Microsoft Security

Recomendaciones de Seguridad en la red para Personas Mayores

Jairo Daniel Pérez Abadía
Senior Customer Engineer
Microsoft Ibérica

SITUACION ACTUAL

Las personas mayores cada vez emplean más Internet y la red como herramientas de comunicación.

- Leer periódicos online con el tamaño de letra que necesiten.
- Ver la tele y escuchar la radio.
- Encontrar números de teléfono o direcciones.
- Realizar gestiones, como transferencias bancarias, compras en el supermercado.
- Encontrar a excompañeros de la escuela, del trabajo o familiares a través de las redes sociales.

- Los usuarios de Internet de más de 60 años invertían una media de 5 horas en línea, y que el 80% de personas mayores utilizaba las redes sociales.

- Más del 50% de estos usuarios habían compartido voluntariamente información personal con individuos que no habían conocido nunca en persona.

En el Correo Electrónico

- Desconfíe de los mensajes de correo electrónico inesperados o con aspecto extraño
- No abra los ficheros adjuntos ni haga clic en los enlaces que aparezcan en estos mensajes de correo sospechosos o de personas desconocidas.
- Extreme las precauciones ante correos electrónicos que le soliciten información personal, datos de acceso o contraseñas de alguna cuenta, ofrezcan un pago o un premio sin motivo (por ejemplo, sin haber participado), o pidan el envío de dinero.
- Su banco o la Agencia Tributaria nunca le pedirá datos personales o de acceso ni por correo electrónico ni por ninguna otra vía.

Utilizar soluciones de seguridad

Son múltiples los proveedores que ofrecen soluciones de seguridad informatica tanto comerciales como gratuitas cuyo uso conviene valorar.

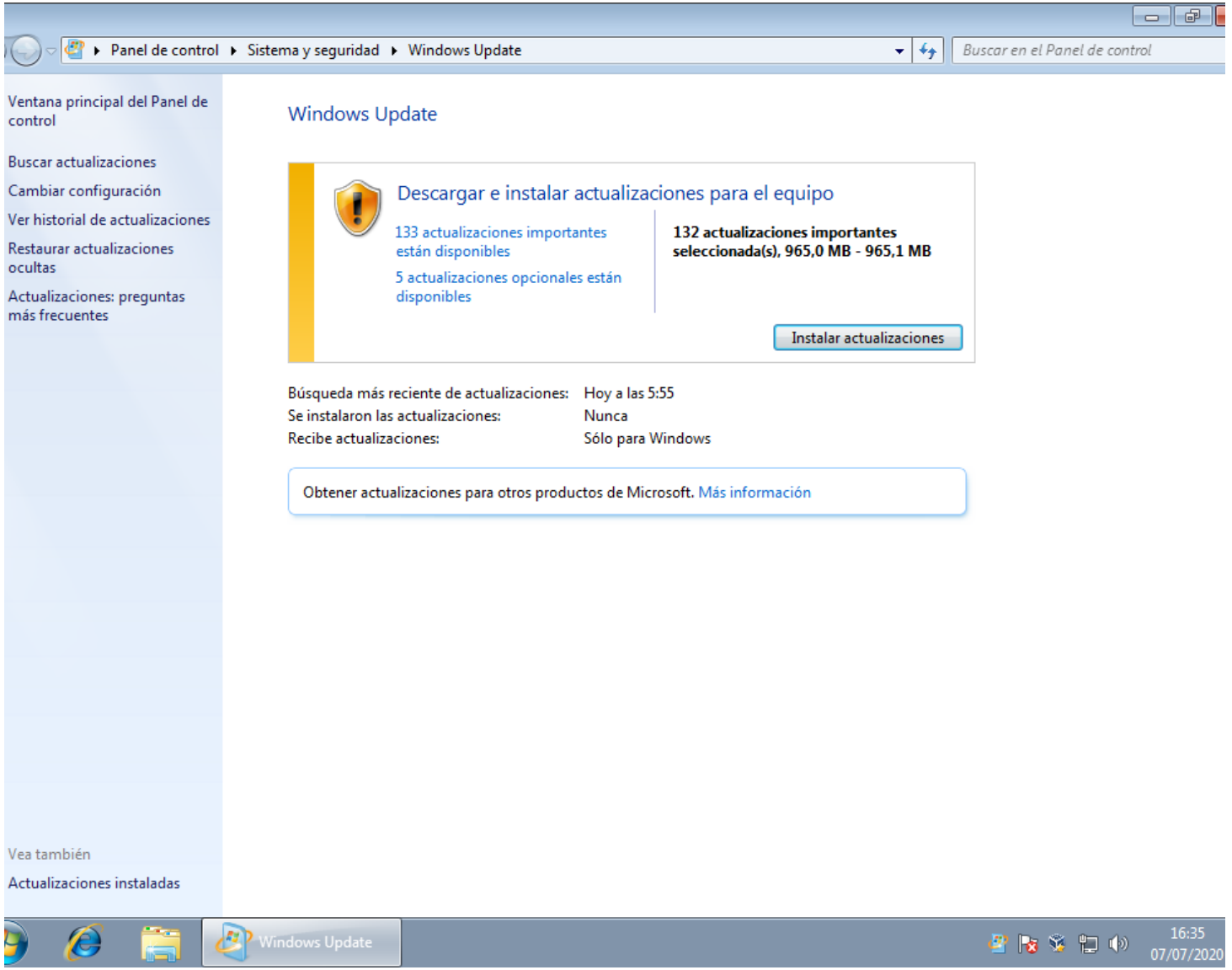
Cortafuegos, Antivirus o Sistemas de Cifrado de Datos son altamente recomendables de usar.

Actualizar el sistema operativo y las aplicaciones

Todos los sistemas operativos cuentan con herramientas para mantener actualizados sus equipos. Y son de uso obligado porque incluyen actualizaciones de seguridad contra amenazas conocidas.

Igualmente, es muy importante la actualización de aplicaciones instaladas a las últimas versiones ya que éstas suelen incluir parches de seguridad.

Cuando las versiones son más antiguas, tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en los programas desactualizados.



Protege tu navegador

Todos los navegadores web incluyen características avanzadas de seguridad cuya activación debemos revisar y configurar porque son las aplicaciones con las que accedemos a Internet y sus servicios.

Debemos prestar atención a los avisos sobre sitios inseguros que muestran los navegadores y *cerrar las sesiones web despues de utilizar el ordenador*.

Cuida tus contraseñas

Para estar seguro en línea se debe contar con una contraseña robusta para uso en los sitios web destinados a banca en línea y comercio electrónico, que tenga minimo 12 caracteres *combinando números, mayúsculas, minusculas y símbolos* y evitando incluir:

- Fechas de nacimiento
- Nombres y apellidos
- Números de teléfono
- Secuencias numéricas fáciles del tipo: 12345678, 0000000, etc.

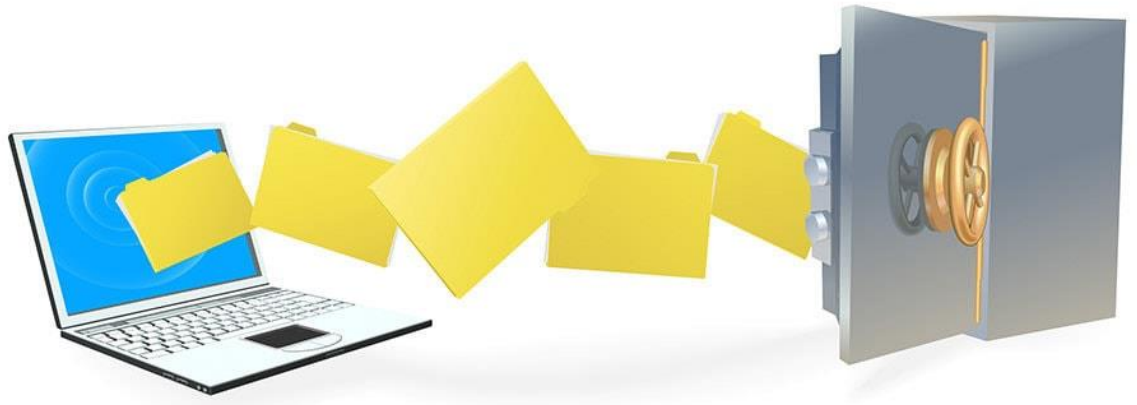
Usa autenticación Multifactor

La autenticación de varios factores (o en dos o más pasos) proporciona un nivel adicional de seguridad en las cuentas a las típicas contraseñas ya que no basta con vulnerar el nombre de usuario y contraseña.

Generalmente, utiliza un código de verificación servido mediante una aplicación móvil o SMS, para aplicar además del nombre de usuario y la contraseña al iniciar sesión

Realiza copias de seguridad

La realización de copias de seguridad es altamente recomendable para un usuario que pretenda proteger la información personal y/o corporativa de un equipo informático.



Las copias de seguridad deben almacenarse en un dispositivo de almacenamiento externo al de nuestro equipo o en un servicio de almacenamiento en nube.

Precaución con las redes Wi-Fi públicas

Las redes Wi-Fi públicas son altamente inseguras, se pueden utilizar para una navegación intrascendental guardando las debidas precauciones, pero no para accesos que requieran mostrar tus datos, accesos y contraseñas o hacer compras por Internet.

Activa la restauración del sistema

La restauración de los sistemas operativos es una herramienta que puede “salvarnos la vida” ante un error del software o instalación de alguna aplicación que no funciona correctamente y también ante la entrada de un virus en nuestro equipo.

Valora el cifrado de datos

Cifrar o “codificar” los datos de tu equipo para mantenerlos protegidos contra amenazas como el robo de datos o la exposición en caso de pérdida, el robo o la retirada inapropiada de equipos.

En las Redes Sociales

- Mantenga la privacidad.
- Denuncie las anomalias.
- No proporcione información personal
- No acepte peticiones de amistad de personas a las que no conoce.

Sentido común

La Prudencia es la mejor barrera contra el malware.

Cuida especialmente:

- Descargas e instalación de aplicaciones de sitios web no seguros.
- Navegación por determinadas páginas de Internet.
- Apertura de correos electrónicos o ficheros adjuntos no solicitados o que llegan de remitentes desconocidos o los que llegan de redes sociales o aplicaciones de mensajería que contienen vulnerabilidades explotables por los ciberdelincuentes.
- Llamadas de extraños simulando ser familiares o conocidos que estan en peligro y solicitando ayuda economica.