Microsoft ha presentado una nueva Iniciativa de Resiliencia de Windows, diseñada para reforzar la seguridad y la estabilidad de sus sistemas, asegurando además que la integridad del sistema no se vea comprometida.

El objetivo, según la compañía, es prevenir incidentes como el que afectó a CrowdStrike en julio pasado, permitir que más aplicaciones y usuarios funcionen sin requerir privilegios de administrador, implementar controles más estrictos para gestionar aplicaciones y controladores no seguros, y ofrecer opciones para proteger los datos personales mediante cifrado.

Entre las características más destacadas se encuentra la Recuperación Rápida de Máquinas, que estará disponible para los usuarios del Programa Windows Insider a principios de 2025.

> *«Esta funcionalidad permitirá a los administradores de TI aplicar correcciones específicas a través de Windows Update en equipos que no puedan arrancar, sin necesidad de acceso físico al dispositivo. Con esta recuperación remota, se podrán resolver problemas generales de manera mucho más eficiente que en el pasado»,* explicó David Weston, vicepresidente de seguridad empresarial y del sistema operativo en Microsoft.

Otra novedad significativa es una actualización que permitirá ejecutar herramientas de seguridad en modo usuario, como cualquier aplicación estándar, en lugar de depender del acceso al núcleo del sistema. Esta funcionalidad se lanzará en modo de prueba en julio de 2025, con el propósito de simplificar la recuperación del sistema y minimizar los efectos de errores o fallos a nivel operativo.

Además, Microsoft está colaborando con socios de seguridad de endpoints para mejorar la resiliencia a través de su Iniciativa de Virus de Microsoft (MVI). Entre las medidas que implementarán se encuentran actualizaciones graduales de productos, procedimientos de recuperación utilizando anillos de implementación, y la garantía de que los cambios tengan un impacto mínimo en los usuarios.

Otras novedades que llegarán a Windows incluyen:

- Un estándar de seguridad basado en hardware para las nuevas PC con Windows 11, incluyendo TPM 2.0 y la seguridad basada en virtualización (VBS) habilitada de forma predeterminada.
- Protección de administrador, donde los usuarios tienen permisos estándar por defecto, pero pueden realizar cambios importantes, como instalar aplicaciones, al autenticar con Windows Hello (actualmente en versión preliminar).
- Compatibilidad con claves de paso en Windows Hello, para una autenticación multifactor (MFA) resistente al phishing.
- Impresión protegida en Windows, eliminando la dependencia de controladores de impresión de terceros.
- Cifrado de datos personales, que asegura los archivos en las carpetas de Escritorio, Documentos e Imágenes usando Windows Hello.
- Hotpatch, una herramienta que permite aplicar actualizaciones críticas de seguridad sin necesidad de reiniciar el sistema.
- DNS de Confianza Cero, que limita los dispositivos Windows a dominios autorizados y bloquea el tráfico saliente IPv4 e IPv6, salvo que sea resuelto por un DNS protegido o autorizado por el administrador de TI.
- Actualización de configuración, que previene desviaciones en la configuración al restaurar automáticamente los ajustes preferidos (ya disponible).

Estas mejoras forman parte de la Iniciativa de Futuro Seguro (SFI) de Microsoft, un proyecto a largo plazo lanzado en noviembre de 2023 para priorizar la seguridad en el diseño de nuevos productos y combatir las amenazas cibernéticas.

Asimismo, Microsoft anunció la ampliación de su programa de recompensas por vulnerabilidades con un nuevo desafío de hacking denominado Zero Day Quest, que busca avanzar en la investigación y la seguridad en áreas como la nube y la inteligencia artificial.

> *«Este evento no solo está enfocado en identificar vulnerabilidades, sino también en*

> *fortalecer y ampliar las colaboraciones entre el Centro de Respuesta de Seguridad de Microsoft (MSRC), los equipos de producto y los investigadores externos, elevando así el nivel de seguridad para todos»,* afirmó Tom Gallagher, vicepresidente de ingeniería del MSRC.