DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern núm. 15 | Septembre 2021

XARXES WIFI PÚBLIQUES I COMPLIMENT RGPD

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

ÍNDEX

XARXES WIFI PÚBLIQUES I COMPLIMENT RGPD

Vos convidem a traslladar-nos les temàtiques que resulten de vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdssi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent

enllaç

"AMB L'ENTRADA EN VIGOR DEL RGPD, AQUESTA ACTIVITAT ES CONSIDERA UN TRACTAMENT DE DADES PERSONALS, PER LA QUAL COSA LA NORMATIVA DE PROTECCIÓ DE DADES SERÀ EXIGIBLE A L'ENTITAT PÚBLICA TITULAR DE LA XARXA WIFI, QUI HAURÀ DE POSAR LES MESURES OPORTUNES PER AL COMPLIMENT DE LA NORMATIVA"

INTRODUCCIÓ

El Reglament Europeu sobre Protecció de Dades 679/2016 (d'ara en avant, RGPD), estableix noves obligacions per a les entitats que posen a la disposició de possibles usuaris una Xarxa Wifi gratuïta o de pagament.

En l'actualitat són moltes les Administracions Publiques que han invertit en la instal·lació d'aquestes xarxes per a proporcionar als ciutadans un servei altament demandat i un valor afegit al servei que presten.

Amb l'entrada en vigor del RGPD, aquesta activitat es considera un tractament de dades personals, per la qual cosa la normativa de protecció de dades serà exigible a l'entitat pública titular de la xarxa WIFI, qui haurà d'adoptar les mesures oportunes per al correcte compliment de la normativa.

D'aquesta manera, a partir de l'entrada en vigor del RGPD ja no resulta possible accedir a xarxes Wifi obertes que no requerisquen la identificació prèvia de l'usuari; és necessari instal·lar un sistema d'identificació (HotSpot) que els exigisca l'acceptació d'unes condicions (Política de privacitat, avís legal i condicions d'ús en el seu cas) abans de permetre'ls l'accés.

Un HotSpot és un punt d'accés que ofereix connexió a Internet a través d'una xarxa sense fil i un encaminador, connectat a un proveïdor de serveis d'Internet. Pel fet que la comunicació s'estableix mitjançant ones, les possibilitats de què siga objecte d'un atac o que una persona aliena s'apodere de la xarxa són significatives, per la qual cosa s'imposa la necessitat que aquesta connexió siga segura i xifrada.

"COM DES D'AQUEST PORTAL ES REALITZARÀ UN REGISTRE D'USUARIS, SEGONS L'ART. 13 DEL RGPD, QUALSEVOL TRACTAMENT QUE S'EFECTUE AMB LES DADES RECAPTADES HAURÀ D'EXPLICAR-SE DE FORMA CLARA I CONCISA Als USUARIS DE LA CONNEXIÓ."

consideracions generals

Com a pas inicial, el responsable de l'establiment ha de realitzar una anàlisi de riscos i, segons els resultats, adoptar totes les mesures de seguretat que es consideren oportunes per a protegir els usuaris d'aquestes xarxes (xifratge, registre d'accés, etc.).

Una de les mesures a implantar consisteix en el fet que la wifi estiga governada per un portal captiu. Es tracta d'una pantalla o portal d'accés, generalment personalitzat, que apareix en connectar-se a la wifi i que obliga l'usuari a fer *login*. En ella, s'explica a l'usuari que desitge connectar-se a la xarxa els termes i condicions d'ús. L'entitat responsable ja no haurà de proporcionar la contrasenya a l'usuari i, a més, així quedarà registrat qui s'ha connectat, en cas que es realitze algun acte il·lícit.

Com des d'aquest portal es realitzarà un registre d'usuaris, segons l'art. 13 del RGPD, qualsevol tractament que s'efectue amb les dades recaptades haurà d'explicar-se de manera clara i concisa als usuaris de la connexió.

El missatge ha d'incloure la informació referent a l'apartat 1 de l'article 13 del RGPD, és a dir qui és el responsable del tractament, per què i per a què es prenen les dades personals i com exercir els drets. Aquesta informació ha d'incloure:

- la identitat i dades de contacte del responsable, representant i delegat de protecció de dades (DPD);
- els destinataris del tractament;
- la finalitat del tractament de la informació recopilada i si se cedirà a tercers l'enviament d'activitats ;
- el termini de conservació de les dades;
- la possibilitat d'exercici de drets i de presentar reclamació davant l'autoritat de control competent.

A més, segons recull l'art. 33 del RGPD, en el cas que s'haja detectat una bretxa que pose en perill la informació recopilada, l'entitat responsable del registre d'usuaris haurà de notificar en menys de 72 hores als usuaris. En cas de no fer-ho dins del termini i en la forma escaient, excepte per causes degudament justificades, el responsable s'enfrontarà a la possible inspecció que determine l'autoritat competent en matèria de protecció de dades, en el cas de la Diputació de València, l'Agència Espanyola de Protecció de Dades (AEPD). Vegeu publicació anterior: *"Directrius per a la correcta la correcta gestió de les bretxes de seguretat".*

"ÉS RECOMANABLE CREAR I MANTINDRE UN REGISTRE D'ACTIVITAT DE LA XARXA PER PART DELS USUARIS QUE ES CONNECTEN A LA MATEIXA COM A SALVAGUARDA, EN EL CAS QUE ES REALITZEN ACTIVITATS IL·LÍCITES A TRAVÉS D'ELLA"

Per això, ha d'incloure's un apartat en el qual es recapte el consentiment exprés de l'usuari per a poder accedir a la xarxa com, per exemple, una casella d'acceptació al costat de la llegenda:

«Sí, he llegit i accepte la política de privacitat i les Condicions i termes d'ús».

En cap cas, aquesta casella pot vindre marcada per defecte, ja que l'acceptació dels termes i condicions per part de l'usuari ha de ser consentida.

REGISTRE D'ACTIVITAT, QUINS REQUISITS HA DE COMPLIR?

És recomanable crear i mantindre un registre d'activitat de la xarxa per part dels usuaris que es connecten a la mateixa com a salvaguarda, en el cas que es realitzen activitats il·lícites a través d'ella.

En els termes i condicions ha d'incloure's, de manera clara, la motivació per la qual s'emmagatzema aquesta informació i recaptar el consentiment explícit i ple de l'usuari. El tipus d'informació que s'emmagatzemarà en aquest registre serà, entre altres:

- les pàgines visitades;
- les sessions de connexió;
- el dispositiu utilitzat per a la connexió;
- l'idioma;
- el sistema operatiu;
- el navegador que es va utilitzar.

En el cas que l'usuari no haja donat el seu consentiment o no se li haja informat degudament d'aquest registre, no es podrà guardar aquesta informació ja que s'estaria cometent un delicte contra la intimitat de l'usuari.

Finalment, si els administradors de la connexió detectaren la comissió d'un delicte per part dels usuaris de la xarxa que atempte contra la llibertat de les persones (coaccions o amenaces), hauran de notificar a les Forces i Cossos de Seguretat de l'Estat (FCSE), ja que en cas que no es fera, s'incorreria en un delicte d'omissió del deure d'impedir delictes o de promoure la seua persecució.

MESURES DE SEGURETAT DE LA XARXA

La xarxa oferida als ciutadans i usuaris ha de comptar amb una sèrie de mesures de seguretat, entre elles:

- Mantindre actualitzat el microprogramari de l'encaminador o del punt d'accés a l'última versió disponible.
- Canviar les credencials d'accés al panell d'administració de l'encaminador o punt d'accés que venen per defecte per altres diferents. Important tindre en compte que la contrasenya ha de ser segura i robusta en cas d'existir.
- Usar com a mínim un xifratge WPA2-PSK per a la transmissió de dades entre l'encaminador i el dispositiu de l'usuari. Amb això s'evita que altres usuaris de la xarxa vegen el que transmeten.
- Canviar el nom que ve per defecte de la xarxa.
- Establir mecanismes de control parental per a evitar l'accés a llocs web perjudicials.

"EL RGPD EXIGEIX LA IDENTIFICACIÓ DE L'USUARI PER A ACCEDIR A la XARXA WIFI I QUE AQUESTA XARXA SIGA SEGURA I ESTIGA ENCRIPTADA. AIXÒ IMPEDEIX A ALTRES USUARIS DE LA MATEIXA XARXA, CAPTAR INFORMACIÓ DELS TERMINALS CONNECTATS"

I COM A USUARI D'UNA XARXA QUÈ HE DE TINDRE EN COMPTE?

Quan vages a usar una xarxa WIFI pública has de tindre en compte que en accedir tinga una política de privacitat on t'informe de com i per a què usaran les teues dades personals. I unes condicions d'ús del servei que has de llegir.

I t'ha de donar l'opció a prestar el teu consentiment perquè puguen tractar les teues dades personals.

El RGPD exigeix la identificació de l'usuari per a accedir a la xarxa WIFI i que aquesta xarxa siga segura i estiga encriptada. Això impedeix a altres usuaris de la mateixa xarxa, captar informació dels terminals connectats.

Per això, mai està de mes saber alguns consells sobre com connectar-se a una xarxa Wifi oberta;

- Desconnecta la sincronització entre dispositius quan utilitzes alguna d'aquestes xarxes.
- Mantingues els teus antivirus, firewall i, en general el teu equip actualitzat.
- Navega només per pàgines les dades de les quals estiguen xifrats mitjançant protocol https.
- Evita entrar en pàgines en les quals hages d'introduir el teu nom d'usuari, contrasenya o qualsevol altra dada que poguera delatar la teua identitat.
- Elimina qualsevol dada que haja quedat gravat en el teu ordinador o dispositiu després de la connexió: historials de cerca i navegació, cookies, etc.

MATERIAL COMPLEMENTARI

- Guia de INCIBE "Seguretat en xarxes WiFi" Consulta aquest enllaç.
- Guia "Privacitat i seguretat en internet" (AEPD). Consulta aquest enllaç.
- "Protecció de dades i Administració Local" (AEPD). Consulta aquest enllaç.
- "Guia de privacitat i seguretat en Internet" (AVPD). Consulta aquest enllaç.
- Resolució núm. 0017/2019 en relació amb a senyal rebut pels dispositius de captació i anàlisi de senyals Wi-Fi que s'instal·len en determinades botigues, a fi de conéixer els recorreguts i trànsits realitzats per terminals electrònics (AEPD). Consulta aquest enllaç.

NOTÍCIES

- **L'AEPD es pronuncia sobre la viabilitat que els particulars instal·len "espiells electrònics" amb càmera de vídeo a la porta del seu habitatge.** Entén l'Agència que la seua mera instal·lació no suposa, *a priori,* un mecanisme de control de les entrades/eixides dels veïns, ni menys encara un hipotètic "tractament de dades", ni és la finalitat per a la qual es concep. En cas de "tractament", estarà justificat quan resulte necessari per a protegir els drets i interessos del propietari, generalment el seu dret a la integritat física i a la propietat. Per tant, el criteri de l'AEPD és que si no existeix una prova objectiva que acredite un ús desproporcionat del dispositiu, el mateix és conforme a la finalitat concebuda. Consulta la Resolució en aquest enllaç.

- **Els ciberincidents de tipus *ransomware* continuen sent l'origen d'una part molt important de les bretxes de dades personals notificades a l'AEPD.** Els ciberincidents de tipus *ransomware* han tornat a ser l'origen d'una part molt important de les bretxes de dades personals notificades a l'AEPD durant el mes de juliol, segons l'últim informe de Notificacions de Bretxes de Dades Personals publicat per l'AEPD. Quasi la meitat de les notificacions indiquen haver patit un incident d'aquest tipus. Consulta l'informe en aquest enllaç.

- **Amb data 20 d'agost, el gegant asiàtic va aprovar el que va denominar la "Llei de Protecció de la Informació Personal" (LPIP). Primera vegada en aqueix país s'estableix un conjunt exhaustiu de normes sobre la recopilació i tractament de dades personals.**
  Aquesta nova regulació exigeix que les empreses obtinguen el consentiment dels usuaris abans de recopilar les seues dades, i té normes sobre com han de garantir la seua protecció quan es transfereixen fora de la RPC. Consulta la notícia en aquest enllaç.