20200210, Nota Informativa, sobre diversos mecanismos para mejorar la seguridad en Internet.

En virtud de mis compromisos contractuales, a continuación le transmito una serie de mecanismos dirigidos a aumentar la seguridad en Internet en sus dispositivos.

La seguridad en Internet está amenazada por todo tipo de malwares, robo de datos o invasiones a la privacidad: en la realidad actual han aumentado los dispositivos conectados, la manera de alojar información y el modo de acceder a servicios y aplicaciones de todo tipo con las que conectan a diario centenares de millones de usuarios.

Todo ello contribuye a que aumenten los riesgos de seguridad. Por ello, se recomienda que las medidas que se enumeran a continuación, pasen a formar parte de la vida diaria de su entidad.

1) A fin de mejorar la seguridad en línea, el primer paso consiste en la **protección de los navegadores web**. 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.

Además de revisar el cifrado de extremo a extremo en la sincronización o el aislamiento de procesos (sandbox), debemos prestar atención a los avisos sobre sitios inseguros que muestran los navegadores. También revisar las extensiones instaladas porque algunas son fuente frecuente de introducción de malware.

El uso de sesiones en “modo invitado” es recomendable en tanto que esté totalmente desligado del perfil original del usuario, incluyendo configuración o historial.

2) Una buena **gestión de contraseñas** es considerada la regla de oro para mejorar la seguridad en línea. Se recomienda tener una contraseña aleatoria fuerte y distinta para cada sitio web. El uso de gestores de contraseñas capaces de generar múltiples contraseñas y recordarlas está siendo aconsejado por expertos en ciberseguridad.

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

El servicio está disponible en la mayoría de servicios importantes de Internet y conviene utilizarlo siempre que se pueda. 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.

4) Se debe evitar el **uso de redes inalámbricas gratuitas**: investigadores de seguridad han demostrado que son fácilmente pirateables.

Ningún usuario debe utilizarlas para nada más allá de una navegación intrascendente y, en ningún caso, con fines profesionales.

5) La realización de **copias de seguridad** es altamente recomendable para un usuario que pretenda proteger la información personal y corporativa de un equipo informático, además de ser una tarea de mantenimiento que contribuye a la salud del hardware. Las copias de seguridad deben almacenarse en un dispositivo de almacenamiento externo al de nuestro equipo o en un servicio de almacenamiento en nube como OneDrive o Dropbox.

6) La **actualizacion del sistema operativo y sus aplicaciones** es otro elemento fundamental. Cuando las versiones son más antiguas, tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en el programa.

En caso de que las anteriores indicaciones le susciten dudas, estoy a su disposición para resolver cualquier controversia al respecto.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de febrero de 2020.

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2020.02.10 08:49:58 +01'00'