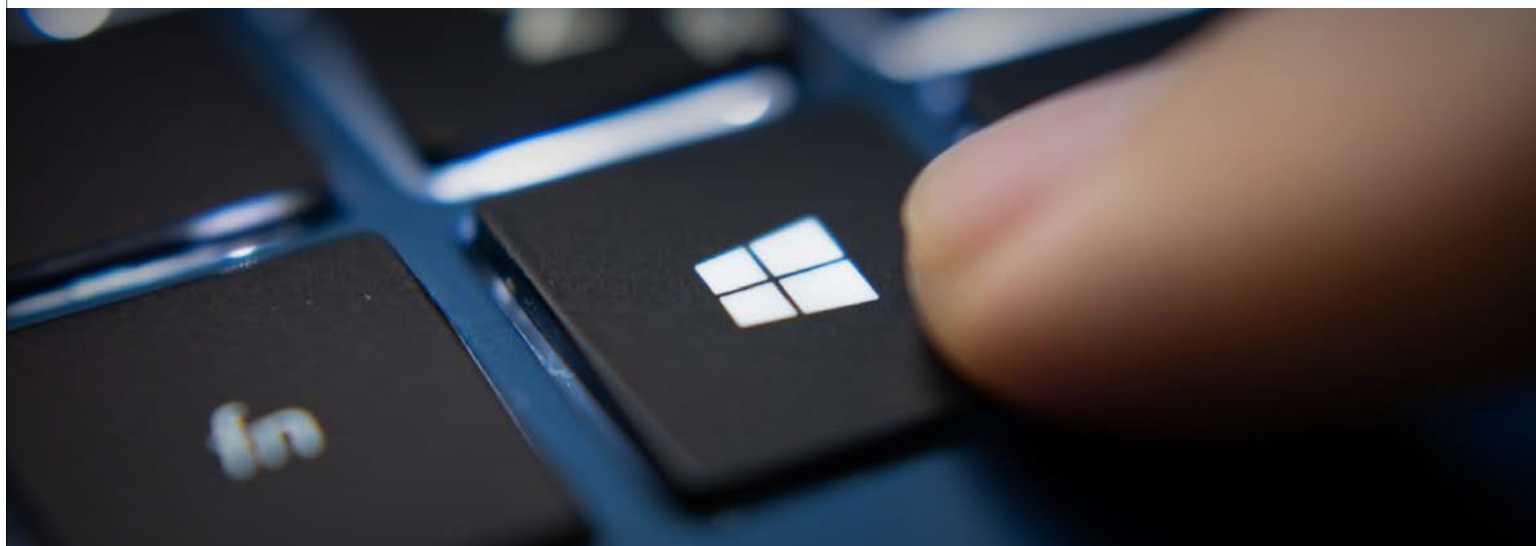




INFORME DE VULNERABILIDADES MICROSOFT 2020

Descubra los peligros de los privilegios de administrador no gestionados y estrategias para controlarlos



TABLA DE CONTENIDO

1	Introducción y Resumen Ejecutivo	3
2	Aspectos Destacados del Informe de 2019	5
3	Vulnerabilidades por Producto	6
	Internet Explorer & Edge	6
	Windows	7
	Windows Office	8
	Windows Server	9
4	Visión de Cinco Años	10
5	Análisis de Expertos	11
	Jane Frankland, Experta en Ciberseguridad	11
	Paula Januszkiewicz, CEO de CQURE	12
	Sami Laiho, MVP de Microsoft y hacker ético	13
6	BeyondTrust Endpoint Privilege Management	14
7	Logrando el Cumplimiento	14
8	Próximos Pasos y Recursos	15
9	Metodología	16
	Cómo Microsoft Clasifica Las Vulnerabilidades	16
	Precisión de Los Datos de Vulnerabilidades	17

1 Introducción y Resumen Ejecutivo

El Informe de Vulnerabilidades de Microsoft, producido anualmente por BeyondTrust, analiza los datos de los boletines de seguridad emitidos por Microsoft durante el año anterior. Todos los Martes, Microsoft publica correcciones para todas las vulnerabilidades que afectan a sus productos, y este informe recopila estos análisis durante el período de un año, ofreciendo una visión holística de las tendencias relacionadas con las vulnerabilidades y, lo que es más importante, cuántas de ellas podrían mitigarse si los privilegios de administrador fueron removidos de las organizaciones.

2019 marca el séptimo año del Informe de Vulnerabilidades de Microsoft e incluye una comparación de tendencias de cinco años, que le brinda una mejor comprensión de cómo crecen las vulnerabilidades y en qué productos específicos.

Resumen Ejecutivo

A continuación se presentan algunas de las conclusiones del Informe de Vulnerabilidades Microsoft de este año, que analiza todos los boletines de Patch Tuesday publicados a lo largo de 2019.

- ▶ En 2019, 858 vulnerabilidades fueron descubiertas por Microsoft
- ▶ El número de vulnerabilidades reportadas ha aumentado un 64% en los últimos 5 años (2015-2019)
- ▶ El 77% de las vulnerabilidades críticas descubiertas en 2019 se habrían mitigado al eliminar los privilegios de administrador
- ▶ El 100% de las vulnerabilidades críticas en Internet Explorer y Edge se habrían mitigado al eliminar los privilegios de administrador
- ▶ El 80% de las vulnerabilidades críticas que afectan a Windows 7, 8.1 y 10 se habrían mitigado al eliminar los privilegios de administrador

Las vulnerabilidades de Microsoft continuaron aumentando en 2019, alcanzando un récord.

Figura 1:
Estadísticas de
Vulnerabilidades
Microsoft (2019)

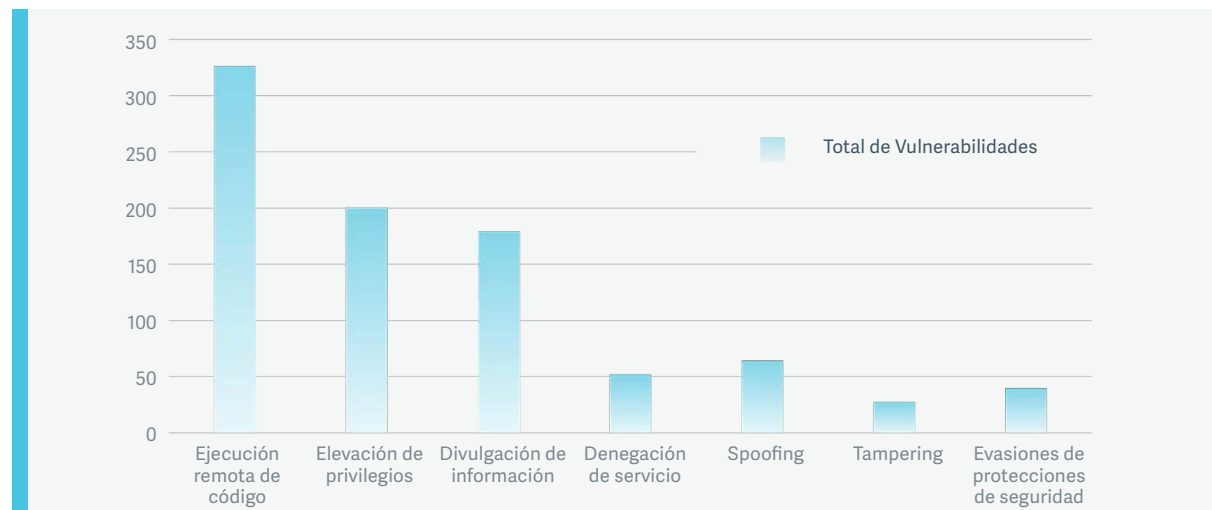


Cómo Microsoft Agrupa las Vulnerabilidades

Cada boletín de seguridad de Microsoft consta de una o más vulnerabilidades, que se aplican a uno o más productos de la compañía. Estas categorías, organizadas por tipo de impacto, consisten en: ejecución remota de código, elevación de privilegios, divulgación de información, denegación de servicio, evasiones de protecciones de seguridad, tampering y spoofing.

Figura 1:

Clasificación de categorías de vulnerabilidades Microsoft (2019)

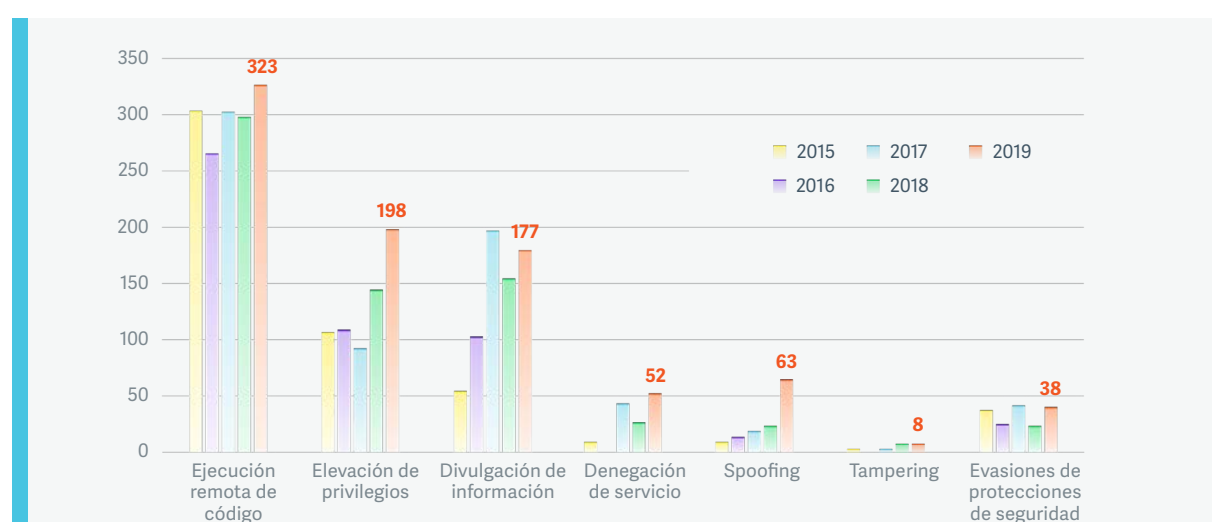


Las vulnerabilidades de RCE en 2019 alcanzaron un récord en 2019, mientras que las vulnerabilidades de elevación de privilegios también aumentaron un 37% desde el año pasado.

Según informes anteriores, la RCE, o Ejecución Remota de Código (Remote Code Execution) representa la mayor proporción del total de vulnerabilidades de Microsoft a lo largo de 2019. De las 323 vulnerabilidades de RCE, 191 se consideraron críticas. De estas vulnerabilidades críticas, la eliminación de los privilegios de administrador habría mitigado el 76%. Las vulnerabilidades de RCE en 2019 alcanzaron un récord, mientras que las vulnerabilidades de elevación de privilegios también aumentaron un 37% desde el año pasado.

Figura 2:

Categorías de vulnerabilidades (2015-2019)



2

Aspectos
Destacados del
Informe de
2019

En 2019, Microsoft informó un **número récord** de vulnerabilidades



858 fue el número total de vulnerabilidades

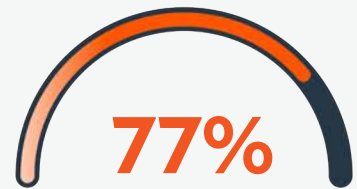


64%



fue el aumento en los últimos 5 años

El número de vulnerabilidades reportadas aumentó de 524 (2015) para 858 (2019)



de las vulnerabilidades críticas podrían haber sido mitigadas

La eliminación de los derechos de admin habría reducido los riesgos significativamente

Cómo podría ayudar la eliminación de los **privilegios de administrador?**



3 Vulnerabilidades por Producto

INTERNET EXPLORER & EDGE

A pesar del dominio de Google Chrome y Firefox, Microsoft Internet Explorer sigue siendo un navegador muy popular. Sin embargo, desde Enero de 2016, Microsoft solo admite y parchea la versión más actual de Internet Explorer. Vale la pena señalar que el fin del soporte de Microsoft Internet Explorer (IE) 10 finalizó el 31 de enero de 2020. A partir de ese momento, IE 11 se convirtió en la única versión compatible de Internet Explorer en Windows Server 2012 y Windows Embedded 8 Standard.

Se descubrieron 33 vulnerabilidades críticas en Internet Explorer 8, 9, 10 y 11 durante 2019. Eliminar los privilegios de administrador podría haber mitigado el 100% del riesgo.

Las vulnerabilidades críticas en Microsoft Edge han aumentado significativamente desde su creación hace dos años, con 86 descubiertas el año pasado. De esos 86, eliminar los privilegios de administrador podría haber mitigado nuevamente el 100% del riesgo.

El 15 de enero de 2020, Edge se cambió a un nuevo motor basado en Chromium, lo que significa que tanto Google Chrome como Edge podrían tener los mismos defectos al mismo tiempo. Con eso, ningún de estos navegadores podrían ser considerados "seguros" para mitigar las vulnerabilidades de Edge.

Figura 4:
Vulnerabilidades de
Microsoft Internet
Explorer y Edge
(2015-2019)

*Eliminar los privilegios
de administrador podría
haber mitigado el 100%
del riesgo.*



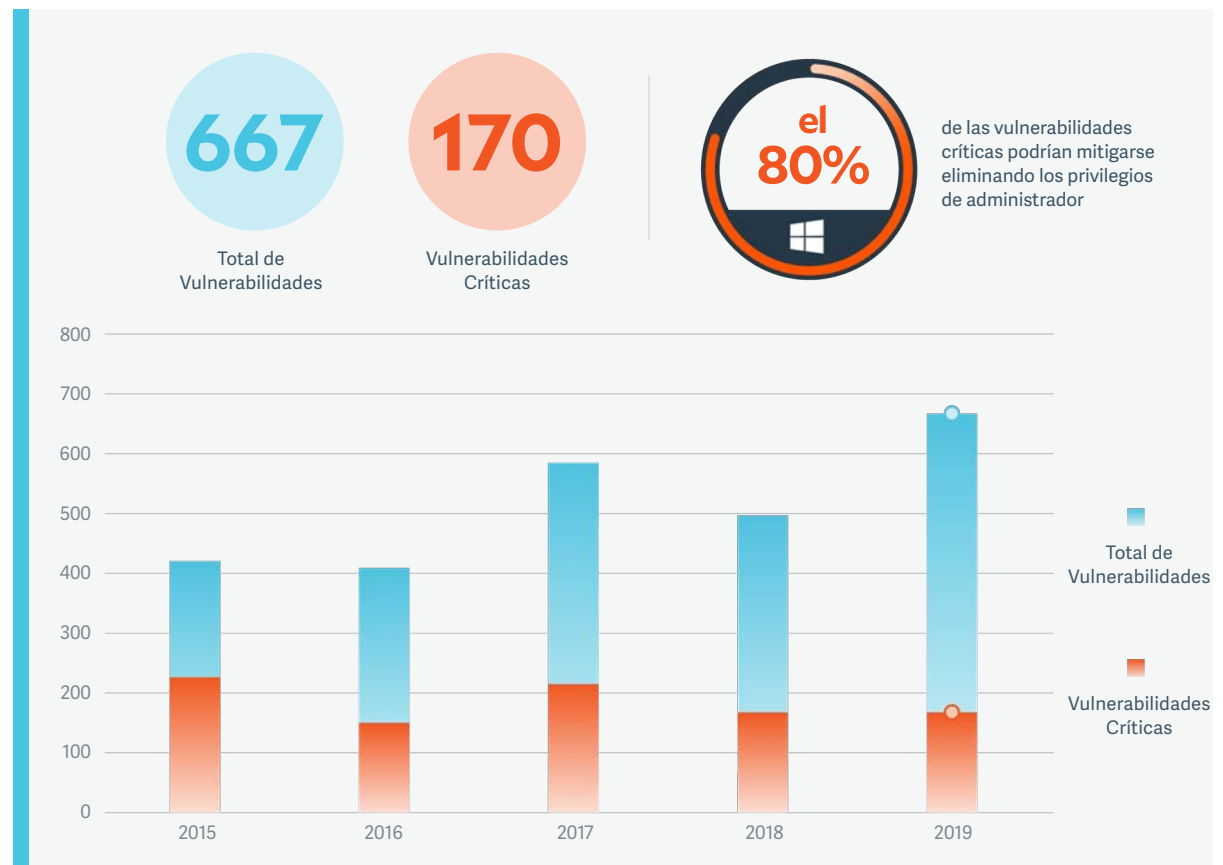
WINDOWS

En 2019, se informaron 667 vulnerabilidades en los sistemas operativos Windows Vista, Windows 7, Windows RT, Windows 8 / 8.1 y Windows 10. Windows 10 se promocionó como el "sistema operativo Windows más seguro" hasta la fecha cuando se lanzó, pero aún experimentó 167 vulnerabilidades críticas el año pasado. De todas las vulnerabilidades de Windows descubiertas en 2019, 170 fueron consideradas críticas.

Eliminar los privilegios de administrador podría haber mitigado el 80% de estas vulnerabilidades críticas.

Figura 5:
Vulnerabilidades de
Microsoft Windows
(2015-2019)

Windows 10 se promocionó como el "sistema operativo Windows más seguro" hasta la fecha cuando se lanzó, pero aún experimentó 167 vulnerabilidades críticas el año pasado.



WINDOWS OFFICE

Después de alcanzar un récord de 102 vulnerabilidades en 2019, Office experimentó una reducción de 40% este año (60). De las 60, solo 7 se consideraron críticas, y eliminar los privilegios de administrador mitigaría el 100% de ellas en todos los productos de Office en 2019 (Excel, Word, PowerPoint, Visio, Publisher y otros).

Figura 6:
Vulnerabilidades
Críticas de Windows
(2015-2019)



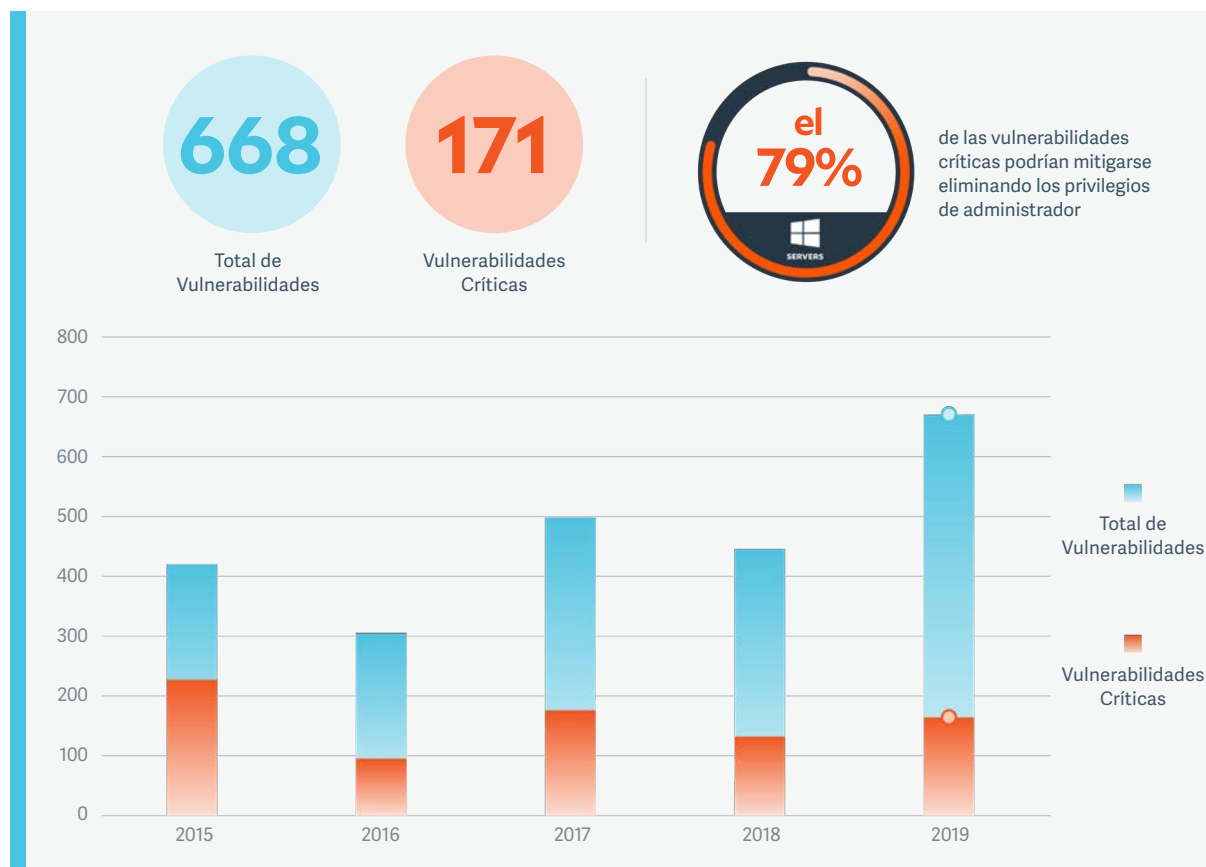
"Las técnicas de prevención como la inclusión en la lista blanca de aplicaciones, la eliminación del acceso administrativo y la adopción de los principios de menor privilegio contribuyen en gran medida a proteger las máquinas de los usuarios y reducir las incursiones en la red, sin restringir severamente la funcionalidad del usuario".

Dr. Eric Cole, fundador y CEO de Secure Anchor Consulting

WINDOWS SERVER

Se informó un total de 668 vulnerabilidades que afectaron a Windows Server en 2019. De las 171 vulnerabilidades con una calificación crítica, el 79% podría mitigarse mediante la eliminación de los privilegios de administrador.

Figura 7:
Vulnerabilidades de
Windows Server
(2015- 2019)



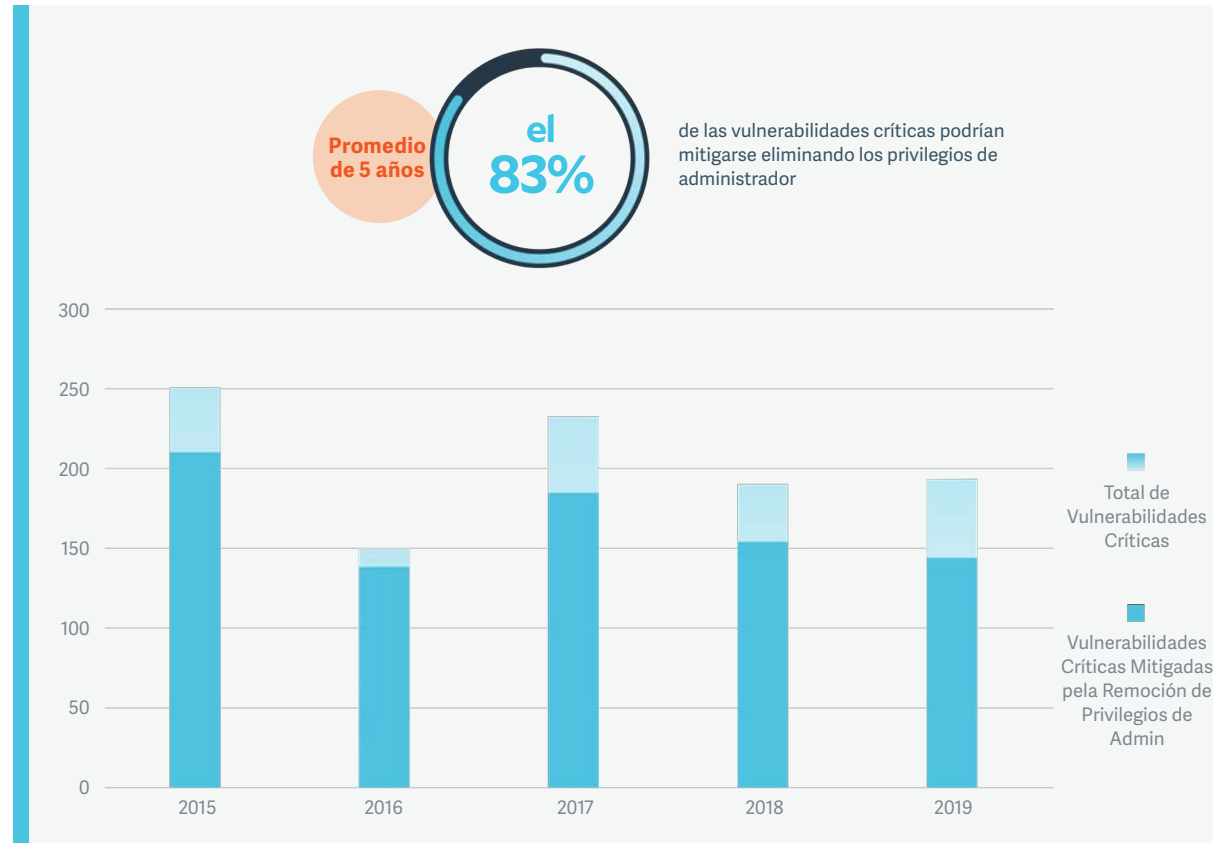
En 2013, se encontraron 252 vulnerabilidades en Microsoft Windows Server, lo que significa que ha habido un aumento significativo en los últimos seis años.

4 Visión de Cinco Años

Las vulnerabilidades críticas continúan introduciendo riesgos y crean una preocupación importante para las organizaciones comprometidas con la protección de sus redes contra las violaciones de datos. El análisis en este informe indica que la mayoría de estas vulnerabilidades pueden mitigarse mediante la eliminación de los privilegios de administrador local.

Figura 8:
Vulnerabilidades críticas
de Microsoft (2015-2019)

Las vulnerabilidades críticas continúan introduciendo riesgos y crean una preocupación importante para las organizaciones comprometidas con la protección de sus redes contra las violaciones de datos.



5 JANE FRANKLAND

Análisis de Expertos

Autora de [IN Security](#) y Oradora de Temas de Ciberseguridad

La cantidad de datos que producimos y compartimos está creciendo exponencialmente, y la infraestructura de seguridad que protege estos datos está bajo un estrés creciente. Con una superficie de ataque creciente, los ataques están aumentando en volumen y calidad. Siendo persistente y complejo, la velocidad e intensidad de estos ataques continúan desafiando cada parte de nuestro ecosistema. El informe de BeyondTrust lo demuestra claramente y no sorprende que las vulnerabilidades aumenten tan significativamente.

Ya sea que los adversarios estén en busca de puntos débiles o los empleados que accidentalmente pongan en peligro la organización a través de prácticas inseguras, las personas históricamente han sido consideradas como el eslabón más débil. Por eso, es probable que prácticamente todas las vulnerabilidades explotadas sean las conocidas por los investigadores y expertos en seguridad. Los sistemas sin parches siguen siendo objetivo fácil para los adversarios que buscan romper una red y obtener acceso a una organización. Incluso después de décadas de campaña, los parches, una práctica básica de seguridad, todavía no se aplican de manera efectiva. Aunque la mayoría de las organizaciones cuentan con procesos para implementar rápidamente parches críticos lanzados por los proveedores en el momento de una vulnerabilidad explotada, muchas luchan con parches de rutina no críticos. Y es este problema el que debemos resolver. Los parches exitosos reducen la explotación de vulnerabilidades, interrupciones significativas del sistema, problemas de disponibilidad, pérdidas financieras y riesgo de reputación.

“ Eliminar los privilegios de administrador es una de las medidas más básicas y poderosas que una organización puede tomar.



Para reducir las amenazas, se recomienda a las organizaciones que eliminen los privilegios de administrador de forma predeterminada. A menudo, trabajan sin darse cuenta de las vulnerabilidades externas que resultan del uso de aplicaciones y sistemas operativos inseguros. Si se descubren antes de un adversario, por ejemplo, durante una evaluación de seguridad o por investigadores de seguridad, entonces las vulnerabilidades pueden ser reparadas. Pero si no lo son, entonces es solo cuestión de tiempo antes de que un adversario los descubra y GAME OVER!

La eliminación de los privilegios de administrador reduce los riesgos de spyware o malware, y evita que terceros hagan lo mismo, haciendo que los datos confidenciales no estén disponibles para acceder, modificar o exportar. Esa estrategia tampoco le permite a los usuarios crear cambios y bloquear usuarios legítimos fuera de los sistemas, o publicar contenido on line no autorizado que pueda causar daños a la marca. Es simplemente una de las medidas más básicas, pero poderosas que una organización puede tomar.

PAULA JANUSZKIEWICZ**Experta en Ciberseguridad y CEO de CQURE**

Hoy en día, las técnicas de ingeniería social utilizadas para dirigirse a usuarios individuales, como el envío de un archivo adjunto de correo electrónico malicioso, son métodos comúnmente utilizados para obtener acceso a las redes corporativas internas. El Informe de Vulnerabilidades de Microsoft muestra esta tendencia a fondo.

Archivos adjuntos o enlaces maliciosos pueden ser utilizados para aprovechar las vulnerabilidades en las aplicaciones de Internet Explorer, Microsoft Edge o Microsoft Office. El hecho del usuario abrir ese enlace o archivo adjunto, conduce al acceso directo al sistema.

Imaginemos que este usuario tenga privilegios de administrador local. En este caso, el atacante puede tener acceso no solo a todos los archivos del sistema que pueden descargarse o cifrarse, sino que también existe una gran posibilidad de reunir credenciales, por ejemplo, de LSASS, para usarlas para atacar otras máquinas en la red. Si el usuario trabaja con privilegios de administrador de servidor o dominio, el atacante puede obtener acceso a esos hosts y servicios críticos. Este también es un entorno perfecto para el ransomware: si los usuarios operan con privilegios de administrador, el ransomware puede propagarse más fácilmente.

Si el principio de menor privilegio se implementó bien y el usuario no utiliza privilegios de administrador para el trabajo diario, el atacante tendría que esforzarse mucho más para escalar privilegios y realizar movimientos transversales a otras máquinas.

La implementación del principio de menor privilegiado es una de las tareas más importantes que las empresas deben hacer para protegerse de las vulnerabilidades mencionadas.

“ Si los usuarios operan con privilegios de administrador, el ransomware puede propagarse más fácilmente.



Si los usuarios operan con privilegios de administrador, el ransomware puede propagarse más fácilmente.

Al elaborar el tema de Privileged Access Management, también es crucial parchear software y sistemas para eliminar todas las vulnerabilidades que puedan ser explotadas.

El uso de las funciones integradas en Windows 10 también podría ser útil cuando se trata de minimizar el riesgo de un ataque exitoso. Windows Defender Exploit Guard es capaz de detener la explotación de las vulnerabilidades existentes en el software mediante la protección de los procesos. Credential Guard puede usarse para aislar las operaciones de credenciales con el uso de la virtualización. Además, la inclusión en la lista blanca de aplicaciones que pueden ejecutarse en la estación de trabajo puede detener la ejecución de código malicioso.

Para concluir, todas las mitigaciones juntas pueden reducir con éxito el riesgo de un ataque exitoso.

SAMI LAIHO***MVP de Microsoft y hacker ético***

Las 858 vulnerabilidades en 2019 son tantas que, aunque parchear reactivamente los sistemas operativos y las aplicaciones es importante, existe una mayor necesidad de proteger proactivamente nuestros entornos. Creo que la mejor protección para los entornos se logra mediante conceptos como Principio de menor privilegio, Lista blanca, AMF y educación / consciencia.

Además del malware común, veo que las mayores amenazas para mis clientes son el ransomware y el phishing. La mayoría del malware tradicional puede mitigarse eliminando los privilegios de administrador. ¡Los resultados son increíblemente buenos en comparación con las medidas reactivas, especialmente cuando se miran las aplicaciones y navegadores de Office!

Otro punto importante: eliminar los privilegios de administrador no se trata solo de seguridad. Significa también que las computadoras funcionarán más rápido, mejor y durante más tiempo, con menos reinstalaciones. Mis clientes más grandes también han medido una reducción del 75% en la cantidad de tickets de Helpdesk después de eliminar los privilegios de administrador. ¡Esto significa que puede ser más seguro y más productivo durante largos períodos de tiempo!

“ Eliminar los privilegios de administrador no se trata solo de seguridad. Significa también que las computadoras funcionarán más rápido, mejor y durante más tiempo.



Eliminar los privilegios de administrador realmente no resuelve el problema del ransomware, aunque ayuda a reducir su propagación. El problema es evidente: necesita permisos registrados para sus datos y, por lo tanto, también puede cifrarlos.

La mejor protección contra ransomware es la lista blanca. La lista blanca mata el ransomware en sus puntos de entrada, como el correo electrónico y los navegadores web.

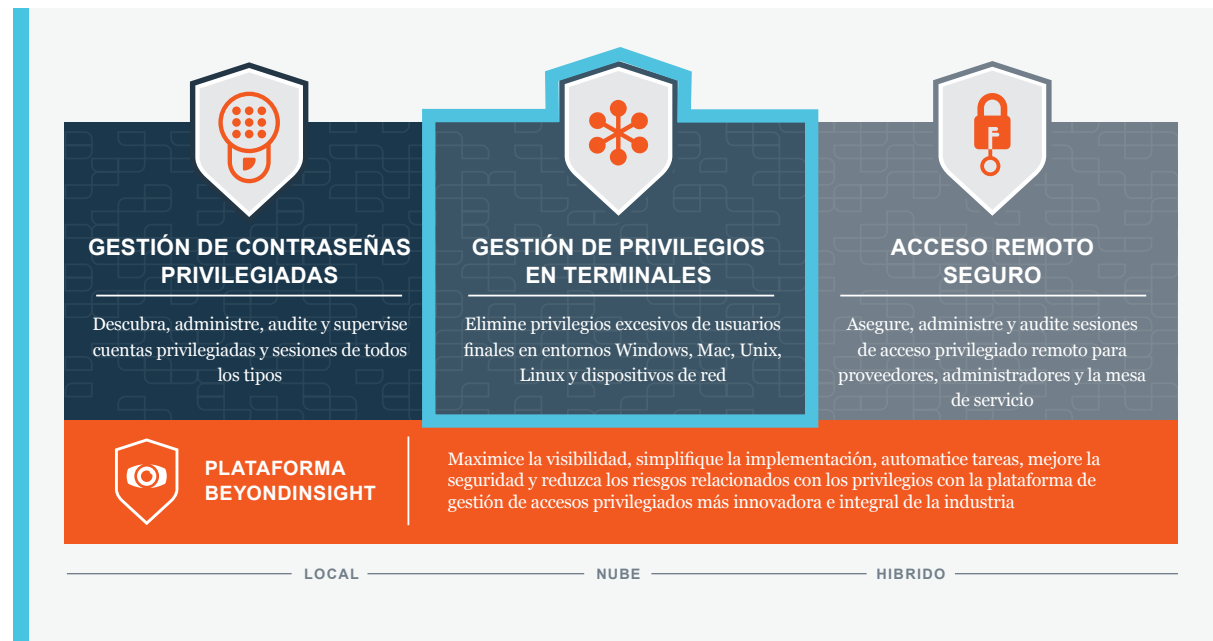
Una de las amenazas más comunes hoy en día es el phishing. No es algo que pueda resolverse solo con protecciones técnicas, ya que es difícil asegurarse de que las personas no escriban sus contraseñas en lugares incorrectos ni reutilicen contraseñas en múltiples servicios. La buena noticia es que el 99% de los ataques de phishing se pueden mitigar mediante la implementación de la autenticación multifactor (MFA). El 1% restante solo se puede combatir con capacitación y aumento de la conciencia, y es por eso que los ataques de phishing simulados deben implementarse en todas las empresas con la capacitación de seguridad obligatoria.

6 BeyondTrust Endpoint Privilege Management

Los resultados de este informe muestran que una gran cantidad de riesgos se pueden mitigar fácilmente si se eliminan los privilegios de administrador, una práctica recomendada por muchos expertos de la industria también. ¿Qué barreras existen que impiden que las organizaciones aborden este riesgo? La solución de seguridad adecuada debe permitir a las organizaciones obtener el menor privilegio con productos que no solo se implementan rápidamente, sino que también logran el equilibrio adecuado entre seguridad y productividad.

La implementación de privilegios mínimos para desktops y servidores es crítica para el Universal Privilege Management, el concepto de BeyondTrust para habilitar Privileged Access Management (PAM). [Endpoint Privilege Management](#) es una solución importante de la cartera BeyondTrust PAM.

Figura 9:
El portafolio de
Soluciones BeyondTrust



La implementación de privilegios mínimos para desktops y servidores es crítica para el Universal Privilege Management, el concepto de BeyondTrust para habilitar Privileged Access Management (PAM). Endpoint Privilege Management es una solución importante para la cartera BeyondTrust PAM

Con Endpoint Privilege Management, puede eliminar rápidamente los privilegios excesivos del usuario final en Windows, Mac, Unix, Linux y dispositivos de red, y lograr una reducción inmediata del riesgo sin afectar la productividad del usuario.

También puede satisfacer las necesidades de cumplimiento interno y externo eliminando los privilegios excesivos, utilizando la lista blanca de aplicaciones y proporcionando un seguimiento de auditoría de la actividad del usuario.

Nuestra solución Endpoint Privilege Management está disponible a través de un dispositivo virtual o físico, y en la nube (SaaS), para que las organizaciones de todos los tamaños puedan lograr la seguridad de los terminales con una solución que sea escalable y rentable

7

Logrando el Cumplimiento

Implementar el principio de privilegios mínimos y eliminar los derechos de administrador es un requisito clave para muchos mandatos de cumplimiento en todo el mundo. Los requisitos de cumplimiento pueden agruparse en tres propósitos principales: proteger, controlar y auditar el uso de los recursos de TI y los datos confidenciales que contienen.

La implementación de una solución integral de gestión de privilegios en terminales como parte de su estrategia de seguridad permite a las organizaciones cumplir con los siguientes requisitos:

- ▶ Seguimiento, control, prevención y corrección del uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones. (CIS, PCI, NIST, HIPAA, GDPR)
- ▶ Implementación de una sola función principal por servidor y habilitación solo de servicios, protocolos, daemons, etc. necesarios según sea necesario para la función del sistema. (PCI, CIS)
- ▶ Recopilación, gestión y análisis de registros de auditoría de eventos que pueden ayudar a detectar, comprender o recuperarse de un ataque. Los registros de auditoría deben especificar la identificación del usuario, el tipo de evento, la fecha y la hora. (CIS, PCI, NIST, HIPAA, GDPR)

Encuentre una lista completa de estos requisitos y cómo las soluciones de BeyondTrust los habilitan en la [Matriz de Cumplimiento](#).

8 Próximos Pasos y Recursos

Al abordar los privilegios de administrador no gestionados, puede lograr rápidamente la seguridad de los terminales al tiempo que elimina las brechas de seguridad y cumple los requisitos de cumplimiento, sin obstaculizar la productividad del usuario.

Póngase en [contacto con BeyondTrust](#) para programar una demo de Endpoint Privilege Management y ver estos recursos adicionales

Whitepaper

- ▶ [A Comprehensive Guide to Endpoint Privilege Management](#)

Estudio de Caso

- ▶ [How the University of Derby Secure their Endpoints with BeyondTrust](#)

Vídeo

- ▶ [A Two-Minute Overview of our Endpoint Privilege Management Solution](#)

Datasheets

- ▶ [Privilege Management para Windows y Mac](#)
- ▶ [Privilege Management para Unix y Linux](#)

9 Metodología

Cada boletín emitido por Microsoft contiene un resumen ejecutivo con información general. Para este informe, una vulnerabilidad se clasifica como una que podría mitigarse eliminando los privilegios de administrador si cumple con los siguientes criterios establecidos por Microsoft en el boletín de vulnerabilidad:

- ▶ Los clientes / usuarios cuyas cuentas están configuradas para tener menos privilegios de usuario en el sistema podrían verse menos afectados que los usuarios que operan con privilegios de usuario administrativos
- ▶ Si el usuario actual ha iniciado sesión con privilegios de usuario administrativos, un atacante podría tomar el control de un sistema afectado

CÓMO MICROSOFT CLASIFICA LAS VULNERABILIDADES

Cada vulnerabilidad puede aplicarse a uno o más productos de Microsoft, y a cada vulnerabilidad se le asigna un tipo de una de siete categorías: ejecución remota de código, elevación de privilegios, divulgación de información, denegación de servicio, omisión de funciones de seguridad, suplantación de identidad, manipulación, que en ocasiones varían según el software o la combinación de softwares afectados.

Una vulnerabilidad de cada tipo a menudo se aplica a una combinación de diferentes versiones de un producto o productos y, a veces, a todas las versiones, por ejemplo todas las versiones de los clientes Windows. A menudo, una vulnerabilidad solo se aplicará a una combinación de productos, como Internet Explorer 11 en Windows 7.

A cada vulnerabilidad también se le asigna una calificación de severidad agregada por parte de Microsoft: crítica, importante, moderada, que también varía según cada software o combinación de softwares afectados.

El Common Vulnerability Scoring System (CVSS) o Sistema de Puntuación de Vulnerabilidad Común es un estándar publicado utilizado por organizaciones de todo el mundo, y proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. La puntuación numérica puede traducirse en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

Ciertas vulnerabilidades se han producido varias veces a lo largo de 2019, que generalmente afectan a diferentes programas. En estos casos, la vulnerabilidad en sí solo se cuenta una vez, con todos los tipos de software afectados atribuidos a esa entrada.

PRECISIÓN DE LOS DATOS DE VULNERABILIDADES

Se han realizado una serie de generalizaciones para cada vulnerabilidad de la siguiente manera:

- ▶ Cada vulnerabilidad se clasificó con el tipo más frecuente para todas las instancias de esa vulnerabilidad
- ▶ No se tuvieron en cuenta las versiones del producto
- ▶ No se tuvieron en cuenta las combinaciones de productos
- ▶ Las vulnerabilidades se contaron tanto para el software como para la versión cuando apropiado (por ejemplo, una vulnerabilidad para Internet Explorer 11 en Windows 10 se considera una vulnerabilidad tanto para Internet Explorer 11 como para Windows



ACERCA DE ENDPOINT PRIVILEGE MANAGEMENT

BeyondTrust [Endpoint Privilege Management](#) combina la gestión de privilegios y el control de aplicaciones para administrar eficientemente los privilegios de administrador en Windows, Mac, Unix, Linux y dispositivos de red, sin obstaculizar la productividad. Haga cumplir los privilegios mínimos y elimine los privilegios de administrador local con un control detallado que se escala para asegurar su universo de privilegios en expansión, al tiempo que crea una experiencia de usuario sin fricciones.

SOBRE BEYONDTRUST

BeyondTrust es el líder mundial en Gestión de Accesos Privilegiados (PAM), que capacita a las organizaciones para asegurar y administrar todo su universo de privilegios. Nuestros productos y plataforma integrados ofrecen la solución PAM más avanzada de la industria, lo que permite a las organizaciones reducir rápidamente su superficie de ataque en entornos tradicionales, en la nube e híbridos.

El enfoque Universal Privilege Management de BeyondTrust asegura y protege los privilegios en contraseñas, terminales y accesos, brindando a las organizaciones la visibilidad y el control que necesitan para reducir el riesgo, lograr el cumplimiento y aumentar el rendimiento operativo. Más de 20,000 clientes confían en BeyondTrust, incluido el 70 % de las empresas de Fortune 500 y una red global de socios.

Obtenga más información en beyondtrust.com/es