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 28| Octubre 2022

COOKIES: CÓMO MINIMIZAR EL SEGUIMIENTO EN INTERNET

Í N D I C E

COOKIES: CÓMO MINIMIZAR EL SEGUIMIENTO EN INTERNET

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 suscribirse a nuestro Boletín informativo accede al siguiente enlace

EDITORIAL: 3ª EDICIÓN ITINERARIO DIVALDATA

Tras las dos ediciones anteriores, desde el 26 de septiembre se inicia la 3ª edición del **itinerario formativo DivalData**, de especialistas en protección de datos personales, que se llevará a cabo en el período comprendido entre septiembre de 2022 y junio de 2023.

La finalidad del recorrido formativo es capacitar al personal de las EELL que desee especializarse en materia de protección de datos personales para liderar o respaldar los procesos de cambio necesarios en el seno de sus entidades para la adecuación normativa, así como para que asuman las funciones del delegado de protección de datos y, en general, al personal que tenga responsabilidades profesionales que se vean afectadas por la nueva regulación en la materia.

El Departamento de protección de Datos y Seguridad de la Información y el Servicio de Formación de la Diputación de Valencia vienen implementando desde 2019 este itinerario formativo exclusivo en el ámbito de las AAPP, con el propósito de capacitar a los empleados públicos de las EELL de la provincia como especialistas en materia de protección de datos personales, dada la escasez de profesionales públicos en dicha materia, especialmente en las administraciones locales.

El itinerario está inspirado en el Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de protección de Datos (Esquema AEPD-DPD), pero adaptado a las singularidades y realidad de las EELL. Se divide en nueve módulos dedicados a diferentes facetas de la protección de datos, abordados a lo largo de nueve meses lectivos y combinando diferentes modalidades formativas –clases presenciales, semipresenciales, en línea, etc- , con una **duración total de 220 horas**. Para la obtención del **diploma de Especialista en Protección de Datos**, el alumnado debe superar todos y cada uno de los controles y evaluaciones de cada módulo y realizar un trabajo final que debe valorarse como Apto. Solo se admite a un reducido grupo entre 30 y 40 personas por edición entre todas las solicitudes presentadas.

El claustro docente está compuesto por un prestigioso grupo de profesionales expertos en la materia, de reconocida trayectoria a nivel nacional, provenientes tanto del sector público como del privado.

INTRODUCCIÓN: ¿QUÉ SON LAS COOKIES?

Las *cookies* son ficheros que guarda nuestro navegador al visitar páginas web, donde se almacenan pequeñas cantidades de datos: las páginas web o los anuncios que visitamos, el idioma, la zona horaria, horas y fechas de conexión, etc. De este modo, se estarían tratando datos personales relativos a nuestra navegación e interacción con las diferentes aplicaciones y contenidos desplegados en la Red.

Las finalidades de las *cookies* son variadas, entre otras, recopilar información sobre los hábitos de navegación del usuario y su actividad dentro de la web, así como almacenar datos de acceso al sitio (nombre de usuario, contraseña, personalización de la página, fecha última visita, etc.) haciendo que la navegación web sea más cómoda para el usuario. Algunas *cookies* también permiten hacer un seguimiento del usuario en sitios web, realizando un perfil anónimo orientado al uso por parte de las empresas de *marketing online.*

Existen diferentes tipos de *cookies.* Se pueden clasificar según su finalidad (técnicas, de personalización, de análisis, de publicidad comportamental), quién las genere (propias o de terceros) o el tiempo que permanecen en los dispositivos (de sesión o persistentes).

Toda esta información redunda en beneficio de las empresas ya que les permite adecuarse mejor a los intereses de los usuarios.

"LAS COOKIES SON FICHEROS QUE GUARDA NUESTRO NAVEGADOR DONDE SE ALMACENAN PEQUEÑAS CANTIDADES DE DATOS QUE SON UTILIZADOS POR LOS SERVIDORES DE LAS PÁGINAS WEBS QUE VISITAMOS. ESTA INFORMACIÓN REDUNDA EN BENEFICIO DE LAS EMPRESAS YA QUE LES PERMITE ADECUARSE MEJOR A LOS INTERESES DE LOS USUARIOS".

OBLIGACIONES: TRANSPARENCIA Y CONSENTIMIENTO

El Reglamento General de Protección de Datos (RGPD) se pronuncia respecto de las *cookies* en su Considerando 30, reconociendo su capacidad para elaborar perfiles de las personas e identificarlas. No obstante, la normativa especial que regula la utilización de *cookies* viene recogida en el artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSI). Las obligaciones legales impuestas por la normativa son dos: la obligación de transparencia y la obligación de obtención del consentimiento.

TRANSPARENCIA

Se nos debe facilitar **información clara y completa** sobre la utilización de las *cookies*. Esta información debe facilitarse con arreglo a lo dispuesto el RGPD, que requiere que el tratamiento de los datos de los usuarios se realice de forma transparente.

En la **política de cookies** deberá incluirse la siguiente información:

a) Definición y función genérica de las cookies.

b) Información sobre el tipo de cookies que se utilizan y su finalidad.

c) Identificación de quién utiliza las cookies

d) Información sobre la forma de aceptar, denegar o revocar el consentimiento

e) En su caso, información sobre las transferencias de datos a terceros países realizadas por el editor.

f) Información sobre la elaboración de perfiles automatizados.

g) Periodo de conservación.

Además, la información debe ser **concisa, inteligible y de fácil acceso.**

CONSENTIMIENTO

Para la utilización de *cookies* será **necesario obtener nuestro consentimiento.** Este puede obtenerse mediante **fórmulas expresas**, como haciendo clic en un apartado que indique "consiento", "acepto" o similares. También puede obtenerse infiriéndolo de una **acción inequívoca** realizada por el usuario. En ningún caso la mera inactividad del usuario implica la prestación del consentimiento por sí misma. Las autoridades en materia de protección de datos han concluido que la opción de **"seguir navegando" no es una forma válida de prestar el consentimiento.**

Quedarían **exceptuadas de la obtención de consentimiento las cookies técnicas necesarias** para permitir la comunicación entre el usuario y la red y las estrictamente necesarias para prestar un servicio expresamente solicitado por el usuario. En este sentido, se ha interpretado que entre ellas se encuentran las *cookies* de "entrada del usuario", de sesión, de seguridad, de sesión del reproductor multimedia, de sesión para equilibrar la carga, de personalización de interfaz y los *plug-in* para el intercambio de contenidos sociales.

"LA OPCIÓN DE "SEGUIR NAVEGANDO" NO ES UNA FORMA VÁLIDA DE PRESTAR EL CONSENTIMIENTO PARA EL USO DE COOKIES".

RIESGOS ASOCIADOS AL USO DE *COOKIES*

Uno de los mayores riesgos del uso de *cookies* es que en muchos casos **recaban tanta información que pueden llegar a invadir nuestra privacidad** al crear un perfil muy certero de quiénes somos. Sobre todo, en el caso de los usos publicitarios, las páginas webs pueden llegar a saber con precisión qué hemos estado viendo, qué nos gusta, cuándo nos conectamos o desde qué dispositivos. Así, llegan a conocer perfectamente nuestros hábitos, opiniones, creencias y otros datos personales de carácter sensible.

Además, en ocasiones, las *cookies* **son explotadas por ciberdelincuentes para llevar a cabo acciones ilícitas:**

- **Vulnerabilidades en el software del equipo o en el navegador web**: Los fallos que tiene el *software* o las vulnerabilidades de los protocolos que utiliza el navegador, pueden permitir que se puedan robar las *cookies* de sesión (credenciales).
- **Tiendas online fraudulentas**: Cuando navegamos por Internet, las *cookies* de terceros registran todas las búsquedas que realizamos, por ejemplo, de productos y servicios. El fraude se produce cuando, usando estos datos almacenados en las *cookies,* el usuario es redirigido hacia tiendas fraudulentas, mediante publicidad engañosa que le muestra precios muy bajos de artículos o servicios de los que previamente ha realizado búsquedas.
- **Noticias falsas o *fake news***: Es una variante de la anterior pero orientada a la visualización de artículos o vídeos de carácter sesgado o sensacionalista que incitan al usuario a acceder a una página web o ver un vídeo. El propietario de la página o el vídeo gana dinero gracias a la publicidad que cuelga en la misma y al volumen de tráfico que recibe.
- **Robo de *cookies* o secuestro de sesión**: Este tipo de ataque se caracteriza porque se introduce una *cookie* modificada en el navegador del usuario que previamente ha accedido a una web controlada por los ciberdelincuentes. Cuando accede a una página que requiere autenticación la *cookie* modificada se hace pasar por la cookie legítima, obteniendo las credenciales del usuario, por ejemplo, de su correo electrónico o redes sociales.

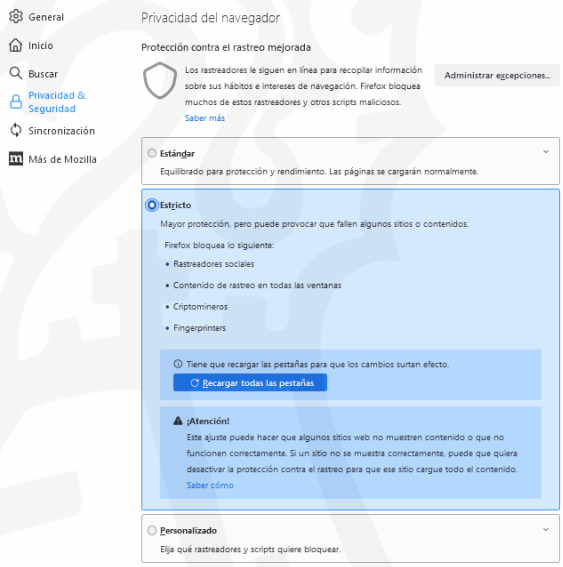
En conclusión, aunque las cookies suponen muchas ventajas tanto para el usuario como para la web, no podemos ignorar que, si no tenemos cuidado o somos conscientes de sus riesgos, **NUESTRA PRIVACIDAD O LA DE NUESTRA ORGANIZACIÓN PUEDE VERSE AFECTADA.**

"LAS COOKIES PUEDEN LLEGAR A INVADIR NUESTRA PRIVACIDAD, AL CREAR UN PERFIL MUY CERTERO DE QUIÉNES SOMOS. ADEMÁS, EN OCASIONES SON EXPLOTADAS POR CIBERDELINCUENTES PARA LLEVAR A CABO ACCIONES ILÍCITAS".

RECOMENDACIONES PARA MINIMIZAR EL SEGUIMIENTO

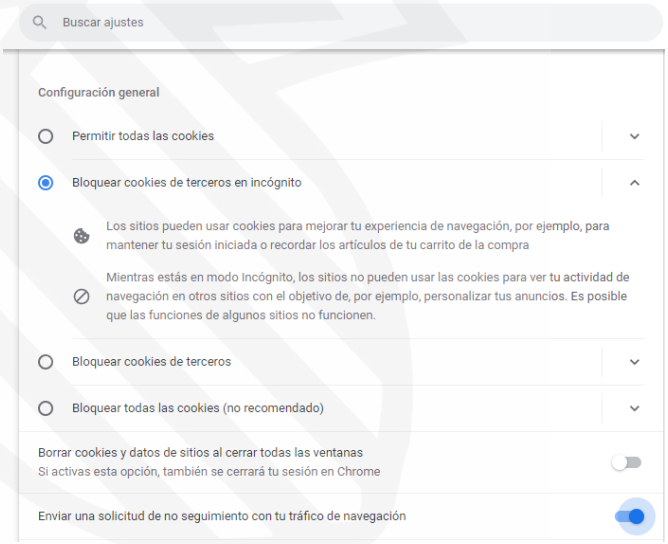
- Si el navegador que utilizas habitualmente dispone de **PROTECCIÓN AVANZADA ANTI-RASTREO/SEGUIMIENTO**, activa o mantén activada esta configuración. Estas opciones permiten varios niveles de protección. Elige el nivel más elevado y que, a la vez, se ajuste a tus preferencias.

MOZILLA FIREFOX



https://support.mozilla.org/es/kb/como-activo-la-funcion-no-rastrear

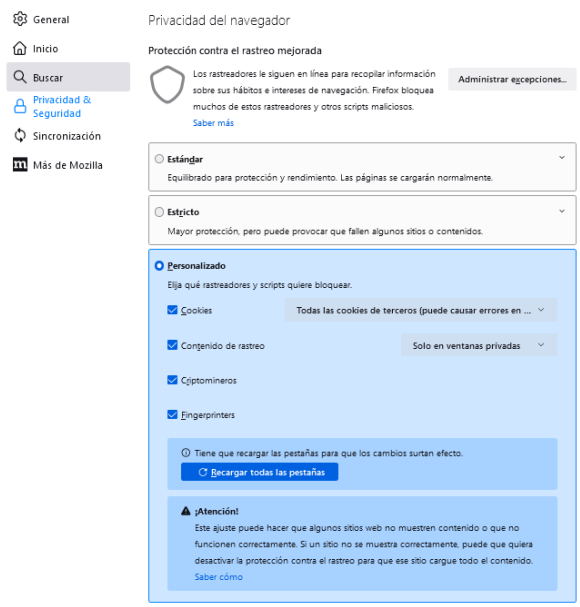
GOOGLE CHROME



https://support.google.com/chrome/answer/2790761?hl=es&co=GENIE.Platform%3DDesktop

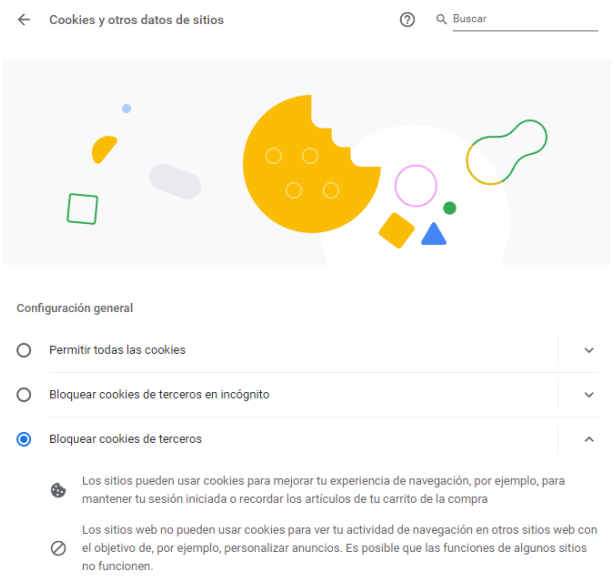
- Si así lo consideras, puedes configurar el navegador para **BLOQUEAR LAS COOKIES DE TERCEROS** o, como mínimo, para bloquearlas cuando navegues en modo privado. En navegadores con protección anti-rastreo/seguimiento, estas opciones estarán integradas en la misma configuración.

MOZILLA FIREFOX



https://support.mozilla.org/es/kb/Deshabilitar%20cookies%20de%20terceros

GOOGLE CHROME



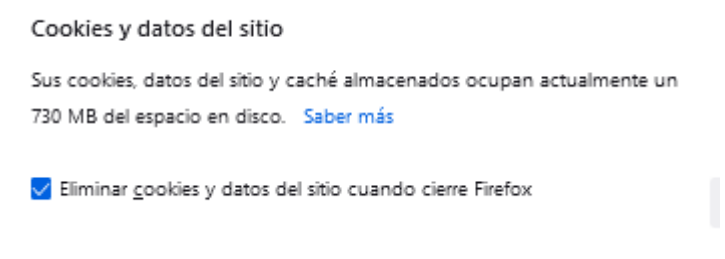
https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=es-419

- Sopesa la utilidad de tener **DOS NAVEGADORES DISTINTOS INSTALADOS**, uno con una

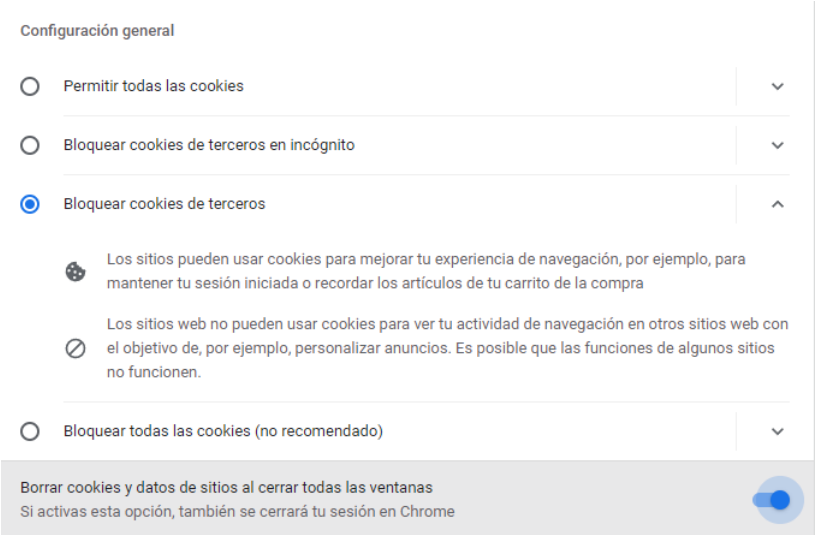
configuración más restrictiva y otro configurado con mayores permisos. De esta forma, si las configuraciones anteriores te impiden acceder a algún servicio concreto, puedes seguir accediendo a ese servicio con el otro navegador minimizando la exposición de tus datos.

- 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.

MOZILLA FIREFOX



GOOGLE CHROME



- Revisa y configura las **OPCIONES DE PERSONALIZACIÓN, PERFILES Y PUBLICIDAD** de aquellas **APLICACIONES, SERVICIOS Y REDES SOCIALES** que utilices.

COOKIES EN LA ADMINISTRACIÓN PÚBLICA

En aquellos dominios pertenecientes a una Administración Pública en los que no se preste ningún servicio que implique una actividad económica, en caso de hacer uso de *cookies*, esta no estaría sujeta a las obligaciones impuestas por la LSSI que mencionábamos antes. En todo caso, tal y como apunta la Agencia Española de Protección de Datos (AEPD), aun no estando obligadas a ello, sería recomendable que se diera cumplimiento a las previsiones de la LSSI en materia de *cookies.*

En cambio, en aquellos dominios pertenecientes a una Administración Pública en los que se presten servicios que constituyan una actividad económica (por ej. venta de libros, entradas, etc.), esta quedaría sujeta al cumplimiento de las obligaciones impuestas por la LSSI en materia de *cookies.*

"EN AQUELLOS DOMINIOS PERTENECIENTES A UNA ADMINISTRACIÓN PÚBLICA EN LOS QUE NO SE PRESTE NINGÚN SERVICIO QUE IMPLIQUE UNA ACTIVIDAD ECONÓMICA, ESTA NO ESTARÍA SUJETA A LAS OBLIGACIONES IMPUESTAS POR LA LSSI. EN TODO CASO, AUN NO ESTANDO OBLIGADAS A ELLO, SERÍA RECOMENDABLE QUE SE DIERA CUMPLIMIENTO A LAS PREVISIONES DE LA LSSI EN MATERIA DE COOKIES".

MATERIAL COMPLEMENTARIO

- Guía sobre el uso de las cookies. (AEPD). Consulta la Guía en este enlace.
- Tecnologías y Protección de Datos en las AA.PP.. Págs. 10-14. (AEPD). Consulta la Guía en este enlace.
- Privacidad y Seguridad en Internet (AEPD, INCIBE, OSI, AVPD). Consulta este enlace.
- Nota Técnica: Medidas para minimizar el seguimiento en internet (AEPD). Consulta este enlace.
- Infografía: Medidas para minimizar el seguimiento en internet (AEPD). Consulta este enlace.
- "Entre cookies y privacidad" (Blog OSI). Consulta este enlace.
- "Por qué borrar las cookies del navegador" (Blog OSI). Consulta este enlace.
- "Te explicamos la relación entre las cookies y tu privacidad mientras navegas" (Blog OSI). Consulta este enlace.
- "Qué son las cookies y cómo mostrarlas en un sitio web" (Blog INCIBE). Consulta este enlace.

NOTICIAS

- **El Gobierno aprueba el Proyecto de Ley para proteger a las personas que informen sobre corrupción.** El texto garantiza la protección efectiva de quienes comuniquen infracciones del derecho de la Unión Europea y el nacional. Consulta la Resolución en este enlace.

- **La AEPD sanciona a la Tesorería General de la Seguridad Social (TGSS) por el acceso indebido y alteración de los datos del reclamante, que había sido víctima de un hurto en el que le sustrajeron su documentación identificativa.** La parte reclamante fue víctima de un hurto en el que le sustrajeron su DNI, carnet de conducir y tarjetas de crédito. Posteriormente, el DNI sustraído fue utilizado para suplantar su identidad y generar diversos perjuicios económicos. Entre ellos, se accedió al perfil en la Seguridad Social del reclamante y se modificaron sus datos (Dirección, teléfono y e-mail) sin su consentimiento. La modificación se llevó a cabo mediante un formulario, aportándose junto al mismo la copia del DNI. El suplantador también se descargó su vida laboral. Con los datos obtenidos del citado documento y con el DNI sustraído se solicitó y se entregó al delincuente una tarjeta de crédito de una entidad bancaria, siendo esta utilizada para generarle diversas deudas. Asimismo, el suplantador abrió varias cuentas falsas a nombre de la reclamante en tres entidades bancarias. La AEPD considera que la mala gestión de la TGSS provocó el acceso indebido a los datos que tantos perjuicios le han ocasionado al reclamante. Consulta la Resolución en este enlace.

- **La AEPD resuelve el recurso de reposición interpuesto por el Ayuntamiento de Ourense contra la resolución que imponía sanción por la toma de fotografías del DNI de una persona con dispositivos personales de las Fuerzas y Cuerpos de Seguridad.** La AEPD concluye que el uso de cámaras o móviles personales de los agentes no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía judicial deben adoptarse. Además, señala la autoridad que dicho dispositivo queda fuera del control del responsable del tratamiento. Consulta la Resolución en este enlace.