DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

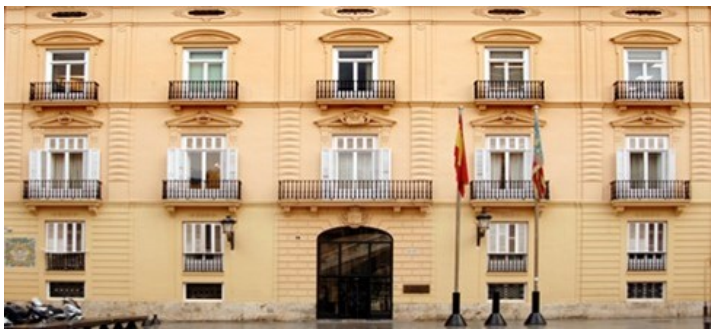
Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 11| Mayo 2021

RIESGOS PARA LA SEGURIDAD EN LA UTILIZACIÓN DE UNA RED WIFI PÚBLICA. CONSEJOS EN SU UTILIZACIÓN

Í N D I C E



RIESGOS PARA LA SEGURIDAD EN LA UTILIZACIÓN DE UNA RED WIFI PÚBLICA. CONSEJOS EN SU UTILIZACIÓN

	Página
Introducción	**2**
Riesgos de la red WIFI pública	**3**
Recomendaciones básicas	**5**
Pautas a tener en cuenta en Protección de Datos	**7**
Material complementario	
Noticias de actualidad	**8**

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

Hasta hace pocos años, la idea de interconectar dispositivos tecnológicos estaba ligada a la clásica distribución de una red de ordenadores cableada que nos permitía, por un lado, tener acceso a un servidor, normalmente de datos y por otro, a Internet. Hoy en día, esta concepción ha cambiado radicalmente. El uso de la tecnología inalámbrica se ha extendido de tal manera que nadie concibe un sistema en el que, para conectarse, sea necesario hacer uso de cables. Nos hallamos inmersos en una era inalámbrica en la que dispositivos como ordenadores personales, smartphones o tablets y elementos IoT pueden llegar a estar interconectados entre sí sin necesidad de hacer uso del cable, a través de ondas electromagnéticas, incorporando esta capacidad de forma nativa, sin necesidad de añadirla artificialmente. La aparición de la red inalámbrica se entiende como una extensión de una red de ordenadores interconectados físicamente, por cable, con un único objetivo: proporcionar libertad de movimientos evitando tener que situarse en una ubicación física determinada a la hora de conectarse a los recursos que pueda ofrecer una organización. Pero a pesar de las ventajas que pueda ofrecer esta funcionalidad, no está exenta de riesgos asociados a su uso, que se deberán analizar y tener en cuenta en cualquier organización a la hora de configurar políticas y medidas que los mitiguen o minimicen y que a su vez, garanticen la seguridad de las comunicaciones.

Definiremos red inalámbrica, como aquella formada por dispositivos capaces de intercomunicarse entre sí o con otra red (como Internet), sin necesidad de elementos físicos que las conecten como pueden ser los cables. Teniendo en cuenta que existen muchos tipos de redes inalámbricas cuya diferencia radica en aspectos como la arquitectura, tecnología o estándares de comunicación entre otros, en esta guía nos centraremos en las más extendidas, las Redes de Área Local Inalámbricas, conocidas como WLAN (en inglés, *Wireless* Local Área *Networks*) o redes wifi.

Como hemos evidenciado, la principal ventaja de contar con un mecanismo de red inalámbrico es la ausencia de cables y, por lo tanto, la ausencia de preocupaciones por el estado, mantenimiento y organización de los mismos.

Sin embargo, uno de los principales inconvenientes asociados a este tipo de conectividad es la naturaleza abierta y accesible de la misma, lo que la convierte en una tecnología más vulnerable que el cable. Además, debido a interferencias de señal y otros factores, como, por ejemplo, los ambientales, podría verse afectada la velocidad de navegación o incluso la propia disponibilidad de la señal. En resumen, la tecnología wifi permite dar servicio a varios usuarios que podrán conectarse cuando así lo deseen y en cualquier lugar donde llegue la señal, mientras que con el cable sólo podrá conectarse aquel que haga uso de dicho cable en el puesto habilitado.

"…UNO DE LOS PRINCIPALES INCONVENIENTES ASOCIADOS A ESTE TIPO DE CONECTIVIDAD ES LA NATURALEZA ABIERTA Y ACCESIBLE DE LA MISMA, LO QUE LA CONVIERTE EN UNA TECNOLOGÍA MÁS VULNERABLE QUE EL CABLE"

RIESGOS DE LA RED WIFI PUBLICA

Cuando nos conectamos a una red wifi-pública desconocemos quién es el administrador o qué medidas de seguridad utiliza para impedir acciones malintencionadas de otros usuarios conectados y, por tanto, podemos exponernos sin necesidad a una serie de riesgos que describiremos a continuación.

Robo de datos transmitidos:

Si la conexión la realizamos sin contraseña, lo que conocemos como una red "abierta", los datos que transmitimos pueden ser leídos por cualquiera, tanto el administrador como otros usuarios que se encuentren conectados a la red.

La información está expuesta a cualquiera que sepa cómo leerla, y para ello no es necesario tener unos conocimientos técnicos muy elevados.

Si el sistema nos pide una contraseña y aparece un candado, como "red protegida", la información se transmite de forma cifrada. No obstante, esto está condicionado por el sistema de seguridad utilizado y la contraseña escogida. De menor a mayor seguridad, los sistemas son WEP, WPA y WPA2. 

Nunca debemos conectarnos a una red WEP ya que se ha demostrado que es vulnerable y que su seguridad equivale a una red abierta (sin contraseña).

Robo de datos almacenados en nuestro equipo

Al formar parte de una red pública en la que existen otros usuarios conectados, nuestro dispositivo está expuesto y visible a los demás usuarios presentes en la misma.

Por tanto, somos susceptibles de recibir cualquier tipo de ataque desde uno de estos equipos conectados.

Infección de los dispositivos

Al conectarnos a una wifi ajena, un usuario malintencionado conectado a la misma red podría tratar de infectar nuestro equipo con algún tipo de virus.

Es importante mantener siempre nuestro equipo actualizado con las últimas actualizaciones de seguridad para el sistema operativo y para las aplicaciones que tengamos instaladas.

Equipos intermediarios malintencionados

Un usuario malintencionado conectado a la red podría configurar su equipo para hacer de intermediario de la comunicación entre nosotros y el servicio (por ejemplo, *Facebook*) modificando o eliminando la información intercambiada, que pasaría a través del ciberdelincuente.

El *hacker* "inocente"

En un momento dado, podemos sentir la tentación de conectarnos a una red ajena abierta o protegida utilizando herramientas de *hacking* wifi. Sin embargo, esta práctica constituye un uso ilícito de servicios de terceros que puede tener consecuencias legales.

Además, puede darse el caso de que esa red wifi no presente contraseña o sea especialmente fácil de hackear precisamente para atraer víctimas a ella y así robar los datos al pícaro usuario.

RECOMENDACIONES BÁSICAS

Nunca debemos utilizar redes wifi no confiables para acceder a servicios donde se intercambie información sensible: información bancaria, recursos corporativos, correo electrónico o acceso a las redes sociales.

Debemos evitar el uso de cualquier servicio en el que la información transferida tenga un componente importante de privacidad. Aunque podemos utilizar las redes públicas para otras acciones, como leer noticias en periódicos online o mirar la previsión del tiempo, no olvidemos que la mayor parte de los dispositivos mantienen un proceso de sincronización continua, por lo que el riesgo continúa existiendo.

Si lo puedes evitar, no te conectes a redes inalámbricas abiertas. Las redes públicas pueden ponernos en peligro. Tanto el administrador como alguno de los usuarios conectados pueden utilizar técnicas para robarnos información.

Mantener siempre el equipo actualizado, con el antivirus instalado correctamente y si es posible, hacer uso de un cortafuegos.

Si vamos a conectarnos, es preferible acceder a una red con seguridad WPA o WPA2. Las redes abiertas y con seguridad WEP son totalmente inseguras.

No inicies sesión (usuario/contraseña) en ningún servicio mientras estés conectado a una red pública. Evita realizar transacciones bancarias, compras online o cualquier otra tarea que suponga el intercambio de datos privados desde redes wifi-públicas.

Deshabilitar cualquier proceso de sincronización de nuestro equipo si vas a usar una red pública.

Tras la conexión, eliminar los datos de la red memorizados por nuestro equipo. Transacciones bancarias, compras online o cualquier otra tarea que suponga el intercambio de datos privados desde redes wifi-públicas.

"TRAS LA CONEXIÓN, ELIMINAR LOS DATOS DE LA RED MEMORIZADOS POR NUESTRO EQUIPO"

PAUTAS A TENER EN CUENTA EN PROTECCIÓN DE DATOS

A continuación, con el objeto de minimizar la exposición indeseada de datos de carácter personal, se relacionan unas pautas básicas:

1. Ten en cuenta la privacidad como una de las características deseables a la hora de elegir un navegador y las aplicaciones que instalas y utilizas en tus dispositivos. Debido a la constante evolución de estos productos debes consultar los últimos análisis que se publican sobre ellos.
2. Evita instalar aplicaciones innecesarias en tu navegador, eso minimizará los riesgos.
3. Mantén actualizado tu navegador para disfrutar de las últimas tecnologías de protección antirastreo.
4. Si el navegador dispone de protección avanzada anti-rastreo/seguimiento, activa o mantén activada esta configuración. Estas opciones permiten varios niveles de protección, elige el nivel más elevado y que, a la vez, se ajuste a tus preferencias. En todo caso, si así lo consideras, puedes habilitar la opción para enviar a los sitios web la señal "*Do not track"* , indicando tu deseo de no ser rastreado.
5. Sopesa la utilidad de tener dos navegadores distintos instalados, uno con una configuración más restrictiva y otro configurado con mayores permisos. De esta forma, si las configuraciones anteriores te impiden acceder a algún servicio concreto, puedes seguir accediendo a ese servicio con el otro navegador minimizando la exposición de tus datos.
6. Puedes configurar el navegador de tal manera que al cerrarse se eliminen las *cookies*. Si esta medida te resulta incómoda para navegar en tus sitios favoritos, puedes optar por borrarlas manualmente cada cierto tiempo.
7. Evita en lo posible iniciar sesión en el navegador, identificándote con un usuario, o al menos, evita que la sesión se mantenga abierta de forma indefinida.
8. Si el navegador no dispone de protección avanzada anti-rastreo/seguimiento, se pueden instalar extensiones que realicen esta función. No obstante, instala únicamente aquellos que ofrezcan garantías. En general, instalar software de terceros en el navegador puede introducir riesgos.
9. Configura las opciones de tu dispositivo para que, si así lo deseas, no se utilice el identificador de publicidad para crear perfiles o mostrar anuncios personalizados basados en la localización o el perfil.
10. Revisa y configura las opciones de personalización, perfiles y publicidad de aquellas aplicaciones, servicios y redes sociales que utilices.

"SOPESA LA UTILIDAD DE TENER DOS NAVEGADORES DISTINTOS INSTALADOS, UNO CON UNA CONFIGURACIÓN MÁS RESTRICTIVA Y OTRO CONFIGURADO CON MAYORES PERMISOS. DE ESTA FORMA, SI LAS CONFIGURACIONES ANTERIORES TE IMPIDEN ACCEDER A ALGÚN SERVICIO CONCRETO, PUEDES SEGUIR ACCEDIENDO A ESE SERVICIO CON EL OTRO NAVEGADOR MINIMIZANDO LA EXPOSICIÓN DE TUS DATOS"

MATERIAL COMPLEMENTARIO

- "Resolución de procedimiento A/00251/2018 instruido por la Agencia Española de Protección de Datos." Consulta este enlace.
- Recomendaciones de seguridad en redes WI-FI corporativas, por CN-CERT. Consulta este enlace.
- Infografía recomendaciones para minimizar los riesgos que el seguimiento en la actividad de navegación puede tener, por la Agencia Española de Protección de Datos. Consulta este enlace.
- Decálogo básico de seguridad por CN-CERT. Consulta este enlace.
- Seguridad en redes wifi por INCIBE. Consulta este enlace.
- Resolución de archivo, referentes al Ayuntamiento de Barcelona por Autoridad Catalana de Protección de Datos (APDCat). Consulta este enlace.
- Guía "Privacidad y seguridad en internet", elaborada por la AEPD y la OSI. Consulta este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) Protección de Datos avala que Interior monitorice redes sociales para detectar bulos sobre la Covid-19.**

  La Agencia Española de Protección de Datos (AEPD) ha avalado que el Ministerio del Interior monitorice las redes sociales para detectar los bulos y *'fake news'* relacionados con la Covid-19, un asunto por el que varios partidos de la oposición pidieron explicaciones tras informarse de esta labor policial en rueda de prensa en Moncloa durante el primer estado de alarma decretado en marzo de 2020.

  Consulta la información en este enlace.

- **El Pleno da luz verde al Proyecto de Ley Orgánica de protección integral a la infancia y la adolescencia frente a la violencia y lo remite al Senado, que recoge la disponibilidad de un canal de denuncia de contenidos ilícitos con el fin de garantizar la protección en Internet.** Consulta la noticia en este enlace.

- **El Comité Europeo de Proteccion de datos adopta un dictamen sobre el proyecto de decisión de adecuación del Reino Unido.** El 14 de abril de 2021, el Comité Europeo de Proteccion de datos ("EDPB") anunció que había adoptado su Opinión sobre el proyecto de decisión de adecuación del Reino Unido emitida por la Comisión Europea el 19 de febrero de 2021. La decisión de adecuación se adoptará formalmente si es aprobada por los Estados miembros de la UE actuando a través del Consejo Europeo**.**

  Consulta la noticia en este enlace.