ALERTA DE SEGURIDAD INFORMATICA

Estimados amigos,

Todas las predicciones sobre las amenazas de ciberseguridad a nivel mundial alertan para que los usuarios actuemos con mas responsabilidad por la seguridad de nuestros datos y sistemas en los próximos meses. La ciberseguridad entendida como tal, no será suficiente para garantizar la seguridad de los datos mas sensitivos o nuestros datos privados. Los datos tendrán que ser protegidos por los usuarios y la tecnología que ellos disponen. Los ataques contra infraestructuras críticas de las naciones se volverán mas frecuentes y por tanto afectarán a los activos mas sensibles, como son: la seguridad nacional, los sistemas de salud, los sistemas de comunicaciones, los sistemas de transporte y producción de energía eléctrica, etc. Debemos pensar que "Los sistemas en la nube están cambiando todo, pero todo está conectado y todo es vulnerable", por esta razón es importante entender, que, en el 2019 los dos principales objetivos para los ciberataques son: los servicios en la nube y los dispositivos de punto final de los usuarios, por lo que se recomienda aplicar las recomendaciones de Zero Trust en la protección de los sistemas.

Entre las principales recomendaciones para la protección de los datos podemos citar:

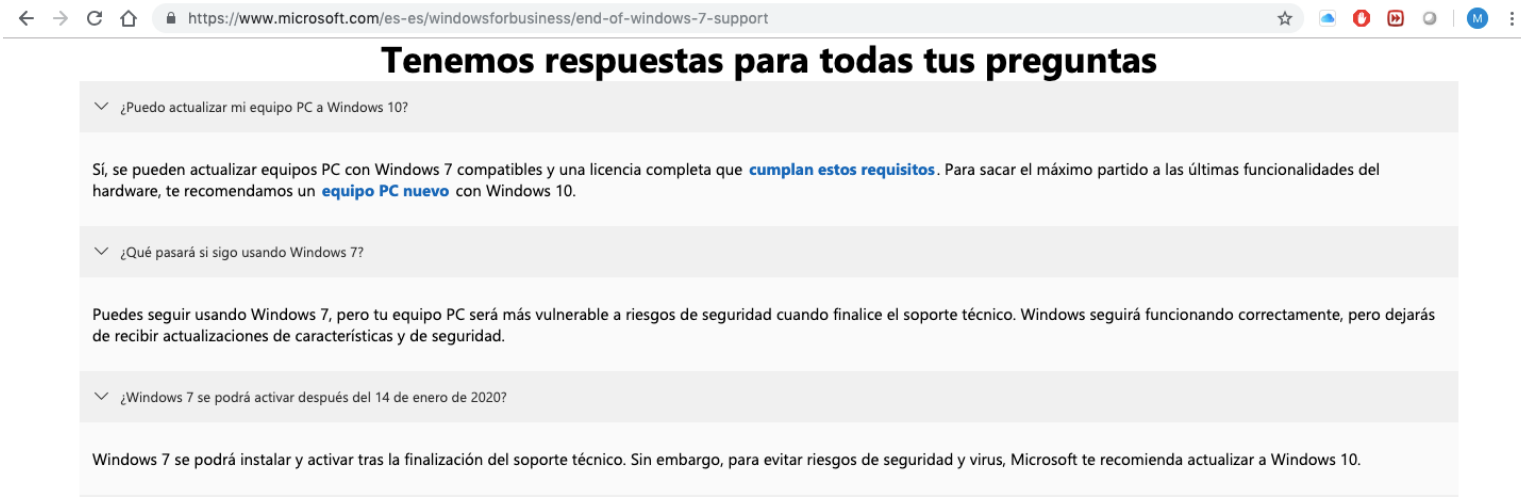
1) Educar a los usuarios en buenas prácticas para evitar descargar malware al sistema, desde emails, pop ups y websites con malware.
2) Las versiones de software deben estar actualizadas, a las versiones mas actuales posibles y con todos los parches de seguridad actualizados.
3) Debemos tener las mejores herramientas para seguridad en Internet, que detecte y bloque el malware.
4) Los sistemas de seguridad perimetral y firewalls requieren altos niveles de control para frenar el uso de aplicaciones y descargas de Internet que representen amenazas.
5) Privilegios limitados para los usuarios, cuando navegan en Internet y descargan archivos de la red.
6) Mantener niveles altos de seguridad en archivos, directorios y particiones cifradas, para evitar que ransomware pueda acceder a ellos.
7) Archivos encriptados, para que el ransomware no pueda encontrar archivos en formatos planos, y toda la encriptación de preferencia este con AES 256 y sin password.
8) Los directorios y archivos deben ser continuamente respaldados, en discos duros externos o drivers USB que habitualmente están desconectados de los sistemas y por tanto no podrán ser capturados por el ramsoware.
9) Los backups deberán realizarse en distintas fechas a fin de que si alguna versión esta comprometida se pueda utilizar la de una fecha anterior.
10) No se recomienda utilizar sistemas de directorio activo, en aquellos sistemas que no están debidamente licenciados y actualizados, en consideración de que por las particiones compartidas y abiertas se puede ocasionar una infección masiva del sistema.

Adicionalmente, los principales Antivirus desde este 2019 funcionarán en sus últimas versiones, y por tanto las únicas seguras, desde Windows 7 Service Pack 1. Todos los sistemas operativos anteriores de Windows presentan vulnerabilidades del sistema que no pueden ser parchados.

Windows 8.1 y 7

Sistemas operativos cliente	Fin de soporte estándar	Fin del soporte extendido
Windows 8.1	9 de enero de 2018	10 de enero de 2023
Windows 7, service pack 1*	13 de enero de 2015	14 de enero de 2020

La respuesta a seguir utilizando Windows 7 se la puede obtener en el siguiente link, medio de comunicación oficial de Microsoft.



Por otro lado, toda PC que se encuentre utilizando Windows XP debe ser descartada y desconectada de la red al ser una fuente de vulnerabilidad e inseguridad del sistema. En el siguiente link se puede encontrar la información respectiva. Ningún software antivirus prestará una solución de seguridad real.

Avira NEXXT SOLUTIONS CRYPTOPHONE Cyberoam A SOPHOS Company open source

Principales marcas de Antivirus en el mercado:

	Win 10	Win 8	Win 7 SP1	Win 7	Win XP
AVIRA[1]	✓	✓	✓	✗	✗
Bitdefender[2]	✓	✓	✓	✗	✗
Kaspersky[3]	✓	✓	✓	✗	✗
Eset[4]	✓	✓	✓	✗	✗
Norton[5]	✓	✓	✓	✗	✗
Avast[6]	✓	✓	✓	✗	✗
AVG[7]	✓	✓	✓	✗	✗
GData[8]	✓	✓	✓	✗	✓ 32 bits
McAfee[9]	✓	✓	✓	✗	✗

Links de las páginas oficiales de los fabricantes con los requerimientos mínimos de los Sistemas Operativos:

1. AVIRA: https://answers.avira.com/en/question/avira-minimum-system-requirements-31036?sh=true
2. Bitdefender: https://www.bitdefender.com/consumer/support/answer/13790/
3. Kaspersky: https://support.kaspersky.com/13910
4. Eset: https://support.eset.com/kb2892/?locale=en_US&viewlocale=en_US
5. Norton: https://support.norton.com/sp/en/us/home/current/solutions/v101390880_EndUserProfile_en_us
6. Avast: https://support.avast.com/en-ww/article/Antivirus-FAQ
7. AVG: https://www.avgsa.co.za/support/avg-system-requirements-supported-operating-systems/
8. GData: https://www.gdatasoftware.com/business/system-requirements
9. McAfee:https://service.mcafee.com/webcenter/portal/oracle/webcenter/page/scopedMD/s55728c97_466d_4ddb_952d_05484ea932c6/Page29.jspx?wc.contextURL=%2Fspaces%2Fcp&articleId=TS102471&_afrLoop=1231002231779076&leftWidth=0%25&showFooter=false&showHeader=false&rightWidth=0%25&centerWidth=100%25#!%40%40%3FshowFooter%3Dfalse%26_afrLoop%3D1231002231779076%26articleId%3DTS102471%26leftWidth%3D0%2525%26showHeader%3Dfalse%26wc.contextURL%3D%252Fspaces%252Fcp%26rightWidth%3D0%2525%26centerWidth%3D100%2525%26_adf.ctrl-state%3D11y7l23nht_9%40PC

NOTA IMPORTANTE: Cualquier información que difiera de la publicada por el fabricante en su sitio web debe ser considerada fraudulenta o ser softwares modificados por hackers (puerta de entrada de Ransomware) con fallas de seguridad.

BIBLIOGRAFIA

https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#517a13d14352