ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

CHARLAS 9 BÁSICOS 2026
“ACTUALIZAR PERIODICAMENTE”

09 de ABRIL, 2026

BENJAMÍN ITURRA PIÑONES
PROFESIONAL ANCI

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

TEMARIO:

- ¿Por qué hay que actualizar?
- Riesgos de no actualizar
- ¿Cómo priorizar?
- ¿Cómo comenzar? (Plan de acción)
- Buenas prácticas operativas
- ¿Cómo disminuir el riesgo?
- Validación post parcheo

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿POR QUÉ HAY QUE ACTUALIZAR?

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

¿Por qué actualizar?

Vulnerabilidad: Error o debilidad en un sistema que alguien puede aprovechar para hacer algo que no debiera.

Vulnerabilidades Conocidas

Nivel de riesgo identificado

Alta probabilidad de explotación

Vulnerabilidades de día 0

No conocidas.

No hay parche.

Dificultad de detección por parte del A.V.

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

¿Por qué actualizar?

- Todo el tiempo aparecen nuevas vulnerabilidades, por lo que “estar al día” hoy, no asegura estar al día mañana o en una semana más.

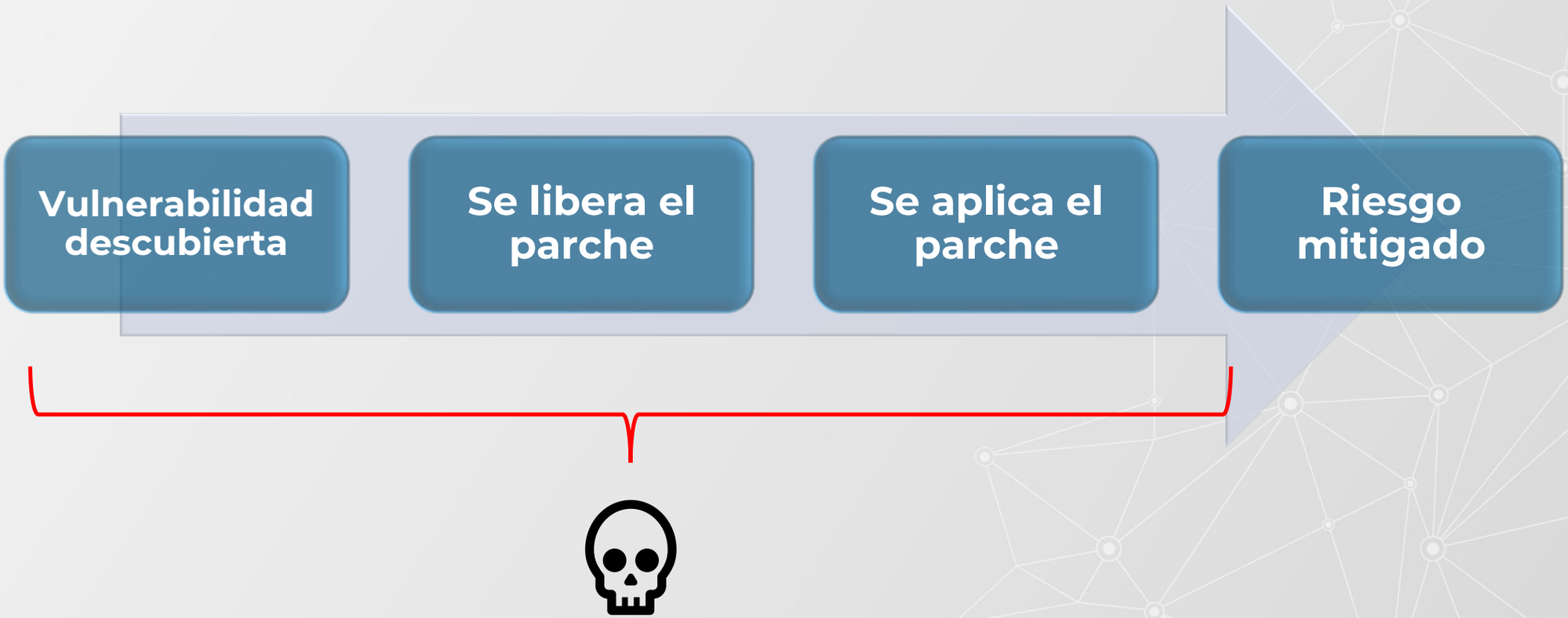
- Algunos ejemplos de vulnerabilidades conocidas que causaron gran impacto:

    - Log4Shell (2021):
    - RCE que permitía tomar el control de un servidor solo con el envío de una línea de código.
    - Afectó a millones de sistemas en todo el mundo, generándose ataques automatizados.

    - ProxyLogon de MS Exchange (2021):
    - Cadena de vulnerabilidades que permitía ataques masivos a servidores de correo electrónico.
    - Miles de organizaciones comprometidas en pocos días.

¿Por qué actualizar?

- **Ventana de exposición**: corresponde al tiempo que transcurre desde que se descubre una vulnerabilidad hasta que se aplica el parche o la medida de mitigación.



ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

RIESGOS DE NO ACTUALIZAR

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Riesgos de no actualizar

Más del 30% de los incidentes de efecto significativo registrados durante el año 2025 utilizaron como acceso inicial la **explotación de una vulnerabilidad** expuesta hacia internet.

Implicancias

- Ransomware
- Fuga de información
- Caídas de servicio
- Instalación de WebShell
- Defacement o simples modificaciones de sitios

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿CÓMO PRIORIZAR?

¿Cómo priorizar?

- Vulnerabilidades críticas (CVSS alto/ explotación activa).

Riesgo	Puntuación CVSS
Nulo	0.0
Bajo	0.1-3.9
Medio	4.0-6.9
Alto	7.0-8.9
Crítico	9.0-10.0

- Sistemas expuestos a internet (superficie de exposición).
- Activos críticos del negocio.

- Datos sensibles.

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿CÓMO COMENZAR?

PLAN DE ACCIÓN

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

¿Cómo comenzar? (plan de acción)

- Inventario de activos
- Identificación de software y versiones
- Definir política de parcheo
- Automatización
- Ventanas de mantenimiento

¿Cómo comenzar? (plan de acción)

Inventario de activos:

- La base para implementar este control es contar con un inventario de activos.
- Para esto se debe llevar un registro de los **equipos, sistemas operativos y aplicaciones** implementadas en estos.

Algunas soluciones Open Source para inventario:

GLPI

SNIPE-IT

OCS inventory

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

BUENAS PRÁCTICAS OPERATIVAS

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Buenas prácticas operativas

- Calendario de parcheo
- Ambiente de pruebas
- Automatización
- Reportes de cumplimiento
- Gestión de excepciones

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿CÓMO DISMINUIR RIESGO?

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

¿Cómo disminuir el riesgo?

- Parcheo oportuno
- Mitigaciones temporales
- Segmentación de red
- Mínimos privilegios
- Seguridad de endpoint

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

VALIDACIÓN POST PARCHEO

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Validación post parcheo

- ✓ Verificar funcionamiento
- ✓ Confirmar aplicación de parche
- ✓ Pentesting
- ✓ Monitoreo post-cambio
- ✓ Plan de rollback

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

CONCLUSIONES

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Conclusiones

- Una buena estrategia nos permitirá acortar ventanas de exposición o al menos hacer que estas no tiendan a infinito.
- Es posible implementar este control con un costo bajo o aprovechando las oportunidades disponibles.
- La base para este y para prácticamente todos los controles de seguridad es contar con un buen registro de inventario.
- La priorización es clave en el éxito de una estrategia de parcheado, es imposible tener todo al día, pero sí se puede gestionar lo más urgente.

Actualizar periódicamente no elimina todos los riesgos, pero no hacerlo deja la puerta abierta.

¡Muchas gracias!

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

🌐 www.anci.gob.cl
📩 ayuda@anci.gob.cl
📞 1510