Webinar Gratuito

Redacción en Ciberseguridad Cautivar al Lector

Alonso Eduardo Caballero Quezada

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

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

Miércoles 5 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

Transmutando hallazgos técnicos en decisiones estratégicas

- El costo invisible de un mal reporte de ciberseguridad
- La meta: Aplicar técnicas de redacción defensiva e ingeniería de texto para persuadir tanto a profesionales técnicos cuanto a los ejecutivos.

El Principio BLUF (Bottom Line Up Front)

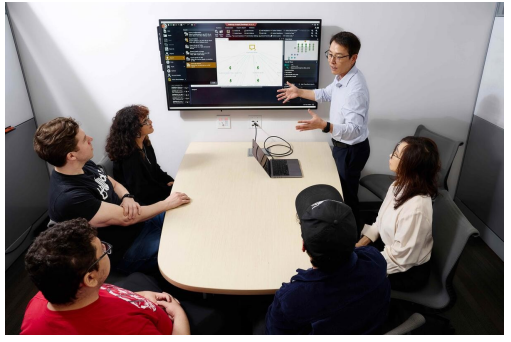
- **¿Qué es BLUF?:** Colocar la conclusión, el riesgo, y la recomendación principal en las primeras dos oraciones.
- **Por que los reportes tradicionales fallan:** El enfoque académico (Introducción → Metodología → Resultados) frustra a quienes toman decisiones.
- **El triángulo de atención:**
  - Ejecutivos: Quieren saber el impacto financiero/operativo de inmediato
  - Gerentes: Quieren saber el alcance y los recursos necesarios
  - Analistas: Quieren el detalle técnico y la prueba de concepto (PoC)

Mapeo de Audiencia y Segmentación

Perfilado del lector:

- C-Level / Board: Riesgo de negocio, cumplimiento, costo de inacción
- Líderes de TI / DevOps: Ventanas de mantenimiento, prioridad de parches, compatibilidad
- Equipos Red/Blue: Exploitabilidad, vectores de ataque, IOCs

Regla de oro: No utilizar la misma sección para diferentes audiencias; se sugiere modularizar tu reporte.



Estructura Modular de un Informe Técnico

- Resumen Ejecutivo: Independiente del resto del documento (máximo 1 página)
- Matriz de Riesgo: Severidad basada en CVSS/EPSS ajustada al contexto del negocio
- Cuerpo Técnico:
  - Descripción clara de la vulnerabilidad
  - Evidencia (pantallazos legibles, logs sanitizados)
  - Impacto real comprobado
  - Remedación específica (no genérica)

Claridad Técnica: Voz Activa y Concisión

Voz Pasiva vs. Voz Activa:

- Incorrecto (Pasivo/Ambiguo): "Fue detectado un acceso no autorizado en el servidor..."
- Correcto (Activo/Directo): "El ciberatacante explotó una vulnerabilidad RCE en el servidor Apache..."

Eliminación de "Paja" (Fluff):

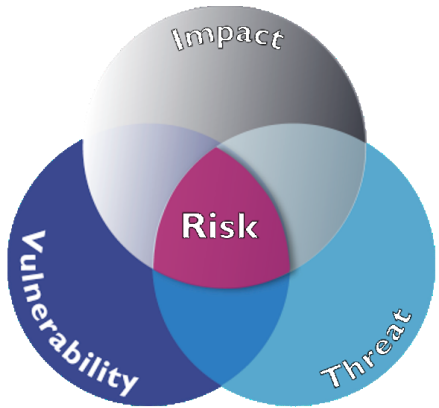
- Evitar adjetivos dramáticos ("catastrófico", "terrible"). Utilizar métricas objetivas
- Sustituir frases redundantes por verbos de acción

Comunicación del Riesgo e Impacto

CVSS no es Riesgo: CVSS mide severidad técnica; el riesgo mide impacto en el negocio

Fórmula simplificada de redacción de impacto:

Riesgo = Amenaza x Vulnerabilidad x Impacto en el Negocio



Sustitución de jerga por consecuencias operativas:

- En lugar de "Inyección SQL en /login.php", escribir "Acceso directo sin contraseña hacia la base de datos de clientes"

Formato Visual, Tipografía y Legibilidad

Jerarquía visual: Uso correcto de encabezados o cabeceras (H1, H2, H3), listas, y negritas.

El arte del Snippet de Código:

- No incluyas capturas de pantalla de terminales gigantescas con fondo negro si vas a imprimir o generar un archivo en formato PDF
- Utilizar sintaxis resaltada y sanitiza datos sensibles (tokens, direcciones IP internas).

Tablas de Remedación: Estado, Prioridad, Esfuerzo estimado, Responsable.

Flujo de Edición y Control de Calidad (Peer Review)

La regla de los dos pares de ojos: Nunca enviar un reporte sin revisión técnica y editorial previa.

Checklist de autocorrección:

- ¿El Resumen Ejecutivo se entiende sin leer el resto del reporte?
- ¿Todas las siglas están definidas la primera vez de su aparición?
- ¿Las recomendaciones asignan claramente un responsable o área?

Herramientas de apoyo: Integración de CI/CD para validar documentación técnica.

Resumen y Checklist de Publicación

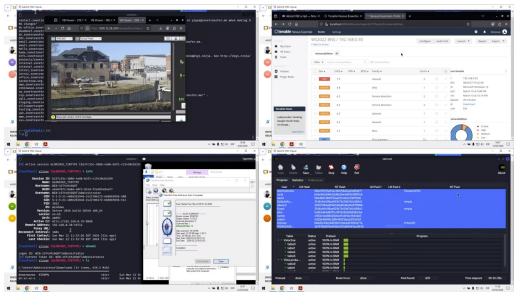
Los 4 pilares de Hack the Reader:

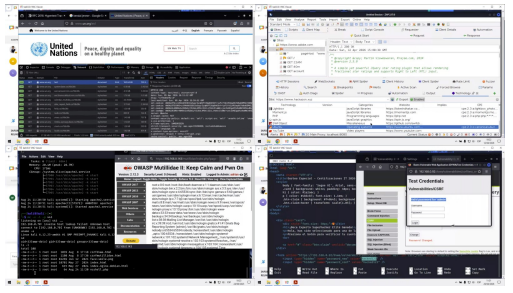
- BLUF: La conclusión siempre va al inicio
- Contexto de Negocio: Severidad técnica no es igual al riesgo para la empresa
- Claridad: Voz activa, párrafos cortos, y eliminación de adjetivos innecesarios
- Formato Impecable: Limpieza visual y automatización del flujo de trabajo

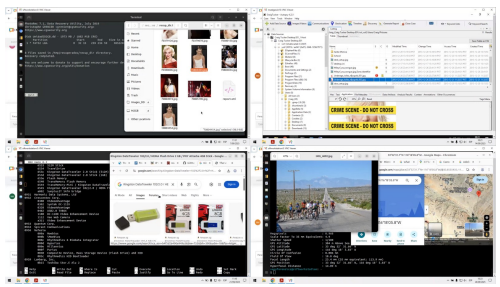
Acción inmediata: Aplica la reescritura de 3 líneas en tu próximo correo electrónico o reporte de incidentes.

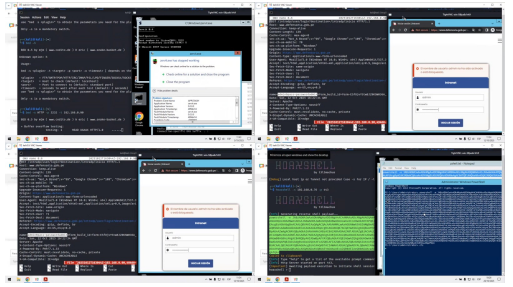
Cursos (Aula Virtual)

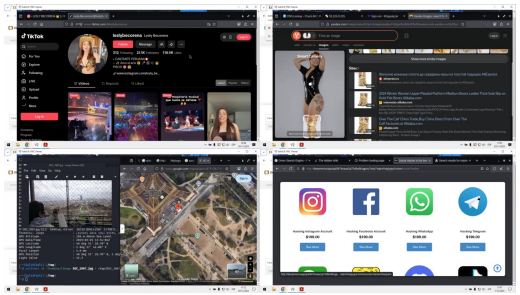
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking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

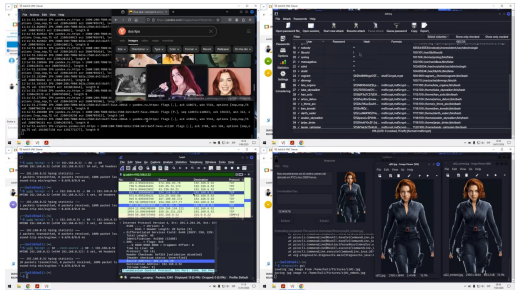












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Redacción en Ciberseguridad Cautivar al Lector

Alonso Eduardo Caballero Quezada

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

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

Miércoles 5 Agosto 2026