CSIRTSALUD-AL-20250729-08

TLP: CLEAR

Incidente Id	CSIRTSALUD-AL-20250729-08
Fecha del reporte	29/07/2025
Entidad	Todas las entidades del ecosistema digital
Título	Alerta Preventiva: Fin de Soporte del Sistema Operativo Microsoft Windows 10
Herramienta de detección	Análisis de Fuentes Públicas / Comunicado Oficial de Microsoft
Activo involucrado	Estaciones de trabajo, equipos portátiles y otros dispositivos que operen con el sistema operativo Microsoft Windows 10.
Tipo de incidente	Riesgo Operativo y de Seguridad por Fin de Ciclo de Vida (EOL)
Nivel de riesgo	Alto

Descripción:

Como parte de las labores de monitorización y vigilancia tecnológica, el equipo CSIRT Salud informa sobre el fin de ciclo de vida (End of Life - EOL) del sistema operativo Microsoft Windows 10, programado oficialmente para el 14 de octubre de 2025. A partir de esta fecha, Microsoft dejará de proporcionar actualizaciones de seguridad, actualizaciones no relacionadas con la seguridad y soporte técnico asistido para todas las ediciones de Windows 10.

La continuidad operativa de estos sistemas sin el soporte del fabricante representa un riesgo ALTO para la seguridad de la información de las Entidades. Los equipos se volverán progresivamente más vulnerables a ciberataques, ya que las nuevas vulnerabilidades descubiertas no serán corregidas (parcheadas), convirtiéndolos en un objetivo principal para actores maliciosos.

Este informe detalla los riesgos asociados y las acciones de mitigación y remediación que deben ser planificadas e implementadas con antelación a la fecha límite.

1. Riesgos Asociados al Fin de Soporte de Windows 10

La permanencia de sistemas operativos sin soporte oficial introduce múltiples fallas de seguridad y riesgos operativos. A continuación, se detallan los más relevantes:

Riesgo	Descripción técnica del riesgo
Exposición a Vulnerabilidades Críticas sin Parche	Los actores de amenazas buscan y desarrollan activamente exploits para vulnerabilidades recién descubiertas (N-days) en sistemas populares. Sin las actualizaciones de seguridad de Microsoft, cualquier vulnerabilidad crítica encontrada en Windows 10 después de octubre de 2025 (por ejemplo, de ejecución remota de código - RCE) permanecerá abierta indefinidamente, permitiendo a los atacantes comprometer sistemas con facilidad.
Incompatibilidad de Software y Pérdida de Funcionalidad	Nuevas versiones de aplicaciones esenciales (navegadores web, suites de ofimática, software de seguridad como antivirus y EDR) podrían dejar de ser compatibles o de recibir actualizaciones en Windows 10. Esto no solo genera problemas de productividad, sino que también crea brechas de seguridad adicionales, ya que el software obsoleto es otro vector de ataque común.
Incumplimiento Normativo y de Estándares de Seguridad	Mantener sistemas operativos sin soporte es una violación directa de múltiples marcos de ciberseguridad y normativas de protección de datos (ej. ISO 27001, PCI-DSS, GDPR). Esto puede resultar en fallos de auditoría, sanciones y la pérdida de certificaciones, afectando la reputación y la confianza en la Entidad.
Aumento del Costo Operativo y de Remediación	Aunque no migrar puede parecer un ahorro a corto plazo, el costo de gestionar los riesgos de un sistema obsoleto es significativamente mayor. Esto incluye la necesidad de implementar controles de seguridad compensatorios (ej. microsegmentación) y el elevado costo de una respuesta a incidentes si un sistema es comprometido.

Vector de ataque:

Un atacante puede explotar la falta de soporte de Windows 10 a través de múltiples vectores. A diferencia de una única vulnerabilidad, el principal vector es el estado de "vulnerabilidad permanente" del sistema operativo. Los escenarios de ataque incluyen:

1. Explotación Directa: Utilización de malware, como ransomware o troyanos, diseñado específicamente para explotar vulnerabilidades que no recibirán parche en Windows 10.

2. Ataques de Phishing y Navegación Web: Un usuario en un equipo con Windows 10 y un navegador obsoleto puede visitar un sitio web malicioso que explote una vulnerabilidad del navegador o del propio sistema operativo para tomar control del equipo.

3. Movimiento Lateral: Una vez que un atacante compromete un equipo con Windows 10 dentro de la red, puede usarlo como un punto de pivote para moverse lateralmente y atacar otros activos más críticos de la infraestructura de la Entidad.

4. Software Vulnerable: La incapacidad de actualizar aplicaciones de terceros a sus últimas versiones crea oportunidades para que los atacantes exploten vulnerabilidades conocidas en dicho software.

Recomendaciones de mitigación:

Debido al alto riesgo que representa, se requiere una planificación proactiva para asegurar la migración completa de los sistemas antes de la fecha límite. Se deben seguir los siguientes pasos:

1. **Realizar un Inventario Exhaustivo**: Identificar todos los equipos y dispositivos dentro de la red de la Entidad que actualmente operan con Windows 10. Priorizar aquellos que manejan información sensible o cumplen funciones críticas.

2. **Planificar la Migración a Windows 11 (Opción Principal)**: La recomendación principal es actualizar todos los equipos compatibles a Windows 11. Se debe verificar la compatibilidad del hardware utilizando la herramienta "PC Health Check" de Microsoft y diseñar un plan de despliegue por fases.

3. **Presupuestar la Renovación de Hardware**: Para los equipos que no cumplan con los requisitos de hardware de Windows 11, se debe iniciar un plan de renovación tecnológica para adquirir nuevos dispositivos con Windows 11 preinstalado.

4. **Evaluar las Actualizaciones de Seguridad Extendidas (ESU) como Medida Temporal**: Para casos excepcionales donde la migración o reemplazo no sea posible antes de la fecha límite (ej. compatibilidad con software crítico), Microsoft ofrecerá un programa de pago de Actualizaciones de Seguridad Extendidas (ESU) por un máximo de tres años. Esta debe ser considerada una solución de puente y no una estrategia a largo plazo, ya que su costo aumenta anualmente.

5. **Implementar Controles Compensatorios (para sistemas en transición)**: En los equipos que permanezcan temporalmente con Windows 10 después de la fecha límite, se deben aplicar medidas de seguridad adicionales, como el aislamiento de la red, la restricción de privilegios de usuario y el fortalecimiento de la monitorización a través de herramientas SIEM y EDR.

Fuentes:

- Ciclo de vida de Windows 10 Enterprise y Education: https://learn.microsoft.com/es-es/lifecycle/products/windows-10-enterprise-and-education