



PLAN DE SENSIBILIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS



Plan de Adecuación LOPD

Servicio Andaluz de Salud



martes, 24 de enero de 2012



PLAN DE SENSIBILIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS



ÍNDICE

Presentación: la Unidad de Gestión de Riesgos
Digitales y a LOPD

Introducción del Plan de Adecuación

El Plan de Sensibilización

Terminología y Actores

Casos Prácticos

Procedimientos

Conclusiones/Preguntas

OBJETIVO

- **Facilitar el desarrollo de procedimientos del Documento de Seguridad en los centros sanitarios.**
 - **Marco Legal.**
 - **Documento de Seguridad.**
 - **Casos Prácticos.**
 - **Procedimientos**

UNIDAD DE GESTIÓN DE RIESGOS DIGITALES (UGRD)

La UGRD tiene como objetivo básico la gestión de la protección de los Sistemas y Tecnologías y de todos sus productos documentales en el ámbito del SAS, en aplicación de los marcos legales actualmente establecidos.

(SSCC. Resolución 223/2003 de 3 de marzo.)

Funciones y procesos:

- Gestión de activos de Sistemas y Tecnologías de la Información
- Análisis y Gestión de Riesgos
- Planificación Estratégica de Seguridad
- Gestión de Seguridad
- Políticas y Estándares
- Difusión y Comunicación
- Verificación de la Seguridad – Auditorías LOPD
- Administración de la Seguridad
- Desarrollo de la Seguridad
- Operación de la Seguridad

UGRD

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.

LEY ORGÁNICA DE PROTECCIÓN DE DATOS

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).

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los si

Artículo 89. *Funciones y obligaciones del personal.*

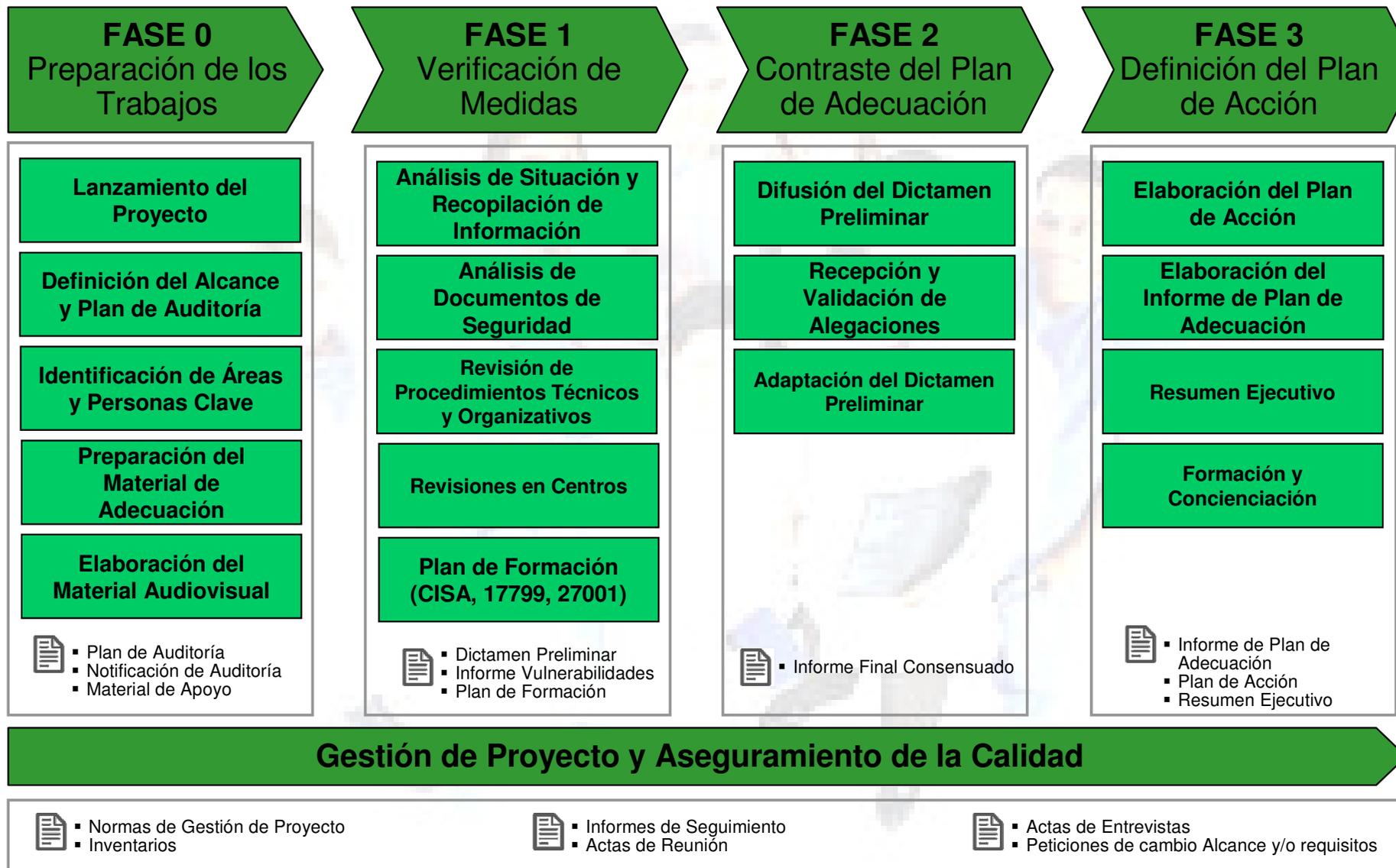
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

EL PLAN DE AUDITORÍAS: Objetivo

- El objetivo del proyecto es la elaboración del plan de adecuación a la legislación vigente en materia de protección de datos de carácter personal de los sistemas de información bajo responsabilidad de los Servicios Centrales y en sus diferentes centros.
- Para la definición de los documentos y planes de adecuación, diseñados para cada uno de estos centros, se cumplirá con lo exigido en el artículo 17 del “Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal”, relativo a Auditorías, concretándose en la realización de revisiones in situ (auditorías) y los correspondientes planes de adecuación para:

- Los Servicios Centrales del SAS
- Dos Hospitales Regionales
- Dos Hospitales de especialidades
- Dos Centros Regionales de Transfusión Sanguínea (CRTS)
- Dos Distritos de Atención Primaria
- Dos Áreas Sanitarias

EL PLAN DE AUDITORÍAS: Enfoque Metodológico



EL PLAN DE AUDITORÍAS: Dictamen Preliminar

C.R.T.S.



DISTRITO SANITARIO



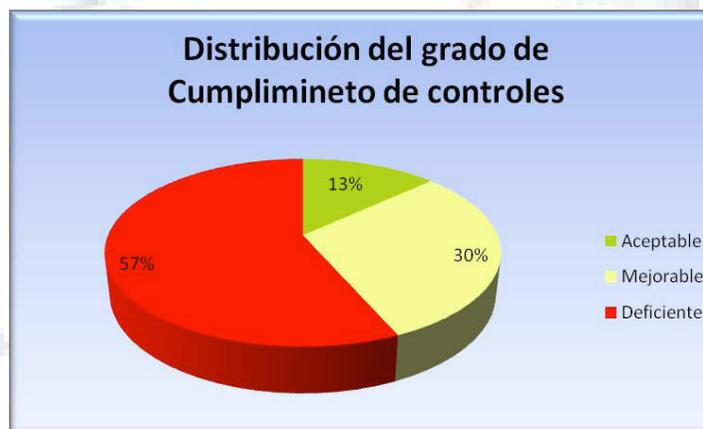
A.G.S.



HOSPITAL



DISTRITO SANITARIO



A.G.S.



EL PLAN DE SENSIBILIZACIÓN: Normativa base

Los contenidos del PLAN, distribuidos por perfiles profesionales, se centran en la difusión y el cumplimiento de:

- Ley Orgánica de Protección de Datos.
- El Reglamento de Medidas de Seguridad.
- La Ley de Autonomía del Paciente.
- El Manual de Comportamiento del Empleado Público de la Junta de Andalucía en el uso de los Sistemas Informáticos y Redes de Comunicaciones.
- Las Instrucciones Internas de la organización relacionadas con estas materias.

EL PLAN DE SENSIBILIZACIÓN: Objetivo

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 el módulo de formación:

- Sensibilización en Protección de Datos (LOPD) de cargos Directivos e Intermedios. Código del módulo 08/1465/0929/GE/P/AI

EL PLAN DE SENSIBILIZACIÓN: Acciones Formativas

| TIPO DE ACCIÓN | CENTROS | SESIONES |
|---|---------|---|
| Sensibilización Equipo Directivo del SAS. | | 1 |
| Sensibilización los Directores de Centros (Hospitales, Áreas, Distritos, CRTS). | | 1 |
| Plan de Sensibilización de cargos directivos e intermedios de Hospitales / Áreas / Distritos / CRTS. Nº de Hospitales + Áreas + Distritos + CRTS (aproximadamente) Año 1: 30 Año 2: 30 | 60 | 3 (Equipo Directivo, Cargos Intermedios, y Responsables de Servios o centros de salud). |
| Formación de formadores de centros. | | 4 (1 x trimestre) |
| Sensibilización Personal Sanitario. Se planificará para dar una cobertura en dos anualidades. Año 1: 13.5 00 Estimado alcanzar 25% plantilla (54.000 aproximadamente) Estimando 30 alumnos por sesión ≈(450 sesiones / año) | 60 | “n” En función del número de personal afectado o centro físico. |
| Sensibilización Personal Administrativo que maneja información sanitaria. Se planificará para dar una cobertura en dos anualidades. Año 1: 2.400 Estimado alcanzar 25% plantilla (9.600 aproximadamente) Estimando 20 alumnos por sesión ≈(120 sesiones / año) | 60 | “n” En función del número de personal afectado o centro físico. |

EL PLAN DE SENSIBILIZACIÓN: Contenidos clave

- Obligaciones de la LOPD 15/99, RMS1720/07, LAP 41/02, M.C.E.P.
- Instrucciones Internas del SAS.
- Responsabilidad y encargos de funciones.
- Responsables de Ficheros y de Seguridad.
- Responsables Funcionales de las Aplicaciones.
- Circuito de incidencias, registros y acceso a la información.
- Documento de Seguridad de la información corporativa del SAS.

EL PLAN DE SENSIBILIZACIÓN:

CASOS PRÁCTICOS

- Publicación de fotografías.
- Solicitud de acceso a Sistemas de Información.
- Publicación de un estudio epidemiológico.
- Destrucción de documentos antiguos.
- Llevarse trabajo a casa.
- Envío de datos personales por correo electrónico.
- Descargar música y software en el trabajo.
- Ejercicio del derecho de rectificación de datos.
- Videovigilancia. Menores.
- Jueces y Tribunales Sindicatos



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.

ACTORES I: Definición de responsables

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

➤ **Responsable del Fichero o Tratamiento:**

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

➤ **Responsable de Seguridad:**

Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

➤ **Responsable Funcional de Aplicación:**

Persona física u órgano específico del S.A.S., que por delegación del Responsable del Fichero tiene bajo su responsabilidad todo lo concerniente a la recogida, grabación, conservación, elaboración, modificación, visualización, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Mantiene contacto diario con la aplicación, conoce su funcionamiento, vela por la seguridad de la misma y trabaja en coordinación con el Responsable de Sistemas y Tecnologías de la Información.

ACTORES II: Identificación de responsables

El Documento de Seguridad hace una recomendación precisa sobre que figuras dentro del SAS deben asumir las responsabilidades en materia de protección de datos.

- 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.

ORGANIZACIÓN DE LA SEGURIDAD

