Webinar Gratuito

Secretos para una Presentación Exitosa de Ciberseguridad

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 12 Agosto 2026

Alonso Eduardo Caballero Quezada

Cuento con más de diecinueve años de experiencia en el área y desde hace quince años me especializo en la áreas de Hacking, Forense, OSINT, Ciberseguridad y temas relacionados.

https://www.linkedin.com/in/alonsocaballeroquezada/

https://x.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

https://wa.me/51949304030

https://t.me/ReYDeS

Introducción

El problema central

- La brecha entre el hallazgo técnico/forense y la toma de decisiones ejecutivas

El enfoque

- Estrategias, diseño visual, y persuasión aplicados a la ciberseguridad

Objetivo

- Aprender a comunicar el valor de la ciberseguridad para influir positivamente en la junta directiva y clientes

Mapeo de Audiencia: ¿A quién le estás hablando?

Comprensión de los perfiles

- CISO, CFO, CEO, auditores, y equipos de operaciones de TI

Mapeo de prioridades

- Alineación de métricas de ciberseguridad con riesgos de negocio, continuidad operativa, y cumplimiento

Anticipación de objeciones

- La técnica de investigación previa para reducir la resistencia al cambio o la negación de presupuesto

Jerarquía de la Información: Principio BLUF

Inversión de la narrativa tradicional

- Entregar el resultado, la consecuencia, y el costo en los primeros segundos

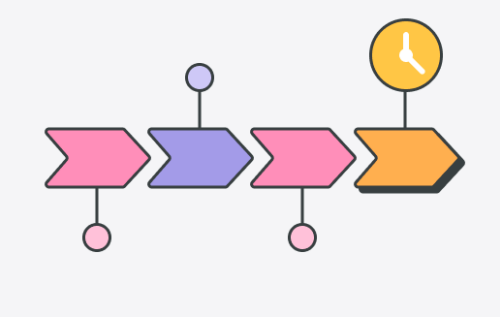
La fórmula BLUF aplicada

Como evitar la audiencia pierda el foco navegando entre datos sin procesar

Narración en Ciberseguridad: Del Caos a Solución

Utilizar líneas de tiempo visuales (Cronologías) para relatar intrusiones o auditorías sin causar pánico.

Los 3 actos del discurso de seguridad:



- **Contexto:** El estado del activo/negocio
- **Conflicto:** El vector de ataque o la vulnerabilidad crítica
- **Resolución:** El plan para remediación y el ROI en ciberseguridad

Eliminación del Desorden y Rediseño Visual

Estado Inicial (El "Antes")

Párrafos densos, capturas de pantalla de terminal ilegibles, y múltiples colores sin jerarquía.

Resultado (El "Después")

Visualización clara de la diferencia en la carga cognitiva de la audiencia

REPORTE DE AUDITORÍA Y VULNERABILIDADES DE SEGURIDAD NVI-2026-08

Resumen ejecutivo de la evaluación de vulnerabilidades realizada en el servidor de pagos central: Durante la última evaluación de postura de seguridad realizada en la infraestructura crítica, el equipo de auditoría identificó múltiples vectores de riesgo operacional asociados a servicios desactualizados y expuestos en la red corporativa interna sin segmentación adecuada.

Detalle técnico de la falla identificada: Se detectó la presencia de la vulnerabilidad CVE-2026-3829 en el servicio LDAP expuesto, la cual permite la ejecución remota de código (RCE) sin autenticación previa mediante el envío de paquetes malformados construidos específicamente para desbordar la memoria del proceso principal.

```
root@sec-srv:~# nmap -sV -p 389,636 192.168.1.105
Starting Nmap 7.94 ( https://nmap.org ) at 2026-08-06 14:22 EST
Nmap scan report for 192.168.1.105
PORT    STATE SERVICE VERSION
389/tcp open  ldap    OpenLDAP 2.4.44 (Vulnerable RCE CVE-2026-3829)
636/tcp open  ssl/ldap OpenLDAP 2.4.44
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Impacto potencial en la continuidad del negocio: La explotación exitosa de esta falla por parte de un actor malicioso interno o externo con acceso al segmento de red permitiría la toma de control total del servidor de base de datos de transacciones, provocando la denegación total del servicio de pagos en línea.

Métricas de riesgo evaluadas: CVSS v3.1 Base Score: 9.8 (CRITICAL) / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Recomendación y plan de mitigación: Aplicar la actualización de seguridad correspondiente al paquete openldap a la versión 2.4.58 o superior inmediatamente, interrumpiendo el servicio durante una ventana de mantenimiento estimada de 45 minutos.

Acción requerida: Aprobar parche crítico para evitar detención del sistema de pagos

IMPACTO DE RIESGO ESTIMADO	ESTADO DE LA VULNERABILIDAD
$50,000 / hora	CVSS 9.8
(Pérdida operativa proyectada)	(Crítica - Control total del servidor)

Vulnerabilidad: Permite acceso root y control total del servidor de pagos.

Solución: Parche listo para instalación (Tiempo de aplicación: 45 min en ventana nocturna).

Principios de Diseño Visual para Reportes

Reducción del "ruido visual"

- Líneas de cuadrícula innecesarias, diagramas de red excesivamente complejos, y textos extensos.

Uso intencional del color

- Limitar la paleta cromática para señalar urgencia y estado (por ejemplo Semáforo de Riesgo)

Sustitución de listas de viñetas

- Por gráficos explicativos simples

Traducir Severidad CVSS a Métricas de Negocio

El error de presentar hallazgos únicamente como CVSS 9.8 o vulnerabilidades sin contexto.

Mapeo de impacto: Transformar datos técnicos en horas de inactividad, costos de recuperación, o multas regulatorias.

Definición de métricas de referencia (Baseline Metrics) para demostrar el progreso del programa de ciberseguridad.

Ejecución de un “Pitch” breve

Ejercicio de simulación de rol y voz frente a la audiencia.

Simulación: Se presenta de forma oral un reporte sobre un hallazgo crítico en la infraestructura interna dirigiéndose hipotéticamente al CFO.

Técnicas en Acción: Uso de voz activa, control de pausas, lenguaje corporal y aplicación estricta de la regla BLUF, sin apoyo de diapositivas densas.

Desglose Post-Pitch: Análisis de los 3 minutos sobre como se manejó la urgencia y el tono de autoridad.

Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Tono, Presencia Escénica, y Gestión de Resistencia

Control de muletillas y la importancia de los silencios estratégicos.

Lenguaje no verbal en presentaciones presenciales y virtuales (encuadre, contacto visual con la cámara).

Cómo responder a interrupciones, preguntas hostiles, o cuestionamientos sobre el retorno de inversión (ROI).

Checklist del Presentador de Ciberseguridad

Lista de verificación antes de cada presentación:

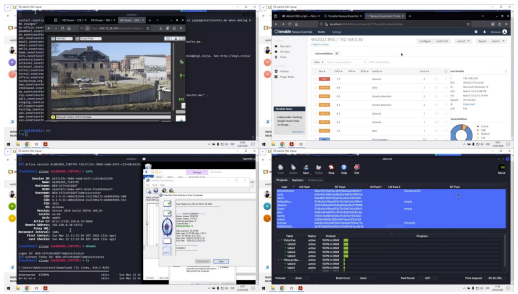
- ¿Está clara la recomendación desde la primera diapositiva (BLUF)?
- ¿Se redujeron los diagramas/textos saturados?
- ¿Las métricas reflejan el riesgo de negocio y no únicamente métricas técnicas aisladas?

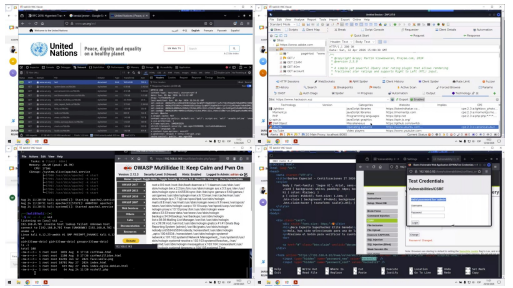
Conclusión y cierre con la llamada a la acción

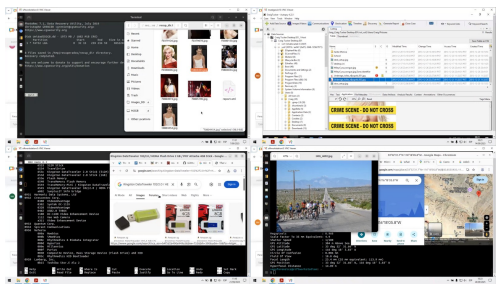
Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

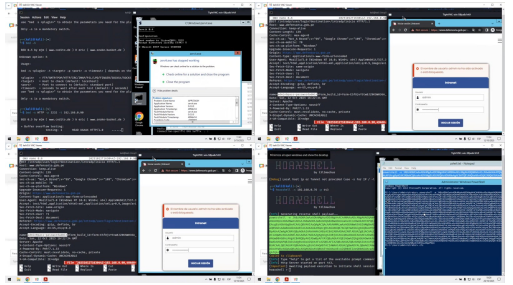
Cursos (Aula Virtual)

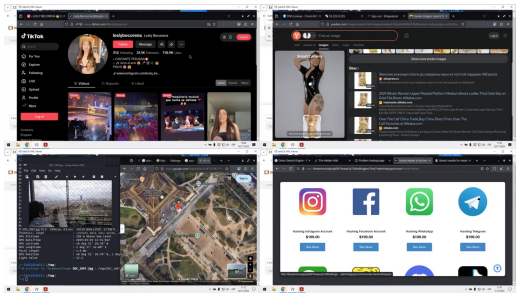
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego Graph CE
- Y más...

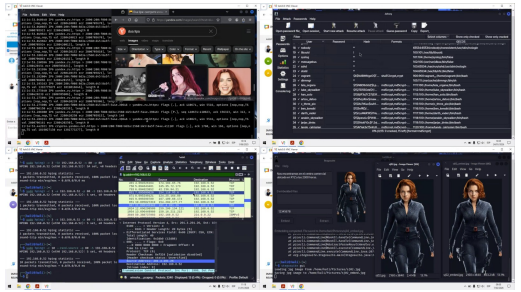












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Secretos para una Presentación Exitosa de Ciberseguridad

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 12 Agosto 2026