MARZO 2020

Buenas prácticas para limitar los riesgos de virus informáticos

Información proporcionada por el Servicio de Seguridad de la Información, D. G. de Telecomunicaciones y Transformación Digital (C. Fomento y Medio Ambiente)

La conectividad de sistemas de información y el amplio uso del correo electrónico han facilitado también la propagación de *malware*, dependiendo de la tipología de estos, como virus y otros códigos maliciosos.

Una debilidad en la protección puede tener consecuencias, tanto en los dispositivos de nuestro puesto de usuario (ordenador, móvil, etc.), como en todo nuestro entorno corporativo de trabajo.

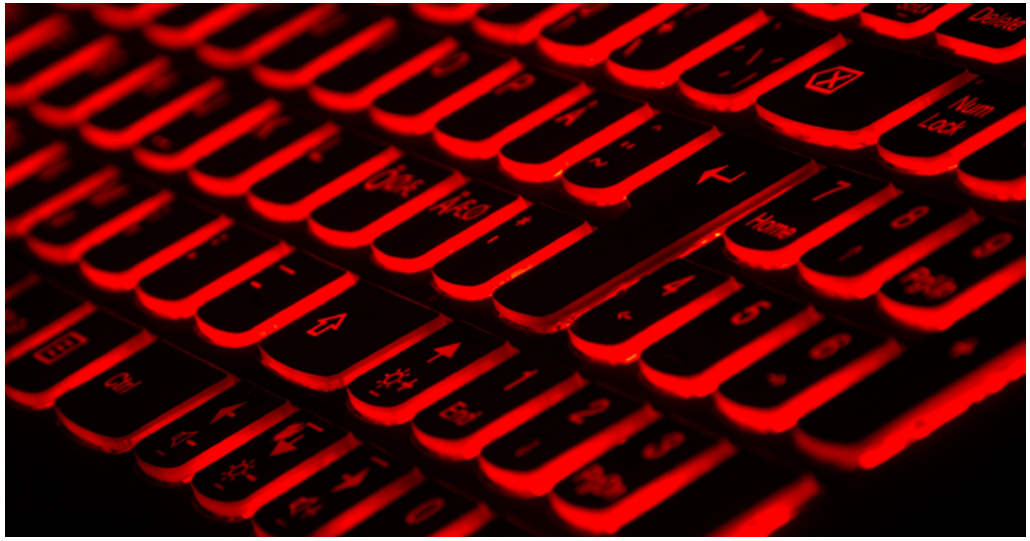
Sensibilización: Es necesario tener conciencia de los riesgos actuales a los que nos exponemos al manejar información digital, y ser cautos; la mejor actuación es la prevención y mantenerte informado te ayuda a conseguirlo.

Antivirus: En tu puesto de usuario dispones de un *antimalware* ya instalado; verifica que está activo, actualizado, y no muestra ninguna alerta o evento pendiente, manteniendo así tu protección al día.

Comprobación de puesto: Analiza con regularidad tu dispositivo de puesto mediante el antivirus, en especial si sospechas de algún comportamiento fuera de lo habitual: lentitud general, aplicaciones desconocidas, alta carga y sobrecalentamiento, etc.

Soportes: Revisa los soportes extraíbles de almacenamiento como pueden ser los USB o discos externos, antes de acceder a su información, y comprueba su contenido previamente con el antivirus corporativo. No utilices soportes desconocidos.

Dispositivos móviles: Cualquier dispositivo móvil puede convertirse en un potencial riesgo, en particular los ordenadores portátiles y los teléfonos móviles inteligentes, dado su movilidad y su posible conexión a distintas redes, siendo un punto habitual de entrada de amenazas.



Office y correo: Muchos virus se envían por correo electrónico y en el interior de documentos Office, en muchas ocasiones incluso te solicitarán permiso. No actives la edición de macros ni deshabilites la vista protegida en las herramientas ofimáticas.

Ejecutables: No ejecutes ficheros de origen dudoso. El *malware* puede aparecer con iconos de documentos conocidos (Word, pdf), pero realmente son ejecutables que al pinchar en ellos activarán la carga dañina. No siempre se visualizan bien las extensiones de tipo de los ficheros, por lo que muestra y verifica esta extensión previamente.

Engaños: En ocasiones, los virus se complementan con actuaciones de SPAM, enviando los correos a múltiples personas; en otras, se complementan con PHISHING reutilizando cadenas de correos, o bien intentan solicitar datos de cuentas de usuario o bancarios. Revisa en especial la guía y recomendaciones sobre el correo electrónico.

Cadenas de mensajes y bulos: Como norma general, ignora los mensajes y correos que piden ser reenviados, ya que podemos estar propagando un malware o bien un enlace al mismo, sin ser conscientes de ello.

Aplicaciones corporativas: Usa sólo las aplicaciones autorizadas en la Administración de la Comunidad de Castilla y León, y siempre desde fuentes confiables, como puede ser realizando las peticiones de instalación corporativas a tu CAU.

Si eres empleado público de la Junta de Castilla y León el uso de medios digitales deberá realizarse conforme a la **política de seguridad** de la ACCyL, así como la política de uso de los **servicios de comunicaciones e informática** para todo usuario de los mismos.

Descubre más conceptos importantes para limitar los riesgos de virus informáticos en la infografía de este mes.