RECOMENDACIONES CONTRA VIRUS

Este documento de Microsoft describe algunas recomendaciones para evitar los VIRUS.
La manera más común de adquirir un Virus es aceptando un correo o mensaje.
La recomendación principal es.

- No abras los mensajes de correo electrónico de remitentes desconocidos.
- No navegar en sitios desconocidos sobre todo en los servidores de la empresa.

Se anexa link original de Microsoft.
https://support.microsoft.com/es-es/windows/proteger-mi-pc-contra-los-virus-b2025ed1-02d5-1e87-ba5f-71999008e026

Proteger mi PC contra los virus - Windows 10 Windows 8.1
Este artículo trata sobre las formas de proteger tu PC de los virus que pueden estropearla o permitir que los delincuentes roben tus datos, información personal o dinero.

- **Usar una aplicación antimalware**: instalar una aplicación antimalware y mantenerla actualizada puede ayudar a defender tu PC contra los virus y otro malware (software malicioso). Las aplicaciones antimalware buscan virus, spyware y otros tipos de malware que intentan entrar en tu correo electrónico, sistema operativo o archivos. Todos los días pueden aparecer amenazas nuevas; por lo tanto, consulta frecuentemente las actualizaciones del sitio web del fabricante de antimalware.
  Microsoft Defender es un software antimalware gratuito que se incluye en Windows y que puedes actualizar automáticamente a través de Windows Update. También hay productos antivirus de terceros entre los que puedes elegir.
- **Más no siempre es mejor**. Ejecutar varias aplicaciones antimalware al mismo tiempo puede hacer que el sistema sea lento o inestable. Si instalas una aplicación antimalware de terceros, Microsoft Defender se desactivará automáticamente. Si instalas una aplicación antimalware de terceros, Microsoft defender se apagará automáticamente.
- **No abras los mensajes de correo electrónico de remitentes desconocidos**, o los archivos adjuntos de correo electrónico que no reconoce, muchos virus se adjuntan a los mensajes de correo electrónico y se propagan tan pronto como se abre el archivo adjunto. Es mejor no abrir ningún archivo adjunto a menos que se trate de algo que estás esperando. Para más información, consulte: Protégete del phishing.
- **Utiliza un bloqueador de ventanas emergentes con tu navegador de Internet** : las ventanas emergentes son pequeñas ventanas del navegador que aparecen en la parte superior del sitio web que estás viendo. A pesar de que la mayoría están creadas por anunciantes, también pueden contener un código malintencionado o inseguro. Un bloqueador de elementos emergentes puede evitar que aparezcan algunas o todas estas ventanas. El bloqueador de ventanas emergentes de Microsoft Edge está activado de forma predeterminada.
- **Si usas Microsoft Edge, asegúrate de que SmartScreen esté activado**: SmartScreen en Microsoft Edge le ayuda a protegerse de los ataques de phishing y malware al advertirle si se ha informado de que un sitio web o una ubicación de descarga no son seguros. Para obtener más información, consulta ¿Qué es SmartScreen y cómo puede ayudar a protegerme?
- **Prestar atención a las notificaciones de Windows SmartScreen**: Tenga cuidado con las aplicaciones no reconocidas que se descargan de Internet. Las aplicaciones no reconocidas tienen más probabilidades de ser inseguras. Cuando descargas y ejecutas una aplicación de Internet, SmartScreen usa la información sobre la reputación de la aplicación para advertirte si la aplicación no es conocida y puede ser maliciosa.
- **Mantén Windows actualizado**: periódicamente, Microsoft publica actualizaciones de seguridad especiales que pueden ayudar a proteger tu PC. Estas actualizaciones pueden evitar virus y otros ataques malintencionados mediante el cierre de posibles carencias de seguridad.
  Puedes activar Windows Update para asegurarte de que Windows reciba estas actualizaciones automáticamente.
- **Usar un firewall**: el Firewall de Windows, o cualquier otra aplicación de firewall, puede ayudar a notificarte sobre actividades sospechosas si un virus o gusano intenta conectarte a tu PC. También puedes bloquear virus, gusanos y atacantes que envíen aplicaciones potencialmente dañinas a tu PC.
- **Usa la configuración de privacidad de tu navegador de Internet:** algunos sitios web pueden intentar utilizar tu información personal para publicidad dirigida, fraude y robo de identidad.
- **Asegúrate de que el Control de Cuentas de Usuario (UAC) esté activado**: cuando se vayan a realizar cambios en tu PC que requieran un permiso de nivel de administrador, el UAC te notificará y te dará la oportunidad de aprobar el cambio. UAC puede ayudar a evitar que los virus realicen cambios no deseados. Para abrir UAC, desliza rápidamente el dedo desde el borde derecho de la pantalla y pulsa en Buscar. (Si utiliza mouse, señale la esquina superior derecha de la pantalla, mueva el puntero hacia abajo y, a continuación, haga clic en Buscar). Escribe uac en el cuadro de búsqueda y luego pulsa o haz clic en Cambiar la configuración del Control de Cuentas de Usuario.
- **Limpia el caché de Internet y el historial de navegación** : la mayoría de los navegadores almacenan información sobre los sitios web que visita y la información que proporciona, como tu nombre y dirección. Si bien puede ser útil tener estos datos almacenados en tu PC, es posible que alguna vez quieras eliminar parte de estos o todos (por ejemplo, cuando usas un equipo público y no quieres dejar información personal allí). Para obtener más información, consulta Eliminar el historial de exploración.

Cualquier duda, comunicarse a Sierra.