GUÍA RÁPIDA
ACTUALIZACIONES DE SEGURIDAD

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

La actualización de seguridad es un **parche que permite corregir vulnerabilidades** presentes en los sistemas operativos, navegadores web, aplicaciones o programas. Es una medida clave para proteger a las instituciones.

El principal problema de no parchar una vulnerabilidad es la **alta exposición a ataques** como un ransomware o filtración de datos. Como consecuencia de ello, una institución puede estar expuesta a una interrupción operacional, en caso de que el sistema presente una falla, como también a un daño reputacional o legal, especialmente si hubo fuga de datos.

¿Qué actualizar?

Todos los dispositivos conectados o que tengan acceso a Internet, ya sea que los uses a diario o con poca frecuencia. Por ejemplo:

- En computadores considera el sistema operativo, softwares, navegadores, etc.
- En routers y puntos de acceso Wifi: firmware.
- En sistemas de pago considera el software de gestión y seguridad.
- En impresoras y escáneres de red: controladores y firmware.

Para gestionar adecuadamente las vulnerabilidades, puedes elaborar un **plan de actualización.**

¿Qué considerar en un plan de actualizaciones?

1. **Inventario:** Conocer todos los activos de la institución es fundamental para evitar que algún dispositivo se quede sin su actualización. Para ello, considera en el inventario todos los computadores, incluso celulares, activos de TI relevantes, servidores y sistemas de IoT.

2. **Prioriza:** Define los activos críticos de tu organización y priorízalos al momento de actualizar. Considera aquellas vulnerabilidades calificadas como críticas y de alto riesgo, así como también las vulnerabilidades publicadas por parte de un fabricante o del CSIRT Nacional, especialmente si están siendo explotadas activamente. Considera su parcheo fuera del ciclo normal.

3. **Planifica:** Elabora un cronograma para actualizar, especificando fecha y hora. De esta manera, te asegurarás de realizar las actualizaciones de manera oportuna.

4. **Actualización automática:** Cuando sea posible, configura los dispositivos y aplicaciones para que se actualicen de forma automática. Algunos softwares avisan cuando los parches están disponibles.

5. **Permisos:** Define roles y responsabilidades sobre quienes pueden actualizar y descargar programas y software.

6 **Implementación:** Al instalar parches, intenta hacerlo de forma paulatina para identificar potenciales problemas o incompatibilidades. Esto permite que, en caso de falla, el impacto afecte a la menor cantidad de usuarios. Asimismo, antes de aplicar un parche en producción, prueba los cambios en un entorno controlado y define un procedimiento de reversión si algo falla.

7 **Monitorización:** Una vez actualizado los sistemas, asegúrate de que se hayan aplicado correctamente los parches y que los sistemas funcionen según lo esperado.

8 **Registro:** Realiza un informe sobre el proceso de actualización: fechas, vulnerabilidades abordadas, versiones y cualquier incidente o problema que haya ocurrido. Esto te ayudará en caso de auditoría y en la mejora continua del proceso de gestión de parches.

9 **Educa:** Capacita a los usuarios sobre la importancia de mantener los sistemas actualizados y cómo hacerlo en sus dispositivos personales e institucionales, en caso de que corresponda.