

## PLAN DE SENSIBILIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS

### IDEAS CLAVE

Material expresamente diseñado para ser impreso y distribuido al alumnado del Plan de Sensibilización con los objetivos de facilitar el seguimiento de las sesiones y servir de guía de consulta.

### TABLA DE CONTENIDOS

<i><u>PRÓLOGO</u></i> .....	<i><u>2</u></i>
<i><u>INTRODUCCIÓN</u></i> .....	<i><u>2</u></i>
<i><u>La Ley</u></i> .....	<i><u>2</u></i>
<i><u>El Plan de Sensibilización – Objetivo</u></i> .....	<i><u>2</u></i>
<i><u>El Plan de Sensibilización – Coordinación</u></i> .....	<i><u>2</u></i>
<i><u>Contenidos implícitos de la sesión</u></i> .....	<i><u>3</u></i>
<i><u>TERMINOLOGÍA</u></i> .....	<i><u>3</u></i>
<i><u>ACTORES</u></i> .....	<i><u>3</u></i>
<i><u>CASOS PRÁCTICOS</u></i> .....	<i><u>4</u></i>
<i><u>1.Publicación de Fotografías</u></i> .....	<i><u>4</u></i>
<i><u>2.Acceso a los Sistemas de Información</u></i> .....	<i><u>4</u></i>
<i><u>3.Publicación de un estudio epidemiológico</u></i> .....	<i><u>4</u></i>
<i><u>4.Destrucción de documentos antiguos</u></i> .....	<i><u>4</u></i>
<i><u>5.Llevarse trabajo a casa</u></i> .....	<i><u>4</u></i>
<i><u>6.Envío de datos personales por correo electrónico</u></i> .....	<i><u>5</u></i>
<i><u>7.Descargar música y software en el trabajo</u></i> .....	<i><u>5</u></i>
<i><u>8.Ejercicio del derecho de rectificación de datos</u></i> .....	<i><u>5</u></i>
<i><u>CONSECUENCIAS</u></i> .....	<i><u>5</u></i>
<i><u>FUENTES DE INFORMACIÓN ADICIONALES</u></i> .....	<i><u>5</u></i>

## PRÓLOGO

El presente documento pretende ser un conjunto reducido de criterios a tener en cuenta por los profesionales del SAS en relación con el cumplimiento de la LOPD en el ejercicio de su actividad profesional.

Dichos criterios están elaborados a partir del material docente empleado en las sesiones de sensibilización en materia de protección de datos, por lo que también es útil como guía para el seguimiento de dichas sesiones.

## INTRODUCCIÓN

### *La Ley*

La Ley Orgánica de Protección de Datos 15/99 y el Reglamento de medidas de seguridad 1720/07, obligan a los responsables de los ficheros del Servicio Andaluz de Salud (Dirección-Gerencia, Secretaría General, Dirección General de Asistencia Sanitaria, Dirección General de Personal y Desarrollo Profesional y Dirección General de Gestión Económica) a adoptar las medidas necesarias para que el personal que use los sistemas de información conozca las normas que afecten al desarrollo de sus funciones. (Artículos 88.1 y 89.2 - RD 1720/2007).

### *El Plan de Sensibilización – Objetivo*

Los contenidos del PLAN, distribuidos por perfiles profesionales, se centran en el cumplimiento de la Ley Orgánica de Protección de Datos, la aplicación del Reglamento de Medidas de Seguridad, la Ley de Autonomía del Paciente, el conocimiento del manual del Empleado Público de la Junta de Andalucía en el uso de los sistemas informáticos y redes de comunicaciones, así como la difusión de las instrucciones internas de la organización relacionadas con estas materias.

El objetivo principal es la sensibilización del 100% de la plantilla del SAS en 4 años, por lo que se pretende cubrir el 25% en 2008. Para ello se procederá a recabar la firma del alumnado como justificante de asistencia.

Esta presentación cubre los siguientes módulos de formación:

- Sensibilización del personal sanitario (LOPD), 08/1467/0929/GE/P/AI
- Sensibilización del personal no sanitario (LOPD), 08/1468/0929/GE/P/AI

### *El Plan de Sensibilización – Coordinación*

La coordinación y ejecución del PLAN se realiza desde la Subdirección de Tecnologías de la Información de la Secretaría General del SAS, a través de la Unidad de Gestión de Riesgos Digitales.

Esta Unidad lleva a cabo las siguientes actuaciones en materia de protección de datos:

- Plan de Auditorías
- Plan de Sensibilización de Centros
- Coordinación de los ejercicios de derechos de la LOPD
- Adecuación a la LOPD de los proyectos de Tecnologías de la Información
- Definición de Políticas y Procedimientos del SAS.
- Elaboración y actualización del Documento de Seguridad.
- Inspecciones de la Agencia Española de Protección de Datos.
- Inspecciones de la Consejería de Justicia y Administración Pública.

## Contenidos implícitos de la sesión

- Obligaciones de la LOPD 15/99, RMS 1720/07, LAP 41/02, M.C.E.P.
- Instrucciones Internas del SAS.
- Consentimiento informado en materia de protección de datos.
- Circuito de incidencias, registros y acceso a la información
- Ejercicio de los derechos de acceso, rectificación y cancelación.
- Deberes del personal en materia de protección de datos y seguridad.
- Documento de Seguridad de la información corporativa del SAS.

Estos contenidos serán expuestos como Casos Prácticos

## TERMINOLOGÍA

- **Datos de Carácter Personal:** cualquier información concerniente a personas físicas identificadas o identificables.
- **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.
- **Consentimiento:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Disociación:** Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- **Derecho de Acceso:** es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.
- **Derecho de Rectificación:** es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.
- **Derecho de Cancelación:** el ejercicio de este derecho dará lugar a que se supriman los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo.
- **Derecho de Oposición:** es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los ciertos supuestos (como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario).

## ACTORES

Es importante reconocer las siguientes figuras que se recogen en el Documento de Seguridad del SAS.

- **Responsable del Fichero:** Director Gerente del SAS, Direcciones Generales y Directores de Centros.
- **Responsable de Seguridad:** Responsables de Tecnologías de la Información.
- **Responsable Funcional de Aplicación:** Directores, Subdirectores y Jefes de Servicio.

## CASOS PRÁCTICOS

### 1. *Publicación de Fotografías*

- Ante cualquier duda sobre el tratamiento de información, consultar al Responsable Funcional de Aplicación o al Responsable de Seguridad.
- Distinguir cuando se hace un uso acorde a la finalidad declarada de los datos de carácter personal.
- Los datos de carácter personal son propiedad de su titular, no de quien los custodia.
- El Responsable del Fichero debe autorizar cualquier uso extraordinario de los datos.
- El consentimiento y otros anexos interesantes está disponible en el Manual de Seguridad Corporativa del SAS.

### 2. *Acceso a los Sistemas de Información*

- Existe un procedimiento para solicitar acceso a los Sistemas de Información.
- Éste debe constar como anexo del Documento de Seguridad y debe estar actualizado por el centro.
- El Responsable Funcional de Aplicación debe ser la figura a la que el usuario/profesional consulte la mayoría de sus dudas respecto de los datos de carácter personal.
- Las credenciales de un usuario relacionan a éste con sus acciones en los Sistemas de Información. Responsabilidades.

### 3. *Publicación de un estudio epidemiológico*

- No ceder o comunicar datos, a no ser que sepamos con seguridad que tienen las autorizaciones necesarias.
- Para datos NO disociados y NO pertenecientes al SNS: Necesidad de Autorización del Paciente y Responsable del Fichero.
- Para datos Disociados: Autorización del Responsable Funcional de Aplicación.
- Registrar la E/S de soportes con datos de carácter personal, sean electrónicos o papel.
- Ante cualquier duda consultar el Documento de Seguridad o al Responsable de Seguridad del centro.

### 4. *Destrucción de documentos antiguos*

- Todos los datos personales, sin importar cual sea su soporte físico debe manejarse con las garantías exigidas en la ley, tanto para su utilización, archivo, custodia y traslado.
- Los documentos con datos personales deben encontrarse siempre “bajo llave” (protegidos).
- Sólo el personal autorizado puede tener acceso a los documentos en papel.
- Para deshacerse de cualquier documento con datos personales hay que proceder a su destrucción previa de forma que se impida su recuperación posterior.
- El traslado de la documentación debe realizarse de forma que se impida el acceso a la misma a personas no autorizadas

### 5. *Llevarse trabajo a casa*

- El tratamiento de datos de carácter personal fuera de los locales de ubicación del fichero debe ser autorizado por el Responsable del Fichero.
- Se deberá garantizar el nivel de seguridad adecuado según lo establecido en el Manual de Seguridad.
- La seguridad abarcará tanto a los equipos del centro de trabajo como de la casa, todos aquellos desde los que se accede o donde aparecen resultados visuales o impresos, así como en los procesos de transmisión de información.

## 6. Envío de datos personales por correo electrónico

- El envío de datos personales por correo electrónico ha de ser **autorizado por el Responsable de Aplicación/Fichero** el cual debe actuar según la LOPD.
- Debe quedar anotado en el **Registro de Entrada/Salida de soportes**.
- La información tiene que **enviarse cifrada**.
- **Cualquier incidencia de seguridad tiene que comunicarse** al Responsable de Seguridad.

## 7. Descargar música y software en el trabajo

- Los equipos informáticos puestos a disposición de los usuarios están destinados a un uso exclusivamente profesional y éstos no gozan de un uso privativo de los mismos.
- Las aplicaciones informáticas tienen una finalidad profesional y no son idóneas para un uso personal o privado.
- Los usuarios se limitarán a ejecutar las aplicaciones informáticas para las que estén autorizados.

## 8. Ejercicio del derecho de rectificación de datos

- El usuario tiene los derechos de Acceso, Rectificación, Cancelación y Oposición (**ARCO**) que puede ejercer en cualquier momento
- La organización tiene la obligación de disponer y regular los procedimientos para el ejercicio de estos derechos por parte de los usuarios.
- Disponemos de **diez días hábiles** para responder a los derechos de rectificación, cancelación y oposición y de **un mes** para el derecho de acceso.
- El silencio administrativo no es posible en el ejercicio de estos derechos.

## CONSECUENCIAS

La adecuación de los centros a la Ley Orgánica de Protección de Datos, además de ser una obligación legal, permite:

- **Cumplimiento del Contrato Programa 2005-2008**
- **Acreditación de Servicios (ACSA)**
- **Acreditación de Centros (ACSA)**

Hemos de considerar las denuncias e inspecciones de las que fuimos objeto:

- **Denuncias ante la Agencia Española de Protección de Datos:**
  - 2008 Hospital Reina Sofía
  - 2007 Hospital Virgen del Rocío
  - 2006 Área Sanitaria Campo de Gibraltar
  - 2006 Distrito Sanitario Málaga
  - 2005 Hospital Carlos Haya ...
- **Inspecciones de la Consejería de Justicia y Administración Pública**
  - 2008 Servicios Centrales del SAS
  - 2007 Distrito Sanitario Almería...

## FUENTES DE INFORMACIÓN ADICIONALES

- [Agencia Española de Protección de Datos](#)
- [Agencia Madrileña de Protección de Datos. Consultas Servicios Sanitarios](#)
- [Unidad de Gestión de Riesgos Digitales](#)
- [Instituto Nacional de Tecnologías de la Comunicación](#)
- [Curso LOPD on-line. Consjería de empleo](#)
- [BOE / BOJA](#)