2º BACHILLERATO EXAMEN FINAL

1º (1p) Explica en qué consiste la programación orientada a objetos, así como objetos, clases y herencia.

2º (3p) Explica en qué consiste el ciclo de vida del software y explica el ciclo de vida clásico.

3º (2p) Explica en qué consiste el malware informático, da tres ejemplos de tipos y explica que consisten.

4º (2p) Explica en qué consiste el cifrado de información, los métodos simétrico y asimétrico.

5º (1p) Explica en qué consiste el DNIe y las ventajas que incluye respecto al DNI tradicional.

6º (1p) Lee el siguiente artículo publicado el El Pais Digital el 16/5/17 y contesta las siguientes preguntas:

a) ¿de qué tipo de amenaza se trata? ¿en qué consiste y cómo podemos combatirlo?
b) ¿Qué medidas debemos de adoptar para reducir riesgos respecto a posibles infecciones o ataques?

Qué hacer si tu sistema se ve afectado por el virus del ‘ransomware’

Protegerse es relativamente fácil si se mantienen las actualizaciones del sistema operativo y no se abren correos de remitentes desconocidos

Es muy posible que no haya oído hablar del *ransomware* hasta el pasado fin de semana, cuando esta técnica coactiva vestida en forma de virus ha puesto en jaque a grandes corporaciones y organismos de 179 países. Sin embargo, esta modalidad de *secuestro* de los datos en forma de virus lleva ya mucho tiempo infectando miles de ordenadores por todo el globo empleando la misma técnica: se accede al sistema (por lo general mediante un adjunto en el *email*), se cifra el contenido, y se pide un rescate en bitcoins para su liberación bajo la amenaza de eliminarlo o hacerlo público.

Viendo que este virus ha comprometido los sistemas de servicios de salud y grandes empresas, uno puede pensar que queda libre del ataque del *ransomware*. Pero este *malware* no distingue particulares de empresas y puede terminar fácilmente comprometiendo la información de su ordenador y pidiendo un rescate por la misma. ¿Cómo debe uno protegerse del ataque? Pese a lo masivo del mismo, lo cierto es que protegerse es relativamente fácil si se siguen los siguientes consejos:

Usar un sistema operativo actual y con las actualizaciones activadas

Microsoft ha estado en la diana desde que se supo que diferentes vulnerabilidades de Windows facilitaron la difusión de WannaCry en los sistemas atacados; pero lo cierto es que la firma de Redmond respondió con rapidez ante la amenaza mediante una actualización o parche de seguridad que impedía el acceso a este código malicioso. ¿Qué falló entonces? Por un lado, la lentitud de las grandes corporaciones en adoptar las actualizaciones en sus sistemas (deben comprobar que la nueva versión no afecta al rendimiento en su red), y por otro lado, la variedad de versiones de Windows existentes entre los usuarios.

Microsoft recuerda que Windows 10, la versión actual de la plataforma, nunca se ha visto afectada por el ataque, pero sin embargo existen miles de ordenadores con versiones anteriores del sistema operativo (muchos de ellos corriendo todavía XP). "Windows es una plataforma hoy en día muy segura", zanja Vicente Díaz, analista de la firma de seguridad Kaspersky. "Lo que sucede es que hay muchas versiones obsoletas en el mercado y con usuarios que no las actualizan", añade. Lo cierto es que ha sido precisamente la desidia de los usuarios el eslabón más débil del sistema que ha sido aprovechado por los atacantes: "Los criminales se aprovechan del hecho de que muchos usuarios no hacen lo suficiente por proteger sus equipos", explica Marty P. Kamden de North VPN.

No abrir adjuntos de remitentes desconocidos

La puerta de entrada del *ransomware* son los adjuntos en los correos electrónicos. Se trata de documentos con títulos sugerentes o que pretenden confundir al usuario, y la máxima principal reside en ser disciplinado en este asunto: nunca abrir un adjunto del que no se esté completamente seguro su origen. Por lo general, ni los bancos ni otro tipo de entidades públicas envían adjuntos en los emails, con lo que si llega alguno, se debe permanecer alerta y nunca, bajo ningún concepto, abrir el documento.

Hacer copias de seguridad con frecuencia

El principal elemento de extorsión que emplea el *ransomware* es la pérdida de datos: si no se paga se borra para siempre todo el contenido cifrado. Si el usuario ha sido disciplinado haciendo copias de seguridad, no temerá tanto perder el contenido de días o incluso horas, que quien lleva meses o años sin respaldar sus datos. "Algunos pequeños negocios que teman perder toda la contabilidad pueden sentirse tentados en pagar, algo que se evita si se hacen copias de seguridad con frecuencia", explica Díaz.

Utilizar antivirus

Parte del mérito del gran incremento en seguridad logrado por Windows reside en Windows Defender, lo que Microsoft define como "centro de seguridad" integrado en las últimas versiones de Windows y que ofrece un servicio antivirus y cortafuegos para el usuario. Los de Redmond se encargar de mantener esta barrera actualizada permanentemente y el usuario debe preocuparse únicamente de mantenerla actualizada (o activar la actualización automática), pero los que empleen versiones de Windows que no integren esta barrera, deberán instalar otro tipo de antivirus y mantenerlo actualizado siempre a la última versión.

Nunca pagar

El mensaje en pantalla que ven los usuarios afectados por el *ransomware*puede resultar tentador: pagar cantidades no muy grandes por el rescate y en minutos tener sus datos de vuelta en los discos duros. Sin embargo, los expertos no recomiendan el pago del rescate bajo ninguna circunstancia: por un lado, es tal la presión de las autoridades y los sistemas de seguridad que muchos de los atacantes simplemente se esfuman y sus servidores son inutilizados, con lo que en muchísimas ocasiones toman el dinero del rescate y no *liberan al rehén* tras el pago. Por otro lado, el pago del *ransomware* sirve de aliciente para fomentar esta actividad delictiva. Está claro que si cada vez son menos los que sucumben, será menos rentable esta forma de criminalidad.