Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Estándar Gestión de Parches

16
CAPÍTULO

Estándar de TI:
Estándar Gestión de Parches

1.0 Propósito y Beneficios

La gestión de parches de seguridad (administración de parches) es una práctica diseñada para prevenir de forma proactiva la explotación de las vulnerabilidades de TI que existen dentro de una organización. Al aplicar actualizaciones (parches) de software o firmware relacionados con la seguridad a los sistemas de TI aplicables, el resultado esperado es reducir el tiempo y el dinero dedicados a lidiar con exploits al reducir o eliminar la vulnerabilidad relacionada.

2.0 Alcance

Este estándar se relaciona específicamente con las vulnerabilidades que pueden abordarse mediante una actualización de software o firmware (parche) y se aplica a todo el software utilizado en los sistemas de la Repartición. Se debe seguir el Estándar de Escaneo de Vulnerabilidades para conocer los requisitos para abordar las vulnerabilidades sin parches.

3.0 Declaración de Información

1. Las Reparticiones deben asignar a un individuo o grupo dentro de las operaciones de TI para que sea responsable de la gestión de parches.
2. Si se subcontrata la gestión de parches, deben existir acuerdos de nivel de servicio que aborden los requisitos de este estándar y describan las responsabilidades para la aplicación de parches. Si el parcheo es responsabilidad del tercero, las entidades deben verificar que se hayan aplicado los parches.
3. Debe existir un proceso para gestionar los parches. Este proceso debe incluir lo siguiente:

    - Monitorear fuentes de seguridad (Apéndice A) para vulnerabilidades, corrección con y sin parches y amenazas emergentes;
    - Supervisar la distribución de parches, incluida la verificación de que se esté siguiendo un procedimiento de control de cambios;
    - Pruebas de estabilidad e implementación de parches; y

- Utilizando una herramienta de distribución de gestión de parches centralizada y automatizada, siempre que sea técnicamente posible, que:

    - mantiene una base de datos de parches;
    - implementa parches en los dispositivos; y
    - verifica la instalación de parches.

4. Debe existir una separación adecuada de funciones para que las personas que verifican la distribución de parches no sean las mismas que distribuyen los parches.
5. De acuerdo con la Política de Seguridad de la Información, todas las entidades deben mantener un inventario de activos de hardware y software. La gestión de parches debe incorporar todos los activos de TI instalados.
6. Se debe priorizar la gestión de parches en función de la gravedad de la vulnerabilidad que aborda el parche. En la mayoría de los casos, las clasificaciones de gravedad se basan en el Sistema de puntuación de vulnerabilidad común (CVSS). Una puntuación CVSS de 7 a 10 se considera una vulnerabilidad de alto impacto, una puntuación CVSS de 4 a 6,9 se considera una vulnerabilidad de impacto moderado y una CVSS de 0 a 3,9 se considera una vulnerabilidad de bajo impacto.
7. En la medida de lo posible, el proceso de aplicación de parches debe seguir el cronograma contenido en la siguiente tabla:

Impacto /Severidad	Parche iniciado	Parche completado
Alto	Dentro de las 24 horas posteriores al lanzamiento del parche	Dentro de 1 semana del lanzamiento del parche
Medio	Dentro de 1 semana del lanzamiento del parche	Dentro de 1 mes desde el lanzamiento del parche
Bajo	Dentro de 1 mes desde el lanzamiento del parche	Dentro de los 2 meses posteriores al lanzamiento del parche, a menos que ISO determine que se trata de un riesgo insignificante para el medio ambiente.

8. Si la aplicación de parches no se puede completar en el plazo indicado en la tabla anterior, se deben implementar controles de compensación dentro de los plazos anteriores y se debe seguir el proceso de excepción.
9. Si un parche requiere reiniciar para su instalación, el reinicio debe realizarse dentro de los plazos descritos anteriormente.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Definiciones de términos clave

Fecha	Descripción de Cambio
Exploit	Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos, o el hardware.
CVSS SIG	Es un grupo de expertos que trabajan sobre el estándar CVSS, que es una forma de puntuar/clasificar la severidad de una vulnerabilidad.

6.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
29/07/2024	Documento inicial, primera revisión	Alejandro Castro Pablo Zalazar

7.0 Documentos relacionados

Instituto Nacional de Estándares y Tecnología, Publicación especial 800-40, Guía de tecnologías de gestión de parches empresariales

Sistema de puntuación de vulnerabilidad común

Apéndice A:

EJEMPLOS DE FUENTES DE SEGURIDAD PARA INFORMACIÓN DE VULNERABILIDAD/PARCHE/AMENAZAS

Estándar de escaneo de vulnerabilidades

- Sitios web de proveedores/listas de notificaciones
- Escáneres de vulnerabilidad
- Pruebas de penetración
- Base de datos nacional de vulnerabilidad