sustantiva
CON•SENTIDO

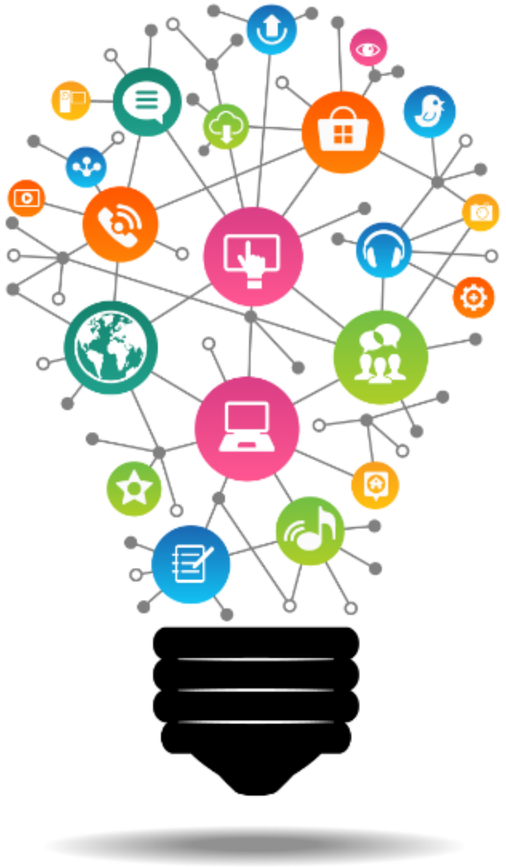
Energiza!

Principios y Estructura para la Documentación de Hallazgos en Seguridad Informática

Introducción

Introducción

- La documentación de hallazgos de seguridad es **una práctica esencial** en la gestión del riesgo.
- Permite comunicar amenazas técnicas de forma comprensible y accionable.
- Facilita la toma de decisiones, el cumplimiento normativo y la mejora continua.

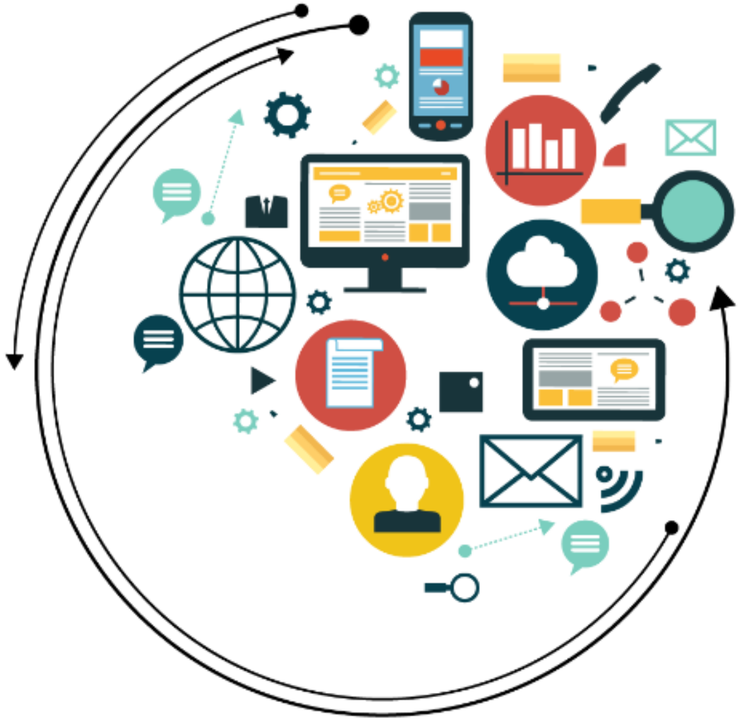


Principios Fundamentales

Principios Fundamentales

📌 Toda documentación técnica debe cumplir con:

1. **Claridad**: Lenguaje comprensible y sin ambigüedades.
2. **Precisión**: Datos exactos y reproducibles.
3. **Priorización**: Enfocar en lo urgente y crítico.
4. **Acción orientada**: Recomendaciones prácticas y aplicables.



Componentes Clave de un Informe

Componentes Clave de un Informe

🧱 Estructura esencial según buenas prácticas (OWASP, SANS):

- **Título**
- **Resumen Ejecutivo**
- **Descripción Técnica**
- **Impacto**
- **Recomendaciones Priorizadas**

🎯 Cada componente cumple una función para públicos diversos (técnico/no técnico).

Ejemplo de Resumen Ejecutivo

Ejemplo de Resumen Ejecutivo

“Se identificaron cinco vulnerabilidades críticas. Se recomienda aplicar inmediatamente los parches descritos en el punto 1, incluyendo la actualización del sistema operativo a su versión estable.”

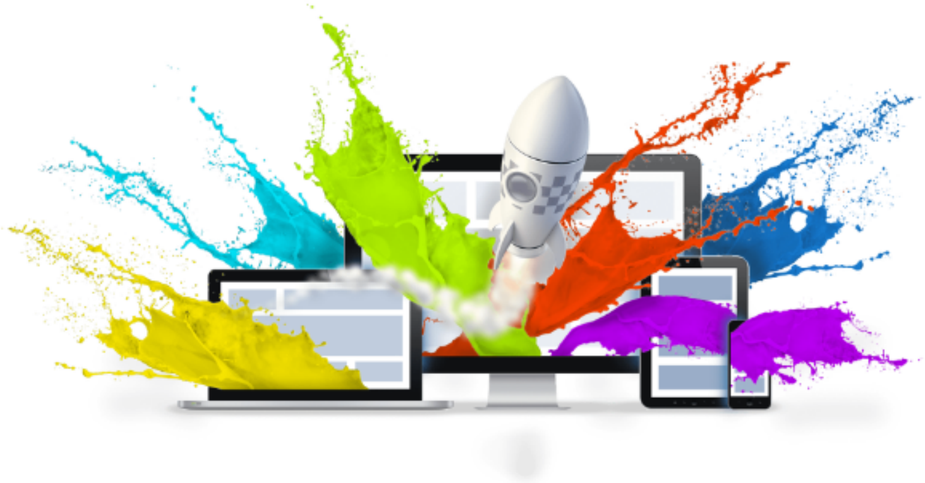
- ✔ Enfocado en tomadores de decisión
- ✔ Lenguaje simple
- ✔ Impacto claro

Ejemplo de Descripción Técnica

Ejemplo de Descripción Técnica

- Herramienta utilizada: Burp Suite
- Vulnerabilidad: SQL Injection
- URL: `https://example.com/login.php?username=…`
- Evidencia: error de MySQL en respuesta

📎 Permite a analistas reproducir y validar el hallazgo



Sección de Impacto

Sección de Impacto

“Esta vulnerabilidad puede ser explotada para acceder a datos sensibles de usuarios, violando los principios de confidencialidad y privacidad.”

⚠️ El impacto debe estar ligado a la seguridad organizacional

Recomendaciones Técnicas Priorizadas

Recomendaciones Técnicas Priorizadas

📌 Ordenadas por criticidad (ej. CVSS):

1. Implementar validación en entradas
2. Aplicar parches
3. Capacitar al equipo

✔️ Claras
✔️ Técnicamente justificadas
✔️ Viables

Estructura Recomendada del Informe

Estructura Recomendada del Informe

1. **Portada**
2. **Tabla de contenidos**
3. **Resumen Ejecutivo**
4. **Introducción**
5. **Hallazgos (descripción + impacto + recomendación)**
6. **Conclusiones**
7. **Anexos (evidencia técnica)**

🎯 Favorece lectura rápida y seguimiento estructurado

Adaptación a Públicos Diferentes

Adaptación a Públicos Diferentes

Público Técnico	Público No Técnico
Lenguaje especializado	Lenguaje claro y simple
Logs, capturas, scripts	Impacto económico/ legal
Instrucciones detalladas	Planes de acción ejecutivos

📎 Un informe profesional debe servir a ambos públicos

Conclusión

Conclusión

- Documentar hallazgos es **clave para la mitigación del riesgo**.
- Aplicar principios de claridad, precisión y priorización mejora la utilidad del informe.
- Una estructura clara y adaptada asegura la comprensión transversal.
- **La documentación efectiva transforma vulnerabilidades en decisiones informadas.**


Energiza!