Ojo al Dato

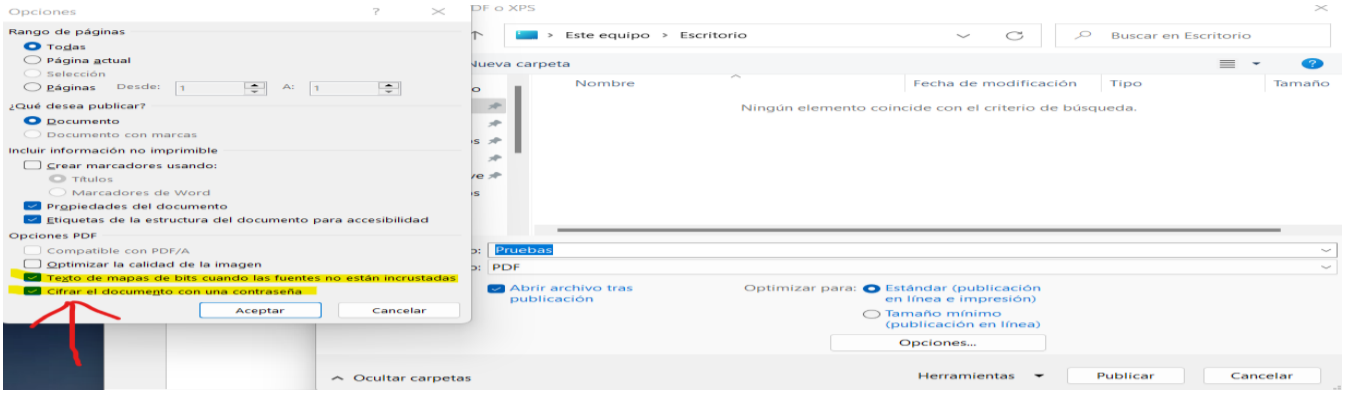
Campaña de concienciación sobre Protección de Datos Personales

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

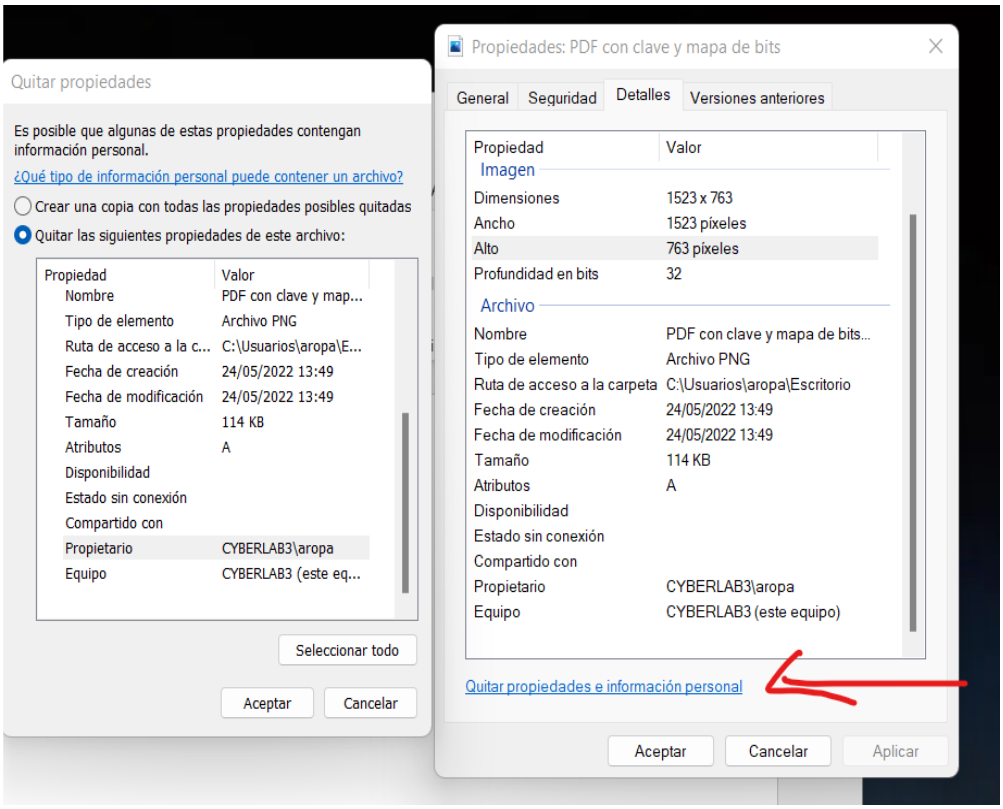
Recuerde: Estos sistemas no son seguros 100%, pero reducen significativamente la exposición.

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.