# FACULTAD DE ESTUDIOS SUPERIORES ZARAGOZA
# DIVISIÓN DE PLANEACIÓN INSTITUCIONAL

## 34.- Mecanismos de revisión, modificación o actualización de herramientas electrónicas y/o de los sistemas de información propios.

**-Gestión de parches y actualización de software.**

Descripción: Este proceso asegura que las herramientas y aplicaciones se mantengan actualizadas con las últimas versiones y parches de seguridad.

Métodos:

- Actualizaciones automáticas: Configurar las herramientas para descargar e instalar parches automáticamente.
- Notificaciones de actualizaciones: Los sistemas pueden alertar a los administradores cuando hay nuevas versiones o actualizaciones críticas disponibles.
- Planificación de actualizaciones: Realizar actualizaciones durante ventanas de mantenimiento planificadas para minimizar la interrupción de los servicios.
- Pruebas de actualizaciones: Antes de implementar actualizaciones a toda la red, se prueban en un entorno controlado o en una pequeña parte de la infraestructura para evitar problemas.

**-Monitoreo continuo de hardware y software.**

Descripción: Monitorear el rendimiento y estado de las herramientas electrónicas en tiempo real para detectar fallos o la necesidad de mantenimiento.

Métodos :

- Sistemas de monitoreo de red: Herramientas que supervisan el estado de los dispositivos de red (switches, routers) y servidores, alertando sobre problemas como sobrecarga, fallos de hardware o software desactualizado.
- Monitoreo de recursos: Controlar el uso de CPU, memoria, almacenamiento y otros recursos para identificar posibles cuellos de botella o la necesidad de mejorar el hardware.
- Alertas automáticas: Configurar alertas que notifiquen sobre problemas de rendimiento o disponibilidad.

**-Auditorías y evaluaciones de seguridad**

Descripción: Revisión periódica de las herramientas electrónicas y sistemas para asegurar que cumplan con las políticas de seguridad.

Métodos:

- Auditorías de seguridad: Revisar los sistemas para identificar vulnerabilidades en hardware, software o configuraciones de red.
- Pruebas de penetración: Simular ataques para identificar debilidades en la red o en las herramientas electrónicas.
- Revisión de logs: Analizar los registros de actividad para detectar patrones inusuales o intentos de intrusión.
- Análisis de vulnerabilidades: Utilizar herramientas especializadas para identificar debilidades conocidas en software o hardware que necesiten actualizaciones.

**-Control de versiones de software**

Descripción: Mecanismo que permite la gestión de versiones de software y herramientas para evitar conflictos o errores al modificar o actualizar aplicaciones.

Métodos:

- Sistemas de control de versiones: Uso de herramientas como Git para gestionar diferentes versiones de software y asegurarse de que las modificaciones se realicen de manera ordenada.
- Ramas de desarrollo: Separar entornos de desarrollo, pruebas y producción para evitar implementar cambios no probados directamente en producción.
- Historial de cambios: Mantener un registro de todas las modificaciones para permitir revertir cambios en caso de error.

## 34.- Mecanismos de revisión, modificación o actualización de herramientas electrónicas y/o de los sistemas de información propios.

**-Pruebas de compatibilidad y actualización**

Descripción: Asegurar que las herramientas electrónicas actualizadas sean compatibles con otros sistemas y software existentes.

Métodos:

- Pruebas en entornos de prueba: Ejecutar las actualizaciones en entornos aislados para verificar la compatibilidad antes de la implementación completa.
- Pruebas de regresión: Asegurarse de que una actualización no rompa funcionalidades que previamente funcionaban bien.
- Pruebas automatizadas: Usar scripts y herramientas que prueben de manera automática si las actualizaciones son compatibles y si el sistema sigue funcionando correctamente.

**-Gestión de cambios**

Descripción: Procesos formales para revisar y aprobar cambios en las herramientas electrónicas dentro de la red o sistema informático.

Métodos:

- Aprobación de cambios: Evaluar y aprobar los cambios propuestos antes de ejecutarlos, asegurando que todos los riesgos y posibles inconvenientes hayan sido considerados.
- Planificación de cambios: Definir cuándo y cómo se realizarán los cambios, minimizando la interrupción de los servicios.
- Revisión post-implementación: Evaluar el éxito del cambio y documentar cualquier incidente.

**-Mantenimiento preventivo de hardware**

Descripción: Implementación de tareas de mantenimiento para asegurar que los dispositivos físicos (servidores, switches, routers, etc.) funcionen correctamente y prevenir fallos.

Método:

- Limpieza de equipos: Mantenimiento físico para evitar problemas como sobrecalentamiento o acumulación de polvo que afecten el rendimiento.
- Reemplazo de piezas: Cambio proactivo de componentes con una vida útil limitada (por ejemplo, discos duros o fuentes de poder) antes de que fallen.
- Monitoreo de temperatura y ventilación: Supervisión de las condiciones ambientales en los centros de datos para garantizar que los dispositivos operen dentro de sus límites óptimos.