# Caja de herramientas de ciberseguridad de la GCA: documento guía para las herramientas de «Actualice sus defensas»

Los ciberdelincuentes no dejan de buscar mecanismos que les permitan acceder a los sistemas y los datos. Uno de ellos es encontrar un punto débil en la configuración o el código de un desarrollador. Este punto débil podría replicarse en toda la base de usuarios, lo que los ciberdelincuentes podrían utilizar en su propio beneficio.

Los fabricantes y los desarrolladores de software publican periódicamente actualizaciones de los sistemas operativos y aplicaciones para resolver los nuevos puntos débiles o vulnerabilidades que se detectan.

- Estas correcciones se conocen popularmente como *parches* y su aplicación, como *parcheado*.

**Es muy importante que los parches se apliquen rápidamente y, si es posible, de forma automática para evitar que se utilicen en un ciberataque.**

- El ataque de ransomware de WannaCry que tuvo lugar en mayo de 2017 aprovechó un defecto que se detectó en el sistema operativo Windows y tuvo consecuencias devastadoras en todo el mundo.
    - Su objetivo no era un sector específico, sino un tipo de dispositivo, por ello:
        - Afectó a usuarios particulares.
        - Afectó a organizaciones pequeñas, medianas y grandes.
        - Afectó a las fuerzas de seguridad, los sistemas de salud, los sistemas de transporte, las telecomunicaciones, los servicios de banca, etc.
    - Se estima que en tan solo 24 horas más de 230 000 sistemas informáticos de 150 países se vieron afectados, lo que supuso unas pérdidas milmillonarias.

- Microsoft había publicado parches para todos los dispositivos compatibles en marzo de 2017:
    - Los que no instalaron estos parches antes del ataque son los que estuvieron en riesgo.
    - Los que sí habían aplicado el parche (ya fuera manual o automáticamente) no se vieron afectados.
    - Todos los que utilizaban Windows XP se vieron afectados porque este sistema operativo ya no contaba con actualizaciones, lo que se conoce como *fin del ciclo de vida* (aunque, dada la gravedad de WannaCry, enseguida se desarrolló un parche).

**Fin del ciclo de vida**
Todos los dispositivos y sistemas operativos tienen un fin del ciclo de vida, es decir, una fecha a partir de la cual ya no reciben mantenimiento ni soporte electrónico y dejan de publicarse parches, por lo que de inmediato se convierten en un riesgo si se detectan nuevas vulnerabilidades. Esto también puede ocurrir si un fabricante deja de dar servicio y nadie se encarga del desarrollo de su grupo de productos.

- Windows 7 alcanzó su fin de ciclo de vida en enero de 2020.
- Windows XP alcanzó su fin de ciclo de vida en abril de 2014.
- *Los sistemas que ya no cuentan con soporte técnico deberían quitarse de la red, actualizarse o reemplazarse.*

**Dispositivos de IoT**
El aumento de los dispositivos del Internet de las cosas (IoT, por sus siglas en inglés), especialmente en el mercado de los productos de consumo, donde las decisiones de compra suelen tener más en cuenta el precio, la facilidad de uso y la funcionalidad que la seguridad, puede incrementar la aparición de potenciales vías de acceso para los atacantes. Muchos tienen características de seguridad limitadas y no permiten la aplicación de parches, por lo que, si tuvieran algún defecto, dejarían la red abierta para los atacantes hasta que se eliminaran físicamente o se implementaran métodos de mitigación adecuados. El margen de acción para eliminar este riesgo, de haberlo, sería mínimo.

En el caso de las aplicaciones antiguas que ya no están en uso y los equipos heredados (equipos antiguos que se han *adaptado* para utilizarse en una red o a través de Internet), es mejor eliminarlos. Lo ideal sería que se hubieran identificado, eliminado o actualizado con las herramientas de «Conozca su sistema», lo que garantizaría que se han adoptado los niveles mínimos de acceso para disfrutar de una funcionalidad normal.

En resumen:

- Los parches y actualizaciones contienen importantes revisiones de seguridad que ofrecen protección ante nuevas vulnerabilidades detectadas, y deberían aplicarse de inmediato, preferiblemente de forma automática (si fuera posible).
    - *Si los parches no se aplican a tiempo, los sistemas informáticos (y, por tanto, toda la organización), estarán en una situación de riesgo.*
- Deshágase de los dispositivos que no permitan aplicar parches (como muchos de los de IoT de consumo general) y de cualquier aplicación o dispositivo que ha dejado de recibir soporte técnico. De lo contrario, estará poniendo en riesgo a su organización.
    - *Si el dispositivo es necesario para la actividad, aíslelo lo máximo posible e impida todo tipo de acceso a Internet y a otros dispositivos.*

- Garantice los niveles mínimos de acceso para conseguir una funcionalidad normal y quite de inmediato el acceso a los empleados que abandonen la organización o a las empresas de terceros (o clientes) con los que ya no mantenga relación.

- Asegúrese de que todo el software y los sistemas están actualizados, cuentan con los últimos parches de seguridad y se revisan periódicamente.

**Utilice las herramientas de «Actualice sus defensas» como ayuda. Establezca una normativa interna que garantice revisiones periódicas de sus activos, de su cadena de suministro y de sus actualizaciones.**

**https://gcatoolkit.org/es/pequenas-empresas/actualice-sus-defensas/**