20211120, Nota Informativa, ciberseguridad sobre navegación segura.

En virtud de mis compromisos contractuales, seguidamente os traslado una serie de principios y recomendaciones sobre la navegación segura.

El **CCN-CERT (Centro Criptológico Nacional)** en el documento titulado "principios y recomendaciones sobre ciberseguridad", al que ya nos acercamos en la anterior Nota Informativa, dedica un apartado a la navegación segura que considero puede ser de mucho interés. A ello pues.

La comunicación en Internet se sustenta en una idea básica: clientes (ordenadores, teléfonos, tabletas,…) llaman a servidores (web, bases de datos…) que proporcionan (sirven) información. Esta comunicación se lleva a cabo a través de un protocolo (http, https9, ftp, etc.).

El cliente está identificado en la red a través de una dirección IP (TCP/IP) y cada vez que se conecta a un sitio web, éste conoce automáticamente la dirección IP, nombre de máquina, la página de procedencia, etc. Se produce un intercambio de información que habitualmente no es visible donde el navegador web es el que facilita la mayoría de estos datos.

- Un alto porcentaje de los usuarios no es consciente de la cantidad de información que, de forma inadvertida e involuntaria, está revelando a terceros al hacer uso de Internet.

- Cada vez que se visita un sitio web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio.

- Al sitio web le resulta trivial averiguar la dirección de Internet de la máquina desde la que se está accediendo, sistema operativo, etc.

• Con ayuda de las “cookies” se puede personalizar aún más la información recabada acerca de los visitantes, registrando las páginas más visitadas, preferencias, tiempo de la visita, software instalado, etc.

Un navegador web, en favor de la máxima usabilidad, permite que se acceda a información aparentemente inofensiva.

• La dirección IP pública con que se conecta el usuario.

o Tu dirección IP es xxx.xxx.xxx.xxx.

o Tu navegador está utilizando 128 bits de clave secreta SSL.

o El servidor está utilizando 1024 bits de clave pública SSL.

• La resolución de la pantalla.

• Qué páginas se leen y cuáles no, qué figuras se miran, cuántas páginas se han visitado, cuál fue el sitio recientemente visitado “Referer”.

• El valor del campo “User-Agent”.

o Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0

• El idioma y zona GMT del sistema operativo.

• Si se aceptan o no “cookies”.

• Las fuentes cargadas en el sistema o plugins instalados y activados. Algunas recomendaciones para mantener una navegación segura10 son:

• Acceder únicamente a sitios de confianza.

• Mantener actualizado el navegador a la última versión disponible del fabricante.

- Configurar el nivel de seguridad del navegador según sus preferencias.
- Descargar los programas desde sitios oficiales para evitar suplantaciones maliciosas.
- Configurar el navegador para evitar ventanas emergentes.
- Utilizar un usuario sin permisos de “Administrador” para navegar por Internet e impedir la instalación de programas y cambios en los valores del sistema.
- Borrar las “cookies”, los ficheros temporales y el historial cuando se utilicen equipos ajenos para no dejar rastro de la navegación.
- Desactivar la posibilidad “script” en navegadores web, como Firefox (NoScript) o Chrome (NotScript), para prevenir la ejecución de los mismos por parte de dominios desconocidos.
- Se recomienda hacer uso de HTTPS (SSL/TLS) frente a HTTP incluso para aquellos servicios que no manejen información sensible. Algunas funcionalidades como HSTS y extensiones como HTTPS Everywhere servirán de gran ayuda para garantizar el uso preferente de HTTPS sobre HTTP durante la navegación web.
- En la medida de lo posible, emplear máquinas virtuales para navegar por Internet.

Además, hay que tener en cuenta que los sistemas de navegación anónima permiten el uso de algunos servicios de Internet, principalmente los basados en navegación web (http/https), de forma desvinculada de la dirección IP origen de la comunicación.

- Anonimizadores.

o Actúan como un filtro entre el navegador y sitio web que se desea visitar.

o Al conectarse al anonimizador, se introduce la URL a visitar y entonces éste se adentra en la red filtrando cookies, javascripts, etc.

• Servidores Proxy.

o Un servidor proxy actúa de pasarela entre la máquina cliente e Internet.

o El servidor proxy actúa de intermediario, se encarga de recuperar las páginas web en lugar del usuario que navega.

• Túneles de Cifrado (TOR, VPS y Darknets).

o Red de "túneles" por las cuales los datos de navegación, debidamente cifrados, atraviesan múltiples nodos hasta llegar a su destino.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 20 de noviembre de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Digitally signed by ZOTANO SANCHEZ SALVADOR - 32028277H
Date: 2021.11.21 09:16:24 +01'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)