Procedimiento de actuación para la activación completa de la Red Docente de un Centro

A lo largo de la tarde del pasado viernes, día 12 de mayo, distintas organizaciones han sufrido incidentes graves de seguridad basados en envíos de correos electrónicos de origen desconocido. Este ciberataque masivo lanzado a escala internacional mediante un malware de cifrado de datos y petición de rescate económico en equipos dotados con el sistema operativo Windows supone un "riesgo importante" para los PCs de los centros educativos.

Según las instrucciones del CCN-CERT e INCIBE, centros especialistas en seguridad a nivel nacional, el virus afecta sólo a equipos Windows. La forma de neutralizarlo consiste en la instalación del parche de seguridad puesto a disposición por Microsoft y en la actualización del antivirus con que cuente el ordenador en aquellos equipos informáticos equipados con Windows. El virus no afecta equipos Linux sin doble arranque Windows.

PROTOCOLO DE ACTUACIÓN CENTRO EDUCATIVO

En la Red de Gestión ya se han revisado y asegurado la red y sus PCs (matrícula, evaluación, gestión económica, etc.) y se encuentra plenamente operativa.

En la Red Docente (infraestructuras y PCs de aulas educativas, laboratorios, etc) y en general para todos aquellos puestos no comprendidos en la Red de Gestión, hay que proceder a protegerlos individualmente antes de restaurar completamente la conectividad. Para ello, el proceso de activación completa de la Red Docente se hará centro a centro de forma independiente, con el objetivo de recuperar la normalidad en cada centro a la mayor brevedad posible. Para ello se abordarán las siguientes actividades.

1. SECURIZACIÓN DE PCS:

- EQUIPOS DEL CENTRO EDUCATIVO:

Las siguientes instrucciones se han de llevar a cabo en cada uno de los equipos conectados a la red docente.

- Se ha dotado a los centros de conectividad parcial (acceso a Educamadrid y a ciertos recursos técnicos) a los centros que tenían encendido el router de comunicaciones. Si su centro tenía apagado el router de comunicaciones y no dispone de conectividad parcial, por favor proceda a encenderlo y se le dotará de la misma en un plazo inferior a un día.
- Si el centro cuenta sólo con equipos con sistema operativo Linux sin doble arranque Windows, no tiene que actuar sobre ellos y tras revisar la sección dedicada a equipos de titularidad privada puede pasar a solicitar la conectividad completa a la Red Docente.
- Si el centro cuenta con equipos con sistema operativo de Microsoft de una versión inferior a Windows XP, NO existe parche de seguridad. Por ello, debe instalarse una versión de sistema operativo, desde cero, que sea Linux, Windows XP o superior, según las licencias con las que cuente. En el resto de equipos con sistema operativo Windows se requiere seguir los siguientes pasos:

i. Desconecte el equipo de la red y enciéndalo.
ii. Aplique la herramienta de detección y desinfección del ransomware de Panda WannaCry Fix.
iii. **Si el equipo está infectado, apagarlo y desconectar de la red hasta nuevas instrucciones.** Si no lo está, continúe con el resto de pasos.
iv. Identifique el sistema operativo y la arquitectura del equipo.
v. Identifique si el equipo cumple los requisitos mínimos para poder aplicar el parche de protección contra el ransomware wannacry.
vi. Descargue las actualizaciones necesarias desde el equipo (en este momento puede conectarlo a la red). Si utiliza un pendrive USB para almacenar los parches necesarios y prefiere utilizarlo en lugar de descargar los parches en cada equipo, puede saltar este paso.
vii. Aplique las actualizaciones en el equipo.
viii. Tras revisar la sección dedicada a equipos de titularidad privada puede pasar a solicitar la conectividad completa a la Red Docente del punto 2 del presente documento.

- EQUIPOS DE TITULARIDAD PRIVADA:

Para los equipos de titularidad privada para los que el centro facilita acceso a la Red Docente, se requiere que el centro facilite a dichos titulares (docentes y familias) las recomendaciones de revisión y securización de los PCs de su propiedad e indique su cumplimiento.

ES MUY IMPORTANTE QUE SE EJECUTE ESTE PARCHE EN TODOS LOS PUESTOS DE ESTAS CARACTERÍSTICAS EN PRO DE LA SEGURIDAD.

2. SOLICITUD DE ACTIVACIÓN COMPLETA:

Una vez realice las anteriores actuaciones en todos los equipos del centro, por favor, solicite la conectividad a la red, a través de su Dirección de Área Territorial, utilizando la hoja de solicitud disponible en las siguientes direcciones

- www.educa2.madrid.org/web/recursostic
- www.madrid.org/portalcau/

y haciéndosela llegar.

COMUNICACIÓN Y SEGUIMIENTO CON LA DIRECCIÓN DE ÁREA TERRITORIAL DE ADSCRIPCIÓN

Ante cualquier duda, póngase en contacto con el responsable técnico de la Unidad de Programas de su Dirección de Área Territorial, facilitándole los datos de contacto del responsable de esta actividad en el centro educativo

DAT	COORDINADOR TIC	TELÉFONO	CORREO
CAPITAL	Concepción de Diego Zamarro	91 720 31 74	concepcion.dediego@madrid.org
	José Luis Ordovás Blasco	91 720 31 93	joseluis.ordovas@madrid.org
	Laura Muñoz Jiménez	91 720 30 93	laura.munoz@madrid.org
	Francisco Rafael García Medina	91 720 22 66	rafael.garcia@madrid.org
	Marta Olmedilla Almarza	91 720 30 42	marta.olmedilla@madrid.org
NORTE	Gonzalo Martín Esteso		gonzalo.martin.esteso@madrid.org
	Javier del Moral Rodríguez	91 720 38 44	javier.delmoral@madrid.org
	Beatriz Rodríguez Merchán		beatriz.rodriguez.merchan@madrid.org
SUR	José Ángel Navarro Piera	91 720 27 53	joseangel.navarro@madrid.org
	Francisca Muñoz Escobar	91 720 27 69	francisca.munoz.escobar@madrid.org
	Antonio López Sastre	91 720 27 99	antonio.lopezsastre@madrid.org
	Manuel Santos González	91 720 27 18	manuel.santos@madrid.org
	Ángel Ocaña	91 720 27 55	angel.ocana@madrid.org
ESTE	Francisco Javier Temprado García	91 887 21 00	franciscojavier.temprado@madrid.org
	Juan Gabriel Gómez	91 887 20 95	juangabriel.gomez@madrdi.org
	Justo Martínez Diez	91 887 20 88	justo.martinez@madrid.org
	Marcos Moreno Sánchez	91 887 20 65	marcosrafael.moreno@madrid.org
OESTE	Jesús Trejo Fernández	91 856 26 08	jesus.trsejo@madrid.org
	Francisca García Bernal	91 856 25 98	francisca.garciaber@madrid.org

RECURSOS DE INFORMACIÓN EN RED

Todos los centros educativos a través de la Red Docente, tienen acceso a las páginas técnicas de Microsoft, de antivirus y educamadrid, en concreto en la sección “recursostic”.

Para seguir correctamente estos pasos, dispone de un procedimiento técnico detallado para ejecución del protocolo descrito, disponible en las siguientes direcciones:

- www.educa2.madrid.org/web/recursostic
- www.madrid.org/portalcau/

Para la descarga de parches deben utilizar los siguientes links:

- Si sus equipos están conectados a líneas ADSL o propias del centro:

- **ftp://ftp.educa.madrid.org/MD**

- Si sus equipos están conectados en la red educativa VLAN100:

- **DAT MADRID CAPITAL: http://195.77.130.4 ➔ http://datcentro.madrid.org**
- **DAT NORTE: http://195.77.130.5 ➔ http://datnorte.madrid.org**
- **DAT SUR: http://195.77.130.6 ➔ http://datsur.madrid.org**
- **DAT ESTE: http://195.77.130.7 ➔ http://dateste.madrid.org**
- **DAT OESTE: http://195.77.130.8 ➔ http://datoeste.madrid.org**

Y le aparecerá una página equivalente a la siguiente:

madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

CONSEJERÍA DE ECONOMÍA, EMPLEO Y HACIENDA
Comunidad de Madrid

Parches de Seguridad para el Entorno Educativo

En esta página puede descargarse los parches de seguridad para la prevención del ataque del WannaCry

Parches Wannacry

Windows 8.1

windows8.1-kb4012213-x64.msu - Parche Windows 8.1 64 bits
windows8.1-kb4012213-x86.msu - Parche Windows 8.1 32 bits

Windows 7

windows7-kb4012212-x64.msu - Parche Windows 7 64 bits
windows7-kb4012212-x86.msu - Parche Windows 7 32 bits

Windows 10 1607

Windows10.0-kb4019472-x64.msu - Parche Windows 10 64 bits
Windows10.0-kb4019472-x86.msu - Parche Windows 10 32 bits

Windows XP

windowsxp_sp3-kb4012598-x86.exe - Parche Windows XP 32 bits

Agencia para la Administración Digital de la Comunidad de Madrid

IMPORTANTE: Con el objeto de no saturar las redes de una forma innecesaria se recomienda realizar las descargas de forma escalonada desde el link de la DAT que le corresponda indicado y, si es posible, ponerlos a disposición del personal del centro en un recurso compartido para su utilización por el mismo.