RECOMENDACIONES EN MATERIA DE PROTECCIÓN DE DATOS EN LOS PROCESOS SELECTIVOS DE EMPLEO PÚBLICO DE LA UNIVERSIDAD DE GRANADA

En virtud de su autonomía y en ejercicio de sus competencias, la Universidad de Granada está facultada para seleccionar a su personal de administración y servicios (en adelante PAS) y docente e investigador (en adelante PDI), a través de los procesos selectivos para acceso, promoción y provisión de empleo público que procedan, con respeto a lo dispuesto por la legislación vigente y a los principios de publicidad, transparencia, igualdad, mérito y capacidad.

El desarrollo de los correspondientes procesos selectivos y, en su caso, de los recursos que se formulen frente a ellos, requiere el tratamiento de datos personales de las personas que concurran a ellos; y, en ocasiones, el tratamiento de datos especialmente sensibles, como la discapacidad u otras circunstancias personales de los aspirantes.

La Universidad de Granada, como responsable del tratamiento de esos datos personales, deberá hacerlo de forma que concilie los principios de publicidad y transparencia, que deben regir todo proceso selectivo de empleo público (art. 55.2 del Estatuto Básico del Empleado Público, en adelante EBEP; y, por todas, STS 2487/2016, de 22 de noviembre); **con la salvaguarda del derecho fundamental a la protección de datos personales de los interesados. Y, en especial, con cumplimiento del mandato legal contenido en el art. 25 del Reglamento General de Protección de Datos (RGPD) de procurar "que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".**

Con esa finalidad, al amparo de la **normativa vigente en materia de protección de datos personales**; la **Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas**; la **Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía**; el **Informe 0002/2022, del Gabinete Jurídico de la Agencia Española de Protección de Datos (en adelante AEPD)**; y, en cumplimiento de las funciones que el artículo 39 del **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en lo sucesivo), encomienda a los Delegados de Protección de Datos, de supervisar el cumplimiento de la normativa de protección de datos y asesorar al responsable del tratamiento y sus empleados sobre las obligaciones que les incumben en la materia; se emiten las siguientes

RECOMENDACIONES

I. Recomendación general: minimización y protección de datos por defecto

De conformidad con lo dispuesto por el RGPD y la Ley Orgánica 3/2018, de Protección de Datos y garantía de los derechos digitales (en adelante LOPDGDD), la Agencia Española de Protección de Datos (AEPD) ha establecido, en resoluciones correspondientes a diversos procedimientos sancionadores y en su informe 0002/2022, relativo a la protección de datos personales en procesos selectivos, que "el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. *Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas*".

Buenas prácticas:

- **La información relativa a los procesos selectivos que se ponga a disposición del público en general, en particular a través de internet, deberá limitarse a la convocatoria y sus bases, y a los distintos actos o fases por los que transcurra su desarrollo,** sin indicación de los datos de carácter personal de los aspirantes. Esa información es suficiente para cumplir con los principios de publicidad y transparencia, y permitir el control de su adecuación a las normas que rigen los procesos selectivos de empleo público (arts. 55 y 78 EBEP y art. 23.2 Constitución).
- **Se deberán adoptar por defecto los medios técnicos necesarios para limitar, solo a las personas que concurran al correspondiente proceso selectivo, el acceso a los listados de admitidos/excluidos y de resultados, o a los recursos** (p. ej., asignándoles un usuario y un código en el momento de registrarse telemáticamente en el proceso; o habilitando al efecto su DNI electrónico o certificado digital). Y ello, de conformidad con las recomendaciones específicas que se recogen a continuación.
- **En las bases de la convocatoria se deberá contener la información básica sobre el tratamiento de los datos personales de los aspirantes**, en los términos

previstos en el artículo 13 RGPD. Un ejemplo de cláusula informativa básica, sería el siguiente:

"Los datos personales recogidos en la solicitud de admisión y en el proceso serán tratados con la única finalidad de la gestión de las pruebas selectivas y las comunicaciones necesarias para ello. El nombre, apellidos y número del documento de identidad se publicará en la forma que determina la disposición adicional séptima de la Ley Orgánica 3/2018, de 5 de diciembre, Protección de Datos Personales y garantía de los derechos digitales. La Universidad de Granada tomará medidas para que esa información no sea indexada por los buscadores de internet. La base legal para el tratamiento de estos datos son las Leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, y el texto refundido de la Ley del Estatuto Básico del Empleado Público. La Universidad de Granada es responsable del tratamiento de esos datos y publica su política de protección de datos en https://secretariageneral.ugr.es/pages/proteccion_datos. Los derechos de protección de datos de los solicitantes se podrán ejercer dirigiéndose al responsable del tratamiento por vía electrónica, a través de la sede electrónica de la Universidad de Granada. Los interesados pueden ejercer sus derechos también ante el Consejo de Transparencia y Protección de Datos de Andalucía.
Pueden consultar información adicional sobre el tratamiento de datos personales en procesos selectivos de personal en el siguiente enlace: https://secretariageneral.ugr.es/pages/proteccion_datos/leyendas-informativas/_img/informacionadicionalprocesosselectivos/%21*".*

II. Recomendaciones específicas

A partir de la recomendación general, a continuación, se hacen otras más específicas y concretas, considerados los riesgos que entraña la difusión de información personal a través de internet.

1. Méritos curriculares de los miembros de las comisiones juzgadoras

Cuando la convocatoria contemple la difusión de los méritos o el "curriculum vitae" de las personas que integren las comisiones juzgadoras, se deberán omitir los datos personales sensibles o excesivos (tales como DNI, fecha de nacimiento, datos de contacto privados y no profesionales, o cualesquiera otros que excedan del ámbito curricular).

En todo caso, esa información solo deberá publicarse durante el plazo para formular posibles recursos frente a la composición de la comisión juzgadora. Ello, sin perjuicio de su conservación

en el expediente administrativo correspondiente, hasta que transcurran los plazos para impugnar los actos de trámite y resolución del proceso.

Buenas prácticas:

- **Al recabar los datos curriculares** de los miembros de las comisiones, se les deberá **informar** de la finalidad del tratamiento, de la conveniencia de no facilitar datos personales excesivos e innecesarios, y de la forma en que pueden, en su caso, ejercer sus derechos de protección de datos ante la Universidad de Granada.
- **Al publicar la información curricular** de los miembros de comisiones juzgadoras, se deberá revisar que no contengan datos personales sensibles y **adoptar por defecto medidas técnicas para evitar el indexado de la información por búsquedas basadas en sus nombres** (p. ej., a través de instrucciones o etiquetas noindex, o similares).
- La **difusión pública** de esta información deberá **limitarse en el tiempo**, al transcurso del plazo de impugnación de la composición de la comisión juzgadora; sin perjuicio de su conservación, a disposición de los candidatos en el expediente correspondiente, hasta que transcurran los plazos de impugnación de los actos de trámite y resolución del proceso.

2. Listados de admitidos o excluidos y listados de calificaciones provisionales y definitivas

En los procesos selectivos para el acceso, promoción y provisión de empleo público, en cualquiera de sus modalidades, la salvaguarda de los principios de igualdad y concurrencia competitiva por mérito y capacidad, hace que la protección de datos se vea limitada por los principios de publicidad y transparencia.

No obstante, **para que esa limitación de la protección de datos sea conforme a derecho, debe ser proporcionada, y no excesiva**. Para ello, el tratamiento de datos personales que se lleve a cabo en el desarrollo del proceso selectivo deberá estar regido por el **principio de minimización**.

Este principio se aplicará a la **cantidad de datos personales** recogidos, a la **extensión de su tratamiento**, a su plazo de **conservación** y a su **accesibilidad**.

Concretamente, por lo que se refiere a su accesibilidad, la AEPD ha declarado que "*sería menos intrusivo y más acorde con lo previsto con la normativa de protección de datos que su publicación afectara y pudiera ser visualizada solo por los que concurren, no al público en general*" (entre otras, vid. la Resolución R/2593/2017 de 29 de septiembre de 2017, recaída en el procedimiento

de declaración de Infracción AP 2:2017, por publicación en abierto a través de internet de las listas de admitidos y excluidos y de los listados con las calificaciones provisionales, y la posibilidad de descargarlos en el correspondiente documento pdf).

La AEPD destaca, a estos efectos, que el resto del público "*carece de una base legítima para el acceso a los datos de apellidos y nombre junto al NIF de cada aspirante o a las causas de exclusión*".

Buenas prácticas:

- Se deberá evitar que los listados de admitidos o excluidos y los listados de calificaciones o resultados sean accesibles, sin consentimiento del interesado, a un número indeterminado de personas.
- **Se recomienda que su publicación se restrinja a las personas que concurran en el correspondiente proceso** (si los listados se publican de forma digital, deberá habilitarse el acceso solo a los aspirantes, bien mediante el uso de DNI electrónico o certificado digital, bien asignándoles un usuario y una contraseña al registrarse telemáticamente en el proceso; o de otro modo similar).
- **Los listados deberán contener sólo los datos personales que sean estrictamente necesarios.** En ningún caso deberá publicarse conjuntamente el nombre de los candidatos y el número completo de su DNI, pasaporte o documento equivalente. Conforme a la Disposición Adicional Séptima de la LOPGDD, cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su **nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias** del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. El grupo de cifras seleccionado será el mismo en todas las publicaciones, a fin de no posibilitar la recomposición íntegra de la numeración de dichos documentos.
- Si se publicaran listados en abierto en internet, deberán adoptarse por defecto medidas técnicas para **evitar el indexado de la información contenida en ellos, a partir del nombre de los interesados** (p. ej., a través de instrucciones o etiquetas noindex, o similares).
- El **tiempo de publicidad de los listados deberá ser adecuado a su finalidad,** debiéndose eliminar del sitio web o físico donde se hayan publicado en cuanto venzan los plazos de impugnación correspondientes.

3. Cupos especiales

Los datos personales que revelen una situación de especial vulnerabilidad de los aspirantes, como es el caso de la discapacidad o el de ser víctima de violencia de género, o cualquier otro dato calificado legalmente como sensible (artículo 9 RGPD), requieren una **especial tutela, para evitar que su tratamiento pueda generar situaciones de discriminación o cualquier perjuicio significativo para las personas afectadas.**

Así resulta de lo dispuesto por los artículos 24 y 25 del RGPD; del artículo 28 de la LOPDGDD; y de los artículos 13 y 40.5 de la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas.

No obstante, en ocasiones **puede haber un interés legítimo en conocer los resultados de los candidatos del turno libre y los del cupo de reserva para personas en situaciones especiales.** Por ejemplo, así ocurrirá en aquellos supuestos en los que las bases del proceso selectivo prevean que si una persona que se haya presentado por el cupo de reserva para personas con discapacidad superase los ejercicios correspondientes, no obtuviera plaza en este cupo, pero su puntuación fuese superior a la obtenida por aspirantes del sistema de acceso general, pueda ser incluida por su orden de puntuación en el sistema de acceso general; o si previeran que, en caso de quedar desiertas plazas del cupo de acceso general se sumarán a las de acceso especial, o a la inversa. Es evidente que, en estos supuestos, existirá un legítimo interés en que los participantes de ambos turnos puedan conocer las listas de admitidos y excluidos indistintamente.

En tales casos, **deberán minimizarse los datos accesibles al resto de participantes**, a fin de conciliar la publicidad con la debida protección de la intimidad de los aspirantes en los que concurra una circunstancia especial; mediante medidas de **pseudoanonimización**. Todo ello, sin perjuicio, de que los aspirantes puedan conocer la identidad completa de otros participantes, cuando ello sea preciso en el caso concreto, para ejercer los derechos que el ordenamiento jurídico les concede (v. gr., STS núm. 400/2020, de 13 de mayo).

Buenas prácticas:

- Además de restringir el acceso a los listados de aspirantes por cada cupo a quienes concurran al proceso selectivo, **se recomienda pseudoanonimizar los datos personales de los candidatos que concurran por cupos especiales** (discapacidad, víctima de violencia de género); no publicando en un mismo listado los nombres de los aspirantes y el cupo por el que concurren;

sustituyendo el nombre de los aspirantes por un código asignado al registrarse en el proceso selectivo, en los listados donde aparezcan clasificados por cupos.

- En la publicación del nombramiento como empleado público tampoco deberá identificarse el cupo o turno por el que se haya concurrido (art. 62 del EBEP).

4. Recursos frente a las resoluciones provisionales o definitivas

Los recursos que, en su caso, se formulen en vía administrativa frente a las resoluciones (provisionales o definitivas) de procesos selectivos de PAS o PDI convocados por la Universidad de Granada contendrán datos personales del recurrente y, en ocasiones, de terceros. Por ello, **su contenido no deberá ponerse a disposición del público en general, ni de forma ilimitada en el tiempo**.

Su contenido **sólo deberá ponerse a disposición de las personas que tengan un interés legítimo en el procedimiento, y sólo durante el tiempo necesario para que puedan ejercitar las acciones y derechos que le asistan**. Se presumirá que tienen interés legítimo el resto de aspirantes de un mismo proceso selectivo, salvo que por el contenido del recurso sea manifiesto que su resultado no puede afectar a terceros; y, en general, quienes puedan resultar afectados por el resultado del recurso.

La difusión del contenido del recurso al público en general, o por más tiempo del preciso para la salvaguarda del legítimo derecho de defensa de terceros interesados, no es acorde con los principios de minimización y limitación de la finalidad, la protección desde el diseño y por defecto, y la responsabilidad pro activa en materia de protección de datos que, conforme a la normativa vigente, corresponde a la Universidad de Granada.

Buenas prácticas:

- Para conciliar la legítima tutela de los terceros interesados con la debida salvaguarda de los datos personales, **el contenido de los recursos sólo estará a disposición de terceros interesados, durante el tiempo necesario para que puedan intervenir en el procedimiento o formular alegaciones.**
- Para ello, se recomienda **anunciar públicamente la existencia del recurso** (p. ej., en la web del servicio de PAS o PDI, según corresponda), identificando el acto recurrido; así como el plazo, lugar y modo en el que podrán acceder a su contenido las personas que acrediten un interés legítimo en el mismo. Asimismo, se recomienda **informar a los terceros interesados**, de forma previa y expresa, de la obligación de no utilizar ni reproducir el contenido de los recursos, para fines distintos al de ejercer su derecho de tutela en el procedimiento de que se trate.

- **El acceso al contenido de los recursos**, por quienes acrediten un interés legítimo se hará en el lugar físico indicado en el anuncio (p. ej. exhibiéndoselo en las dependencias del servicio de PAS o PDI), o bien facilitándoles el acceso de forma telemática (p. ej. habilitando para quienes hayan concurrido al mismo procedimiento un acceso identificado -mediante un código, su DNI electrónico o su certificado digital- o una clave para descifrar el archivo que contenga la documentación del recurso).
- En caso de que se haya optado por habilitar el acceso al contenido de los recursos de forma telemática, para cumplir con la debida **limitación en el tiempo**, se deberá establecer una caducidad de las claves o forma de acceso coincidente con el plazo indicado en el anuncio del recurso.

Por último, y a fin de facilitar la implementación de estas recomendaciones, **se acompaña un Anexo de "Medidas para controlar la exposición pública de datos personales".**

Y para que así conste a los efectos oportunos, y quedando a su disposición para cualquier otra aclaración, lo firmo en Granada a 31 de mayo de 2022.

María del Carmen García Garnica
Delegada de Protección de Datos
Universidad de Granada

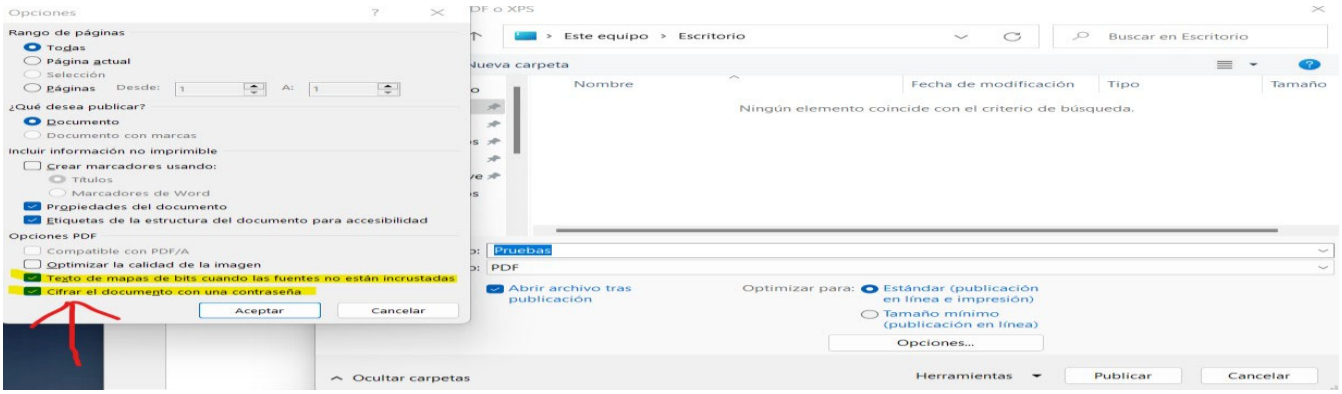
ANEXO

MEDIDAS PARA CONTROLAR LA EXPOSICIÓN PÚBLICA DE DATOS PERSONALES

Para cumplir con el mandato legal contenido en el art. 25 del Reglamento General de Protección de Datos de "Protección de datos desde el diseño y por defecto", y en particular, con lo contemplado en su apartado 2 (*"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.* ***Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas"***), a continuación, **se detallan una serie de medidas** dirigidas a bloquear el acceso por parte de personas no autorizadas a documentos que contengan datos de carácter personal y evitar la exposición indebida de datos personales.

PONER UNA CLAVE A UN PDF

En Word, en el menú **"Archivo"** pulse **"Exportar documento"**. Seleccione **"Documento PDF"**. Aparecerá una ventana similar a la de la imagen. Pulse sobre **"Opciones"** y marque las casillas que indica la flecha roja ("texto de mapa de bits cuando las fuentes no están incrustadas" y "cifrar documento con una contraseña"). Al darle a aceptar le pedirá la clave con la que desee guardarlo.



Al marcar estas dos casillas **está generando un fichero que no está en modo texto**, sino gráfico, **por lo que, a los indexadores**, tipo Google**, les cuesta ver el contenido**. Además, como el documento está cifrado con una contraseña, los indexadores no podrán verlo y las personas que no conozcan la clave no podrán acceder a su contenido.

LibreOffice tiene un método similar y puede utilizar también la aplicación de Acrobat.

Evite subir el pdf a aplicaciones de conversión en línea (ej. ILovePDF), ya que está subiendo información sensible y queda copia en una web externa. En su lugar, utilice una aplicación descargada previamente en el ordenador.

Recuerde: Cuando vaya a publicar un documento PDF que contenga datos personales en la Web **súbalo como imagen** y nunca como documento de texto así **dificultará la indexación.**

ENVIAR INFORMACIÓN CIFRADA POR EMAIL

Si lo que desea es enviar datos personales por email, proceda previamente a cifrar esa información.

Los pasos están en este mini tutorial del blog de seguridad informática: Como enviar información cifrada por email. (ugr.es) http://sl.ugr.es/0cDx

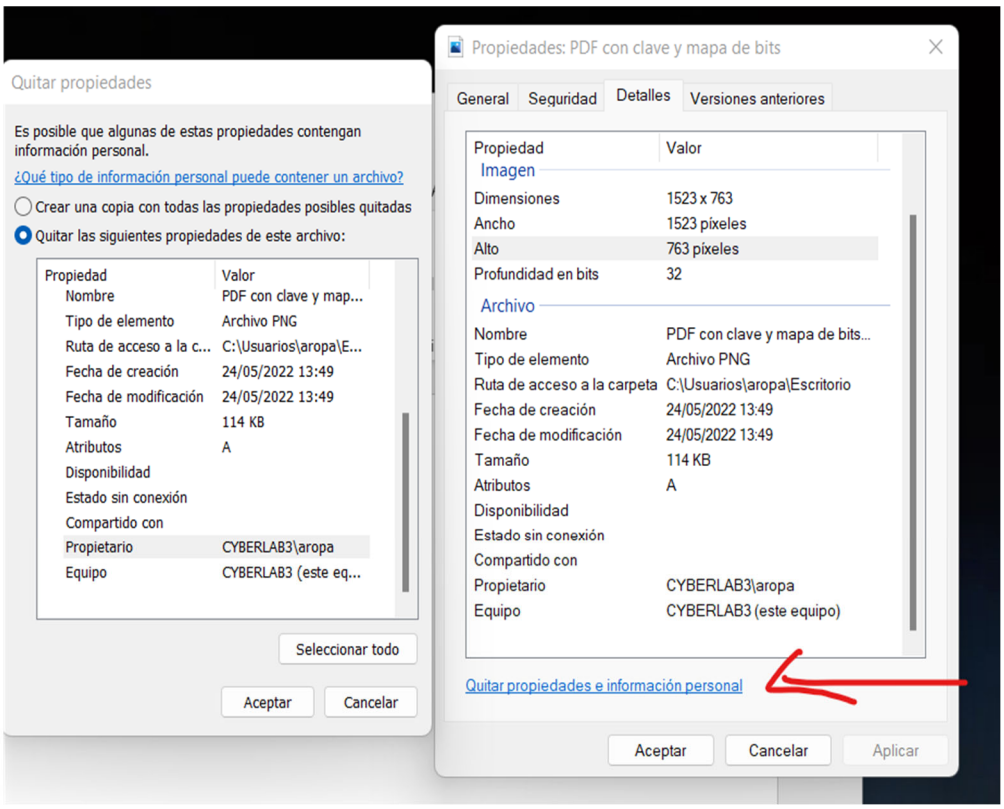
Recuerde: Estos sistemas no son seguros 100%, pero reducen significativamente la exposición.

QUITAR METADATOS

Los metadatos son información adicional, en ocasiones de carácter personal, que a menudo se envía o publica inconscientemente, aumentando la exposición de datos personales frente a terceros.

Para más información, puede ver este post del blog de seguridad informática Limpieza de metadatos en los documentos de la Universidad de Granada (ugr.es) http://sl.ugr.es/0cDy

Puede utilizar la herramienta http://lime.ugr.es desde dentro de UGR o en Windows puede quitar los metadatos desde el **menú "Propiedades del fichero".** En la pestaña **"Detalles"** pinche en **"Quitar propiedades"**. Esto le llevará a otra ventana donde podrá quitarlas ("quitar las siguientes propiedades de este archivo" y "quitar propiedades e información personal").



EVITAR QUE LOS BUSCADORES INDEXEN LA INFORMACIÓN

Para evitar la indexación de la información, en particular cuando ésta se vincula con nombres de personas físicas determinadas, tiene **dos opciones**:

a) **Introducir el parámetro noindex** en su página html en la parte de las cabeceras donde están las meta etiquetas del html, que es lo que miran los buscadores para clasificar las páginas y donde se ponen normalmente qué palabras clave tiene la página. La sintaxis es:

```
<meta name="robots" content="noindex">
```

Debe ponerse al principio de la página web.

b) Otra opción es crear dentro del directorio raíz del servidor web, un fichero llamado robots.txt, e incluir en él las páginas que desea que no se indexen.

Aquí tiene un ejemplo del contenido de un fichero robots.txt:

```
User-agent: Googlebot
Disallow: /nogooglebot/

User-agent: *
Allow: /

Sitemap: http://www.example.com/sitemap.xml
```

Esto es lo que hace el archivo robots.txt:

1. El user-agent Googlebot no puede rastrear ninguna URL que comience por http://example.com/nogooglebot/.
2. El resto de los user-agents pueden rastrear todo el sitio. Se podría haber omitido esta regla y el resultado habría sido el mismo, ya que los user-agents pueden rastrear todo el sitio de forma predeterminada.
3. El archivo de sitemap del sitio está en http://www.example.com/sitemap.xml.

Por último, si quiere poner algo a nivel más técnico puede hacer que **a determinados directorios de su servidor web solo puedan acceder las personas que tengan una clave determinada** que se le facilite al efecto. Si es un servidor Apache puede configurar un fichero **.htaccess** dentro del directorio que desea (puede consultar más información en la página web de Apache https://httpd.apache.org/docs/2.4/es/howto/htaccess.html o http://sl.ugr.es/0cDB).

Recuerde: Estas normas no dan seguridad al 100% de que Google no nos rastree, **pero, si no lo ponemos, seguro que sí nos indexará** antes o después.