DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 15 | Septiembre 2021

REDES WIFI PÚBLICAS Y CUMPLIMIENTO RGPD

Í N D I C E

REDES WIFI PÚBLICAS Y CUMPLIMIENTO RGPD

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: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"CON LA ENTRADA EN VIGOR DEL RGPD, DICHA ACTIVIDAD SE CONSIDERA UN TRATAMIENTO DE DATOS PERSONALES, POR LO QUE LA NORMATIVA DE PROTECCIÓN DE DATOS SERÁ EXIGIBLE A LA ENTIDAD PÚBLICA TITULAR DE LA RED WIFI, QUIEN DEBERÁ PONER LAS MEDIDAS OPORTUNAS PARA EL CUMPLIMIENTO DE LA NORMATIVA"

INTRODUCCIÓN

El Reglamento Europeo sobre Protección de Datos 679/2016 (de ahora en adelante, RGPD), establece nuevas obligaciones para las entidades que pongan a disposición de posibles usuarios una Red Wifi gratuita o de pago.

En la actualidad son muchas las Administraciones Publicas que han invertido en la instalación de estas redes para proporcionar a los ciudadanos un servicio altamente demandado y un valor añadido al servicio que prestan.

Con la entrada en vigor del RGPD, dicha actividad se considera un tratamiento de datos personales, por lo que la normativa de protección de datos será exigible a la entidad pública titular de la red WIFI, quien deberá adoptar las medidas oportunas para el correcto cumplimiento de la normativa.

De este modo, a partir de la entrada en vigor del RGPD ya no resulta posible acceder a redes Wifi abiertas que no requieran la identificación previa del usuario; es necesario instalar un sistema de identificación (HotSpot) que les exija la aceptación de unas condiciones (Política de privacidad, aviso legal y condiciones de uso en su caso) antes de permitirles el acceso.

Un HotSpot es un punto de acceso que ofrece conexión a Internet a través de una red inalámbrica y un enrutador, conectado a un proveedor de servicios de Internet. Debido a que la comunicación se establece mediante ondas, las posibilidades de que sea objeto de un ataque o que una persona ajena se apodere de la red son significativas, por lo que se impone la necesidad de que dicha conexión sea segura y cifrada.

"COMO DESDE ESTE PORTAL SE VA A REALIZAR UN REGISTRO DE USUARIOS, SEGÚN EL ART. 13 DEL RGPD, CUALQUIER TRATAMIENTO QUE SE EFECTÚE CON LOS DATOS RECABADOS DEBERÁ EXPLICARSE DE FORMA CLARA Y CONCISA A LOS USUARIOS DE LA CONEXIÓN."

CONSIDERACIONES GENERALES

Como paso inicial, el responsable del establecimiento debe realizar un análisis de riesgos y, según los resultados, adoptar todas las medidas de seguridad que se consideren oportunas para proteger a los usuarios de estas redes (cifrado, registro de acceso, etc.).

Una de las medidas a implantar consiste en que la wifi esté gobernada por un portal cautivo. Se trata de una pantalla o portal de acceso, generalmente personalizado, que aparece al conectarse a la wifi y que obliga al usuario a hacer *login*. En ella, se explica al usuario que desee conectarse a la red los términos y condiciones de uso. La entidad responsable ya no tendrá que proporcionar la contraseña al usuario y, además, así quedará registrado quién se ha conectado, en caso de que se realice algún acto ilícito.

Como desde este portal se va a realizar un registro de usuarios, según el art. 13 del RGPD, cualquier tratamiento que se efectúe con los datos recabados deberá explicarse de forma clara y concisa a los usuarios de la conexión.

El mensaje debe incluir la información referente al apartado 1 del artículo 13 del RGPD, es decir quién es el responsable del tratamiento, por qué y para qué se toman los datos personales y cómo ejercer los derechos. Esta información debe incluir:

- la identidad y datos de contacto del responsable, representante y delegado de protección de datos (DPD);
- los destinatarios del tratamiento;
- la finalidad del tratamiento de la información recopilada y si se va a ceder a terceros el envío de actividades;
- el plazo de conservación de los datos;
- la posibilidad de ejercicio de derechos y de presentar reclamación ante la autoridad de control competente.

Además, según recoge el art. 33 del RGPD, en el caso de que se haya detectado una brecha que ponga en peligro la información recopilada, la entidad responsable del registro de usuarios deberá notificar en menos de 72 horas a los usuarios. En caso de no hacerlo en tiempo y forma, salvo por causas debidamente justificadas, el responsable se enfrentará a la posible inspección que determine la autoridad competente en materia de protección de datos, en el caso de la Diputación de Valencia, la Agencia Española de Protección de Datos (AEPD). Véase publicación anterior: "*Directrices para la correcta la correcta gestión de las brechas de seguridad".*

"ES RECOMENDABLE CREAR Y MANTENER UN REGISTRO DE ACTIVIDAD DE LA RED POR PARTE DE LOS USUARIOS QUE SE CONECTAN A LA MISMA COMO SALVAGUARDA, EN EL CASO DE QUE SE REALICEN ACTIVIDADES ILÍCITAS A TRAVÉS DE ELLA"

Por ello, debe incluirse un apartado en el que se recabe el consentimiento expreso del usuario para poder acceder a la red como, por ejemplo, una casilla de aceptación junto a la leyenda:

«Sí, he leído y acepto la política de privacidad y las Condiciones y términos de uso».

En ningún caso, esta casilla puede venir marcada por defecto, ya que la aceptación de los términos y condiciones por parte del usuario debe ser consentida.

REGISTRO DE ACTIVIDAD, ¿QUÉ REQUISITOS DEBE CUMPLIR?

Es recomendable crear y mantener un registro de actividad de la red por parte de los usuarios que se conectan a la misma como salvaguarda, en el caso de que se realicen actividades ilícitas a través de ella.

En los términos y condiciones debe incluirse, de forma clara, la motivación por la que se almacena esta información y recabar el consentimiento explícito y pleno del usuario. El tipo de información que se almacenará en dicho registro será, entre otros:

- las páginas visitadas;
- las sesiones de conexión;
- el dispositivo utilizado para la conexión;
- el idioma;
- el sistema operativo;
- el navegador que se utilizó.

En el caso de que el usuario no haya dado su consentimiento o no se le haya informado debidamente de dicho registro, no se podrá guardar dicha información ya que se estaría cometiendo un delito contra la intimidad del usuario.

Por último, si los administradores de la conexión detectaran la comisión de un delito por parte de los usuarios de la red que atente contra la libertad de las personas (coacciones o amenazas), deberán notificar a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), ya que en caso de que no se hiciera, se incurriría en un delito de omisión del deber de impedir delitos o de promover su persecución.

MEDIDAS DE SEGURIDAD DE LA RED

La red ofrecida a los ciudadanos y usuarios debe contar con una serie de medidas de seguridad, entre ellas:

- Mantener actualizado el *firmware* del *router* o del punto de acceso a la última versión disponible.
- Cambiar las credenciales de acceso al panel de administración del *router* o punto de acceso que vienen por defecto por otras diferentes. Importante tener en cuenta que la contraseña debe ser segura y robusta en caso de existir.
- Usar como mínimo un cifrado WPA2-PSK para la transmisión de datos entre el *router* y el dispositivo del usuario. Con ello se evita que otros usuarios de la red vean lo que transmiten.
- Cambiar el nombre que viene por defecto de la red.
- Establecer mecanismos de control parental para evitar el acceso a sitios web perjudiciales.

"EL RGPD EXIGE LA IDENTIFICACIÓN DEL USUARIO PARA ACCEDER A LA RED WIFI Y QUE ESTA RED SEA SEGURA Y ESTÉ ENCRIPTADA. ESTO IMPIDE A OTROS USUARIOS DE LA MISMA RED, CAPTAR INFORMACIÓN DE LOS TERMINALES CONECTADOS"

Y COMO USUARIO DE UNA RED ¿QUÉ DEBO TENER EN CUENTA?

Cuando vayas a usar una red WIFI pública debes tener en cuenta que al acceder tenga una política de privacidad donde te informe de cómo y para qué van a usar tus datos personales. Y unas condiciones de uso del servicio que debes leer.

Y te debe dar la opción a prestar tu consentimiento para que puedan tratar tus datos personales.

El RGPD exige la identificación del usuario para acceder a la red WIFI y que esta red sea segura y esté encriptada. Esto impide a otros usuarios de la misma red, captar información de los terminales conectados.

Por ello, nunca está de mas saber algunos consejos sobre cómo conectarse a una red WiFi abierta;

- Desconecta la sincronización entre dispositivos cuando utilices alguna de estas redes.
- Mantén tus antivirus, firewall y, en general tu equipo actualizado.
- Navega solo por páginas cuyos datos estén cifrados mediante protocolo https.
- Evita entrar en páginas en las que tengas que introducir tu nombre de usuario, contraseña o cualquier otro dato que pudiera delatar tu identidad.
- Elimina cualquier dato que haya quedado grabado en tu ordenador o dispositivo después de la conexión: historiales de búsqueda y navegación, cookies, etc.

MATERIAL COMPLEMENTARIO

- Guía de INCIBE "Seguridad en redes WiFi" Consulta este enlace.
- "Privacidad y seguridad en internet" GUIA (AEPD). Consulta este enlace.
- "Protección de datos y Administración Local" (AEPD). Consulta este enlace.
- "Guía de privacidad y seguridad en Internet" Guia (AVPD). Consulta este enlace.
- Resolución nº 0017/2019 en relación con a señal recibida por los dispositivos de captación y análisis de señales Wi-Fi que se instalan en determinadas tiendas, al objeto de conocer los recorridos y tránsitos realizados por terminales electrónicos (AEPD). Consulta este enlace.

NOTICIAS

- **La AEPD se pronuncia sobre la viabilidad de que los particulares instalen "mirillas electrónicas" con videocámara en la puerta de su vivienda.** Entiende la Agencia que su mera instalación no supone, *a priori,* un mecanismo de control de las entradas/salidas de los vecinos, ni menos aún un hipotético "tratamiento de datos", ni es la finalidad para la que se concibe. En caso de "tratamiento", estará justificado cuando resulte necesario para proteger los derechos e intereses del propietario, generalmente su derecho a la integridad física y a la propiedad. Por tanto, el criterio de la AEPD es que si no existe una prueba objetiva que acredite un uso desproporcionado del dispositivo, el mismo es acorde a la finalidad concebida. Consulta la Resolución en este enlace.
- **Los ciberincidentes de tipo *ransomware* siguen siendo el origen de una parte muy importante de las brechas de datos personales notificadas a la AEPD.** Los ciberincidentes de tipo *ransomware* han vuelto a ser el origen de una parte muy importante de las brechas de datos personales notificadas a la AEPD durante el mes de julio, según el último informe de Notificaciones de Brechas de Datos Personales publicado por la AEPD. Casi la mitad de las notificaciones indican haber sufrido un incidente de este tipo. Consulta el informe en este enlace.
- **Con fecha 20 de agosto, el gigante asiático aprobó lo que denominó la "Ley de Protección de la Información Personal" (LPIP). Primera vez en ese país se establece un conjunto exhaustivo de normas sobre la recopilación y tratamiento de datos personales.**
  Esta nueva regulación exige que las empresas obtengan el consentimiento de los usuarios antes de recopilar sus datos, y tiene normas sobre cómo deben garantizar su protección cuando se transfieren fuera de la RPC.
  Consulta la noticia en este enlace.