Día 1: Del hallazgo al reporte

Michel Faúndez

Fecha: 20.11.2025

Agenda

Sección 1	INTRODUCCIÖN Y CONTEXTO
Sección 2	MARCO LEGAL Y PREPARACIÓN (EL ESCUDO)
Sección 3	ESTRATEGIA Y METODOLOGÍA (EL MAPA)
Sección 4	EJECUCIÓN TÉCNICA (LA ACCIÓN)
Sección 5	EL REPORTE (EL PRODUCTO)
Sección 6	MÁS ALLÁ DEL REPORTE (SOFT SKILLS)
Sección 7	PRÁCTICA (MANOS A LA OBRA)
Sección 8	REFERENCIAS

SECCIÓN 1: INTRODUCCIÓN Y CONTEXTO

1 Introducción

A todos nos gusta encontrar información e informar , sin embargo siempre todo tiene reglas claras, y un contexto

SECCIÓN 2: MARCO LEGAL Y PREPARACIÓN (EL ESCUDO)

Normativas y Compliance (El "Por qué")

- El pentesting ayuda a cumplir con normativas internacionales exigidas en Chile.
  Destacamos
- **ISO 27001:2013:** El control A.12.6.1 exige la gestión de vulnerabilidades técnicas.
  En la actualidad Evidenciamos este control como anexo en el punto 8.8 de la ISO 27002:2022
- **NIST CSF 2.0:** Identificar y Proteger son funciones core que requieren evaluación continua.
- **PCI DSS:** Obligatorio para procesar tarjetas. Exige pentests anuales y tras cambios significativos.

Marco Legal Chileno (Lo crítico)

- **Ley N° 21.459 (Delitos):** Sanciona el acceso ilícito (Art. 2), interceptación y daño a datos. Es la base penal.
- **Ley N° 21.663 (Marco):** Establece obligaciones de reporte para servicios esenciales.

Otros:
La Ley de Fraude y Abuso Informático
(CFAA, por sus siglas en inglés) (EEUU)

- The Computer Misuse Act 1990
(CMA) (Reino Unido)

Documentación Previa 1 (Contratos)

Acuerdo de Confidencialidad (NDA)

- **Definición de Información confidencial: ¿** Qué datos están protegidos ?
- **Plazos de vigencia:** Duración de la obligación de secreto.
- **Exclusiones:** Información que no está protegida.
- **Jurisdicción:** Ley que rige el acuerdo.

Master Service Agreement (MSA)

- **Alcance del trabajo:** Qué se va a hacer (y qué no).
- **Límites de responsabilidad:** Hasta dónde te cubres.
- **Seguros profesionales:** Requisitos de cobertura.

Documentación Previa 2: Tu "Salvoconducto”

- Jamás inicies pruebas sin la documentación firmada. Esto distingue al pentester del cibercriminal.
- **NDA (Acuerdo de Confidencialidad):** Protege la información sensible del cliente.
- **Acuerdo de Servicios (MSA):** Define términos comerciales y legales.
- **Autorización de Pruebas** Documento técnico explícito que autoriza el ataque a IPs/Dominios específicos durante una ventana de tiempo definida.

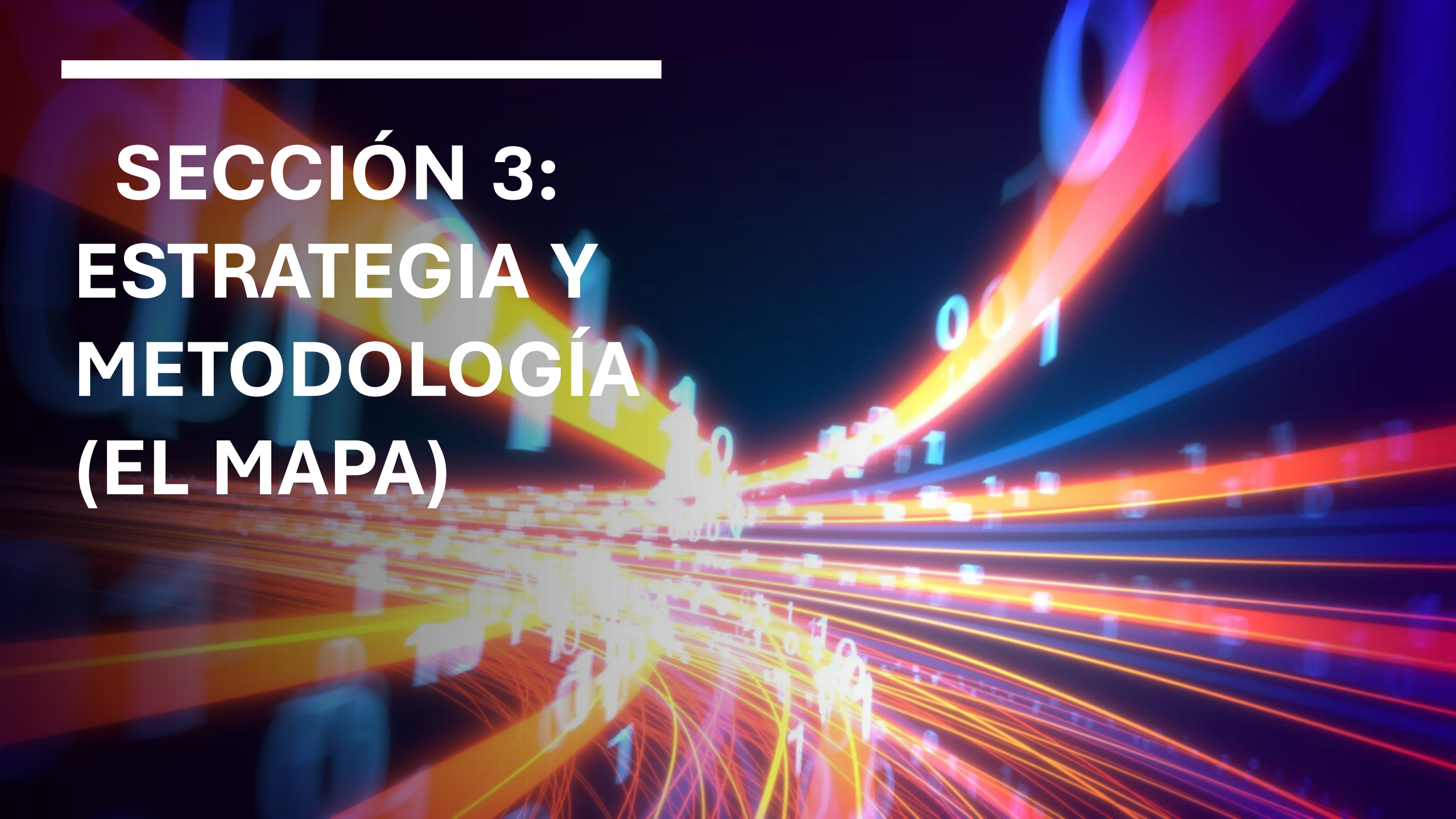
Scoping: Definiendo los Límites

Un alcance mal definido puede resultar en problemas legales o pérdida de dinero.

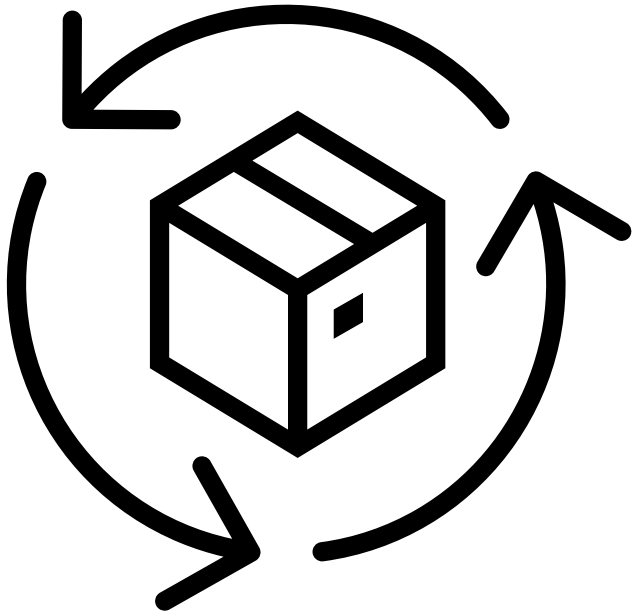
¿Qué SÍ se toca?: IPs, URLs, aplicaciones móviles específicas.

¿Qué NO se toca?: Servidores de terceros, infraestructura crítica en producción, bases de datos legadas frágiles.

Reglas de Juego (ROE): ¿Se permite Ingeniería Social? ¿DoS? ¿Horarios de prueba?



SECCIÓN 3: ESTRATEGIA Y METODOLOGÍA (EL MAPA)



Ciclo de vida (fase) Pentesting

- **Planificación:** Definición del alcance y reglas de juego (ROE).
- **Descubrimiento:** Recolección de información y escaneo.
- **Ataque/Explotación:** Confirmación de vulnerabilidades.
- **Reporte:** El producto final que recibe el cliente.

Tipos de Pruebas

- **Black Box (Caja Negra):** Simula un atacante externo real. Sin información previa. Mayor esfuerzo de reconocimiento.
- **Grey Box (Caja Gris):** Acceso parcial (ej. credenciales de usuario). Balance ideal costo-beneficio.
- **White Box (Caja Blanca):** Acceso total (código fuente, diagramas). Auditoría exhaustiva.

Metodologías

PTES

Penetration Testing Execution Standard. Cubre desde la pre-interacción hasta el reporte.

OWASP WSTG

Guía paso a paso para probar vulnerabilidades web*.

OSSTMM

Manual de Metodología Abierta de Testeo de Seguridad. Enfoque científico y métrico.

Metodologías *

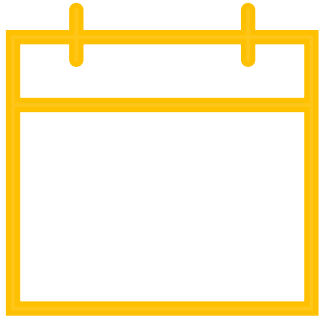
ISSAF

Information System Security Assessment Framework

NIST

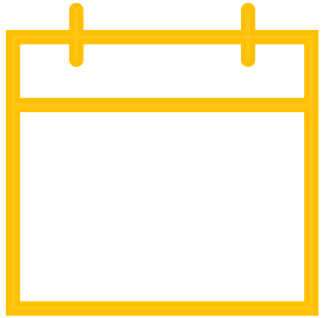
Publicación especial 800-115 del NIST

Tiempos Referenciales**



METODOLOGÍA	FASES CLAVE	DURACIÓN TÍPICA	ENTREGABLES
OWASP Testing Guide	1. Configuración/Despliegue 2. Gestión de Sesión/Autenticación 3. Pruebas de inyección 4. Lógica de Negocio	2-4 semanas	Informe de Vulnerabilidades Web (incluyendo OWASP Top 10), Calificación de Riesgo por Vulnerabilidad, Recomendaciones de Remediación Específicas del código.
PTES	1. Interacción Previa (Definición de Alcance) 2. Recolección de Inteligencia (Footprinting) 3. Modelado de Amenazas 4. Análisis de Vulnerabilidades 5. Explotación 6. Post-Explotación (Elevación de Privilegios/Persistencia) 7. Reporte	3-6 semanas	Informe Final con Resumen Ejecutivo, Listado de Vulnerabilidades con Pruebas de Concepto (PoC), Calificación de Riesgo (CVSS/Similar), Plan de Remediación Detallado.
OSSTM	1. Pre-análisis (Definición de Alcance y Reglas) 2. Testing de los 5 Canales (Data, Human, Physical, Wireless, Telecom) 3. Análisis de Resultados (Cálculo de RAVs) 4. Elaboración del Reporte	Depende de la cantidad de "Canales" a evaluar). 2-8 semanas (base 1 semana)	Certificado de Seguridad (con puntaje RAV o Risk Assessment Values), Informe Detallado de las Capacidades de Defensa, Métricas Cuantificables de riesgo por canal. Puede ser adaptable dependiendo del Canal.

Tiempos Referenciales**



METODOLOGÍA	FASES CLAVE	DURACIÓN TÍPICA	ENTREGABLES
ISSAF	**1. Planificación y Preparación** (Alcance, Reglas) **2. Evaluación** (Recolección de Información, Mapeo, Identificación de Vulnerabilidades, Penetración, Escalada de Privilegios, Mantenimiento de Acceso). **3. Reporte, Limpieza y Destrucción de Artefactos** (**Cubrir Huellas**).	**4-8 semanas** (Debido a su profundidad y detalle).	Resumen Ejecutivo para la Gestión, **Informe Técnico Detallado** (incluyendo herramientas y *exploits* usados), Lista de Vulnerabilidades Priorizadas con Recomendaciones de Mitigación
NIST SP 800-115	1 . Planificación 2. Ejecución (Descubrimiento, Análisis de Vulnerabilidades, Explotación) 3. Post-Ejecución (Reporte y Limpieza)	4 a 8 semanas	Plan de Pruebas de Seguridad Aprobado, Documentación de los hallazgos con base en los objetivos del negocio, Recomendaciones alineadas con políticas y estándares de seguridad.

SECCIÓN 4: EJECUCIÓN TÉCNICA (LA ACCIÓN)

El Toolbox del Pentester

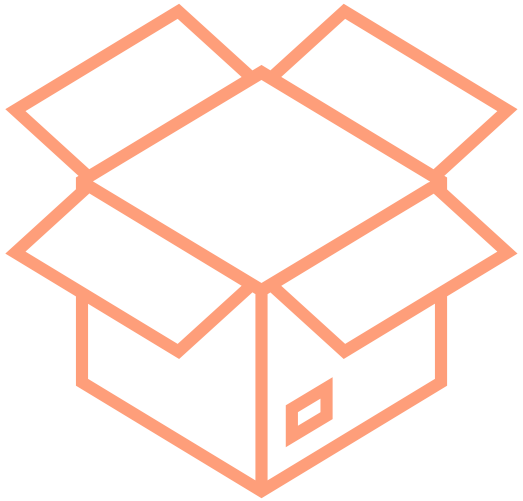
Escáner de puertos

Escáner de vulnerabilidad

Proxy web

Recuperación avanzada de contraseña

Sniffer de red



"Las mejores herramientas a las que puede recurrir el líder para mejorar su desempeño son: el estudio, el pensamiento crítico, la reflexión, la acción compartida, el ejemplo".

Día 2: Del hallazgo al reporte

Michel Faúndez

Fecha: 21.11.2025

Agenda

Sección 1	INTRODUCCIÓN Y CONTEXTO
Sección 2	MARCO LEGAL Y PREPARACIÓN (EL ESCUDO)
Sección 3	ESTRATEGIA Y METODOLOGÍA (EL MAPA)
Sección 4	EJECUCIÓN TÉCNICA (LA ACCIÓN)
Sección 5	EL REPORTE (EL PRODUCTO)
Sección 6	MÁS ALLÁ DEL REPORTE (SOFT SKILLS)
Sección 7	PRÁCTICA (MANOS A LA OBRA)
Sección 8	REFERENCIAS

SECCIÓN 5: EL REPORTE (EL PRODUCTO)

Estructura básica del contenido de un informe

Item	Descripción
Introducción	El informe comienza con una **Introducción** que ofrece un resumen general de la evaluación de seguridad, lo cual resulta esencial para contextualizar el documento. Esta sección proporciona información detallada sobre el **alcance** del proyecto, los **objetivos** planteados, el **contexto** en el que se desarrolló y cualquier **limitación** relevante que pudiera haber afectado los hallazgos. Su propósito fundamental es establecer el tono del informe y brindar a los lectores una visión clara del propósito general y del enfoque utilizado en la evaluación
Metodología	Detalla de forma exhaustiva el procedimiento utilizado a lo largo de la evaluación, especificando las **herramientas**, las **técnicas** y los **enfoques** que se emplearon. Es crucial que esta descripción sea lo suficientemente detallada como para permitir que cualquier lector comprenda exactamente cómo se realizaron los análisis y las pruebas. Mantener una alta transparencia en la metodología es clave, ya que esto incrementa significativamente la **credibilidad** y la confianza en el informe final.
Hallazgos	Constituye el núcleo del informe, ya que en ella se presentan los **resultados concretos** de la evaluación de seguridad. Se describen detalladamente las **vulnerabilidades** encontradas, cualquier sistema que pudiera estar comprometido, las **debilidades** identificadas y cualquier otro resultado significativo. Cada hallazgo se complementa con información esencial que incluye: una descripción clara de la vulnerabilidad, su posible **impacto potencial** en la organización y las **recomendaciones específicas para su mitigación** y corrección.
Evaluación de riesgos	es la sección encargada de analizar y determinar el peligro asociado a los hallazgos identificados en la evaluación. En ella, se **asignan niveles de gravedad** a cada vulnerabilidad y se explican claramente las **implicaciones** que estos representan para la seguridad general de la organización. Este proceso es vital, ya que permite a los responsables de la toma de decisiones **priorizar** de manera efectiva qué acciones correctivas deben implementarse primero para mitigar el riesgo más alto.

Estructura básica del contenido de un informe

Item	Descripción
Evaluación de riesgos	Es la sección encargada de analizar y determinar el peligro asociado a los hallazgos identificados en la evaluación. En ella, se **asignan niveles de gravedad** a cada vulnerabilidad y se explican claramente las **implicaciones** que estos representan para la seguridad general de la organización. Este proceso es vital, ya que permite a los responsables de la toma de decisiones **priorizar** de manera efectiva qué acciones correctivas deben implementarse primero para mitigar el riesgo más alto.
Recomendaciones	Se dedica a proporcionar las acciones específicas necesarias para corregir los hallazgos y, en consecuencia, mejorar el nivel de seguridad. Estas sugerencias deben ser **claras, accionables** y directamente enfocadas en la **mitigación de los riesgos** identificados. Opcionalmente, se puede incluir un **plan de acción detallado** que guíe paso a paso la implementación de las soluciones sugeridas, asegurando una corrección efectiva de las vulnerabilidades.
Conclusiones	Tiene como objetivo **resumir los aspectos más destacados** de todo el informe y ofrecer una perspectiva general sobre la **efectividad** de las medidas de seguridad que se encuentran actualmente en uso. Adicionalmente, esta parte puede incluir reflexiones finales y observaciones clave acerca de la importancia estratégica de **abordar los riesgos de seguridad** de una manera proactiva y continua dentro de la organización.
Anexos o Apéndices	Se adjunta al informe principal en ciertos casos para facilitar **detalles adicionales**, **evidencia técnica** o **información de respaldo** que sirve para validar y sustentar tanto los hallazgos presentados como las recomendaciones sugeridas. Estos elementos complementarios son cruciales para aquellos lectores que requieran una profundidad de información mayor a la incluida en el cuerpo principal del documento.

Estructura del Reporte Profesional

Informe ejecutivo

Proporcionar una visión general rápida para facilitar la toma de decisiones estratégicas y la asignación de recursos.

Informe Técnico

Proporcionar la información detallada y técnica necesaria para que el personal de seguridad pueda comprender y corregir las vulnerabilidades.

Informe ejecutivo

- **¿Qué encontramos?** Se comunica de forma directa el **problema crítico principal** identificado.
- **¿Qué riesgo representa?** Se traduce ese problema en el **impacto potencial** que puede tener sobre la operación, las finanzas o la reputación de la organización.
- **¿Qué hacer primero?** Se recomienda la **acción inmediata y prioritaria** que la dirección debe autorizar para mitigar el riesgo más grave.
- Este enfoque asegura que los líderes tomen **decisiones informadas** sin necesidad de navegar por el detalle técnico.

Informe técnico

Estructura de una Vulnerabilidad (CVSS)

- **Descripción:** Qué es el problema.
- **Impacto:** Qué tan malo es.
- **Reproducibilidad:** Pasos para replicarlo.
- **Mitigación:** Cómo solucionarlo.

Evidencias

- **Capturas de pantalla:** Antes y después.
- **Logs y salidas de comandos:** Prueba técnica.
- **Comandos ejecutados:** Para la reproducibilidad.

Del Hallazgo al Papel

Capturando la Evidencia

¿Qué constituye una buena evidencia?

La evidencia debe permitir a cualquier otro consultor reproducir el hallazgo paso a paso.

Screenshots Completos: Incluye la URL y la barra de estado.

Logs de Tráfico: Peticiones y respuestas HTTP crudas (Burp Suite).

Comandos: Sintaxis exacta utilizada en terminal.

Video: Para flujos complejos o condiciones de carrera.

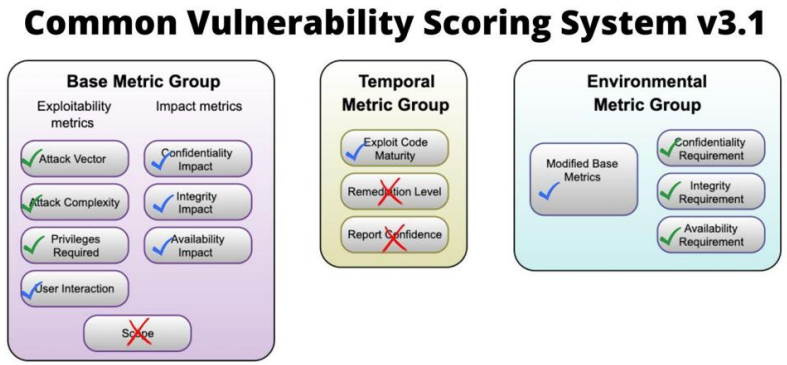
Documentación de vulnerabilidades

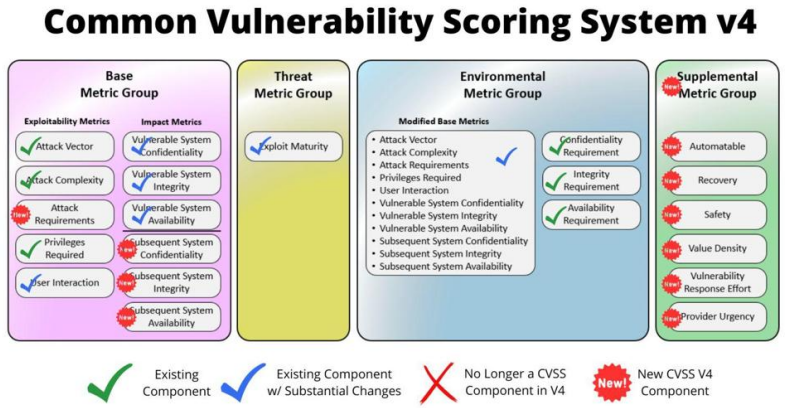
- **1. Nombre y Tipología del Hallazgo**
  - Cada vulnerabilidad se identifica con un **nombre descriptivo** que define su naturaleza específica. Esto garantiza una **referencia única** dentro del informe, facilitando las discusiones técnicas y la indexación para seguimientos futuros.
- **2. Nivel de Gravedad (Criticidad/Clasificación)**
  - Se asigna una calificación de riesgo (Baja, Media, Alta, Crítica) a la vulnerabilidad. Esta clasificación es esencial para **priorizar de manera objetiva** las acciones de remediación, concentrando los recursos en los riesgos de mayor impacto.
- **3. Descripción del Hallazgo**
  - Se proporciona una **descripción técnica detallada** de la vulnerabilidad. Este detalle abarca el proceso de descubrimiento, los componentes o sistemas afectados, y la clasificación precisa de la amenaza que introduce.
- **4. Impacto del Hallazgo**
  - Se describe el efecto potencial de la vulnerabilidad en función de los tres pilares de la seguridad: **confidencialidad, integridad y disponibilidad**. Este análisis es crucial para dimensionar las posibles consecuencias operacionales de su explotación.
- **5. Mitigación o Recomendaciones para una Solución**
  - Se proponen **medidas específicas y accionables** para resolver la vulnerabilidad y mitigar el riesgo asociado. Las recomendaciones pueden ser de índole técnica, como ajustes de configuración o actualizaciones de *software*, o la modificación de políticas de seguridad.

Documentación de vulnerabilidades

- **6. CVSS (Common Vulnerability Scoring System)**
  - El **CVSS** es un estándar universal que asigna una puntuación numérica a la gravedad de la vulnerabilidad, basándose en factores como la complejidad y el impacto. Su valor principal es facilitar la **priorización comparativa** de las acciones correctivas.
- **7. Referencias sobre el Hallazgo y Mitigación**
  - Se incluyen **enlaces de soporte y referencias** a recursos adicionales (como boletines de seguridad, informes técnicos o parches), así como enlaces a **CVEs** (*Common Vulnerabilities and Exposures*), si están disponibles, para una verificación y contexto más profundos.
- **8. Prueba de Concepto (PoC)**
  - De ser factible, se adjunta una **Prueba de Concepto (PoC)** que demuestra la explotación de la vulnerabilidad, a menudo mediante material visual (imágenes o video). Este recurso ayuda a los **directivos** a comprender mejor la dimensión real del riesgo.
- **9. Fecha de Descubrimiento y Notificación**
  - Se registra la **fecha precisa del hallazgo** y la fecha en que se realizó la **notificación formal** a los propietarios o responsables de los sistemas afectados. Es indispensable documentar el método de comunicación empleado.
- **10. Responsables de la Evaluación**
  - Se identifica claramente al profesional o al **equipo técnico** que ejecutó la evaluación de seguridad y que se encargó de documentar cada vulnerabilidad en el informe.

Calculadora CVSS





¿Qué es la Calculadora CVSS?
Herramienta estándar para evaluar la severidad de vulnerabilidades de seguridad.
Genera una puntuación del 0.0 al 10.0 (Bajo a Crítico).
Permite priorizar parches y respuestas a incidentes basándose en datos objetivos.

Componentes de la Puntuación:
Métricas Base: Cualidades intrínsecas de la vulnerabilidad.
Métricas Temporales: Factores que cambian con el tiempo (ej. existencia de un exploit).
Métricas Ambientales: Factores específicos del entorno del usuario final.

Formación Oficial (FIRST.org):
Es crucial utilizar la metodología oficial para evitar discrepancias en las puntuaciones.
Portal de Aprendizaje: https://learn.first.org/
Catálogo de Cursos: https://learn.first.org/catalog

Proceso Colaborativo y Valoración del Informe Final

Aspecto Clave	Descripción de la Expectativa del Cliente	Justificación / Beneficio para el Cliente	Estrategia de Entrega Recomendada
Colaboración	Los clientes esperan un diálogo activo y la integración de sus comentarios en el entregable.	Asegura la **relevancia estratégica** del informe al alinearlo con el contexto y las prioridades internas del cliente.	Planificar un proceso de revisión asíncrona seguido de una sesión de aclaración dedicada.
Adaptación	Requisitos para ajustar el lenguaje, adaptar el enfoque o incluir la Respuesta de la Gerencia (plan de acción).	Permite que el informe sea inmediatamente **accionable** y elimina barreras para su aceptación interna (ej. eliminar lenguaje polémico).	Ofrecer tiempo y espacio para que el cliente solicite cambios o adiciones significativas.
Propósito	El informe se utilizará como base para fines internos críticos.	Convierte el informe en una **herramienta estratégica** (ej. justificación de financiación ante la junta directiva) o un **plan operacional** (ej. fundamento para la implementación de remediaciones).	Reconocer que el cliente invierte en un informe que debe ser lo **más completo y valioso posible** para sus necesidades.
Proceso	Revisar el documento, hacer preguntas y explicar las necesidades de adaptación.	Maximiza la utilidad del documento al resolver dudas y asegurar que el producto final sea **hecho a la medida** y entendible por sus equipos.	**Entregar un borrador primero**, conceder tiempo de revisión, y luego realizar una sesión de revisión colaborativa.

SECCIÓN 6: MÁS ALLÁ DEL REPORTE (SOFT SKILLS)

Habilidades Interpersonales

Habilidad Interpersonal	Descripción	Aplicación en Ciberseguridad
Comunicación Efectiva	La capacidad de transmitir ideas, información y riesgos de forma clara, concisa y adecuada al público (técnico o no técnico).	Explicar un riesgo de seguridad al CEO o redactar un informe de incidente claro.
Trabajo en Equipo y Colaboración	Participar activamente y de manera constructiva con los demás para alcanzar un objetivo común.	Coordinar con el equipo de TI y los desarrolladores para parchar una vulnerabilidad.
Liderazgo	Inspirar, motivar y guiar a un equipo o a la organización hacia los objetivos, tomando la iniciativa y responsabilidad.	Dirigir la respuesta durante un incidente de seguridad crítico.
Negociación y Persuasión	Influir en las decisiones de otros para adoptar medidas, invertir recursos o cambiar comportamientos.	Convencer a un gerente de departamento para que implemente una política de seguridad estricta.
Empatía	La capacidad de entender y compartir los sentimientos o las perspectivas de los demás.	Entender la frustración del usuario cuando se implementan controles de seguridad restrictivos.
Gestión de Conflictos	La habilidad para manejar disputas o desacuerdos de manera constructiva, buscando una solución mutuamente aceptable.	Mediar entre los equipos de desarrollo y operaciones sobre la implementación de nuevos controles de seguridad.

Habilidades Intrapersonales

Habilidad Intrapersonal	Descripción	Aplicación en Ciberseguridad
Pensamiento Crítico	Analizar hechos, evaluar riesgos, cuestionar suposiciones y formar juicios racionales.	Determinar si un e-mail sospechoso es phishing real o una falsa alarma.
Adaptabilidad y Flexibilidad	La capacidad de ajustarse rápidamente a nuevos entornos, tecnologías, prioridades o situaciones inesperadas.	Aprender rápidamente una nueva herramienta de seguridad que se acaba de implementar.
Gestión del Tiempo y Organización	Priorizar tareas, planificar y ejecutar el trabajo de manera eficiente para cumplir con los plazos.	Balancear tareas diarias (monitoring) con proyectos a largo plazo (upgrades).
Resiliencia y Gestión del Estrés	Mantener la calma y la efectividad bajo presión, especialmente durante crisis o incidentes mayores.	Manejar una noche de trabajo mientras se contiene un ataque de ransomware.
Iniciativa y Proactividad	Actuar sin necesidad de ser dirigido, identificando problemas u oportunidades y tomando acción.	Identificar una vulnerabilidad potencial en un sistema y proponer una solución antes de que se explote.
Aprendizaje Continuo	La curiosidad y el compromiso de seguir adquiriendo nuevos conocimientos y habilidades constantemente.	Mantenerse al día con las últimas técnicas de ataque y defensa.

Habilidades Blandas y Manejo de Cliente

- **El Rol del Traductor:**
- Tu trabajo es traducir *Riesgo Técnico* (SQL Injection) a *Riesgo de Negocio* (Pérdida financiera/reputacional).
- Gerencia no habla TCP/IP; habla dinero y continuidad operativa.
- **Gestión de la Negación ("Es un falso positivo"):**
- Es común que el cliente se ponga a la defensiva.
- **Solución:** No entres en discusiones de ego. Responde con la **Prueba de Concepto (PoC)** en mano. Los datos matan el relato.

Habilidades Blandas y Manejo de Cliente

•**Manejo de Expectativas y Scope Creep:**
•Cliente: *"¿Ya que estás ahí, puedes revisar también este otro servidor?"*

- Pentester: *"Eso excede el alcance (Scope) firmado. Podemos revisarlo en una nueva iteración."* (Protege tu tiempo y el contrato).

Empatía con el Desarrollador:

- No eres un juez, eres un consultor.
- Evita el tono: "Mira lo mal que hiciste esto".
- Usa el tono: "Aquí hay una oportunidad de mejora para blindar el sistema".

Disclosure y Vulnerabilidades

¿Qué pasa cuando encuentras algo crítico? El manejo de la información es vital.

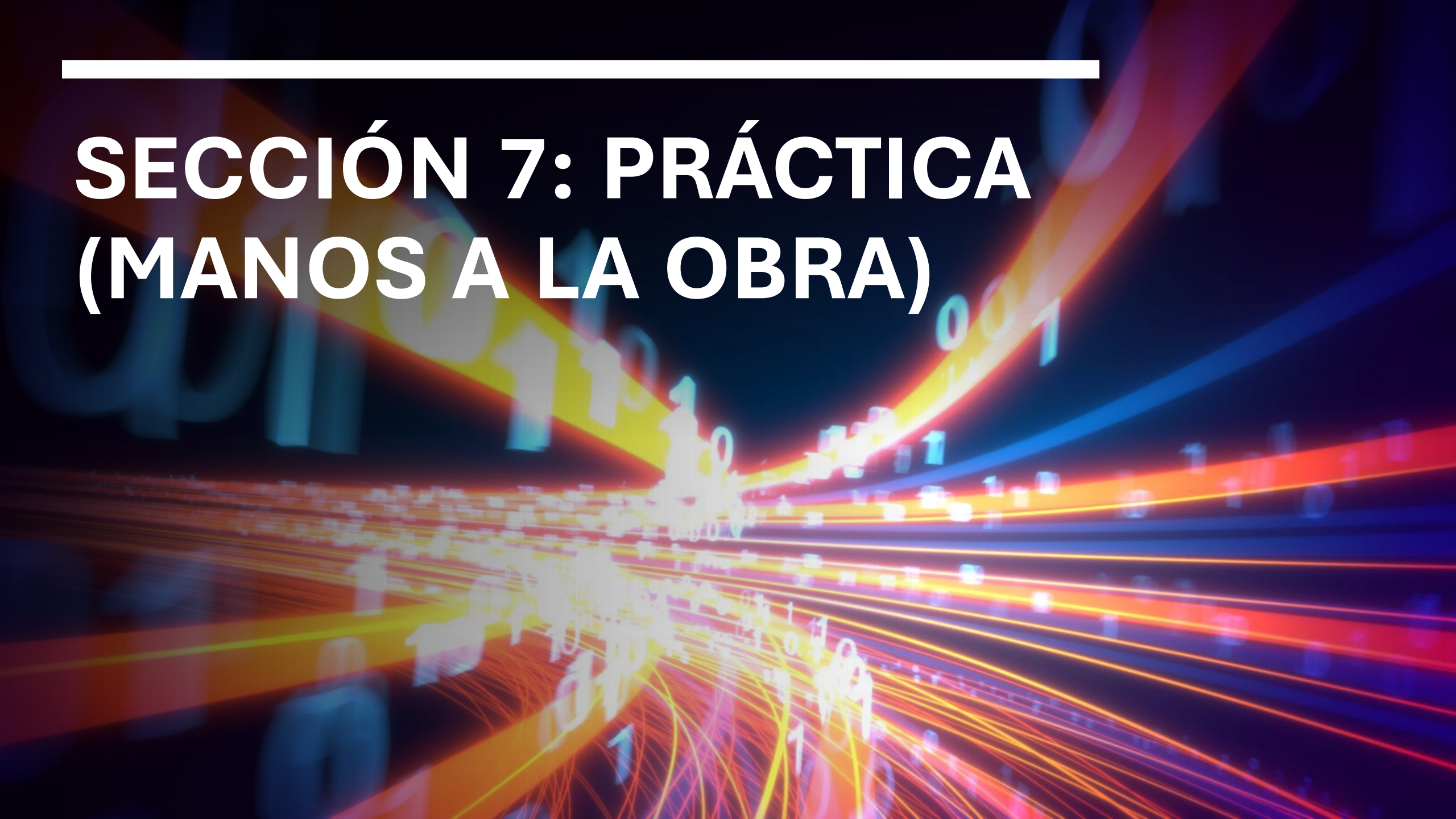
Coordinated Vulnerability Disclosure (CVD): Reportar al vendor/dueño y dar un tiempo razonable para el parche antes de publicar.

Ley Marco (21.663): Obliga a operadores de servicios esenciales a reportar incidentes significativos al CSIRT Nacional.

Uso de CVSS v4.0: Estándar objetivo para puntuar la severidad (Base, Amenaza, Ambiental).

Checklist Final: Antes de Entregar

- Scope firmado y adjunto
- Reporte generado en un formato que pueda ser abordado (docx, pdf)
- Resumen ejecutivo revisado
- Recomendaciones Priorizadas
  Evidencias (capturas, logs) guardadas
- CVSS calculado para cada hallazgo
- Gráficos de riesgo incluidos**
- Compliance mapeado (ej. ISO 27001)
- Cliente notificado y copia de seguridad en repositorio interno

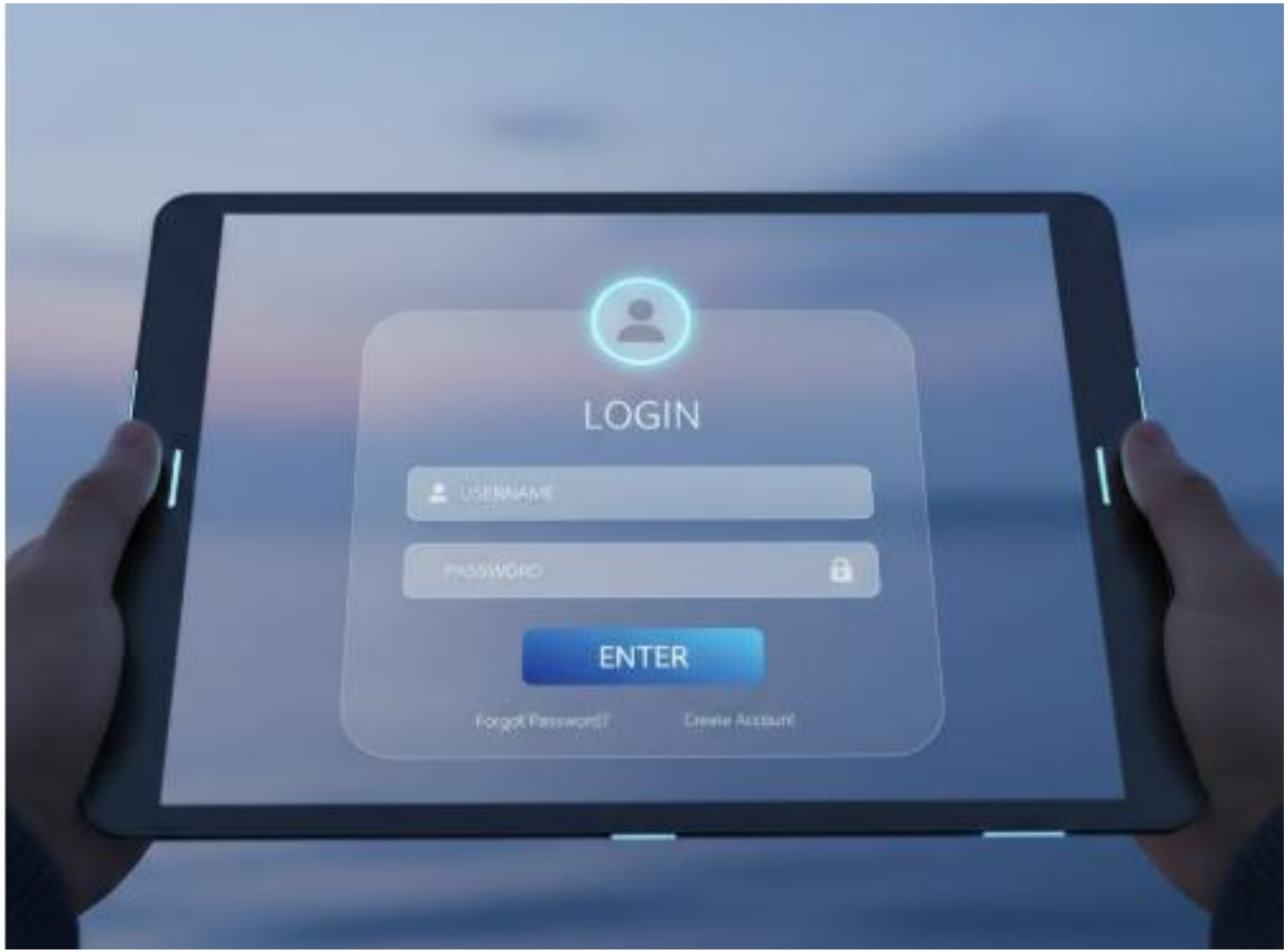


SECCIÓN 7: PRÁCTICA (MANOS A LA OBRA)

Ejercicio Práctico (Introducción)

Comencemos a ver algo mas práctico.

LOGIN



El Escenario

1

2

3

La Tarea

1 2 3

Encontraste una vulnerabilidad de SQL Injection en un formulario de login.
La URL afectada es /login.php . La payload ' OR '1'='1 te permite bypassear la autenticación.
Tienes una captura de pantalla mostrando acceso a datos de administrador.

- Actividad:
- 1. Calcula CVSS (Base score ?)
- 2. Redacta Impacto (1 párrafo)
- 3. Propone una Mitigación (Acción Inmediata)
- 4. ¿Que número(s) representa la vulnerabilidad presentada?

Creación de reporte sencillo con pwndoc

- https://pwndoc.github.io/pwndoc/#/installation

¿Cuál es el documento considerado el "salvoconducto" técnico que autoriza explícitamente el ataque a IPs y dominios específicos dentro de una ventana de tiempo definida?

A. Autorización de Pruebas

B. Informe Técnico de Vulnerabilidades

C. Acuerdo de Confidencialidad

D. Acuerdo de Servicios (MSA)

¿Qué tipo de prueba de pentesting simula a un atacante externo sin conocimiento previo del sistema, requiriendo un mayor esfuerzo en la fase de reconocimiento?

A. Caja Blanca (White Box)

B. Caja Gris (Grey Box)

C. Auditoría de Código

D. Caja Negra (Black Box)

¿Qué metodología de pentesting se destaca por su enfoque métrico y el análisis de "5 Canales" (Datos, Humano, Físico, Inalámbrico y Telecomunicaciones)?

A. PTES

B. OSSTMM

C. OWASP WSTG

D. NIST SP 800-115

En el contexto de una prueba de penetración, ¿Cuál es el propósito principal del Acuerdo de Confidencialidad (NDA)?

A. Definir los términos comerciales y legales del servicio, como los límites de responsabilidad.

B. Autorizar explícitamente el ataque a direcciones IP y dominios específicos en una ventana de tiempo definida.

C. Establecer las reglas de enfrentamiento (ROE), como los horarios de prueba y las técnicas permitidas.

D. Proteger la información sensible del cliente a la que el pentester pueda acceder durante la evaluación.

¿Cuál es el público principal del "Informe Ejecutivo" y qué busca comunicar?

A. Está dirigido al equipo técnico y busca proporcionar los pasos exactos para reproducir y corregir cada vulnerabilidad.

B. Está dirigido a la gerencia y busca comunicar el riesgo en términos de impacto al negocio para facilitar la toma de decisiones estratégicas.

C. Está dirigido a auditores externos y busca demostrar el cumplimiento de normativas como PCI DSS o ISO 27001.

D. Está dirigido al equipo legal y busca detallar las posibles infracciones a la Ley N° 21.459 encontradas durante las pruebas.

Si un cliente reacciona a la defensiva y afirma que un hallazgo es un "falso positivo", ¿cuál es la respuesta más profesional y efectiva según el material?

A. Presentar de manera calmada la Prueba de Concepto (PoC) que demuestra la explotabilidad de la vulnerabilidad.

B. Eliminar el hallazgo del informe para mantener una buena relación con el cliente y evitar conflictos.

C. Aceptar la opinión del cliente y marcar el hallazgo como de bajo riesgo sin más investigación.

D. Iniciar una discusión técnica para demostrar la superioridad de conocimientos y defender el hallazgo.

Conclusión

Hacer un reporte, o tener un hallazgo, no hace el recorrido o el camino para presentarlo.

- **El Reporte es el Producto:** El cliente no paga por el exploit, paga por el entendimiento del riesgo y la solución. Si el hallazgo no se comunica bien, el trabajo técnico pierde su valor.
- **La Firma es la Frontera:** La diferencia entre un ciberdelincuente y un pentester profesional es la autorización escrita. Sin documentos firmados (NDA, MSA, Autorización), no hay ética ni legalidad.
- **Traductor de Riesgos:** Nuestro rol es traducir fallas técnicas complejas (como una inyección SQL) en impactos de negocio comprensibles para la gerencia, entender riesgos y vulnerabilidades , va de la mano a saber abordarlas de forma efectiva.
- **Metodología sobre Herramientas:** Las herramientas cambian, pero una metodología sólida (OWASP, PTES, NIST) garantiza consistencia y calidad profesional.

Palabras Finales

Muchas gracias por su atención

SECCIÓN 8: Referencias

Contacto : Michel Faúndez

- Mi camino en ciberseguridad comenzó con una base en Matemática de la Universidad del Bío-Bío, la cual he complementado intensamente con especializaciones en seguridad. Cuento con un Diplomado en Red Team de Capacitación USACH y certificaciones como eJPT (Penetration Testing) de INE y CEHP de EC-Council. Además, he profundizado en Gestión de Incidentes como Implementador Líder ISO 27035, entre otras formaciones y enseñanzas.
- Actualmente, me desempeño como Consultor de Ethical Hacking y DevSecOps en PentestSPA, donde mi rol como Pentester me permite aplicar conocimientos tanto ofensivos como defensivos. Soy un colaborador activo en comunidades clave de ciberseguridad como Fundación Sochisi, Partyhack y Blueteam Latam, y he tenido la oportunidad de ser speaker en diversas instancias.
- Me considero un profesional autodidacta y proactivo, siempre buscando el crecimiento constante y el perfeccionamiento en ciberseguridad. Valoro mucho el trabajo en equipo y me gusta compartir mis conocimientos técnicos con respeto y empatía, tanto en entornos colaborativos como formativos.
- **Mi LinkedIn:** https://www.linkedin.com/in/mfaundez/

Glosario Básico

Término	Definición Profesional
NDA (Acuerdo de Confidencialidad)	Contrato legal diseñado para **proteger la información sensible** del cliente a la que el evaluador pueda acceder. Define claramente la información protegida, los plazos de vigencia y la jurisdicción aplicable.
MSA (Master Service Agreement)	Documento legal que establece los **términos comerciales y contractuales** generales del acuerdo de servicios, incluyendo las responsabilidades y los límites del trabajo.
Autorización de Pruebas	El **documento formal y explícito** que otorga permiso para realizar el ataque. Debe especificar los activos (IPs/Dominios) y la **ventana de tiempo** exacta para la ejecución de la prueba.
Scoping	El proceso crítico de **definir los límites y el alcance** de la prueba. Establece con precisión qué sistemas, URLs o aplicaciones **serán incluidos** y cuáles quedan estrictamente fuera del ejercicio.
ROE (Reglas de Juego/Enfrentamiento)	Detalles operacionales que complementan el *scoping*. Definen si están permitidas acciones como la Ingeniería Social o ataques de Denegación de Servicio (DoS), y delimitan los horarios de ejecución de la prueba.
Ley N° 21.459 (Delitos)	La normativa penal chilena que constituye la **base legal** para sancionar delitos informáticos, incluyendo el acceso ilícito, la interceptación y el daño no autorizado a datos.
Compliance	El **cumplimiento** de normativas, estándares o marcos de referencia (ej., ISO 27001, NIST CSF, PCI DSS) que imponen la exigencia de gestionar y corregir vulnerabilidades técnicas.

Glosario Básico

Término	Definición Profesional
NDA (Acuerdo de Confidencialidad)	Contrato legal diseñado para **proteger la información sensible** del cliente a la que el evaluador pueda acceder. Define claramente la información protegida, los plazos de vigencia y la jurisdicción aplicable.
MSA (Master Service Agreement)	Documento legal que establece los **términos comerciales y contractuales** generales del acuerdo de servicios, incluyendo las responsabilidades y los límites del trabajo.
Autorización de Pruebas	El **documento formal y explícito** que otorga permiso para realizar el ataque. Debe especificar los activos (IPs/Dominios) y la **ventana de tiempo** exacta para la ejecución de la prueba.
Scoping	El proceso crítico de **definir los límites y el alcance** de la prueba. Establece con precisión qué sistemas, URLs o aplicaciones **serán incluidos** y cuáles quedan estrictamente fuera del ejercicio.
ROE (Reglas de Juego/Enfrentamiento)	Detalles operacionales que complementan el *scoping*. Definen si están permitidas acciones como la Ingeniería Social o ataques de Denegación de Servicio (DoS), y delimitan los horarios de ejecución de la prueba.
Ley N° 21.459 (Delitos)	La normativa penal chilena que constituye la **base legal** para sancionar delitos informáticos, incluyendo el acceso ilícito, la interceptación y el daño no autorizado a datos.
Compliance	El **cumplimiento** de normativas, estándares o marcos de referencia (ej., ISO 27001, NIST CSF, PCI DSS) que imponen la exigencia de gestionar y corregir vulnerabilidades técnicas.

Glosario Básico

Término	Definición Profesional
Informe Ejecutivo	Sección dirigida a la **Gerencia y el Directorio**. Su objetivo es comunicar el riesgo de negocio, el impacto estratégico y las acciones prioritarias, **sin utilizar jerga técnica**.
Informe Técnico	Sección dirigida al **personal de seguridad y TI**. Proporciona la información **detallada y procesable** necesaria para comprender, reproducir y corregir las vulnerabilidades.
PoC (Prueba de Concepto)	**Evidencia demostrativa** (generalmente visual) que confirma la explotación exitosa de la vulnerabilidad. Es esencial para validar el hallazgo y responder a cualquier intento de negación.
CVSS (Scoring System)	**Estándar universal** que asigna una puntuación numérica a la gravedad de la vulnerabilidad. Esta puntuación es crucial para la **priorización comparativa** de las tareas de remediación.
Traductor de Riesgos	El rol esencial del evaluador, que consiste en **convertir el Riesgo Técnico** (ej., fallo de *software*) a un **Riesgo de Negocio** (pérdida financiera o daño reputacional) para la toma de decisiones.
Vulnerabilidad	Una debilidad o fallo identificado en un sistema, cuya documentación integral incluye su descripción, impacto, pasos de reproducibilidad y estrategia de mitigación.
CVD (Coordinated Disclosure)	El proceso ético de reportar un hallazgo crítico al vendedor/dueño, otorgándole un **plazo razonable** para desarrollar y liberar un parche antes de la publicación pública del fallo.
Evidencias	El conjunto de **pruebas técnicas** (capturas de pantalla, *logs* y salidas de comandos) que respaldan y confirman los hallazgos. Deben ser suficientes para que cualquier consultor pueda **reproducir** el resultado.

Bibliografía Metodologías y Frameworks

- [20] OWASP Foundation - "Penetration Testing Methodologies"
- URL: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- [21] Sapphire.net - "OWASP Methodology Security Testing Phases" (2024-05-20)
- URL: https://www.sapphire.net/blogs-press-releases/owasp-methodology/
- [23] GeeksforGeeks - "Penetration Testing Execution Standard (PTES)" (2019-10-24)
- URL: https://www.geeksforgeeks.org/software-engineering/penetration-testing-execution-standard-ptes/
- [24] LinkedIn - "Penetration Testing Methodologies: OWASP, OSSTMM, PTES" (2024-05-29)
- Author: Maxwell Ferreira
- URL: https://www.linkedin.com/pulse/penetration-testing-methodologies-owasp-osstmm-ptes-maxwell-ferreira-norrc
- [26] Datami - "Penetration Testing Execution Standard: 7 PTES Stages" (2025-06-02)
- URL: https://datami.ee/blog/penetration-testing-execution-standard-7-ptes-stages/
- [27] VikingCloud - "What is the Penetration Testing Execution Standard (PTES)?" (2025-09-01)
- URL: https://www.vikingcloud.com/blog/what-is-penetration-testing-execution-standard
- [28] OWASP Foundation - "Penetration Testing Methodologies v4.1" (2011-12-31)
- URL: https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- [30] PTES - "The Penetration Testing Execution Standard"
- URL: http://www.pentest-standard.org/index.php/Main_Page

Bibliografía Metodologías y Frameworks

- [31] OWASP - "OWASP Web Security Testing Guide"
- URL: https://owasp.org/www-project-web-security-testing-guide/
- [79] DataGuard - "An overview of penetration testing methodologies" (2024-10-14)
- URL: https://www.dataguard.com/blog/penetration-testing-methodologies/
- [80] Sprinto - "List of Penetration testing methodologies" (2025-01-09)
- URL: https://sprinto.com/blog/penetration-testing-methodologies/
- [85] IBM - "Top Penetration Testing Methodologies" (2024-01-23)
- URL: https://www.ibm.com/think/insights/pen-testing-methodology
- [93] Indusface - "Complete Guide to Penetration Testing Methodology" (2025-08-12)
- URL: https://www.indusface.com/blog/penetration-testing-methodologies/
- [99] Qualysec - "Top 10 Penetration Testing Methodologies (Expert Guide)" (2025-05-19)
- URL: https://qualysec.com/penetration-testing-methodologies/
- [102] Datami - "Pen Testing Methodology: Top 5 Methodologies" (2025-06-02)
- URL: https://datami.ee/blog/top-5-methodologies/
- [104] N-ix - "Top 4 penetration testing methodologies to use in 2025" (2025-04-24)
- URL: https://www.n-ix.com/penetration-testing-methodologies/

Bibliografía Estructura de Reportes

- [1] TCM Security - "What is a Penetration Testing Report?" (2024-10-24)
- URL: https://tcm-sec.com/what-is-a-penetration-testing-report/

- [4] Offensive Security - "Penetration Test Report for Internal Lab and Exam" (PWK Example Report v1)
- URL: https://www.offsec.com/pwk-online/PWK-Example-Report-v1.pdf

- [10] PurpleSec - "Sample Penetration Test Report - Example Institute"
- URL: https://purplesec.us/wp-content/uploads/2019/12/Sample-Penetration-Test-Report-PurpleSec.pdf

- [19] HackTheBox - "Penetration testing reports: A powerful template and guide" (2025-08-19)
- URL: https://www.hackthebox.com/blog/penetration-testing-reports-template-and-guide

- [83] Terra Security - "The Essential Penetration Test Report Template" (2025-05-26)
- URL: https://www.terra.security/blog/the-essential-penetration-test-report-template

- [84] Scytale - "How to Create an Effective Plan for Penetration Testing Reports" (2025-06-24)
- URL: https://scytale.ai/resources/how-to-create-an-effective-plan-for-penetration-testing-reports/

- [89] eSecurity Planet - "How to Write a Pentesting Report - With Checklist" (2023-11-28)
- URL: https://www.esecurityplanet.com/networks/pentest-report/

- [92] PentestPad - "What to Include in a Professional Pentest Report" (2025-04-04)
- URL: https://www.pentestpad.com/blog/what-to-include-in-a-professional-pentest-report-a-complete-guide

- [95] Microminder CS - "Penetration Testing Report: Key Elements and Best Practices" (2025-08-24)
- URL: https://www.micromindercs.com/blog/penetration-testing-report

Bibliografía Reportes en Español

- [39] RINKU - "Cómo hacer un informe de PENTESTING para el eCPPTv2"
- URL: https://rinku.tech/informe-ecpptv2/
- [42] RINKU - "Cómo hacer un informe de PENTESTING (PLANTILLA GRATIS)" (Video, 2024-04-10)
- URL: https://www.youtube.com/watch?v=vW3C_0BFtAU
- [45] RINKU - "Cómo hacer tu primer informe de PENTESTING" (2025-04-30)
- URL: https://rinku.tech/mi-primer-informe-pentesting/
- [48] 4Geeks - "Informe de Resultados de Pruebas de Penetración (con ejemplos)" (2025-04-24)
- URL: https://4geeks.com/es/lesson/como-hacer-reporte-prubas-de-penetracion-con-ejemplos-y-plantilla
- [54] Hacker Mentor - "Modelo de Informe de Resultados Pentesting"
- URL: https://www.hacker-mentor.com/modeloinformepentesting
- [57] Hacknoid - "¿Cómo presentar un informe de Ethical Hacking?" (2023-02-26)
- URL: https://www.hacknoid.com/hacknoid/presentar-informe-ethical-hacking-plantilla-descargable/

Bibliografía Marco Legal y Ético

- [152] PixelQA - "Ethical & Legal Considerations in Penetration Testing" (2025-03-23)
- URL: https://www.pixelqa.com/blog/post/ethical-legal-considerations-penetration-testing
- [155] Sentrium - "Legal requirements and compliance for penetration testing" (2025-07-06)
- URL: https://www.sentrium.co.uk/insights/what-are-the-legal-aspects-of-penetration-testing
- [158] PlusClouds - "Legal Aspects of Penetration Tests: Legal Processes and Permissions" (2023-07-24)
- URL: https://plusclouds.com/us/blogs/legal-aspects-of-penetration-tests-legal-processes-and-permissions-1
- [161] Roubin - "Legal and Ethical Considerations in Penetration Testing" (2025-09-01)
- URL: https://www.roubin.co.uk/blog/legal-and-ethical-considerations-in-penetration-testing
- [164] CarbonSec - "The Legal Aspects of Ethical Hacking"
- URL: https://www.carbonsec.com/legal-aspects-of-ethical-hacking/
- [167] Vertex Cybersecurity - "The Legal and Ethical Considerations of Penetration Testing" (2024-07-23)
- URL: https://www.vertexcybersecurity.com.au/the-legal-and-ethical-considerations-of-penetration-testing/

Bibliografía NDAs y Contratos

- [151] Template.net - "Cybersecurity NDA (Non-Disclosure Agreement) Template" (2025-03-10)
- URL: https://www.template.net/editable/148052/cybersecurity-nda-non-disclosure-agreement
- [154] GoNitro - "NDA Template" (2016-03-09)
- URL: https://www.gonitro.com/resources/nda-template
- [157] Portant - "International NDA Template - Easy, Online & Free"
- URL: https://www.portant.co/contract-templates/international-nda-template
- [160] GenieAI - "Cyber Security Non Disclosure Agreement - India"
- URL: https://www.genieai.co/en-in/template/cyber-security-non-disclosure-agreement
- [163] eSign - "Free Cyber Security Non-Disclosure Agreement (NDA) | PDF" (2024-06-07)
- URL: https://esign.com/nda/cyber-security/
- [166] NDA Template - "Non-Disclosure Agreement (NDA) Template – Sample"
- URL: https://nondisclosureagreement.com
- [169] LegalZoom - "Non-Disclosure Agreement Templates" (2023-11-05)
- URL: https://www.legalzoom.com/templates/agreements/non-disclosure-agreements
- [170] Penetration Testing - "MSA - Master Service Agreement" (2025-05-08)
- URL: https://www.penetration-testing.com/legal-+-documents/msa

Bibliografía Documentos de Alcance (Scope)

- [171] ClickUp - "Penetration Testing Scope of Work Template" (2025-03-19)
- URL: https://clickup.com/templates/scope-of-work/penetration-testing

- [174] Saudi NCA - "Penetration Testing Standard Template"
- URL: https://cdn.nca.gov.sa/api/files/public/upload/3a098671-bd77-4d76-a24d-7518ae9ac953_STANDARD_Penetration_Testing_Template_en-.pdf

- [177] Trio.so - "Free Penetration Testing Policy Template for Your Organization" (2024-10-08)
- URL: https://www.trio.so/blog/penetration-testing-policy-template/

- [180] Timeless IMS - "Penetration Test Scoping Document"
- URL: https://www.timelessims.co.uk/wp-content/uploads/Timeless%20IMS%20Security%20Pen%20Testing%20and%20Scoping%20document%20v1.0.pdf

- [183] PurpleSec - "Sample Penetration Testing Policy Template" (2025-07-23)
- URL: https://purplesec.us/resources/cyber-security-policy-templates/penetration-testing/

- [186] SANS - "Pen Test Scope Worksheet" (2025-09-10)
- URL: https://www.sans.org/posters/pen-test-scope-worksheet

Bibliografía Vulnerability Disclosure

- [172] OWASP - "Vulnerability Disclosure Cheat Sheet" (2019-12-31)
- URL: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

- [175] Fortinet - "Vulnerability Disclosure: Risks, Significance, and Best Practices"
- URL: https://www.fortinet.com/resources/cyberglossary/vulnerability-disclosure

- [178] Arçelik - "Vulnerability Disclosure Procedure"
- URL: https://www.arcelikglobal.com/en/vulnerability-disclosure-procedure/

- [181] CISA - "Coordinated Vulnerability Disclosure Program" (2025-04-30)
- URL: https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program

- [184] HHS - "Vulnerability Disclosure Policy" (2021-01-07)
- URL: https://www.hhs.gov/vulnerability-disclosure-policy/index.html

- [187] US Commerce - "Vulnerability Disclosure Policy" (2023-06-28)
- URL: https://www.commerce.gov/vulnerability-disclosure-policy

- [189] European Commission - "Vulnerability Disclosure Policy"
- URL: https://commission.europa.eu/legal-notice/vulnerability-disclosure-policy_en

Bibliografía Gestión de Incidentes

-
- [173] DataGuard - "Cyber Security Incident Response Plan" (2024-01-31)
- URL: https://www.dataguard.com/cyber-security/incident-response-plan/

- [176] Balbix - "The Comprehensive Cybersecurity Incident Response Guide" (2025-03-23)
- URL: https://www.balbix.com/insights/cybersecurity-incident-response-a-comprehensive-guide-for-security-leaders/

- [179] Microsoft - "Incident response overview" (2024-11-05)
- URL: https://learn.microsoft.com/en-us/security/operations/incident-response-overview

- [182] NIST - "Computer Security Incident Handling Guide" (SP 800-61r2)
- URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- [185] Australian Cyber Security Centre - "Cyber Incident Response Plan"
- URL: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf

- [188] CREST - "Cyber Security Incident Response Guide"
- URL: https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

Bibliografía Compliance NIST Cybersecurity Framework

- #### [22] SBS CyberSecurity - "NIST CSF Risk Assessment Services" (2025-09-03)
- URL: https://sbscyber.com/services/nist-cybersecurity-framework-assessment
- [25] CyberSaint - "NIST Cybersecurity Assessment Tool" (2024-04-22)
- URL: https://www.cybersaint.io/blog/nist-cybersecurity-framework-assessment-tool
- [32] NIST - "The NIST Cybersecurity Framework (CSF) 2.0"
- URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- [35] NIST - "Assessment & Auditing Resources" (2025-04-01)
- URL: https://www.nist.gov/cyberframework/assessment-auditing-resources
- [156] Cymulate - "NIST Compliance Checklist & Guide" (2025-08-31)
- URL: https://cymulate.com/blog/nist-compliance-checklist/
- [162] LegitSecurity - "NIST Compliance Checklist: A Guide" (2025-02-05)
- URL: https://www.legitsecurity.com/aspm-knowledge-base/nist-compliance-checklist-step-guide
- [168] XM Cyber - "NIST Cybersecurity Framework (CSF) Checklist for 2024" (2025-06-17)
- URL: https://xmcyber.com/the-nist-cybersecurity-framework-2-0-checklist/

Bibliografía Compliance ISO 27001

- [60] Scrut.io - "Understanding ISO 27001 penetration testing: Scope, controls, and compliance" (2025-08-21)
- URL: https://www.scrut.io/hub/iso-27001/penetration-testing

- [63] BlazeInfosec - "ISO 27001 Penetration Testing - The Complete Guide" (2025-05-19)
- URL: https://www.blazeinfosec.com/post/iso-27001-penetration-testing/

- [66] Qualysec - "ISO 27001 Penetration Testing – A Comprehensive Guide" (2025-01-15)
- URL: https://qualysec.com/iso-27001-penetration-testing-a-comprehensive-guide-2023/

- [72] HackerOne - "ISO 27001 and Pentesting: What You Need to Know" (2024-04-30)
- URL: https://www.hackerone.com/blog/iso-27001-and-pentesting-what-you-need-know

Bibliografía Frameworks Generales

- [153] Security Compass - "15 Essential Regulatory and Security Compliance Frameworks" (2025-06-22)
- URL: https://www.securitycompass.com/blog/regulatory-security-compliance-frameworks-standards/
- [159] Cynomi - "8 Key Cybersecurity Compliance Standards and Frameworks" (2025-08-26)
- URL: https://cynomi.com/learn/cybersecurity-compliance-standards-and-frameworks/
- [165] FINRA - "Small Firm Cybersecurity Checklist" (2023-11-30)
- URL: https://www.finra.org/compliance-tools/cybersecurity-checklist

Bibliografía Categorías testing

- [82] BlueVoyant - "Penetration Testing: Complete Guide to Process, Types, and Tools" (2025-01-21)
- URL: https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-tools
- [96] Redscan - "Types of Penetration Testing: Black Box, White Box & Grey Box" (2024-01-23)
- URL: https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/
- [97] Qualysec - "Types of Pen Testing in Cyber Security: A Comprehensive Guide" (2025-02-12)
- URL: https://qualysec.com/types-of-pen-testing/
- [100] N-ix - "Types of penetration testing: A comprehensive guide" (2024-11-04)
- URL: https://www.n-ix.com/types-of-penetration-testing/
- [101] Sprocket Security - "Top 8 Penetration Testing Types, Techniques, and Best Practices" (2024-11-20)
- URL: https://www.sprocketsecurity.com/blog/pentesting-types-2
- [103] BrightSec - "9 Penetration Testing Types" (2025-03-24)
- URL: https://brightsec.com/blog/penetration-testing-types/
- [110] Coursera - "What Are the Different Types of Penetration Testing?" (2025-06-04)
- URL: https://www.coursera.org/articles/types-of-penetration-testing

Bibliografía Categorías testing

- [98] CyberSapiens - "Which tools should be used to perform a wireless infrastructure penetration test" (2025-06-05)
- URL: https://cybersapiens.com.au/which-tools-should-be-used-to-perform-a-wireless-infrastructure-penetration-test/
- [105] VikingCloud - "What is Wireless Penetration Testing?" (2025-09-08)
- URL: https://www.vikingcloud.com/blog/what-is-wireless-penetration-testing
- [111] Threat Intelligence - "What is Wireless Penetration Testing?" (2024-11-06)
- URL: https://www.threatintelligence.com/blog/wireless-penetration-testing

Bibliografía Physical & Social Engineering

- [112] ISACA - "Physical Penetration Testing" (White Paper, 2023-09-04)
- URL: https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing

- [115] Sprocket Security - "Social Engineering Penetration Testing: A Practical Guide" (2024-09-26)
- URL: https://www.sprocketsecurity.com/blog/social-engineering-penetration-testing-a-practical-guide

- [118] University of Twente - "Two methodologies for physical penetration testing using social engineering"
- URL: https://research.utwente.nl/files/5468345/ACSAC_pentesing_methodology_%5B1%5D.pdf
- [121] Ares Security - "A Deep Dive into Physical Penetration Testing" (2024-10-31)
- URL: https://aressecuritycorp.com/2024/11/01/physical-penetration-testing/

- [124] Tesserent - "What Is Physical Penetration Testing? Pen testing explained" (2024-12-10)
- URL: https://tesserent.com/resources/what-is-physical-penetration-testing-pentests-explained

- [127] PurpleSec - "Social Engineering Penetration Testing: Attacks, Methods, and Tools" (2025-07-17)
- URL: https://purplesec.us/learn/social-engineering-penetration-testing/

- [130] PurpleSec - "13 Physical Penetration Testing Methods That Work" (2025-07-17)
- URL: https://purplesec.us/learn/physical-penetration-testing/

Bibliografía Categorías Cloud & IoT Testing

- [113] Passcurity - "Penetration Testing in 2025: New Focus on Cloud and IoT Security" (2025-04-28)
- URL: https://passcurity.com/penetration-testing-2025-cloud-iot-security/
- [116] Haxoris - "IoT and Embedded Device Penetration Testing" (2024-10-31)
- URL: https://haxoris.com/services/penetration-testing/iot
- [119] Integrity360 - "What is IoT penetration testing and why do you need It?" (2024-09-15)
- URL: https://insights.integrity360.com/what-is-iot-penetration-testing-and-why-do-you-need-it
- [122] Praetorian - "IoT Penetration Testing that Identifies Security Risks" (2024-06-30)
- URL: https://www.praetorian.com/services/iot-penetration-testing/
- [125] Bright Defense - "What is IoT Penetration Testing?" (2025-06-25)
- URL: https://www.brightdefense.com/resources/iot-penetration-testing/
- [128] CloudTribe - "What Is IoT Penetration Testing?"
- URL: https://cloudtri.be/pentest/iot/
- [131] Microminder CS - "IoT Penetration Testing: Why It Matters and How It's Done" (2025-07-30)
- URL: https://www.micromindercs.com/blog/iot-penetration-testing

Bibliografía API & Mobile Testing

- [114] SecureIdeas - "API and Mobile App Penetration Testing"
- URL: https://www.secureideas.com/api-and-mobile-app-penetration-testing
- [117] Appknox - "What is API Security for Mobile Apps? Why Is It Important?" (2025-03-11)
- URL: https://www.appknox.com/blog/complete-guide-on-api-security-for-mobile-apps
- [120] Akamai - "What Is API Penetration Testing?" (2025-03-18)
- URL: https://www.akamai.com/glossary/what-is-api-penetration-testing
- [123] VeraSafe - "Mobile App and API Penetration Testing Service"
- URL: https://verasafe.com/cybersecurity-solutions/mobile-app-penetration-testing/
- [126] Qualysec - "Mobile App Security Testing" (2025-06-19)
- URL: https://qualysec.com/mobile-app-security-testing/
- [129] Datami - "Mobile Application Penetration Testing Services" (2025-08-31)
- URL: https://datami.ee/services/pentest/mobile-app-penetration-testing/

Bibliografía Herramientas de Pentesting

- [59] Campus Ciberseguridad - "Burp Suite una herramienta de pentesting" (2025-06-15)
- URL: https://www.campusciberseguridad.com/blog/burp-suite-una-herramienta-de-pentesting/
- [62] Logic Solutions - "Explorando las herramientas más eficaces para el pentesting en 2024" (2024-09-18)
- URL: https://www.logicsolutions.es/es/blog/explorando-las-herramientas-mas-eficaces-para-el-pentesting-en-2024
- [65] Campus Ciberseguridad - "Metasploit. La herramienta esencial en Ciberseguridad" (2025-08-11)
- URL: https://www.campusciberseguridad.com/blog/metasploit-herramienta-esencial-ciberseguridad/
- [68] Check Point - "Las 19 mejores herramientas para pruebas de penetración" (2024-03-27)
- URL: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-penetration-testing/top-19-penetration-testing-tools/
- [71] Metasploit - "Metasploit | Penetration Testing Software" (2025-06-05)
- URL: https://www.metasploit.com
- [74] Tecnógrafos - "Las 13 herramientas más usadas para pentesting y hacking" (2022-05-11)
- URL: https://tecnografos.es/2022/05/12/las-13-herramientas-mas-usadas-para-pentesting-y-hacking-por-los-profesionales/
- [77] HackMetrix - "Penetration Testing: 5 herramientas que ayudan a su ejecución" (2024-08-08)
- URL: https://blog.hackmetrix.com/penetration-testing/

Bibliografía Templates

- [16] Julio Cesar Fort - "public-pentesting-reports"
- URL: https://github.com/juliocesarfort/public-pentesting-reports

- [190] MTK911 - "pentest-report-template" (2020-04-01)
- URL: https://github.com/MTK911/pentest-report-template

- [191] Heath Adams (TCM Security) - "TCM-Security-Sample-Pentest-Report" (2019-05-26)
- URL: https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report

- [192] h0tPlug1n - "Web-Penetration-Testing-Report-Sample" (2021-09-02)
- URL: https://github.com/h0tPlug1n/Web-Penetration-Testing-Report-Sample

- [196] cyber-cfreg - "Penetration-Test-Report-Template" (2022-02-28)
- URL: https://github.com/cyber-cfreg/Penetration-Test-Report-Template

- [199] Reconmap - "pentest-reports" (2020-08-27)
- URL: https://github.com/reconmap/pentest-reports

- [202] Ryan Sapone - "Web-Pentest-Report" (2024-04-25)
- URL: https://github.com/Ryan-Sapone/Web-Pentest-Report

- [205] PwnDoc - "pwndoc: Pentest Report Generator" (2025-08-25)
- URL: https://github.com/pwndoc/pwndoc

Bibliografía Checklists

- [194] Harshinsecurity - "web-pentesting-checklist" (2020-10-24)
- URL: https://github.com/harshinsecurity/web-pentesting-checklist

- [197] Hrishikesh7665 - "Android-Pentesting-Checklist" (2022-12-30)
- URL: https://github.com/Hrishikesh7665/Android-Pentesting-Checklist

- [203] OWASP - "OWASP Web Application Penetration Checklist v1.1"
- URL: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf

- [206] Indusface - "API PenTesting Checklist (XLSX)"
- URL: https://www.indusface.com/downloads/api-pen-testing-checklist-indusface.xlsx

- [200] A-Lign - "A Comprehensive Checklist for Penetration Testing" (2025-05-29)
- URL: https://www.a-lign.com/articles/penetration-testing-checklist

Bibliografía Reportes Públicos

- [193] PentestReports.com - "Free Penetration Test Report Templates"
- URL: https://pentestreports.com/templates
- [195] PurpleSec - "Sample Vulnerability Assessment Report - Example Institute"
- URL: https://purplesec.us/wp-content/uploads/2019/12/Sample-Vulnerability-Assessment-Report-PurpleSec.pdf
- [198] PurpleSec - "Sample Network Vulnerability Assessment Report"
- URL: https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf
- [201] MaxAPEX - "Vulnerability Assessment Report Template"
- URL: https://www.maxapex.com/wp-content/uploads/2024/07/Vulnerability-Assessment-Report-Template.pdf
- [204] Indusface - "Vulnerability Assessment Report"
- URL: https://www.indusface.com/images/download/Vulnerability_Assessment_Sample_Report.pdf
- [207] Invia - "Vulnerability Assessment and Penetration Testing Report"
- URL: https://invia.com.au/App/media/sample%20vapt%20report.pdf
- [208] Overleaf - "Penetration Test Report Template (LaTeX)" (2025-09-30)
- URL: https://www.overleaf.com/latex/templates/penetration-test-report-template/gbzgfgsnqyvq