# La información

## 1. Confidencialidad de la Información

**¿Qué es la confidencialidad?** Una norma de seguridad reconocida internacionalmente define la confidencialidad como la propiedad de la información *"por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados*". Es decir, la información confidencial es aquella que debemos proteger del acceso de personas no autorizadas.

Pero, **¿qué consideramos información confidencial?** Pues es toda aquella que tenemos que proteger del acceso de otras personas. No importa el soporte, el tipo de información o incluso si se comunica verbalmente. En el otro extremo tenemos la información de uso público, como por ejemplo cualquier material publicitario que utilicemos con nuestros usuarios.

**¿Por qué decimos que una información es confidencial?**

1. Porque es **información crítica** para nuestro trabajo.
2. Porque es **información "sensible"** y puede haber otras organizaciones interesadas.
3. Porque está **protegida por la legislación**, como por ejemplo los datos personales.
4. Porque nos hemos comprometido **con un tercero** a mantener la información en secreto: un usuario, un socio, un proveedor, etc.

**¿Qué debemos hacer al gestionar información confidencial?**

- Firmar un acuerdo de confidencialidad con cualquier persona u organización a la que le demos acceso a la información.
- Evitar que personas no autorizadas tengan acceso a la información confidencial que utilizamos, no dejándola a la vista ni en directorios o sistemas en los que pueda ser accedida por otras personas.
- Aplicar medidas de cifrado cuando la información sea especialmente sensible.

# 2. Los datos personales

Según la legislación española en protección de datos, un dato de carácter personal es "*cualquier información concerniente a personas físicas identificadas o identificables*".

Es decir, un DNI es un dato de carácter personal, una fotografía es un dato de carácter personal, y la estatura de alguien es un dato de carácter personal si podemos de alguna forma saber a quién pertenece.

Hemos de tener en cuenta que legislación de protección de datos es de obligado cumplimiento para cualquier organización española, y cumplir con ella es tan sencillo como llevar a cabo unos sencillos trámites administrativos y poner en marcha algunas medidas de seguridad básicas.

En nuestro caso, debemos evitar el acceso de personas no autorizadas a los datos personales que tengamos en nuestra organización, gestionarlos siempre de la manera adecuada e informarnos cuando tengamos alguna duda.

Aunque en Internet existen numerosos recursos, para cualquier duda podemos recurrir a la Agencia Española de Protección de Datos, cuya dirección web es http://www.aepd.es.

# 3. Cifrado de la información

A la hora de proteger la información en formato electrónico, una de las medidas más eficaces es el cifrado de la información. Mediante esta técnica podemos codificar cualquier fichero y hacerlo inaccesible a otras personas que no sepan la clave de descifrado.

**¿Qué información debemos cifrar?**

- Toda aquella que sea de vital importancia en nuestro trabajo y sobre todo, si su difusión podría ser un problema.
- Si trabajamos con datos personales de nivel alto como datos de salud, la legislación requiere que los almacenemos cifrados en ciertas circunstancias.
- También es recomendable cifrar un fichero si lo vamos a enviar a usuarios y/o proveedores. Así, aunque alguien “capture” el fichero, no podrá acceder a su contenido.

Aunque existen múltiples herramientas para el cifrado de información, muchas aplicaciones de compresión de ficheros y ofimática disponen de la posibilidad de comprimir con contraseña, lo puede ser suficiente en la mayoría de los casos.

# 4. Copias de seguridad

Las copias de seguridad son uno de los principales elementos para evitar la pérdida de información cuando tenemos un problema.

Aunque en general este tipo de sistemas los gestiona el personal de informática, hay varios aspectos que hay que tener en cuenta:

- **Información**: Debemos asegurarnos de que se está realizando copia de seguridad de toda la información que utilizamos en nuestro trabajo. Por ejemplo, de la información que guardamos en “Mis documentos”.
  Es necesario que almacenemos la información en los sistemas y directorios de los que sabemos que se hace copia. Si tenemos dudas, podemos hablar con el personal de informática.
- **Soportes externos**: Si para trabajar utilizamos soportes como discos duros externos, debemos asegurarnos de que se hace copia de la información que almacenan.
  Si las copias las hacemos en soportes como CDs, DVDs o incluso lápices USBs, debemos siempre almacenarlos en lugares protegidos.
- **Frecuencia**: Si hacemos copias periódicas de nuestra información, debemos definir una periodicidad adecuada para que un problema con nuestro equipo no suponga la pérdida de las últimas semanas o meses de trabajo.
- **Salida de copias**: Si tenemos que trasladar las copias fuera de la organización (por ejemplo, hasta otra oficina o nuestro domicilio), debemos cifrarlas, para evitar que si las perdemos alguien pueda acceder a su contenido.

# 5. Clasificación de la información

Cualquiera de nosotros gestiona información de distinta índole durante su trabajo diario: planes estratégicos, datos económicos y financieros, expedientes de alumnos, datos de salud, exámenes, etc.

Es normal que no toda la información con la que trabajamos tenga la misma importancia. En algunos casos será información pública, en otros casos será para uso interno y en otros será muy crítica.

Por tanto, es normal que todos estos tipos de información necesiten medidas de seguridad diferentes. Por ejemplo, la información pública apenas tendrá restricciones de acceso, mientras que el acceso a la información confidencial estará muy restringido.

En el caso de que nuestra organización tenga definidos los diferentes tipos de información según su importancia, debemos aplicar las medidas que nos haya indicado. Entre otras, tenemos que tener en cuenta lo siguiente:

- **Marca los documentos** que utilices con el nivel de seguridad que te hayan dicho en cada caso.
- **Aplica cifrado** a los tipos de información más sensible.
- Ten en cuenta qué tipo de información puede almacenarse en **soportes extraíbles** o distribuirse por correo electrónico. Si necesitas hacerlo, que sea siempre utilizando cifrado.
- **No imprimas** aquella información cuya impresión no está permitida.
- **No intentes acceder** a información a la que no tienes acceso.

# 6. Metadatos

Un “metadato” es aquella información que incluyen los ficheros digitales pero que no forma parte del contenido. Algunos ejemplos son la fecha de creación, la fecha de modificación o el autor del fichero.

Tenemos que tener en cuenta que cada tipo de fichero tiene sus propios metadatos. Por ejemplo, mientras que un fichero ofimático puede contener el autor del documento, una imagen puede incluir además sus dimensiones y una fotografía información de dónde se tomó la foto o incluso el modelo de cámara utilizado.

Aunque pueden ser muy útiles, en algunos casos esta información puede proporcionar información valiosa sobre nosotros: nombres de usuario, fechas de los documentos, ubicación de las fotografías, aplicación utilizada, etc.

Por ello, debemos eliminar cualquier metadato antes de enviar el fichero a otra persona o organización. Para ello, algunos programas de ofimática incorporan funcionalidades para eliminar esta información y también es posible borrar algunos metadatos mediante la opción de botón derecho -> Propiedades -> Detalles.