



Mayo 12 de 2017

ALERTA DE SEGURIDAD INFORMÁTICA

VULNERABILIDADES EN PLATAFORMAS MICROSOFT

RECOMENDAMOS ACTUALIZAR LOS SISTEMAS OPERATIVOS

Bogotá. El Ministerio TIC, el Centro Cibernético Policial CCP y colCERT en desarrollo de sus funciones y en la búsqueda de mejorar los niveles de seguridad de las entidades del estado, les solicita realizar la revisión de sus plataformas Microsoft; es decir; deben actualizar los sistemas operativos de sus estaciones de trabajo y servidores, con el fin de mantenerlos al día en lo que se denominan "parches" críticos y de seguridad que se emiten a través de boletines por parte de Microsoft.

La razón de esta alerta y solicitud, es por la filtración de una serie de exploit aplicables a las siguientes versiones de sistemas operativos:

Windows:

- Xp, Vista, 7, 8, 10, 2000, 2003, 2008, 2012.
- Que afecta los servicios (tcp/445) SMB/ (tcp/139) NBT.
- Llegando a permitir tomar control de la estación o servidor que haya sido comprometido.

En comunicación con el equipo de seguridad de Microsoft, emiten un boletín sobre esta situación; en el link en el cual recomiendan actualizar el sistema operativo, de acuerdo a la versión con "parches" ya disponibles. También recomiendan estar en la versión de Windows 10.

<https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/>

El ministerio TIC y el CCP, promueven en las entidades del estado de nivel nacional y territorial la cultura de seguridad de la información; el ministerio TIC



invita a las entidades a revisar sus avances en la implementación del modelo de seguridad y privacidad de la información, acorde con lo expuesto en el decreto 2573 del 12 de diciembre del 2014 y el decreto único reglamentario 1078 del 26 de mayo del 2015.

El Centro Cibernético Policial, da las siguientes recomendaciones a los cibernautas:

- Nunca haga clic en enlaces dentro de un correo electrónico desconocido y siempre ignore los que le solicite estas acciones.
- No responda mensajes que le soliciten información personal o financiera.
- Aplicar las medidas de prevención y control para restringir el acceso e instalación de programas maliciosos y realizar pruebas de vulnerabilidad a los sistemas de información, garantizando la resiliencia.
- Se recomienda realizar Backup (copias de información) de manera periódica.
- Mantener actualizado los sistemas de antivirus en los computadores.
- Evitar ingresar a sitios web desconocidos.
- Se recomienda realizar Backup (copias de información) de manera periódica.

Ante cualquier eventualidad no duden en comunicarse con el Ministerio TIC al correo incidentes-seginf@minticgov.co, a través de la página del Centro Cibernético Policial <https://caivirtual.policia.gov.co/> o @caivirtual en Twitter y colCERT al correo contacto@colcert.gov.co.

