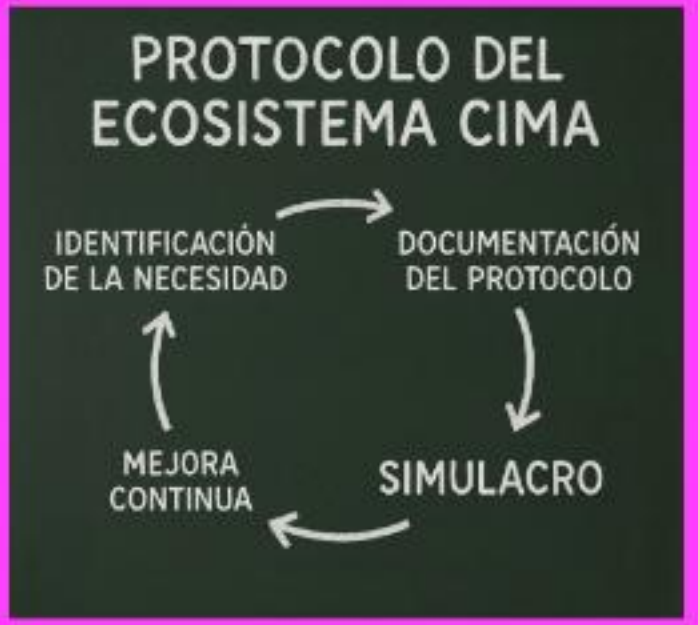
Una Estos espacios controlados nos permiten:

- Practicar la toma de decisiones bajo presión.
- Evaluar la eficacia de nuestros canales de comunicación interna y externa.
- Mejorar la coordinación entre equipos clave.
- Entrenar la gestión del estrés y capacidad de reacción en situaciones críticas.
- Identificar oportunidades de mejora, fortalecer nuestra cultura preventiva.

Más allá de validar nuestros planes de continuidad, protocolos y gestión de crisis, estos ejercicios fomentan una cultura organizacional más consciente, ágil y preparada para lo inesperado.

💡 La prevención no se improvisa. Se entrena.

Cada simulacro es una oportunidad para construir organizaciones más seguras, responsables y sostenibles.



🌍 Actualidad

Adidas fue un ciberincidente a través de un proveedor externo de atención al cliente

A finales de mayo de 2025, Adidas sufrió una brecha de datos causada por un proveedor externo de atención al cliente. El incidente expuso información personal de algunos usuarios que habían contactado con el soporte, incluyendo nombre, correo electrónico, teléfono, género, fecha de nacimiento y posiblemente dirección, aunque no se vieron comprometidas contraseñas ni datos financieros. Adidas contuvo rápidamente el incidente, notificó a los afectados y reforzó la seguridad en su cadena de suministro para evitar futuras vulnerabilidades similares.

📌 **Detalles clave del incidente**

- **Fecha del anuncio**: 23 de mayo de 2025
- **Tipo de ataque**: brecha en un **proveedor tercero de atención al cliente**, no un hackeo directo a los sistemas de Adidas.
- **Datos comprometidos**: nombres, correos electrónicos, teléfonos, género, fecha de nacimiento y posiblemente direcciones postales de clientes que habían contactado al help desk.
- **Lo que NO se vulneró**: ni contraseñas, ni datos financieros o de tarjetas.

✔️ **Recomendaciones para clientes**

- Revisa tu correo y teléfono por si recibes notificaciones oficiales.
- Mantente alerta ante posibles intentos de phishing.
- Verifica siempre enlaces y contactos oficiales de Adidas.
- Infórmate sobre cómo protegerte de las brechas de datos.

🌍 Actualidad internacional

🕵️‍♂️💸 La pandilla de cibermalos LockBit, "avergonzada" por el ciberataque a una escuela

En una insólita muestra de “código ético” delictual, el grupo de ransomware LockBit ofreció de forma gratuita una clave de descifrado tras descubrir que uno de sus afiliados había atacado al Distrito Escolar 16 de Olympia, Illinois, el 26 de febrero de 2023. Publicaron disculpas públicas declarando sentirse “muy avergonzados” por haber afectado a “niños pequeños e inocentes” y revelaron que eliminaron los datos robados para colaborar en su recuperación.

LockBit afirmó haber expulsado a ese afiliado de su red y recalcó que, a pesar de ser un RaaS, mantiene “líneas rojas” incluso en el mundo clandestino.

Esta noticia nos recuerda que incluso en los rincones más oscuros del cibercrimen aún pueden existir vestigios de conciencia.
Que un grupo como LockBit —dedicado al ransomware y normalmente motivado por el lucro— se disculpe públicamente y libere una clave de descifrado tras afectar a una escuela, nos deja una paradoja incómoda: hasta los ciberdelincuentes establecen sus “líneas rojas”.

Pero no deberíamos romantizar esta acción. No se trata de ética real, sino de reputación y control del negocio.

El verdadero problema es que un sistema educativo —que debería ser intocable— esté tan expuesto a amenazas digitales. La reflexión más profunda no es si los delincuentes sienten vergüenza, sino por qué seguimos sin proteger como sociedad lo que más deberíamos cuidar: a los más vulnerables.

www.ciberso.com
info@ciberso.com
CIBERSO
+34 681 28 60 02