Evento sobre Protección y Monitorización de la Seguridad de las Bases de Datos

Madrid, 22 de septiembre de 2010

Medidas de protección en la gestión de los datos

EVALOPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

María José Blanco Antón
Subdirectora General del Registro General de Protección de Datos

Facilitar el cumplimiento de la LOPD

→ **Objetivo de la Agencia**

Medidas de protección en la gestión de los datos

- Guía del Responsable de Ficheros

- Guía de Seguridad de Datos

- Guía de Videovigilancia

- Guía de Relaciones Laborales

Medidas de protección en la gestión de los datos

NOTIFICACIONES TELEMATICAS A LA AEPD

Formulario electrónico www.agpd.es

e-Administracion

Facilitar la notificación de ficheros a la Agencia

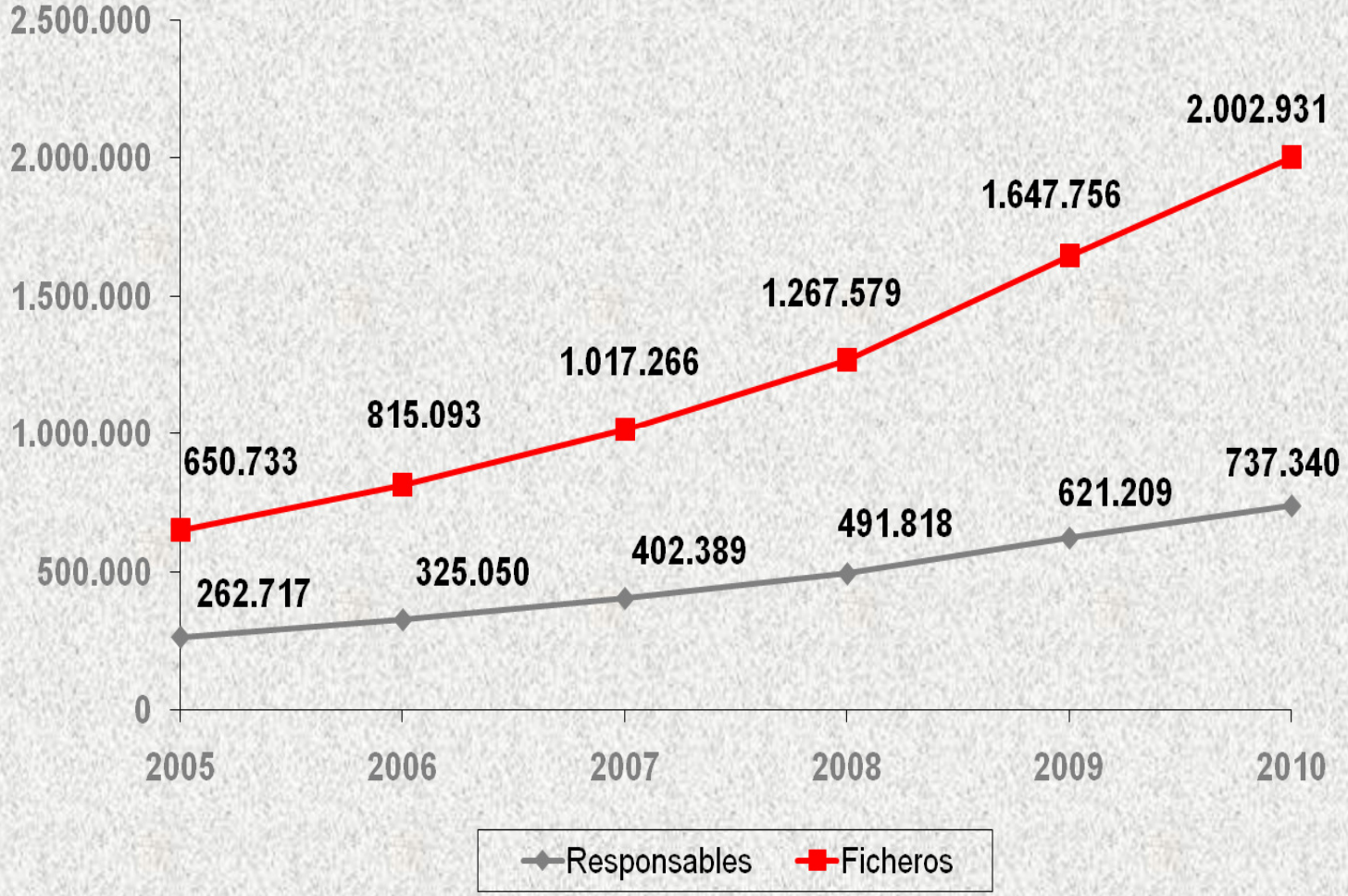
- **Titularidad pública y privada**
- **Notificaciones tipo (precumplimentadas): Recursos humanos, Nóminas, Clientes/proveedores, Comunidades Propietarios, Pacientes, …**
- **Firma electrónica: @firma**

dni · Camerfirma · izenpe s.a. · CATCert Agència Catalana de Certificació · ANF AC · FNMT · ACA · Autoritat de Certificació de la Comunitat Valenciana · ancert Agencia Notarial de Certificación · firmaprofesional · Banesto CA

- **Buzón de notificación electrónica: SISNOT- DEU**

Medidas de protección en la gestión de los datos

Evolución de la inscripción en el RGPD 31-8-2010



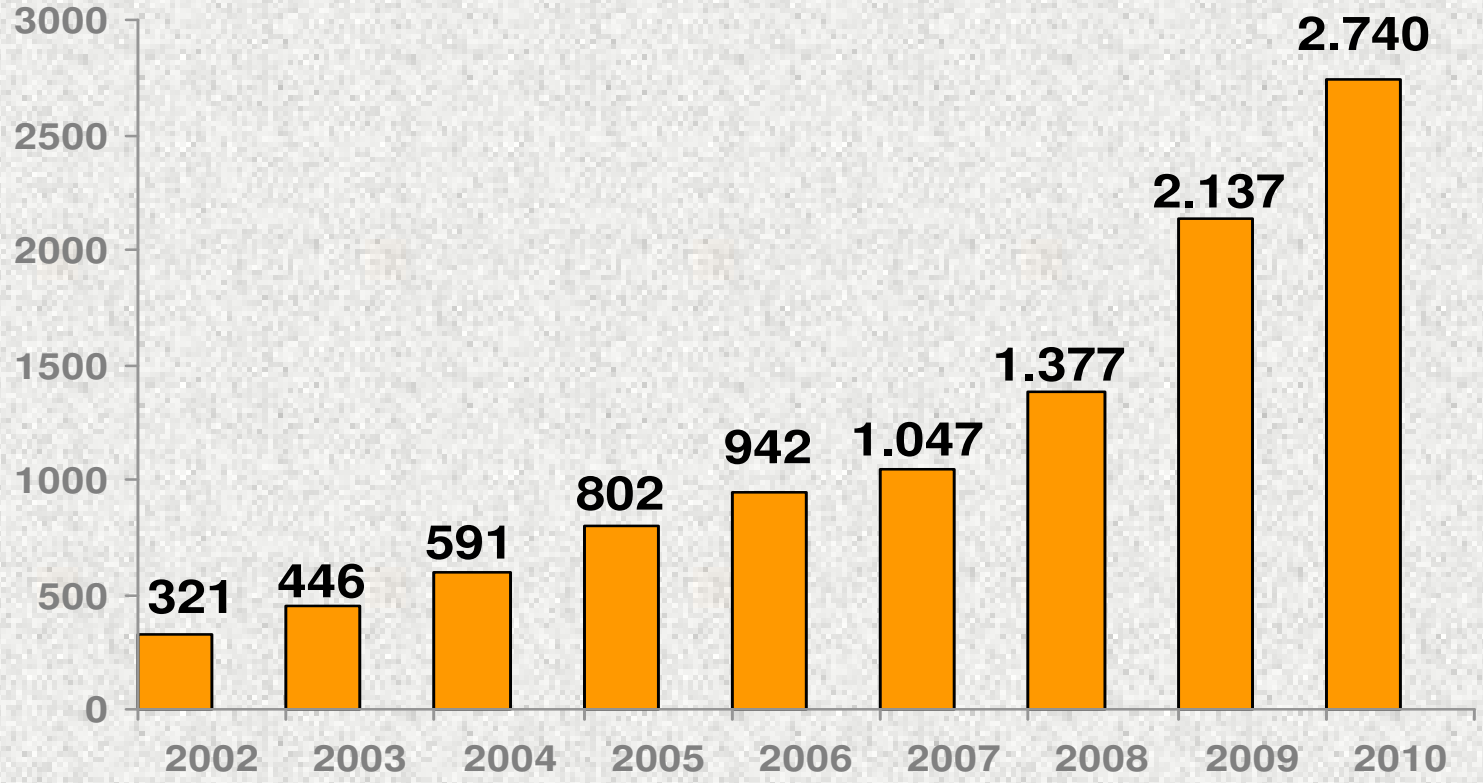
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Evento de Protección de Monitorización de la Seguridad de las Bases de Datos

Madrid, 22 de septiembre de 2010

Medidas de protección en la gestión de los datos

Media diaria de operaciones de inscripción en RGPD



Medidas de protección en la gestión de los datos

SITUACIÓN:

- La inscripción de ficheros en el RGPD no se corresponde con la situación real
  - PYMES, microPYMES y profesionales
- Desconocimiento LOPD
- Complejidad

→ Incumplimiento LOPD

Medidas de protección en la gestión de los datos

www.agpd.es

- Promover cultura LOPD
- Comprometer a las entidades responsables con la protección de datos
- Herramienta de autoevaluación
- Facilitar el cumplimiento de LOPD

Objetivos y destinatarios

- **INSTRUMENTO ÚTIL**
- **Lenguaje simple y adecuado**
- **Documentación de apoyo y ayuda interactiva vinculada a las preguntas**
- **Procedimiento sencillo**
- **Anónimo y recuperable**
- **Timing adecuado**
- **Informe de situación**

- **Entidades responsables de ficheros, encargados de tratamiento y responsables de seguridad**

Requerimientos básicos previos

- Conocer la organización
- Disponer de 45 a 60 minutos
- Conceptos básicos: ¿qué es un dato personal?, ¿puedo tener ficheros?, ¿soy responsable?, ¿estoy prestando un servicio a un tercero?, ….
- Sinceridad en las respuestas

+ Sinceridad → + Veracidad

Presentación

Introducción

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD-, establece un conjunto de principios, derechos y deberes que requieren adaptar las organizaciones para su cumplimiento. Empresas, asociaciones, autónomos, o administraciones, tratan datos personales para su gestión ordinaria y ello les obliga a plantearse muchas preguntas:

- ¿Qué son datos personales?
- ¿Qué es un fichero?
- ¿Qué es un tratamiento?
- En caso de tratar datos, ¿hay algún dato exento de la LOPD?
- ¿Cuáles son mis obligaciones?

Esta herramienta ofrece respuesta a éstos y a muchos otros interrogantes mediante un procedimiento de diagnóstico basado en un autotest basado en preguntas con respuesta múltiple. Basta con realizar el mismo para que al final, la Agencia Española de Protección de Datos, le facilite un informe con indicaciones y recursos que le orienten, en su caso, para cumplir con lo dispuesto en la LOPD.

El informe que emitirá el programa depende de sus respuestas por ello no olvide seguir las siguientes instrucciones:

1. Lea atentamente la información previa, le ayudará a comprender los principales conceptos y a identificar los elementos que debe conocer de su organización antes de iniciar el autotest.
2. Cada pregunta incluye un pequeño enlace a una "ayuda", si no comprende la pregunta pínchelo y léalo atentamente.
3. El test le ocupará aproximadamente entre 30 y 45 minutos. Si Ud. desea abandonarlo se le proporcionará un código que le permite reanudarlo en cualquier momento guardando la información.
4. El test es completamente anónimo, la Agencia Española de Protección de Datos no identifica a quienes lo realizan y su formalización no genera responsabilidad alguna.
5. El resultado del test es meramente orientativo. Es una herramienta de ayuda cuyos resultados dependen de las respuestas facilitadas. Por lo tanto, su realización no exime del cumplimiento de la LOPD ni podrá exhibirse con la finalidad de justificar o eximir la responsabilidad ante una eventual infracción.

Conceptos Previos

Realice esta suma

44 + 45 = 89

Iniciar Encuesta Continuar Encuesta

Evaluaciones

- Test general "Cumplimiento de la LOPD": registro, información, principios, derechos ARCO, terceros, nivel de seguridad
- Test de seguridad "Cumplimiento de medidas de seguridad": nivel, sistema de tratamiento, documento, funciones, incidencias, acceso, soportes, identificación
- Independientes
- Informe de autoevaluación:

Generación → Revisión → Seguimiento

Salir

Encuestas Disponibles

EVALUA - Test de cumplimiento de la LOPD.

Este test le permitirá evaluar el grado de cumplimiento de la normativa sobre protección de datos. Si se aproxima por primera vez a la protección de datos es aconsejable haber leído los conceptos previos incluidos en la página anterior y muy recomendable haber consultado nuestra Guía del Responsable de Ficheros disponible en la web de la AEPD www.agpd.es.

Seleccionar

EVALUA - Test de cumplimiento de medidas de seguridad

Este test se ha diseñado para facilitar la verificación de las medidas de seguridad previstas por el Reglamento de Desarrollo de la Ley Orgánica de Protección de datos. Para realizarlo es recomendable la consulta `previa de nuestra Guía de Seguridad de Datos disponible en la web de la AEPD www.agpd.es.

Seleccionar Ver Resultados

versión:0.8.5

Salir

Encuestas Disponibles

EVALUA - Test de cumplimiento de la LOPD.

Este test le permitirá evaluar el grado de cumplimiento de la normativa sobre protección de datos. Si se aproxima por primera vez a la protección de datos es aconsejable haber leído los conceptos previos incluidos en la página anterior y muy recomendable haber consultado nuestra Guía del Responsable de Ficheros disponible en la web de la AEPD www.agpd.es.

Seleccionar

EVALUA - Test de cumplimiento de medidas de seguridad

Este test se ha diseñado para facilitar la verificación de las medidas de seguridad previstas por el Reglamento de Desarrollo de la Ley Orgánica de Protección de datos. Para realizarlo es recomendable la consulta `previa de nuestra Guía de Seguridad de Datos disponible en la web de la AEPD www.agpd.es.

Seleccionar Ver Resultados

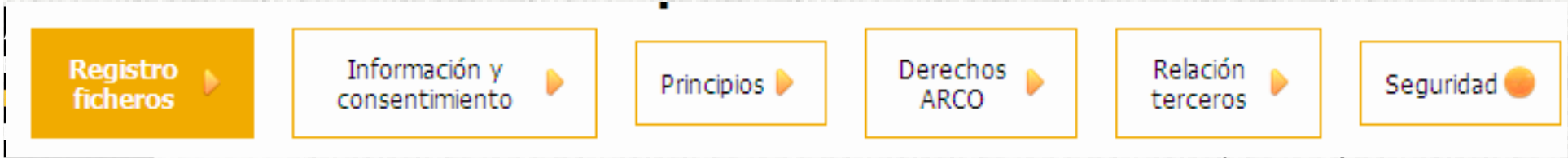
versión:0.8.5

Medidas de protección en la gestión de los datos

Cumplimiento de la LOPD

Acercamiento basado en la gestión:

- **¿Tengo ficheros?**
- **¿Cómo obtengo los datos?**
- **¿Cómo trato los datos?**
- **¿Y si ejercen un derecho?**
- **¿Qué relaciones tengo con terceros?**
- **¿Garantizo la seguridad?**



Registro ficheros

Salir

Cumplimiento LOPD

Registro ficheros | Información y consentimiento | Principios | Derechos ARCO | Relación terceros | Seguridad

Introducción

Antes de iniciar el cuestionario es conveniente tener en cuenta algunos conceptos básicos que nos permitirán conocer dos aspectos esenciales: Si tratamos datos personales sujetos a lo dispuesto por la LOPD. Si somos el responsable de un fichero o tratamiento o lo que se denomina un encargado del tratamiento. Un dato personal no e... leer más...

Ayuda

Pregunta

Con la información de la que dispone actualmente ¿cree que Vd. o su empresa realizan tratamientos de datos de carácter personal?

- (•) Si
- ( ) No se realizan tratamientos de datos.

1 de 3

Siguiente >

Guardar

versión:0.8.5

Cumplimiento de medidas de seguridad

Seguridad – principio de protección de datos:

- **Confidencialidad, integridad y disponibilidad de los datos personales**
- **Obligación de responsables de ficheros y encargados de tratamiento**
- **Todos los ficheros y tratamientos**

Cumplimiento de medidas de seguridad

Objetivos:

- Facilitar información sobre las medidas de seguridad que deben implantarse
- Permitir comprobar y autoevaluar el grado de cumplimiento

MEDIDAS DE SEGURIDAD DE DATOS PERSONALES

- La seguridad de los datos personales es una obligación legal

Art. 9 LOPD. *Seguridad de los datos*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

MEDIDAS DE SEGURIDAD DE DATOS PERSONALES

El Reglamento de desarrollo de la LOPD (aprobado por RD 1720/200/), en su Título VIII desarrolla las medidas de seguridad:

- Datos de carácter personal
- Principio de seguridad
- Reglamento de mínimos
- Medidas técnicas
- Medidas organizativas
- Ciclo de vida

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

- Artículo 5.2. **Definiciones**
- Título VIII. **MEDIDAS DE SEGURIDAD**
  - Capítulo I. **Disposiciones generales** (arts. 79 - 87)
  - Capítulo II. **Del documento de seguridad** (art. 88)
  - Capítulo III. **Medidas aplicables a ficheros y tratamientos AUTOMATIZADOS**
    - Sección Primera. Medidas de seguridad de nivel **básico** (arts. 89 - 94)
    - Sección Segunda. Medidas de seguridad de nivel **medio** (arts. 95 - 100)
    - Sección Tercera. Medidas de seguridad de nivel **alto** (arts. 101 - 104)
  - Capítulo IV. **Medidas aplicables a ficheros y tratamientos NO AUTOMATIZADOS**
    - Sección Primera. Medidas de seguridad de nivel **básico** (arts. 105 - 108)
    - Sección Segunda. Medidas de seguridad de nivel **medio** (arts. 109 - 110)
    - Sección Tercera. Medidas de seguridad de nivel **alto** (arts. 111 - 114)

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Disposiciones generales. Niveles de seguridad: Básico, Medio y Alto
Aplicación de niveles

- **ALTO** — Datos especialmente protegidos
  Fines policiales sin consentimiento de las personas afectada
  Violencia de género
- **MEDIO** — Infracciones administrativas o penales
  Servicios de información sobre solvencia patrimonial y crédito
  Administraciones Tributarias - potestades tributarias
  Entidades financieras - servicios financieros
  Seguridad Social, Mutuas
  Elaboración de perfiles
- **MEDIO (+ registro de accesos)** Operadores TELECO – tráfico y localización
- **BÁSICO** — Cualquier otro fichero o tratamiento de datos de carácter personal
  Ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:
  - transferencia dineraria - entidades de las que los afectados sean asociados o miembros,
  - tratamiento incidental o accesorio, sin guardar relación con la finalidad
  - Salud - grado o condición de discapacidad o invalidez - cumplimiento de deberes públicos

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Las medidas de seguridad tienen que aplicarse a cualquier fichero o tratamiento de datos de carácter personal, con independencia:

- **de quién realice el tratamiento**
  - Encargado del tratamiento
    - Diferentes modos de prestación del servicio (art. 82)
  - Prestación de servicios sin acceso a datos personales
    - Cláusula informativa en el contrato (art. 83)
- **desde dónde se realice**
  - Acceso a datos a través de redes de comunicaciones, sean o no públicas (art. 85)
  - Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento
    - Dispositivos portátiles (art. 86)
- **cómo se realice**
  - Ficheros temporales o copias de trabajo de documentos (art. 87)

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Documento de seguridad (art. 88)

- Buenas prácticas. Determina la participación del personal en la política de seguridad de la organización
- Único o individualizado, en función de sistemas de tratamiento, otros criterios del responsable
- Recogerá las delegaciones de autorizaciones
- Medidas para el transporte de soportes y documentos, y para la reutilización y/o destrucción de los documentos y soportes.
- Recogerá las situaciones excepcionales:
  - Uso de dispositivos portátiles,
  - Medidas compensatorias, imposibilidad aplicación medidas prevista
  - Encargado:
    - Identificación de los ficheros o tratamientos que se traten en concepto de encargado
    - Posibilidad de delegar la llevanza del documento
- Interno, actualizado
  - Debe revisarse ante cambios relevantes: un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Nivel Básico

Ficheros automatizados y no automatizados	
Art. 89. Funciones y obligaciones del personal Art. 90. Registro de incidencias Art. 91. Control de acceso Art. 92. Gestión de soportes y documentos	
Sólo automatizados	**Sólo no automatizados**
Art. 93. Identificación y autenticación - personalizada Art. 94. Copias de respaldo y recuperación - verificación - pruebas datos reales. Medidas correspondientes	Art. 106. Criterios de archivo - posibilitar derechos ARCO Art. 107. Dispositivos almacenamiento - mecanismos apertura Art. 108. Custodia de los soportes - en el proceso de tramitación

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Nivel Medio

Ficheros automatizados y no automatizados
Responsable de seguridad (art. 95, art. 109) Auditoria (art. 96, art. 110)
Sólo automatizados
Art. 97. Gestión de soportes Art. 98. Identificación y autenticación Art. 99. Control de acceso físico Art. 100. Registro de incidencias

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD
Nivel Alto

Ficheros automatizados	Ficheros no automatizados
Art. 101. Gestión y distribución de soportes Art. 102. Copias de respaldo y recuperación Art. 103. Registro de accesos Excepción: - Responsable – persona física – único usuario Art. 104. Telecomunicaciones - Cifrado en redes públicas o inalámbricas	Art. 111. Almacenamiento de la información - Archivadores, áreas restringidas Art. 112. Copia o reproducción - Personal autorizado Art. 113. Acceso a la documentación - Mecanismo identificación por diferentes usuarios Art. 114. Traslado de documentación - Impedir acceso, manipulación

Medidas de protección en la gestión de los datos

Ficheros no automatizados-Nivel alto

- Copia o reproducción:
  - **bajo el control del personal autorizado en el documento de seguridad**
  - **Destrucción de las copias o reproducciones desechadas.**
- Acceso a la documentación.
  - **exclusivamente el personal autorizado**
  - **Identificación de accesos a documentos que puedan ser utilizados por múltiples usuarios.**
  - **Registro de accesos de personas no autorizadas**

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

- **Disposición adicional única**

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto

Medidas de protección en la gestión de los datos

REGLAMENTO LOPD. MEDIDAS DE SEGURIDAD

Disposición transitoria segunda. Plazos de implementación

Ficheros nuevos manuales y/o automatizados

Aplicación del nivel básico, medio o alto correspondiente desde su **creación**

Ficheros existentes

Automatizados	- Seguridad Social, Mutuas, Perfiles → 1 año (Medio) - Violencia de género → 1 año (Medio) → 18 meses (Alto) - Teleco (tráfico, localización) → 1 año (Medio) → 18 meses (Registro de accesos) - Adaptación resto de ficheros → 1 año (arts. 93, 94, 101, 104)
No automatizados	- Básico (1 año) - Medio (18 meses) - Alto (2 años)

Salir

Encuestas Disponibles

EVALUA - Test de cumplimiento de la LOPD.

Este test le permitirá evaluar el grado de cumplimiento de la normativa sobre protección de datos. Si se aproxima por primera vez a la protección de datos es aconsejable haber leído los conceptos previos incluidos en la página anterior y muy recomendable haber consultado nuestra Guía del Responsable de Ficheros disponible en la web de la AEPD www.agpd.es.

Seleccionar

EVALUA - Test de cumplimiento de medidas de seguridad

Este test se ha diseñado para facilitar la verificación de las medidas de seguridad previstas por el Reglamento de Desarrollo de la Ley Orgánica de Protección de datos. Para realizarlo es recomendable la consulta `previa de nuestra Guía de Seguridad de Datos disponible en la web de la AEPD www.agpd.es.

Seleccionar Ver Resultados

versión:0.8.5

Cumplimiento de medidas de seguridad

- Conocer la <u>situación de partida</u>
  - Ficheros, grado de cumplimiento de seguridad, concienciación, grado de mejora, …
- Revisar documentación
  - Documento de seguridad, políticas, normas, procedimientos, …
  - Guía de seguridad
  - En su caso, informe de auditoria
- Identificar <u>necesidades</u>
  - Situación inicial, revisión, planificación, …
- <u>Ámbito</u>
  - Ficheros automatizados, no automatizados, parcialmente automatizados
  - Nivel básico, medio, alto

→ AUDITORIA vs AUTOEVALUACION

Nivel de medidas de seguridad que se desea evaluar

La normativa sobre protección de datos, establece obligaciones distintas dependiendo de la naturaleza de los datos de carácter personal que se tenga previsto tratar, tales como, las formas de recabar el consentimiento o el nivel de medidas de seguridad a implantar en los ficheros. Así, las medidas de seguridad exigibles a los ficheros y tratamient... leer más...

¿Desea evaluar el cumplimiento de las medidas de seguridad de nivel básico?

- ○ Sí.
- ○ No

1 de 6

Guardar y Salir

Atención durante el uso de la herramienta Evalúa no utilice las funciones de avance y retroceso del navegador.

versión:0.8.12

Nivel de medidas de seguridad que se desea evaluar

Será necesario determinar el sistema de tratamiento que se está realizando, es decir, el modo en que se organiza la información. Atendiendo al sistema de tratamiento, los sistemas podrán ser automatizados, no automatizados o parcialmente automatizados. En función de las respuestas proporcionadas, la herramienta le presentará las preguntas relacion... leer más...

Nivel alto ¿Cuál es el sistema de tratamiento que se desea evaluar?

- ○ Automatizado.
- ○ No Automatizado (manual).
- ○ Parcialmente Automatizado (mixto).

6 de 6

< Anterior | Finalizar

Atención durante el uso de la herramienta Evalúa no utilice las funciones de avance y retroceso del navegador.

versión:0.8.12

Medidas de protección en la gestión de los datos

Cumplimiento de medidas de seguridad

Medidas comunes (nivel básico, medio, alto)

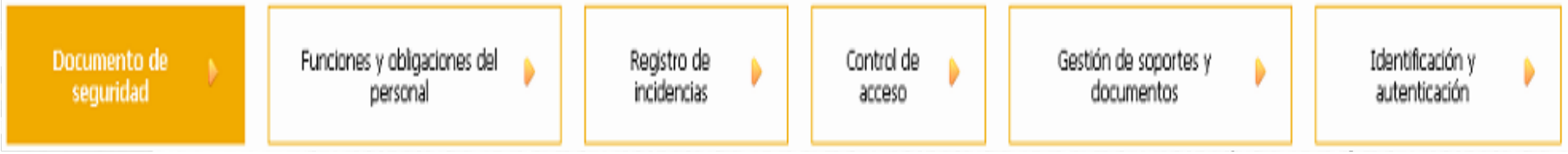
Documento de seguridad → Funciones y obligaciones del personal → Registro de incidencias → Control de acceso → Delegación de autorizaciones → Trabajo fuera locales → Encargado de tratamiento → Soportes y documentos → Ficheros temporales → Auditoría → Criterios de archivo → Otras prestaciones de servicios

Sistemas automatizados

Identificación y autenticación → Copias de respaldo → Control de acceso → Registro de incidencias → Registro de accesos → Telecomunicaciones → Soportes y documentos

Sistemas no automatizados

Almacenamiento de la información → Custodia de soportes → Accesos → Soportes y documentos



Nivel de seguridad alto y Tratamiento parcialmente automatizado (Mixto)

Información Formulario

El documento de seguridad es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

- ámbito de aplicación: especificación detallada de los recursos protegidos;
- medidas, normas, procedimientos, reglas y estándares de seguridad;
- funciones y obligaciones del personal;
- estructura y descripción de los ficheros y sistemas de información;
- procedimiento de notificación, gestión y respuesta ante incidencias;
- procedimiento de copias de respaldo y recuperación de datos;
- medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

A partir del nivel medio de medidas de seguridad, además de los apartados anteriores, deberán incluirse los siguientes:

- identificación del responsable de seguridad y,

Siguiente >

Atención durante el uso de la herramienta Evalúa no utilice las funciones de avance y retroceso del navegador.

Nivel de seguridad alto y Tratamiento parcialmente automatizado (Mixto)

El documento de seguridad es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar. Los apartados mínimos qu... leer más...

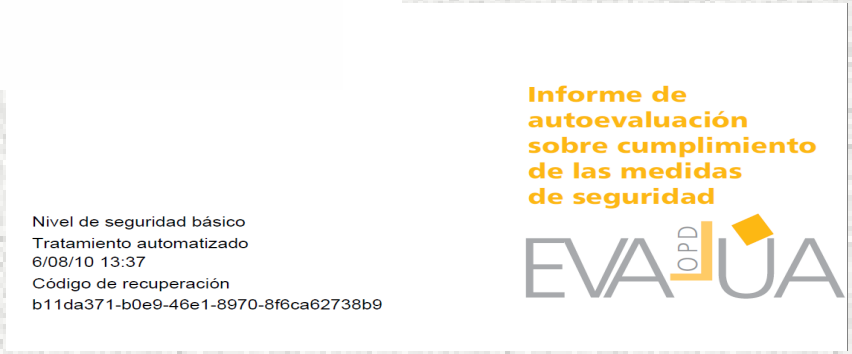
¿Ha elaborado el responsable del fichero el Documento de Seguridad? Por favor, con el fin de que el informe de autoevaluación incluya el mayor nivel de detalle de las deficiencias detectadas, conteste a todas las preguntas de este bloque aún en el caso de que haya contestado que el responsable del fichero no ha elaborado el Documento de Seguridad.

- ○ Sí.
- ○ No

Atención durante el uso de la herramienta Evalúa no utilice las funciones de avance y retroceso del navegador.

Resultados

- Informe de autoevaluación sobre cumplimiento de la LOPD
- Informe de autoevaluación sobre cumplimiento de las medidas de seguridad



Medidas de protección en la gestión de los datos

Resultados

- **Informe final basado en las respuestas facilitadas.**
- **Formula recomendaciones de actuación.**
- **No vincula a la AEPD: anonimato**

GENERACIÓN → REVISIÓN → SEGUIMIENTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Muchas gracias