Seguridad informática

Tips para tener en cuenta a la hora de utilizar dispositivos informáticos

1. Usa un antivirus.
Parece mentira que aún haya que decirlo. El uso de un programa antivirus es básico para utilizar un ordenador. Casi que debería ser lo primero en instalarse, tras el sistema operativo. Así estará protegido de virus, spyware y demás amenazas. Un sólo equipo desprotegido puede afectar a la seguridad de toda la empresa.
2. Asegura las redes.
Usa un buen firewall para proteger el acceso a la red privada y cifra la información que se envíe por la red. Si no, cualquiera podría entrar desde el exterior y curiosear libremente por todos los dispositivos conectados a ella.

3. Protege tu Wii.
Usa una contraseña fuerte y no se la des a cualquiera: en caso de que tengas visitas a menudo y quieras darles acceso a Internet mientras están en el negocio, configura una red para invitados. Lo más seguro es ocultar la SSID de la red, de modo que hay que conocer su nombre para conectarse a ella por primera vez. También puedes filtrar el acceso por dirección MAC. De esta manera sólo podrán conectarse los dispositivos que hayas identificado por medio de su dirección física.

4. Cuidado con dónde te conectas.

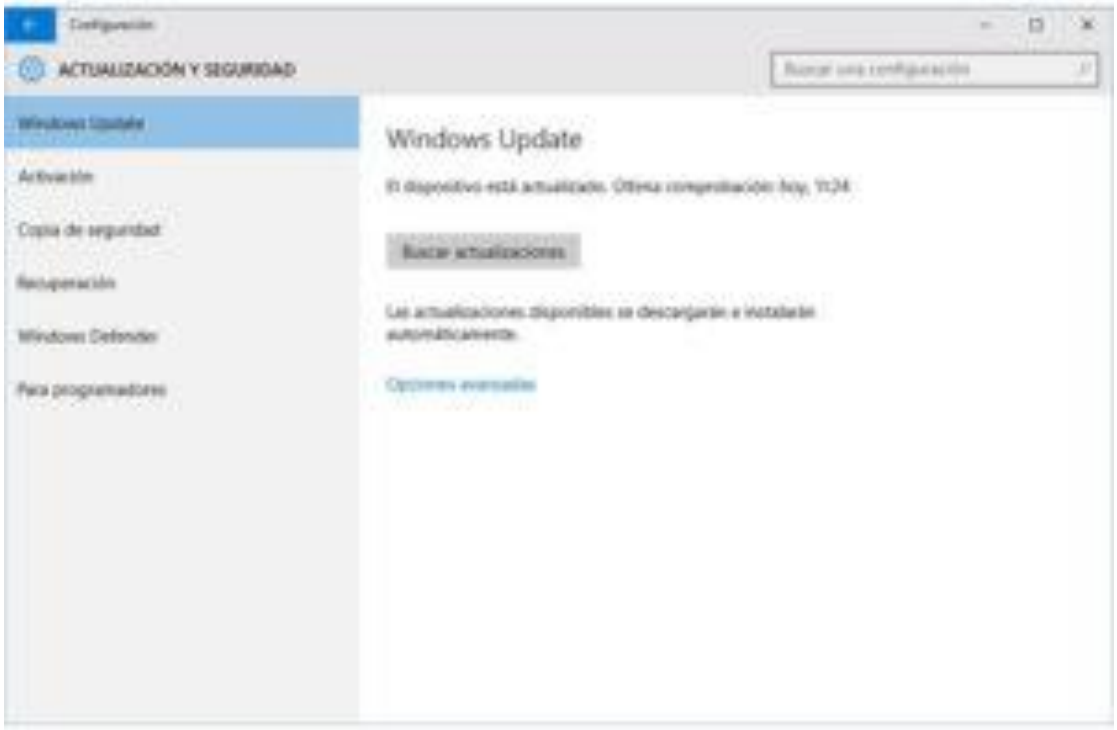
Por mucha seguridad que haya en la red corporativa, si luego conectas el portátil a cualquier red wiki abierta lo puede que lo estés echando todo por tierra. Es habitual llevar el portátil para adelantar trabajo mientras tomas algo en una cafetería, esperando un vuelo, en una feria o congreso, etc. Debes tener en cuenta que las redes públicas gratis pueden ser muy inseguras.

Usa en lo posible conexiones cifradas y procurando llevar trabajos delicados mientras estés conectado ahí. Es preferible que compartas la conexión de datos del Smartphone a conectar con una red pública. Lo aconsejable, en todos los casos, es usar una VPN.

5. Mantén los ordenadores actualizados.

Lo normal es que los fabricantes del software publiquen regularmente actualizaciones de sus programas. Comprueba que tanto el sistema operativo como las aplicaciones que usas cuenten con los últimos

parches de seguridad y, por supuesto, que la base de datos del antivirus esté actualizada.



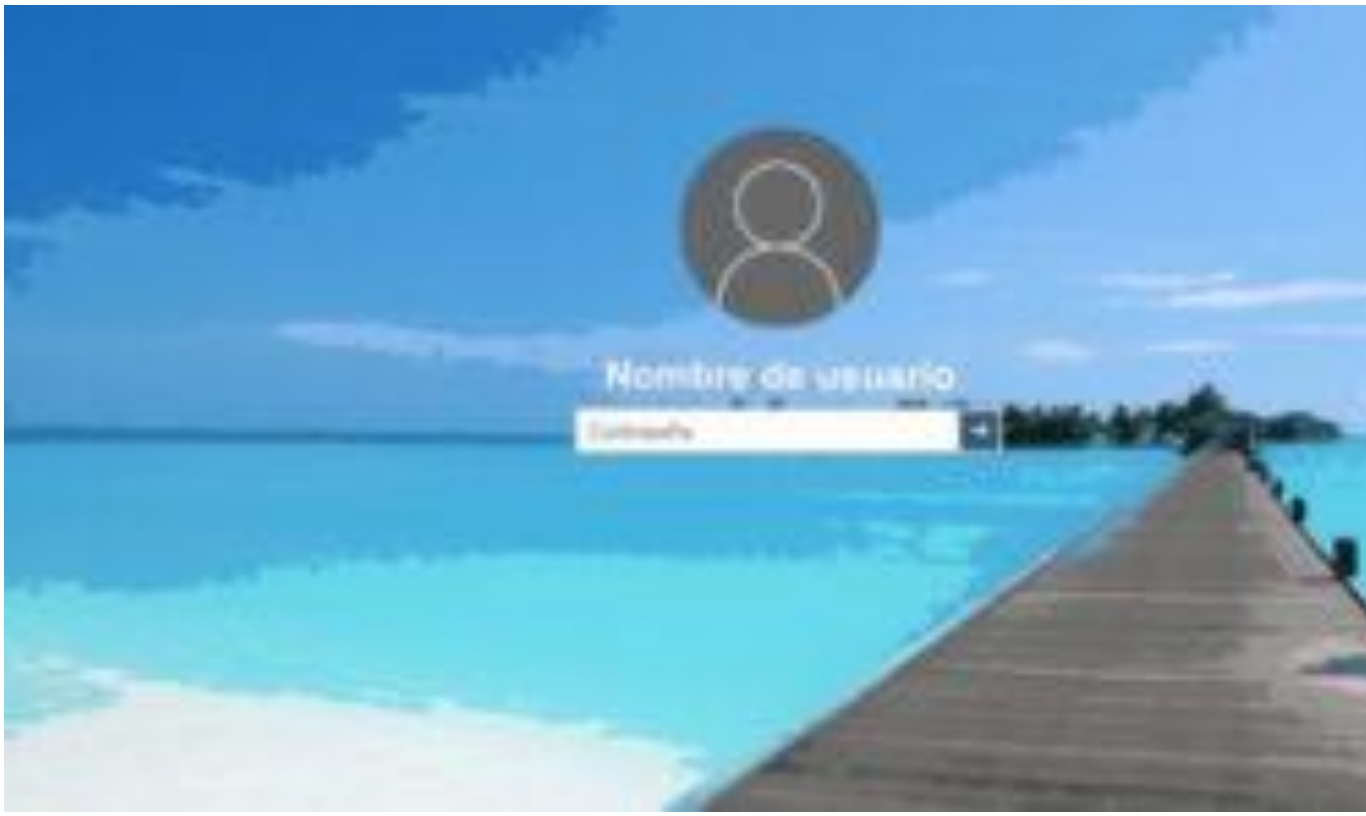
6. Usa contraseñas seguras.
Otro clásico consejo. Por favor, no uses “123456”, ni tu nombre, ni el de tus hijos o tu mascota, como clave. De hecho, lo mejor es usar cadenas de caracteres aleatorias que incluyan letras, números y otros símbolos menos habituales. Si a ti te resulta difícil recordarla ¿cuánto más le costará adivinarla a un posible intruso?

7. No instales cualquier cosa.

Nunca instales programas procedentes de fuentes desconocidas. No descargues nada de páginas sospechosas o que no conozcas. Puedes estar instalando software malicioso sin saberlo.

8. Configura el bloqueo del ordenador.

Te levantas un momento de la mesa, te entretienes un rato con otra cosa… y, sin darte cuenta, le has dado acceso a tu ordenador, a sus datos y a la red de la empresa a todo el que haya pasado por delante. Configura el sistema para que, al poco tiempo sin actividad por tu parte, se bloquee la pantalla y exija identificarse para volver a poder usarlo.



9. Ojo con lo que publicas en redes sociales.

Nunca está de más que te pienses las cosas antes de subirlas a redes sociales. Puedes estar revelando al mundo mucho más de lo deseable

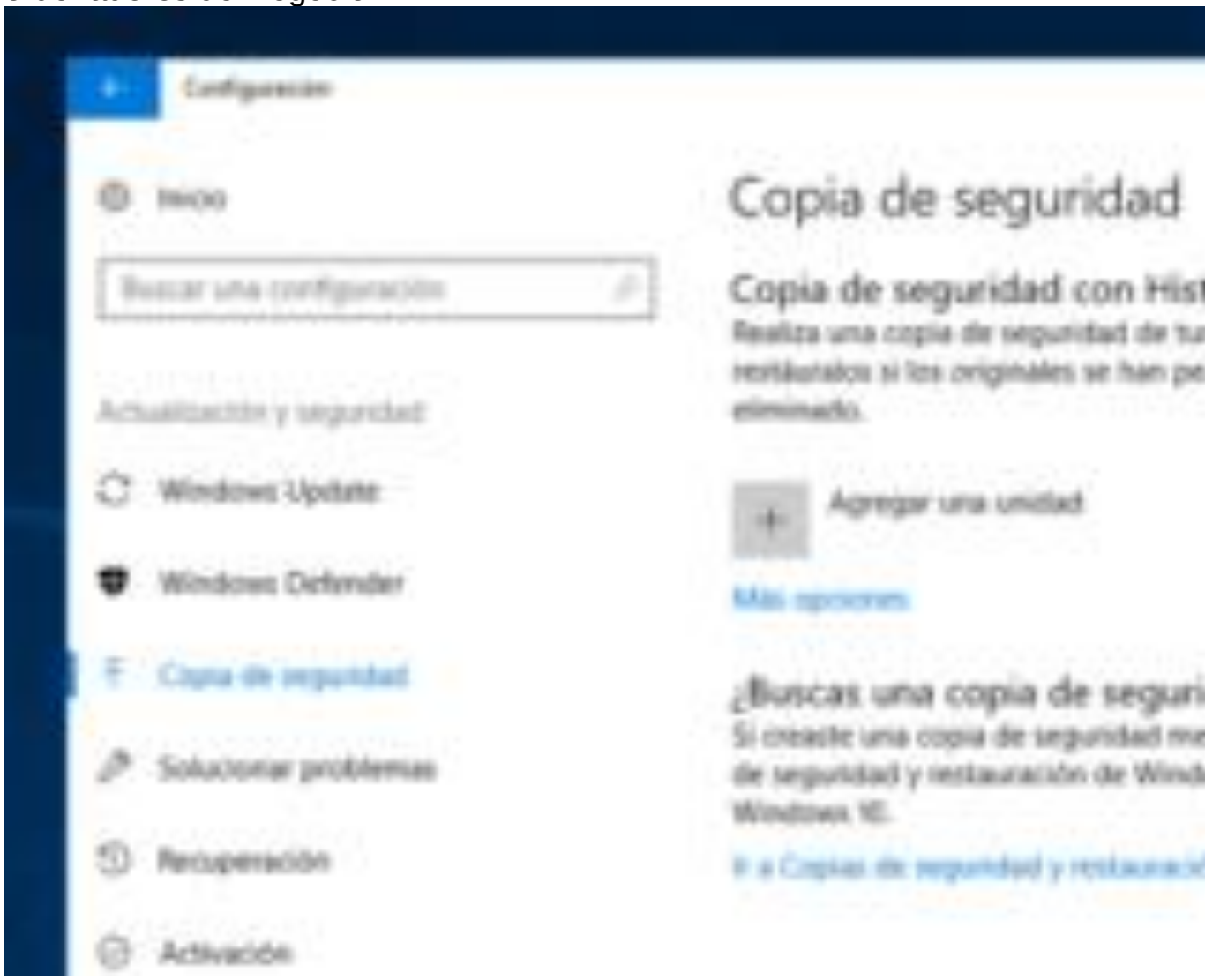
10. No conectes discos externos a lo loco.

Instalamos un firewall impenetrable. Compramos un antivirus segurísimo y lo actualizamos a diario. Ponemos contraseñas larguísimas a todo. Y luego conectamos alegremente cualquier memoria USB al ordenador. Asegúrate de deshabilitar la ejecución automática tanto de almacenamiento USB como de discos ópticos y de que el antivirus las examine nada más conectarlas

11. Haz copias de seguridad.

Si le dieran a cualquier periodista de tecnología o experto de seguridad un euro cada vez que han hecho esta recomendación…

bueno, ricos no serían, pero habrían recaudado lo suficiente como para invitar a unas cañas a los amigos. Debes configurar las copias de seguridad automáticas de los datos importantes todos los ordenadores del negocio.



12. Usa la nube con criterio.
Emplear servicios online no es una mala solución en sí. Al contrario, ya que así se solventan muchos de los riesgos que conlleva el uso de copias físicas (pérdida, averías, virus, etc.). Asegúrate de emplear una empresa de confianza, usa contraseñas seguras, no te conectes desde cualquier sitio… es decir, aplica también todos estos consejos cuando accedas a la nube.
13. Controla el acceso a los equipos.
Los dispositivos de trabajo no debería usarlos nadie más que tú. No prestes el ordenador a cualquiera, ni se los dejes a los niños para jugar un rato. En el caso de una empresa, debe controlarse el acceso físico a los equipos por parte de personal no autorizado.

14. No pierdas de vista los dispositivos móviles.
Portátiles, Smartphone y demás dispositivos móviles son candidatos a ser objeto de robo o pérdida. En el caso del teléfono, no olvides que se trata de un auténtico ordenador que contiene gran cantidad de información sensible. Si lo extravías, no sólo estarás dando acceso a los datos de tu negocio: estarás exponiendo toda tu vida. Extrema la precaución, unos segundos frente a un móvil desbloqueado pueden ser suficientes para un intruso.

15. Paciencia y sentido común
La mayoría de estos consejos se pueden concretar en este: actúa con cabeza y que no te puedan las prisas. Sí, esperar a que se haga una copia de seguridad es muy aburrido, y tener que introducir una contraseña larguísima cada vez que dejas de usar el ordenador un minuto es un auténtico rollo. Pero piensa en esos segundos de pánico en los que creíste que el ordenador se había estropeado. O en aquella vez que, efectivamente, lo hizo. ¿A qué hubieras dado cualquier cosa por haber hecho un respaldo de los datos?
Recuerda: el eslabón débil de la cadena de seguridad eres tú mismo. Si no lo olvidas, ya has hecho la mitad del trabajo.

Actividad:

Según su criterio, nombrar cuales de estos tips son los que se utilizan generalmente y cuales no utilizamos a diario.

En el caso de los que no utilizamos, explicar muy brevemente cual es el impacto que piensan ustedes podría tener esta acción.

Recuerden que a fecha límite de entrega es el 22/09 a i mail: Sebasleclercq2@gmail.com