Universidad Zaragoza
1542

Trabajo Fin de Grado

"Seguridad y privacidad en el uso de las TIC en Marketing"

Autor/es

Fernando Martín Miedes

Director/es

María Jesús Lapeña Marcos

Facultad de Economía y Empresa

2016-2017

INFORMACIÓN

Título del Trabajo: Seguridad y privacidad en el uso de las TIC en Marketing

Work title: Security and privacy in the use of ICT in Marketing

Autor: Fernando Martín Miedes

Director del trabajo: María Jesús Lapeña Marcos

Titulación: Grado de Marketing e Investigación de Mercados

INFORME EJECUTIVO

A lo largo del presente trabajo se va a abordar el estudio de los conceptos de seguridad y privacidad contemplados en la LOPD (Ley Orgánica de Protección de Datos) centrándonos sobre todo en el ámbito informático. Analizaremos las leyes y normas en materia de seguridad de la información, privacidad y derecho a la intimidad. Revisaremos el estado del arte tanto en España como fuera de ella y consideraremos aspectos como el uso de contraseñas y control de accesos a la hora de acceder a la información, copias de seguridad..., teniendo en cuenta los distintos niveles de criticidad de la información.

Una vez presentado el marco teórico, aplicaremos todo lo estudiado a un caso práctico. Se realizará una auditoria a una empresa y al Servicio Aragonés de Salud, con el objetivo de analizar el grado de cumplimiento de la Ley Orgánica de Protección de Datos. El objetivo de dichas auditorias será detectar posibles fallos de seguridad o incumplimiento de la ley y proponer acciones de mejora. Se revisaran guías de adaptación de la LOPD y diseñaremos un cuestionario para el análisis. Finalizaremos con las conclusiones derivadas del trabajo realizado.

ABSTRACT

In this work we will speak about the study of the concepts of security and privacy under the data protection Act (organic law of data protection) focusing in the computer field. Discuss the laws and rules in matter of security of the information, privacy and right to the privacy. Will review the State of the art both in Spain as out of it and will consider aspects as the use of passwords and control of access at the time of access to the information, copies of security..., taking in has them different levels of criticality of the information.

In the framework theoretical, apply all it studied to a case practical. We do an audit to a company and to Servicio Aragonés de Salud, with the objective of analyzing the degree of compliance of it law organic of protection of data. The aim of the audits will be detect possible errors of security or breach of the law and propose solutions. Are revision guides of adaptation of the LOPD and will design a questionnaire for the analysis. We will finish with the conclusions of the work.

ÍNDICE

FIGURAS

1. INTRODUCCIÓN

1.1 SITUACIÓN ACTUAL Y PLANTEAMIENTO DEL PROBLEMA

Actualmente, tanto a nivel de usuario como a nivel de empresa, toda la información es procesada y almacenada en medios informáticos como servidores, discos duros, pendrives... La manera actual de gestionar la información proporciona muchas ventajas, como el ahorro de espacio, sencillez y rapidez a la hora de buscar una información, facilidad a la hora de compartirla... pero esto conlleva algunos riesgos.

Por lo tanto, hay que tener en cuenta ciertas medidas en lo referente a la protección y uso de todos los datos que contienen estos dispositivos informáticos, ya que pueden contener información privada y hay que evitar el acceso de cualquier persona o entidad ajena. Para poder preservar la confidencialidad de los datos almacenados contemplaremos las medidas organizativas y técnicas propuestas en la Ley Orgánica de Protección de Datos.

Revisaremos en profundidad los conceptos de seguridad informática y derecho a la privacidad, así como la normativa relacionada y su aplicación, con el fin de conocer las medidas que ponen o deben poner en práctica las empresas y el grado de cumplimiento legal cuando trabajan con datos confidenciales.

1.2 OBJETIVOS

Como objetivo general del estudio nos proponemos profundizar en el tema de la seguridad y la privacidad en el uso de las TIC, en términos de protección de datos y sus implicaciones, con el objetivo de aplicarlo a un caso práctico.

Como objetivos específicos nos proponemos:

- Revisar la normativa y legislación vigente en materia de seguridad informática y derecho a la privacidad.
- Concienciar sobre la importancia de la protección de datos confidenciales en la actividad empresarial.
- Conocer las distintas herramientas y medidas organizativas y técnicas que existen para garantizar la seguridad de la información.
- Realizar una auditoria en términos de cumplimiento de la Ley Organiza de Protección de Datos.

- Analizar los resultados obtenidos, reflexionar los fallos encontrados y proponer mejoras.
- Diseñar una guía de adaptación para el cumplimiento de la LOPD dirigida a PYMES.

1.3 ESTRUCTURA DEL TRABAJO

Tras esta introducción, el trabajo lo estructuraremos en 3 apartados fundamentales:

En primer lugar, presentamos el marco teórico de la materia en estudio; nos centramos en definir los conceptos fundamentales, seguridad de la información y privacidad, destacando el porqué de su importancia. También hablaremos sobre el proceso de análisis y gestión de riegos y cómo realizarlo. Además haremos una revisión de la normativa en materia de seguridad de la información, concretamente la ISO 27001, el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos Personales, en la cual centraremos nuestro estudio.

El tercer apartado, nos centramos en hacer una aplicación práctica de todo, en primer lugar diseñaremos un cuestionario que nos servirá para conocer las medidas contempladas en el tratamiento de datos personales y a continuación, apoyándonos en el cuestionario, valoraremos el grado de cumplimiento de la LOPD en dos entornos diferentes que nos ofrecerán perspectivas distintas: una pequeña empresa y un organismo público. Para terminar este apartado, como resultado del estudio, presentamos una guía para ayudar a las PYME a cumplir con lo dispuesto en la LOPD.

A continuación en el cuarto apartado, presentaremos las conclusiones del estudio; y completaremos con el apartado de la bibliografía.

Adjuntamos además, unos anexos en los que recogemos documentos/formularios (como el de inscripción de ficheros) recopilados del sitio web de la Agencia Española de Protección de Datos que facilita el cumplimiento de la LOPD a las empresas.

2. MARCO TEÓRICO

2.1 LA SEGURIDAD DE LA INFORMACION Y EL DERECHO A LA PRIVACIDAD

Respecto al mundo empresarial se considera el activo más importante y por tanto, hay que protegerla y asegurarla; hay que evitar que esté accesible a personas no autorizadas y, asimismo, hay que evitar su pérdida y su modificación.

"La información es poder"; la información es valiosa, crítica y sensitiva:

- Crítica; porque es un elemento imprescindible para las operaciones de la empresa.
- Valiosa; por ser el activo más importante de la empresa.
- Sensitiva; por tratarse, en ocasiones, de datos personales o confidenciales que solo deben ser manejados por personal autorizado.

Por ello es fundamental que existan mecanismos de seguridad para poder estar a salvo ante cualquier problema que podamos tener.

Podemos definir la seguridad informática como el conjunto de medidas de protección de las infraestructuras computacionales así como todo lo que esté relacionada con ella, principalmente la información que contiene. Distinguimos la seguridad lógica, que refiere a la seguridad ante el uso del software y el acceso por parte de los usuarios de la información, y la seguridad física, cuyo objetivo es proteger físicamente los distintos recursos, infraestructuras e instalaciones.

En definitiva se trata de proteger tanto la información como el sistema informático en su totalidad, para garantizar, en particular, que no se produce acceso, uso, divulgación o destrucción no autorizada de la misma.

2.1.1 Definición de Seguridad de la Información

Podemos definir la seguridad de la información como el conjunto de sistemas y procedimientos que garantizan la confidencialidad, la integridad y la disponibilidad de la misma; además de forma complementaria podremos considerar otras propiedades como: autenticidad, no repudio, trazabilidad y confiabilidad.

A continuación definimos cada una de estas dimensiones de seguridad de la información.

-Confidencialidad: consiste en la prevención de la divulgación de la información a personas o sistemas que no están autorizados para ello. El acceso es únicamente para las personas que estén autorizadas; tendría que ser un requisito en el mundo empresarial.

-Integridad: en términos de seguridad se refiere al correcto tratamiento de la información, para evitar que al trabajar, haya pérdida, deterioro o modificación errónea

de la misma. Preservando la integridad conservaremos la información de forma inalterada, a menos que se modifique por personal autorizado para ello, siempre dejando constancia de esa modificación.

-Disponibilidad: condición por la cual la información debe ser accesible para aquellas personas que estén autorizadas para acceder a ella.

-Autenticidad: se refiere al aseguramiento de la identidad respecto al origen de la información con objeto de tener la certeza de que los datos provienen de la fuente que dice ser. Para solucionar el problema de la autenticidad podemos recurrir a sistemas como el de la firma electrónica digital.

-No repudio: sirve para evitar que tanto el receptor (no repudio de origen) como el emisor (no repudio en destino) nieguen la transmisión de un mensaje.

-Trazabilidad: propiedad que permite conocer la historia y trayectoria de los datos.

-Confiabilidad: la información debe de ser obtenida de fuentes fiables para que tenga mayor validez.

2.1.2 El Derecho a la Privacidad. Garantizar la Confidencialidad

Como acabamos de ver, para garantizar la seguridad de la información, una de las dimensiones que hay que preservar es la confidencialidad, con ello podemos garantizar el derecho a la privacidad. La privacidad podemos definirla como el derecho o la capacidad de una organización o individuo para conservar y mantener de manera confidencial los datos que maneja.

Tener privacidad significa tener una zona libre de observadores. Las ventajas de la privacidad pueden dividirse en:

- En el ámbito privado, la privacidad es necesaria para que podamos mantener relaciones sociales variadas. Las personas tenemos y mostramos diferentes facetas de nosotros mismos en función de cada contexto.
- En el ambiente laboral, al ayudar a preservar secretos corporativos, la privacidad protege la competitividad empresarial.
- En el ámbito político, la privacidad protege a las sociedades democráticas y pluralistas. La libertad política requiere que las personas tengan el derecho de mantener en secreto su voto, sus asociaciones, y sus ideas políticas, si así lo desean.

La privacidad nos proporciona seguridad y relajación; nos permite resguardarnos en una zona libre de intrusiones y miradas externas para hacer aquello que no haríamos en público por pudor, miedo al ridículo, o miedo a lo que otros puedan pensar de nosotros.

2.1.3 Análisis y Gestión de Riesgos

A la hora de llevar a cabo un estudio acerca de la seguridad informática y de la información en una organización, debemos de realizar un análisis y gestión de riesgos y así podremos hacer una valoración de los distintos riesgos que nos podemos encontrar y podremos aplicar medidas que permitan el control de los mismos.

Un análisis de riesgos es un proceso sistemático que estima la magnitud de los riesgos a los que está expuesta una organización, es decir, un proceso de identificación y evaluación del riesgo a sufrir un ataque, comparándolo con el costo que significa la prevención de este suceso.

Para entender mejor este proceso es importante tener claros una serie de conceptos que explicaremos a continuación:

- Vulnerabilidades: son todas las cosas que no hemos tenido en cuenta a la hora de proteger nuestros activos, lo cual puede acarrear efectos negativos; podríamos decir que son las debilidades del sistema. Las vulnerabilidades hacen posible que las amenazas se materialicen y afecten a los activos.
- Amenazas: la amenaza informática es todo lo que puede ocasionar un daño a los activos del sistema. Las amenazas lo que hacen es aprovecharse de las vulnerabilidades del sistema y así poder tener acceso a los distintos equipos y manipularlos sin autorización. Las amenazas pueden deberse a: personas, condiciones físico-ambientales o al software. Así, pueden ser:
    - Naturales: se refiere a los fenómenos naturales, las cuales pueden producir daños si no se toman medidas para evitarlos como por ejemplo: no tener bien aislados y ventilados los cuartos donde se localizan equipos lo que conllevaría humedades y excesos de temperatura que afectarían a los sistemas.
    - Físicas: se refiere al acceso a los lugares en donde se encuentran los distintos equipos que almacenan o contienen la información. Hace referencia a la falta de control de acceso del personal y al posible robo de información mediante dispositivos de almacenamiento portátil (pen-drive).
    - Factor humano: son las más habituales y derivan por la falta de información y concienciación del personal.
    - De sistemas: englobaría hardware y software, en donde nos encontramos con errores de programación, lo que serían deficiencias en el sistema. Que son igual de importantes que un mal uso de los mismos.
- Exposición o impacto: es el daño sobre el activo derivado de la materialización de la amenaza; estos impactos pueden acarrear a la empresa pérdida de dinero, de información, de imagen (por tanto, de confianza), etc.
- Riesgo: que es la posibilidad de que ocurra un problema de forma repentina.

2.1.4 Auditoria Informática

Se trata de hacer una evaluación, de la manera más objetiva y crítica posible, con el fin de analizar y valorar como se utilizan los recursos informáticos para saber si son eficaces, eficientes y si son adecuados para la consecución de los objetivos y metas de un organismo o empresa.

El proceso de auditoria se compone de: planificación, recogida de información, evaluación y redacción del informe de auditoría; a través de este proceso nos centraríamos en la consecución de los siguientes objetivos:

- Analizar la eficacia de los sistemas de la empresa.
- Comprobar el cumplimiento de la normativa.
- Revisar que los recursos informáticos se están gestionando eficazmente.

2.2 MARCO LEGAL Y ESTÁNDARES NACIONALES E INTERNACIONALES

En este apartado hacemos una revisión de las leyes y normas en materia de seguridad de la información. Analizaremos la norma ISO 27001, que define los requisitos óptimos para elaborar un sistema de gestión de la seguridad de la información; también el Esquema Nacional de Seguridad (ENS), el cual determina las medidas a implantar para poder garantizar la seguridad en operaciones electrónicas con la administración pública. Además, revisaremos otros referentes metodológicos en seguridad y terminaremos centrándonos en la Ley Orgánica de Protección de Datos (LOPD), objeto central de este proyecto.

2.2.1 Norma ISO 27001

La norma ISO 27001, especifica qué requisitos son necesarios para implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

La norma ISO, cuyas siglas significan, International Organization for Standardization. Es una Organización Internacional de Normalización nacida tras la segunda guerra mundial, concretamente el 23 de febrero de 1974. Está formada por un conjunto de Institutos de normas nacionales correspondientes a 163 países, teniendo cada país un miembro en esta organización. Para una buena coordinación del sistema posee una sede central en Ginebra (Suiza).

Los estándares ISO son de aplicación voluntaria, ya que al ser un organismo no gubernamental no tiene autoridad legal para forzar su implantación; ésta solo recae en los distintos países, que son los únicos que pueden decidir su carácter obligatorio. ISO desarrolla estándares requeridos por el mercado, estándares que son resultado del previo consenso entre gobiernos, industrias, usuarios, etc.; por tanto ISO determina un marco mundial.

En lo que respecta a seguridad informática, hemos de centrarnos en la 27001, es un estándar que proporciona un modelo para establecer, implantar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), fue establecido en 2005 y es el único estándar aceptado internacionalmente. Cuando nos referimos a estándar, hacemos referencia a la publicación hecha por ISO en donde están detalladas las especificaciones técnicas, cuyo objetivo es ayudar a incrementar la fiabilidad de productos, materiales y en este caso servicios y procesos.

El Sistema de Gestión de Seguridad de la Información (SGSI) es el pilar sobre el que se construye la norma ISO 27001, que es un estándar certificable, lo que quiere decir que cualquier organización que lo tenga implantado podrá pedir una auditoria y así poder ser acreditada con la certificación ISO 27001. Su propósito es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados (aunque una protección total sea imposible). Su implantación formaliza y sistematiza la gestión en procedimientos escritos, instrucciones, formularios y registros que aseguran la eficiencia de la organización y su mejora progresiva.

El SGSI protege los activos de información de una organización independientemente del soporte en el que se encuentren (escritos, correo electrónico, imágenes, etc.). Su implantación y diseño depende de las necesidades concretas, los objetivos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización. La seguridad no es un producto, es un proceso; por tanto; la organización ha tenido que realizar un estudio acerca del nivel de riesgos que asume y ha tenido que implantar controles para dichos riesgos, implantando políticas y procedimientos relacionados que le lleven a la revisión y mejora del sistema de manera continua.

Tenemos que tener en cuenta que implantar un SGSI no garantiza el 100% de seguridad, pero sí proporciona innegables ventajas:

- Compromiso: El registro de las actividades permite garantizar y demostrar la eficacia de la organización en todos los niveles y así probar la diligencia razonable de sus administradores (Aspecto organizacional).

- Conformidad con requisitos legales: El registro permite observar todas las leyes y normativas aplicables al alcance (Aspecto legal).

- Gestión de los riesgos: Obtención de un mejor conocimiento de los sistemas de información (Aspecto funcional).

- Credibilidad y confianza: Clientes y usuarios se tranquilizan al constatar que una certificación brinda una diferenciación frente a la competencia (Aspecto comercial).

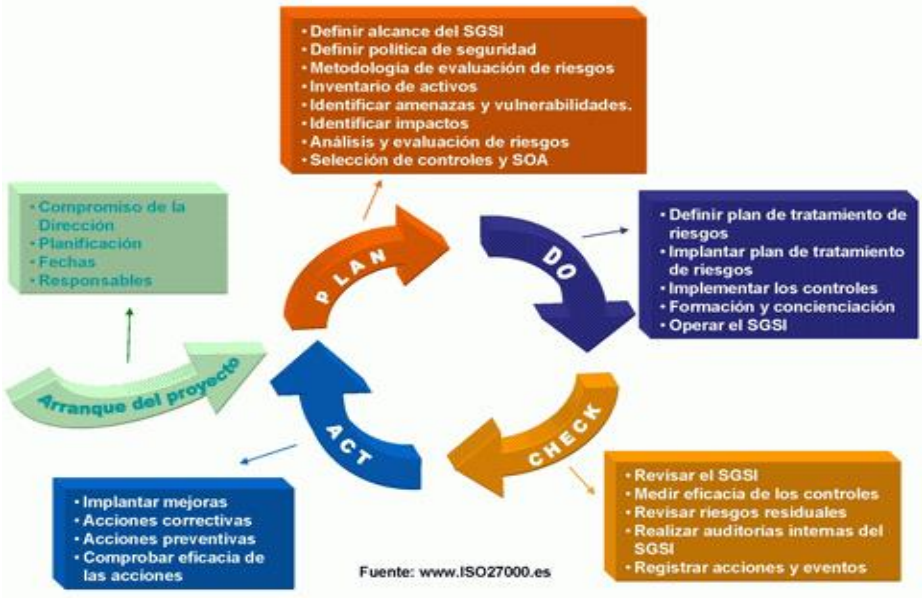
- Reducción de costes: vinculados a los incidentes y posibilidad de disminución de las primas de seguro (Aspecto financiero).

- Mejora de sensibilización del personal: hacia la seguridad y a sus responsabilidades en la organización (Aspecto humano).

El SGSI, Sistema de Gestión de la Seguridad de la Información, tiene por objeto la información, entendiendo por información todo conjunto de datos en poder de una entidad o institución que posean valor para la misma, independientemente de la manera en que se guarde o trasmita, de su origen o de su fecha de elaboración.

Para establecer un SGSI en base a la ISO 27001, se toma como modelo el ciclo continuo PDCA que es usado normalmente en los sistemas de gestión de calidad.

Figura 1. Etapas SGSI



Fuente: www.iso27000.es

Este modelo sigue una serie de etapas, relacionadas cada una con la anterior, lo cual genera un ciclo continuo que permite a las empresas establecer un modelo de calidad; en este caso nos centramos en la seguridad de la información. Las etapas son las siguientes:

1. Establecer el SGSI (Plan)

Esta etapa es fundamental; define la estructura del SGSI, valida el alcance y se elabora la documentación específica de la sección. Las especificaciones, además de ser un elemento a lograr, también son un elemento a mejorar, aunque lo mejor sería realizar rigurosamente esta etapa y evitar tener que realizar cambios. En el momento que sea posible, conviene realizar pruebas según sea requerido para probar los resultados.

2. Implementación y Operación del SGSI (Do)

Durante esta etapa se desarrollan los controles que integran la declaración de aplicabilidad (SoA: Statement of Applicability), a la par se lleva a cabo la ejecución del programa: organizar, dirigir, asignar recursos y supervisar la ejecución.

3. Monitorizar y revisar (Check)

Pasado un periodo previsto de antemano, se realizarán una serie de revisiones y auditorías al SGSI para detectar las áreas de oportunidad en la eficiencia de implantación de controles de seguridad y así poder determinar si el SGSI se está adaptando correctamente a los objetivos propuestos.

4. Mantener y Mejorar (Act)

Según se vayan obteniendo los resultados tendremos que revisar continuamente y decidir según los resultados obtenidos (Ciclo de mejora continua).

Es fundamental tener un SGSI, ya que, como hemos dicho anteriormente la información es un activo importante en una organización. Un buen sistema que preserve la confidencialidad, integridad y disponibilidad de la información ayuda a mantener los niveles de competitividad, de imagen, de cumplimiento legal y de rentabilidad que son necesarios para obtener los objetivos de la organización.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

2.2.2 Esquema Nacional de Seguridad

Con el fin de mejorar la seguridad, el Esquema Nacional de Seguridad en el Real Decreto 3/2010, de 8 de enero, regula el ámbito de la administración electrónica, tiene como objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Los objetivos del Esquema Nacional de Seguridad (ENS) son:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un tratamiento continuado de la seguridad.

El Esquema se centra en la aplicación de un conjunto de medidas de seguridad (75 controles en total) decididas en base a un Análisis de Riesgos sobre los activos y Sistemas de información relacionados con la Administración Electrónica.

Se hace una categorización de los niveles de seguridad según las dimensiones de seguridad de cada uno de los sistemas de información que forman parte del alcance. Los niveles: básico, medio y alto se calculan según el impacto en la organización.

Figura 2. Esquema Nacional de Seguridad

Fuente: www.administracionelectronica.gob.es

Según la Ley Orgánica de protección de Datos, las medidas de seguridad que una empresa debe implantar en su Sistema de Gestión de la Seguridad de la Información, son las que se explican a continuación.

Documento de Seguridad. Identificación y Autenticación:

1) Existencia de una lista actualizada de usuarios autorizados que tengan acceso autorizado al sistema de información (art.11.1 y 12.3).

2) Procedimientos de identificación y autenticación informáticos:

a) Contraseñas: procedimiento de creación, asignación, conservación y cambio periódico (art.11.2 y 11.3).

b) Identificación de usuario, de manera inequívoca y personalizada (art.18.1).

c) Limitación de acceso incorrecto reiterado (art.18.2).

Control de Acceso:

1) Los usuarios tendrán únicamente acceso a los datos/recursos de acuerdo a su puesto laboral y tareas definidas en el documento (art.12.1).

2) Deberán implantarse mecanismos que eviten el acceso no autorizado a otros recursos: establecimiento de perfiles de usuario (art.12.2).

3) Control de acceso físico a servidores y CPD (art.19).

4) De cada acceso se guardarán: identificación usuario, fecha y hora, fichero accedido, tipo de acceso y su autorización o denegación, guardando la información que permita identificar registro accedido (art.24.2).

5) Los mecanismos de acceso estarán bajo el control directo del Responsable de Seguridad, sin que pueda permitirse la desactivación (art.24.3).

6) Registro y conservación de accesos lógicos al fichero por un plazo no inferior a 2 años (art.24.4)

7) Para accesos a través de redes de telecomunicaciones, deberán tener las mismas medidas que para accesos en modo local (art.5).

Funciones y obligaciones del personal:

1) Definición en el Documento de Seguridad de las funciones y obligaciones de grupos de usuarios y/o perfiles (art.9.1).

2) Conocimiento por parte del personal de las normas y medidas de seguridad que les son aplicables (art.9.2).

3) Identificación y funciones del/los Responsables de Seguridad (art.15 y 16).

4) Trabajo fuera de ubicación principal debe ser expresamente autorizado (art.6).

5) Listado de personal con acceso a Servidores y/o CPD (art.19).

6) Listado de personal con privilegios administrativos informáticos sobre aplicaciones y ficheros (art.12.4).

Estructura de los Ficheros y del Sistema Informático:

1) Descripción y estructura informática del Fichero (campos ID)

2) Descripción y estructura del Sistema Informático (enumeración de equipos, redes, programas, etc...)

Gestión de Soportes:

1) Identificación, inventariado y almacenamiento (art.13.1).

2) Autorización necesaria para salida de soportes (art.13.2).

3) Cifrado de soportes en caso de operaciones externas de mantenimiento (art.20.4).

4) Medidas y procedimientos para la destrucción de soportes (art.20.3).

5) Registro de Entrada de Soportes (art.20.1).

6) Registro de Salida de Soportes (art.20.2).

7) Distribución de soportes con mecanismos de cifrado de datos (art.26).

Registro de Incidencias:

1) Contenido mínimo: tipo de incidencia, momento en que se produce, efectos producidos, persona que comunica, medidas adoptadas (art.10).

2) Contenido adicional: Procedimiento de restauración de datos, datos restaurados y datos grabados manualmente (art.21.1).

Procedimientos de Copias de Respaldo y Recuperación datos:

1) Deberán garantizar la restauración de los datos al momento anterior a producirse la pérdida (art.14.2).

2) Realización de copias de backup al menos con una frecuencia semanal (art.14.3).

3) Necesaria autorización para la ejecución de procedimientos de restauración de datos (art.21.2).

4) Almacenamiento externo de copias y procedimientos de restauración de datos (art.25).

Actualización y Auditoria:

1) Revisión y actualización del Documento de Seguridad en función de cambios relevantes en la Organización (art.8.3).

2) Auditoria cada 2 años. Conservación de Informe a disposición AEPD (art.17).

3) Revisión periódica de la información de control de los accesos informáticos a ficheros y aplicaciones (art.24.5).

Medidas específicas para datos en soporte papel:

1) Control de acceso a la documentación.

2) Medidas de conservación y almacenamiento.

3) Procedimientos y mecanismos de destrucción que impidan posterior recuperación de la información que contienen.

Todas estas medidas organizativas para el control de la seguridad están encaminadas a preservar las características de confidencialidad, exactitud y disponibilidad.

2.2.3 Otras normas y referencias nacionales e internacionales

Cualquier empresa puede solicitar una auditoria para obtener la certificación ISO 27001.A continuación veremos algunos ejemplos de certificaciones en seguridad de la información menos conocidas, las individuales, es decir, aquellas certificaciones a las cuales los profesionales acuden para tener una "marca" de calidad y demostrar sus conocimientos y dominios en el campo de la seguridad de la información. Estas

certificaciones son usadas por las empresas para buscar trabajadores que tienen los conocimientos necesarios para ayudarles a mejorar en el campo de la seguridad de la información y la seguridad informática.

- CISSP (Certified Information Systems Security Professional): certificación de alto nivel profesional otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc), que tiene como objetivo reconocer a los profesionales con formación en el área de seguridad de la información.
- Certified Information Systems Auditor (CISA): Certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA) (Information Systems Audit and Control Association).
- Criterios de Evaluación de Seguridad en Tecnologías de la Información (CESTI): Conjunto de criterios para evaluar la seguridad informática de productos y sistemas. El producto o sistema sometido a evaluación, denominado objetivo de evaluación (OE) es sometido a un examen detallado de sus características de seguridad, que culmina con extensas pruebas de funcionamiento y test de penetración.
- CISM (Certified Information Security Management): define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer.

En España también contamos con entidades encargadas de gestionar las certificaciones, vamos a centrarnos en La Asociación Española de Normalización y Certificación (AENOR). Es una entidad española de normalización y certificación en todos los sectores industriales y de servicios.

Es el representante de España en ISO en cuanto a su vertiente de normalización; en su vertiente de certificación opera como una empresa privada más de certificación y no tiene ninguna exclusividad sobre el resto. En materia de seguridad tiene como misión, garantizar la protección eficaz de la información empresarial y garantizar la seguridad de los sistemas de información y de los procesos informáticos.

La certificación del sistema de Gestión de Seguridad de la Información de AENOR, de acuerdo a UNE-ISO/IEC 27001, contribuye a fomentar las actividades de protección de la información en las organizaciones, mejorando su imagen y generando confianza frente a terceros. Este esquema de certificación es aplicable a cualquier tipo de organización independientemente del sector en el que actúe.

Una vez superado el proceso de auditoría, si el sistema cumple con los requisitos de la norma UNE-ISO/IEC 27001 la empresa obtendría:

- El certificado AENOR de Sistemas de gestión de Seguridad de la Información.
- El certificado IQNet, su certificado AENOR será reconocido en el ámbito internacional.
- La licencia de uso de la marca Seguridad de la Información de AENOR.

Logo de certificación ISO 27001:

Figura 3. Marca Certificación Aenor **Figura 4. Marca Certificado iQNet**

Fuente: www.aenor.es

2.2.4 Normativa en materia de protección de datos. La LOPD

El marco legal en materia de protección de datos era un tema pendiente en materia legislativa. El primer real decreto data de 1999; después de unos años de experiencia se tuvo que proceder a desarrollarla y se pasó de 29 a 158 artículos, se aclararon determinados conceptos, como por ejemplo el de actividades domésticas, se regularon los ficheros en papel (el anterior Reglamento de Desarrollo 994/1999 solo regulaba los automatizados) y se completó el conjunto de medidas de seguridad aplicables en cada caso.

Se fijó una normativa propia para ficheros de régimen electoral, datos estadísticos, registro civil, fuerzas de seguridad, etc. La ley es aplicable en el ámbito de legislación española, cuando los afectados o medios usados se hallan en territorio español.

Todo el marco legal de protección de datos esta recogido en:

- Artículo 18 de la Constitución Española.
- Directiva 95/45/CE; de protección de datos personales.
- Ley Orgánica 15/1999, de desarrollo de la Ley Orgánica 15/1999.
- Real Decreto 428/1993, Estatuto de la Agencia Española de Protección de Datos.

Los principios en los que se fundamenta la LOPD son: finalidad, exactitud, derecho al olvido, consentimiento, datos especialmente protegidos, seguridad, acceso individual y publicidad. Se trata de garantizar la calidad de los datos, derecho de información en la recogida de datos y necesidad de consentimiento del afectado, protección de datos como ideología, sindical... deber de secreto y acceso limitado por terceros. De estos principios se derivan los derechos que todo ciudadano tiene respecto a sus datos personales: los derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO).

Como hemos dicho, la ley establece una serie de medidas de seguridad, atendiendo al nivel de criticidad de la información. Las medidas de seguridad en el ámbito de las TIC son, para cada uno de los niveles de información, las siguientes:

- Nivel básico: registro de incidencias, control de acceso, identificación y autenticación, gestión de soportes y documentos, copias de seguridad. Estas medidas afectan a los datos de nivel básico como: nombre, apellidos, domicilio, teléfono y correo electrónico.
- Nivel medio: creación de un responsable de seguridad, auditorías, registro de entrada/salida de soportes, control de acceso físico, etc. Afectan a los datos de nivel intermedio como: datos financieros, infracciones administrativas e infracciones penales.
- Nivel alto: etiquetado y cifrado de soportes, cifrado de portátiles, almacenar copias de seguridad fuera de las instalaciones, telecomunicaciones cifradas, etc. Estas medidas han de aplicarse a la información más crítica como: datos sobre religión, ideología, salud y origen racial.

La Agencia de Protección de Datos es el ente de derecho público, con personalidad jurídica propia, que garantiza los derechos que emanan de la LOPD.

En el ámbito internacional, hemos de contemplar las trasferencias de datos. Una transferencia internacional de datos, es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE).

La ley contempla tanto la exportación de los datos como la importación:

- Exportación: El exportador de datos es la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero.

- Importación: es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargado del tratamiento o tercero.

Para realizar transferencias internacionales de datos, será necesaria la autorización previa de la Agencia Española de Protección de Datos. Incluso cuando el Estado en el que se encuentre el importador ofrezca un nivel de seguridad adecuado de protección, seguirá siendo necesario notificarlo al Registro General de protección de Datos. La autorización de trasferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la LOPD y en el RLOPD.

La LOPD diferencia los casos en los que la trasferencia internacional tiene como país de destino uno que proporcione un nivel de protección adecuado, de aquellos en los que no ocurra así. Algunos países que hasta la fecha tienen un nivel adecuado de protección son: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Estados Unidos.

3. CASO PRÁCTICO: Auditoría de cumplimiento de la LOPD

En este apartado nos centraremos en hacer una aplicación práctica de todo, nos planteamos realizar auditorías de cumplimiento de la LOPD en entornos profesionales, con el fin de obtener información sobre el grado de sensibilización y concienciación en lo relativo a la necesidad de hacer un tratamiento seguro, ético, legal y responsable de los datos personales. Elegimos dos entornos diferentes, que nos ofrecerán perspectivas distintas: una pequeña empresa y un organismo público.

En primer lugar diseñaremos un cuestionario que nos servirá para conocer las medidas contempladas en el tratamiento de datos personales. Para el diseño del cuestionario nos basamos en la información facilitada por la AEPD en su sitio web.

A continuación, en el punto siguiente, apoyándonos en este cuestionario, valoramos el grado de cumplimiento de la LOPD en una PYME. Y después, llevamos a cabo la evaluación de cumplimiento de la LOPD en un entorno totalmente diferente: un organismo público, el Servicio Aragonés de Salud. Será significativo el contraste de resultados.

Para terminar este apartado, como resultado del estudio, presentamos una guía que hemos elaborado para ayudar a las PYME a cumplir con lo dispuesto en la LOPD.

3.1 CUESTIONARIO SOBRE CUMPLIMIENTO DE LA LOPD

Elaboramos un cuestionario con el objetivo de poder responder a la pregunta: ¿Sabes si cumples con la normativa en materia de protección de datos personales?

Para la realización del cuestionario, nos apoyaremos en la información y recursos disponibles en el sitio web de la Agencia Española de Protección de Datos (AGPD); determinaremos cuáles son los aspectos relevantes a la hora de saber si se cumple la normativa y podemos usar una herramienta llamada “Evalúa” (también disponible en el sitio web); es un programa sencillo, anónimo y gratuito que permite a las empresas y administraciones autoevaluar el grado de cumplimiento de la Ley Orgánica de Protección de Datos (LOPD) en el ejercicio de su actividad.

Evalúa ofrece respuestas a las dudas a las que habitualmente se enfrentan quienes manejan datos personales. Consiste en un test basado en preguntas con respuesta múltiple que está accesible para cualquier usuario que lo quiera realizar. Una vez finalizado, genera un informe con indicaciones y recursos que orientan en el cumplimiento de la legislación.

Por tanto nuestro test está pensado para el usuario que toma contacto por vez primera con la LOPD y busca saber si cumple la normativa de forma sencilla.

En el cuestionario, ha de preguntarse sobre los siguientes aspectos:

- Registro de ficheros, se refiere a la obligación de registrar todo fichero de datos personales en la AEPD.
- Información y consentimiento, por parte del afectado, para el uso de sus datos personales.
- Información sobre los principios que rigen el tratamiento de los datos personales.
- Derechos ARCO (Derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento).
- Relación con terceros, en lo que se refiere a compartir datos personales (comunicaciones de datos, transferencias internacionales de datos personales...).
- Cuestiones de seguridad (documento de seguridad, medidas organizativas y técnicas, etc.).

CUESTIONARIO SOBRE EL CUMPLIMIENTO DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El objetivo que tenemos con la realización de este cuestionario sobre el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal es conocer si la entidad encuestada cumple la normativa correspondiente, además nos permite conocer qué tipo de medidas debemos de aplicar para su cumplimiento.

Fecha:.....
Empresa:.....
Auditor:.....

1. ¿Dispone su empresa de datos de carácter personal?

De acuerdo con la normativa vigente se considera dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables. Por tanto podemos considerar dato de carácter personal todo dato sobre empleados de la empresa, clientes, proveedores, colaboradores o terceros, siempre que se trate de personas físicas.

SI ☐ NO ☐

2. ¿Tiene los correspondientes ficheros dados de alta en el registro de la AEPD?

Toda persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad uso o contenido de datos de carácter personal deberá dar de alta los correspondientes ficheros en un registro de la respectiva APD (Agencia de Protección de Datos) indicando, entre otras cosas, el tipo de datos que tiene y las finalidades a los que los destina.

SI ☐ NO ☐

2.1. ¿Están los ficheros de datos convenientemente actualizados?

SI ☐ NO ☐

3. ¿Dispone la empresa de empleados?
Para una empresa, el mero hecho de tener empleados ya significa ser responsable de sus datos y a su vez ser también responsable de los datos que éstos manejen en el desarrollo de sus funciones.

SI ☐ NO ☐

3.1. ¿Les ha informado de cuáles son sus derechos LOPD?
Los empleados tienen derecho a conocer cuáles son sus derechos en relación a sus propios datos.

SI ☐ NO ☐

4. ¿Tiene datos de clientes y/o proveedores?
Si su empresa trabaja con datos de clientes y/o proveedores tiene que cumplir con numerosas medidas de seguridad con esos datos que pueden incluso ser cada vez más severas en relación con la sensibilidad de los datos tratados.

SI ☐ NO ☐

5. ¿Trabaja con terceras empresas que accedan a sus datos?
Empresas que le presten servicios que usted tenga externalizados como asesorías fiscales, laborales, jurídicas, gestorías, informáticos, empresas de limpieza , seguridad o incluso comerciales autónomos.

SI ☐ NO ☐

6. ¿Dispone de cámaras de seguridad?
Entendemos por cámaras de seguridad cualquier cámara que se encuentre ubicada en su establecimiento y trate datos.

SI ☐ NO ☐

7. ¿Dispone de ordenadores que gestionen o almacenen datos personales?
Entenderemos por ordenadores cualquier sistema o elemento que permita el tratamiento automatizado de datos de carácter personal.

SI ☐ NO ☐

8. ¿Tiene una web corporativa?
Entendemos por web corporativa cualquier portal web que, bajo la responsabilidad de la empresa, promocione o venda directamente los productos o servicios de su empresa.

SI ☐ NO ☐

9. ¿Sabría responder al ejercicio de un derecho de acceso, rectificación, cancelación u oposición por parte de algún interesado?
ualquier interesado le puede requerir para que le informe de los datos que tiene la empresa de él y la finalidad con que los trata, o para que proceda a rectificar los datos que tenga, para cancelar los datos o incluso para oponerse al tratamiento de los mismo.

SI ☐ NO ☐

10. ¿Dispone su empresa de un Documento de Seguridad actualizado?
El Documento de Seguridad es el documento principal donde se recogen las principales medidas de seguridad implantadas por cada responsable de fichero (en nuestro caso empresa).

SI ☐ NO ☐

A la vista de las respuestas obtenidas, se analizará el grado de cumplimiento (o incumplimiento) de la LOPD y se harán las recomendaciones necesarias.

3.2 VALORACIÓN DEL CUMPLIMIENTO DE LA LOPD EN UNA PEQUEÑA EMPRESA

En nuestro caso, hemos pasado el cuestionario, a una persona que, desde hace bastantes años, es el dueño de una empresa. Para salvar el anonimato de la empresa no se dará ningún nombre y nos referiremos a ella como "Empresa Max". Esta empresa maneja información personal (aunque no del máximo nivel de criticidad) y, por tanto, tiene que cumplir con la LOPD; trata con proveedores, maneja datos de empleados...

La empresa, está ubicada en un polígono de Zaragoza. El día que acudimos allí para realizar la entrevista observamos las características de las instalaciones y las medidas de seguridad. El edificio está rodeado por una valla que no es muy alta por tanto no supone un obstáculo en caso de querer acceder al recinto alguna persona ajena a la empresa; dispone de una puerta para el acceso de personal y clientes, la cual está siempre abierta y por ello, permite el acceso a cualquier persona. El personal está provisto de una tarjeta identificativa para fichar a la entrada y a la salida de su jornada; el personal únicamente administrativo no lleva ninguna tarjeta. La zona en donde están los dispositivos informáticos, se encuentra en una sala que cuenta con una sola puerta para acceder y no existe control para ello.

Así, en cuanto a la seguridad física de las instalaciones, sin entrar en una valoración exhaustiva, los primeros consejos que podríamos dar serian:

- Instalación de una valla más alta.
- Instalación de un sistema de llamada en la puerta de acceso al edifico.
- Proveer a todo el personal de una tarjeta identificativa
- Mejorar la puerta de acceso a la sala de dispositivos informáticos y establecer un control.

Centrándonos en nuestro objetivo, pasamos a valorar el cumplimiento de la LOPD a través del cuestionario que hemos elaborado. El dueño de la empresa Max realizo el cuestionario; se detectaron muchos fallos y un deficiente tratamiento de los datos personales, con incumplimiento legal. Algunos de los fallos detectados son los siguientes:

- Falta de actualización de ficheros.
- No informa a sus empleados acerca de sus derechos.
- Incorrecto tratamiento de la documentación de clientes y proveedores.
- Falta de contratos de confidencialidad con terceras empresas.
- Incumplimiento legal sobre el sistema de cámaras de seguridad.
- Actualización página web corporativa.

Después de una revisión del mismo, pasados unos días se le proporcionó un diagnóstico de actuación; teniendo en cuenta las opciones marcadas en su test le aconsejamos un servicio que incluya las siguientes actuaciones:

- Actualización de ficheros de datos ante el registro de la AEPD.
  De acuerdo con la Ley, no es suficiente tener dados de alta unos ficheros en el registro de la Agencia sino que es necesario que estos ficheros reflejen la realidad del tipo de datos manejados o tratados en cada caso. Por ello es recomendable tener una revisión periódica del tipo, nivel y clase de datos que se manejan en cada momento y dar cuenta de las posibles modificaciones ante el registro, evitando así los riesgos de sanciones por incumplimiento del principio de calidad de datos.

- Documentos y cláusulas de información de los empleados
  Toda persona de la que se tengan datos de carácter personal tiene el derecho a que se le informe, entre otras cosas, de la existencia de un fichero bajo la responsabilidad de la empresa y de la posibilidad de ejercer unos determinados derechos. Esto se puede hacer mediante distintos mecanismos como documentos informativos, contratos u otros documentos. El incumplimiento de estas obligaciones puede dar lugar a sanciones de hasta 60.000€.

- Política interna de privacidad de datos y Formación a los trabajadores sobre el tratamiento de datos
  Los empleados de una empresa pueden ser su principal fuente de problemas puesto que, ya sea por desconocimiento o por mala fe, pueden cometer infracciones con los datos que manejan, pudiendo dar lugar a sanciones para su empresa que pueden alcanzar los 600.000 €. Esto se puede evitar informando a los empleados de cuáles son las políticas de la empresa para el tratamiento de datos de carácter personal o realizando cursos de formación sobre la LOPD, para informar a los trabajadores sobre los procedimientos más apropiados para tratar datos de carácter personal.

- Cláusulas en facturas y/o en contratos, cartas informativas, contratos de tratamiento de datos, documentos para la cesión de datos, etc…
  Si se dispone de datos de carácter personal de clientes o proveedores deberán adoptarse diferentes medidas para asegurar el cumplimiento de los principios de la Ley. El incumplimiento de las preceptivas medidas de seguridad con los datos de clientes o proveedores puede dar lugar a sanciones de hasta 600.000€ por infracción cometida.

- Documentación para terceros
  De acuerdo con la normativa, cuando una empresa externa le preste servicios para los que necesite o pueda acceder a datos personales que sean responsabilidad de su empresa (como, por ejemplo, datos de sus empleados o clientes) será necesario que cumpla con numerosas medidas de seguridad, como la formalización de contratos de seguridad de datos, compromisos de confidencialidad, etc. El incumplimiento de estas formalidades no sólo le puede generar problemas a su colaborador sino también a su propia empresa.

- Documentación sobre video vigilancia
  Las videocámaras que se instalen en una empresa deberán cumplir con ciertas exigencias marcadas por la normativa. Por ejemplo, deberán inscribirse en el registro de la Agencia correspondiente, instalar unos paneles informativos e informar sobre el ejercicio de los derechos ARCO.
  El incumplimiento de estas prevenciones, además de poder significar sanciones de la AEPD, puede también ocasionar que no se puedan utilizar legalmente las imágenes obtenidas por medio de las cámaras y, por tanto, impedir que las imágenes se puedan utilizar ante un Tribunal como prueba de un eventual delito.
  La normativa establece que los datos informatizados deben seguir unas medidas específicas que garanticen la seguridad de los datos. El incumplimiento de las mismas puede dar lugar a importantes sanciones.

- Políticas de seguridad de datos, Avisos legales, Condiciones de Uso del portal, Condiciones Generales de la Contratación
  En caso que se traten datos de carácter personal en la web, por ejemplo, por medio de un formulario de contacto, el portal web deberá cumplir con unas específicas exigencias legales establecidas tanto en la Ley Orgánica de Protección de Datos (LOPD) como en la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE). El incumplimiento de cada Ley puede dar lugar a sanciones de hasta 600.000€ por infracción según el caso.

- Asesoramiento jurídico continuado
  Un asesoramiento jurídico personalizado, más allá de solucionar cualquier duda jurídica que le pudiere surgir relacionada con la protección de datos o de actualizar el estado LOPD de la empresa de acuerdo con sus necesidades y las imposiciones de la normativa, le permitiría también llevar a cabo las actuaciones oportunas respecto de cada ejercicio de derecho, evitando sanciones de hasta 300.000€ o más por infracción, que se podrían derivar de un incumplimiento o cumplimiento parcial o tardío en la respuesta del ejercicio de un derecho.

3.3 AUDITORIA DEL CUMPLIMIENTO DE LA LOPD EN EL SERVICIO ARAGONÉS DE SALUD

En este apartado hacemos una evaluación del cumplimiento de la LOPD en una institución pública; en este caso analizaremos el Servicio Aragonés de Salud (SALUD). La valoración ha sido posible gracias a que en dicho servicio nos han facilitado información para poder realizar el estudio.

Como hemos dicho, es una institución pública y además maneja datos del máximo nivel de criticidad, por tanto ha de ser estricta en el cumplimiento de la LOPD. En efecto, como ahora explicaremos, lleva a cabo un estricto control y tienen pocos fallos (y por tanto, pocas mejoras a realizar) pero algún aspecto siempre se puede mejorar. Veremos que acata una legislación europea, nacional y autonómica, la cual detallaremos y analizaremos ahora.

La legislación europea. Se trata de legislación en materia de seguridad y protección de datos aplicable en el ámbito de la Unión Europea; se compone de:

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016

La legislación Nacional. Se trata la legislación en materia de seguridad y protección de datos (en particular, en el ámbito de la salud) aplicable en el ámbito del Estado Español; se compone de:

- Ley Orgánica de Protección de Datos de Carácter Personal
- Reglamento de desarrollo de la LOPD
- Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Modificación del Esquema Nacional de Seguridad.
- Ley de Autonomía del Paciente y Documentación Clínica
- Ley de Procedimiento Administrativo Común de las AAPP

La legislación autonómica. También se contempla legislación en materia de seguridad y protección de datos aplicable en el ámbito de la comunidad autónoma de Aragón:

- Política de seguridad de las TIC del Servicio Aragonés de Salud (BOA de 14/04/2015)
- Inscripción de ficheros LOPD de 2010 del Servicio Aragonés de Salud (BOA de 02/07/2010)
- Inscripción y modificación de ficheros LOPD de 2015 del Servicio Aragonés de Salud (BOA de 18/03/2015)
- Delegación de competencia de los derechos ARCO en los Gerentes de Sector y 061 (BOA de 30/12/2016)

Para realizar el análisis he visitado la Gerencia del Servicio Aragonés de Salud, ubicado en Zaragoza en la Plaza de la Convivencia nº 2. En este edificio está la sede central de la gestión sanitaria de todos los centros sanitarios de la Comunidad Autónoma de Aragón. El edificio se compone de cinco plantas en las cuales están distribuidas la Dirección de Gerencia y las cuatro direcciones de área que son: la Dirección de Área de Coordinación Asistencial, la Dirección de Área de Coordinación Económico – Administrativa, la Dirección de Área de Recursos Humanos y la Dirección de Obras, Instalaciones y Equipamientos. También se encuentra en este edificio el Centro de Gestión Integrada de Proyectos Corporativos, que, entre las diferentes competencias que tiene, se encuentra la gestión de sistemas y tecnología de la información, proyectos de sistemas de información hospitalaria y del control y cumplimiento de toda la normativa referente a la Ley Orgánica de Protección de Datos.

La competencia de la Gerencia tiene distribuida por toda la geografía aragonesa diferentes centros de atención especializada (Hospitales, centros de especialidades médicas) y centros de atención primaria (Centros de salud); por tanto, para completar en mayor medida nuestro análisis tomaremos como ejemplo un centro de salud para ver cómo se aplican todas estas medidas.

Para acceder al edificio del Servicio Aragonés de Salud pasamos directamente a información y registro ubicado en la planta baja. Para acceder al resto de las plantas del edificio nos encontramos con una guarda de seguridad que nos pregunta acerca del propósito de nuestra visita y a qué planta nos dirigimos; esta guarda dispone a la vez de un sistema de video vigilancia para controlar los accesos a las diferentes plantas. Todos los trabajadores del edifico entran por la misma puerta de acceso que el público.

Cada trabajador tiene su ordenador personal e intransferible al cual solo se puede acceder con sus credenciales (usuario y contraseña), que le permite acceder al contenido de sus competencias y solo a ellas, siendo imposible el acceso a la información de otros departamentos dentro de la Gerencia del Servicio Aragonés de Salud. En función del cargo que cada uno tiene, puede acceder a mayor o menor información de contenidos pero siempre en función de sus competencias.

Cuando **organismos y personal externo** al Servicio Aragonés de Salud tienen que realizar actividades que requieren la conexión con los sistemas informáticos del SALUD (y acceso posterior a datos personales) deberán de firmar un Acuerdo de Confidencialidad y cumplir una serie de obligaciones establecidos en ese acuerdo. (Ver Anexo I.)

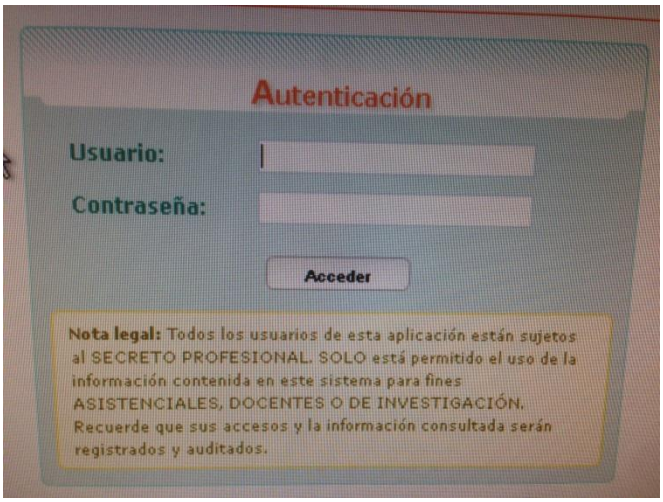
Como el Servicio Aragonés de Salud (SALUD) ostenta la responsabilidad de los ficheros, los cuales contienen datos de carácter personal de nivel alto, inscritos en la Agencia de Protección de Datos, de acuerdo a la legislación en materia de protección de datos de carácter personal, tiene que tomar medidas y pautas para llevar a cabo una protección eficaz. Entre todos los ficheros con los que trabaja, son de vital importancia los ficheros que componen la Historia Clínica Digital Única de Aragón, a los cuales

tienen acceso los diferentes profesionales que trabajan dentro de esta institución en Hospitales y Centros de Salud.

Si, analizamos el funcionamiento de cualquier Centro de Salud de la Comunidad Autónoma de Aragón podemos valorar cuáles son las medidas que llevan a cabo para conseguir la protección de datos de carácter personal.

El personal de un centro de salud consta de una serie de administrativos, los médicos y los enfermeros. Cada médico posee un usuario y una contraseña, además de una tarjeta con banda magnética cifrada y con contraseña para poder acceder a la información; todos los accesos quedan registrados para evitar que se entre a información que no sea de un paciente suyo, ya que al historial clínico de cada persona solo puede acceder su médico.

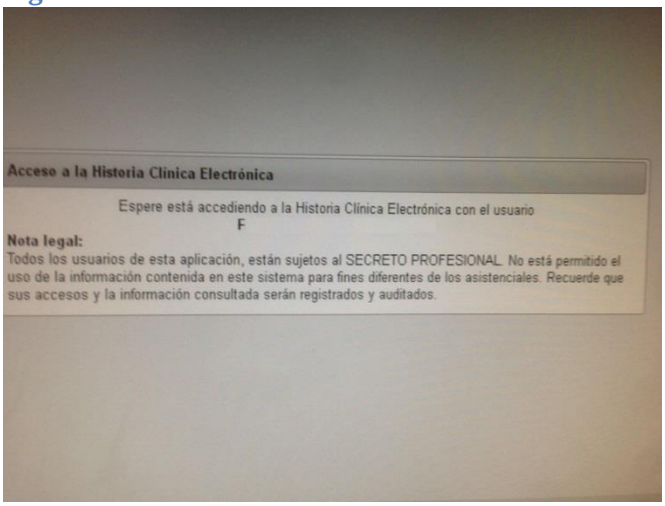
Figura 5. Autenticación intranet SALUD



Fuente: SALUD

En caso de que un médico quiera acceder a una información sobre algún paciente que esté en un hospital, debe de identificarse a través de un código.

Figura 6. Autenticación historia clínica unificada



Fuente: SALUD

De ninguna manera alguien externo puede tener acceso a la información. En cuanto a la seguridad del edificio, hay a la entrada una zona de recepción, pero, como el paso de pacientes es continuo, no se pide ninguna información; además, los dispositivos de acceso a la información están en cada despacho y éstos, si no están ocupados, están siempre cerrados con llave.

Todas estas medidas y procedimientos de seguridad se establecen en base a un comité que se compone de un mínimo de 5 hasta un máximo de 15 miembros, entre los cuales estarán incluidos presidente y secretario y vocales, designados todos ellos por la Dirección Gerencia del Servicio Aragonés de Salud entre personal facultativo y de enfermería, así como expertos en los diversos campos que atañen a la documentación clínica electrónica de los distintos sectores sanitarios. Uno de ellos deberá ser el Responsable de Seguridad TIC del Servicio Aragonés de Salud. Este comité se encarga de velar por el cumplimiento de los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos en relación sus datos personales.

Concretamente, se atribuyen al comité las siguientes funciones:

- Velar por la actualización y vigencia de la Política de Seguridad TIC.
- Aprobar y realizar el seguimiento de objetivos, iniciativas y planes estratégicos en materia de seguridad de la información.
- Elevar propuestas de revisión del marco normativo de seguridad.
- Analizar el registro de gestión de incidencias y elaborar propuestas en el uso seguro de la información.

Con todo esto y con la información recogida con el cuestionario sobre el cumplimiento de la Ley Orgánica de Protección de datos de carácter personal (que también se utilizó para recabar la información de la empresa Max), podemos decir que el Servicio Aragonés de Salud tiene inscritos y actualizados sus ficheros de datos personales; sus trabajadores están debidamente informados acerca de sus derechos LOPD; también comparte datos con terceros haciendo cumplir un acuerdo de confidencialidad; el sistema de cámaras de seguridad cumple con las normas establecidas; en cuanto a las competencias de los derechos ARCO, la Dirección Gerencia del Servicio Aragonés de Salud ha delegado dichas competencias en los Gerentes de Sector y 061 (BOA de 30/12/2016); cuenta con dotación de ordenadores y tiene su página web.

Después del análisis de todo el sistema de seguridad que tiene establecido el SALUD y de la extensa normativa en la que se basa y cumple, además de todos los controles que tiene para evitar cualquier percance, es difícil hacer recomendaciones para mejorar. Lo único que sería recomendable, es que se creara una dirección o departamento centralizado, en lugar del Comité, desde donde se llevaran todos los aspectos de seguridad.

Teniendo en cuenta toda la información anteriormente recogida tanto en la pequeña empresa como en el SALUD, podemos apreciar que en la pequeña empresa hay grandes deficiencias en el cumplimiento de la LOPD, mientras que en el Servicio Aragonés de Salud llevan un estricto cumplimiento de dicha ley.

3.4 GUÍA PRÁCTICA PARA EL CUMPLIMIENTO DE LA LOPD PARA PYMES

En este apartado presentamos una guía práctica que hemos elaborado dirigida a las PYMES para el cumplimiento de la LOPD; en particular, detallaremos la estructura y contenido que ha de tener un documento de seguridad. Las acciones que han de llevarse a cabo para cumplir con lo dispuesto en la LOPD son:

1. Inscripción/registro de los ficheros de datos personales en la AEPD. (ver modelo obtenido de la AEPD en el anexo II y III)
2. Nombrar un responsable de seguridad.
3. Elaboración de un documento de seguridad.
   Este documento es de obligado conocimiento por todo el personal que tenga acceso a los sistemas de la organización y en él se recogen las medidas, procedimientos y estándares que se deben seguir para garantizar la seguridad de la información.
4. Determinar las funciones y obligaciones del personal
   Todo el personal de la organización deberá de ser consciente de todas las medidas de seguridad establecidas para la protección de la información; será el responsable de seguridad quien las de a conocer. Todas estas medidas deberán de estar reflejadas en el documento de seguridad indicando qué funciones tiene que desemplear cada empleado; si es conveniente, se mandarán recordatorios a modo de circulares para asegurarse que todo el personal conoce todas las medidas e informando, en su caso, de cualquier modificación que hubiere.
   Cada miembro del personal que tiene acceso a los datos ha de tener asignado un perfil de usuario y una contraseña, los cuales tienen que ser confidenciales y no revelar bajo ningún concepto para evitar que personal ajeno a la organización tenga acceso a la información; además los empleados que manejen información de carácter personal tienen el deber de guardar la confidencialidad. También dispondrán de procedimientos para notificar cualquier incidencia o fallo que descubran.
   En caso de que no cumplan sus obligaciones, la AEPD podrá aplicar sanciones según el grado de incumplimiento, que pueden ser infracciones leves, graves o muy graves.
5. Notificar, gestionar y solucionar incidencias
   Toda incidencia, entendiendo como tal cualquier incumplimiento de las normas establecidas en el documento de seguridad o cualquier tipo de anomalía que se pueda dar en la información de carácter personal, deberán de ser notificadas y gestionadas; además se deberá de crear un registro en el que se anoten todas ellas.

Una vez que la incidencia es detectada, debe de ser notificada al director de la organización a través del responsable de seguridad del fichero en el que se ha producido la incidencia. El responsable del fichero deberá de crear un registro para notificar el tipo de incidencia, qué efectos se han derivado de dicha incidencia y qué tipo de medidas se han utilizado para corregirlas.
Habrá que indicar dónde se han producido las incidencias y la hora y fecha; también será necesario indicar quien ha realizado el proceso, qué datos han sido restaurados y qué datos se han tenido que grabar manualmente durante el proceso de recuperación.

6. Revisión del documento de seguridad
   El documento de seguridad deberá de ser actualizado en todo momento y revisado. El documento se tendrá que adaptar a los cambios normativos que pueda realizar la LOPD.

A continuación explicamos la estructura y contenido que ha de tener el documento de seguridad; en él se detallan una serie de medidas, normas y procedimientos para manipular de forma segura los datos de carácter personal. Para detallar la estructura de dicho documento y el contenido que debe de tener hemos tomado como referencia la guía de seguridad de la Agencia Española de Protección de Datos.

1. Ámbito de aplicación
   Todas las medidas, normativas y procedimientos deberán de aplicarse a los ficheros que contengan datos de carácter personal; además también habrá que aplicarlas a los sistemas de información, equipos y soportes utilizados para el tratamiento de dicha información.
2. Asignar el responsable de seguridad y sus funciones
   La asignación de un responsable de seguridad es fundamental, sobre esta persona recaerá la responsabilidad sobre los ficheros y tratamientos de los mismos, además de decidir acerca de la finalidad, contenido y tratamiento de los mismos. Si hay más de un responsable de seguridad habrá que indicar quién se encarga de cada fichero. Se detallarán cuáles son las funciones que tiene que realizar cada responsable de seguridad para garantizar el cumplimiento de la ley.
   Sus obligaciones son:
   - Notificar al Registro General de protección de datos la existencia de los distintos ficheros para luego llevar a cabo su inscripción.
   - Garantizar que los datos se han tenido forma lícita y legítimamente y, además, están siendo utilizados para los fines que fueron recabados.
   - Deberán informar a las personas afectadas por datos de carácter personal recogidos.
   - Cuando se comparta información con terceros deben de garantizar el cumplimiento de la normativa de la LOPD.

3. Medidas de identificación y autentificación
   Para el tratamiento de datos personales las medidas de identificación y autentificación son muy importantes; para la identificación se utilizará un nombre de usuario y la autentificación se llevará a cabo por contraseñas que serán asignadas de manera aleatoria; las contraseñas, para que sean lo más seguras posibles, deberán estas formadas por minúsculas, mayúsculas, números y caracteres especiales. La contraseña se deberá de renovar cada cierto tiempo para garantizar una mayor seguridad.
4. Control de acceso
   Los responsables de los ficheros deberán de fijar una serie de medidas y procedimientos para que únicamente puedan acceder a los datos el personal autorizado para ello; además deberá de tener un lista con los usuarios y perfiles en donde figure también los accesos autorizados para cada uno de ellos.
5. Registro de accesos
   Para garantizar una mayor seguridad se deberá de tener un sistema en donde queden reflejados todos los accesos realizados, con su fecha y hora, y contar con un responsable que se encargue de revisar esa información al menos una vez al mes.
6. Gestión de soportes y documentos
   Los soportes y documentos en donde haya información de carácter personal deberán facilitar la identificación de la información que contienen; además, deberán de ser inventariados y a éstos solo podrán tener acceso aquellas personas que se encuentren autorizadas.
7. Control de acceso físico
   Los equipos físicos que dan soporte a los sistemas de información deberán de encontrarse en habitaciones cerradas con llave y a las que solo tendrá acceso el personal autorizado; en caso de que una persona ajena quiera acceder deberá de notificarlo al responsable de seguridad y éste realizar un registro de la hora de entrada y de salida y el día, por si ocurriera alguna incidencia.
8. Acceso a través de redes de comunicación
   En función del nivel de criticidad de los datos, cuando se trasmitan datos de carácter personal mediante redes inalámbricas o públicas, se deberá de llevar a cabo un cifrado de los datos para que su visualización no sea tan fácil.
9. Utilización de ficheros fuera de su localización habitual
   El responsable de seguridad será el encargado de dar la autorización para que se lleve a cabo el almacenamiento de datos en dispositivos portátiles o el tratamiento de estos fuera de las instalaciones y además deberá de realizar un registro de periodo, fecha, día y hora en la que se ha realizado.
10. Traslado de documentación.
    En caso de que la documentación debiera de ser trasladada, se deberá de contar con una serie de medidas para evitar su visualización o robo; deberá de ir en carpetas con tapas opacas y con gomas; en caso de que la información sea de nivel alto, deberá de ser trasportada en vehículos pertenecientes a la organización y son sistema GPS.

11. Realización de copias de seguridad y recuperación
    Deberá de haber un responsable que se encargue de realizar copia de todos los datos así como de los procedimientos que se utilicen en la recuperación; las copias deberán de encontrarse en un lugar distinto de donde se encuentren los equipos informáticos.
12. Realización de copias de trabajo de documentos o ficheros temporales
    Aunque dichos documentos o ficheros sean para su utilización en un periodo determinado, también será necesario aplicar las medidas de seguridad que establece la LOPD; una vez finalice su periodo de uso, deberán de ser eliminados.
13. Realización de copia o reproducción de documentos
    Esto solo podrá realizarse bajo el control y la supervisión del personal que está autorizado para ello.

Para terminar, a modo de resumen, presentamos en la siguiente tabla los pasos que cualquier empresa debe de seguir para dar cumplimiento a lo dispuesto en la LOPD:

Figura 7. Guía cumplimiento de la LOPD

PASOS PARA CUMLIR LA LOPD
1. Inscripción/registro de los ficheros de datos personales en la AEPD.
2. Nombrar un responsable de seguridad.
3. Elaboración de un documento de seguridad. ▪ Determinar el ámbito de aplicación ▪ Determinar el responsable de seguridad ▪ Aplicar medidas de identificación y autentificación ▪ Controlar los accesos ▪ Registrar los accesos ▪ Gestionar los soportes y documentos ▪ Controlar el acceso físico ▪ Acceso de datos a través de redes de comunicación ▪ Utilización de ficheros fuera de su localización habitual ▪ Traslado de documentación ▪ Realizar copias de respaldo y recuperación ▪ Realizar copias de trabajo de documentos ▪ Realizar copia o reproducción de documentos
4. Determinar las funciones y obligaciones del personal
5. Notificar, gestionar y solucionar incidencias
6. Revisión del documento de seguridad

4. CONCLUSIONES

- El activo más importante de una organización es la información que posee; por ello invertir en seguridad es imprescindible.
- Es importante que todos nos concienciemos de la importancia de realizar nuestras operaciones de manera online de forma segura para evitar riesgos innecesarios.
- Toda empresa que maneje y trate con información personal debe aplicar la normativa de protección de datos personales; la LOPD es de obligado cumplimiento para toda empresa que maneje datos personales.
- La implantación de un sistema de seguridad de la información y gestionarlo de manera adecuada es la mejor forma de garantizar la seguridad de la información.
- Es necesario que cada organización disponga de un documento de seguridad, en donde se detalle las distintos procedimientos de seguridad que se deben aplicar a los diferentes niveles de datos.
- Sobre la LOPD todavía hay mucho desconocimiento, y muchas empresas, sobre todo PYMES no la cumplen.
- El cumplimiento de la LOPD en grandes empresas y en organismos públicos es mucho mayor. En particular, en el SALUD (objeto de una parte de nuestro estudio) el grado de seguridad es alto (nuestros datos están bien protegidos).
- La tecnología es muy reciente y la sociedad no es plenamente consciente de los peligros que puede generar el uso “no seguro” de los datos.
- Todo el mundo debería de tener un mínimo de conocimientos acerca de la seguridad y protección de datos para evitar incidencias, sobre todo las empresas.
- Las certificaciones en ISO 27001, van en aumento. Para obtenerla es necesario pasar una auditoria que garantice que se dispone de un buen Sistema de Gestión de Seguridad de la Información (SGSI).

5. BIBLIOGRAFÍA

Estudio sobre la privacidad de los datos personales y la seguridad de la información online. Agencia Española de Protección de Datos. http://www.agpd.es. [Fecha de consulta: 6 de diciembre de 2016]. Disponible en: https://observatorio.iti.upv.es/media/managed_files/2009/02/13/estudio_intecoaepd_privacidad_redes_sociales_def.pdf

Privacidad y protección de datos. Gobierno de España. https://www.cnig.es. [Fecha de consulta: 7 de diciembre de 2016]. Disponible en: https://www.cnig.es/proteccionDatos.do

ISO 27001.El portal de ISO 27001 en español. http://www.iso27000.es. [Fecha de consulta: 10 de diciembre de 2016]. Disponible en: http://www.iso27000.es/sgsi.html

Transferencias internacionales de datos. Agencia Española de Protección de Datos. http://www.agpd.es. [Fecha de consulta: 10 de diciembre de 2016]. Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

Guía del responsable de ficheros. Agencia Española de Protección de Datos. http://www.agpd.es [Fecha de consulta: 11 de diciembre de 2016]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

Guía de seguridad. Agencia Española de Protección de Datos. http://www.agpd.es [Fecha de consulta: 20 de diciembre de 2016].Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

Guía de seguridad de datos. Agencia Española de Protección de Datos. http://www.agpd.es [Fecha de consulta: 21 de diciembre de 2016]. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema nacional de Seguridad en el ámbito de la Administración Electrónica. http:/www.boe.es. [Fecha de consulta: 4 de enero de 2017]. Disponible en: https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

Esquema nacional de Seguridad. Gobierno de España. https://administracionelectronica.gob.es. [Fecha de consulta: 4 de enero de 2017]. Disponible en: https://administracionelectronica.gob.es/ctt/ens#.WKBpJFXhDDd

Orden de 16 de marzo de 2015, del consejo de Sanidad, Bienestar Social y Familia, por la que se aprueba la política de seguridad de las Tecnologías de la Información y la Comunicación en el Servicio Aragonés de Salud y se crean el Comité de seguridad de la información y la figura del Responsable de seguridad. http:/www.boa.aragon.es. [Fecha de consulta: 7 de enero de 2017]. Disponible en:
http://www.boa.aragon.es/cgi-bin/EBOA/BRSCGI?CMD=VEROBJ&MLKOB=848345964545

Publicado el decreto que regula la estructura orgánica del Departamento de sanidad y del Servicio Aragonés de Salud. Gobierno de España. https://www.cnig.es. [Fecha de consulta: 5 de enero de 2017]. Disponible en:
http://aragonhoy.aragon.es/index.php/mod.noticias/mem.detalle/area.1020/id.175543

6. ANEXOS

ANEXO I

GOBIERNO DE ARAGON
Departamento de Sanidad

salud
servicio aragonés de salud
Centro de Gestión Integrada de Proyectos Corporativos

ACUERDO DE CONFIDENCIALIDAD

20 de enero de 2017

El Servicio Aragonés de Salud, en adelante SALUD, ostenta la responsabilidad de los ficheros que componen la Historia Clínica Digital Única de Aragón, los cuales contienen datos de carácter personal de nivel alto inscritos en la Agencia de Protección de Datos, de acuerdo a la legislación en materia de protección de datos de carácter personal.

Conforme a las exigencias contenidas en la legislación en materia de protección de datos de carácter personal, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, es preceptiva la celebración de un convenio regulador del acceso a datos de carácter personal para su tratamiento posterior por personal externo a SALUD, no constituyendo este supuesto comunicación de datos conforme a la citada Ley.

De acuerdo a la exigencia establecida en el punto anterior y en virtud del acuerdo existente entre el Departamento de Sanidad, el SALUD y el INSS para la explotación de la información clínica por parte de los **MÉDICOS INSPECTORES DE LA ADMINISTRACIÓN DE LA SEGURIDAD SOCIAL**, el firmante declara que realiza actividades que requieren la conexión con los sistemas informáticos del SALUD y acceso posterior a datos personales, obteniendo por ello la condición de tercer encargado del tratamiento de los datos personales contenidos en los ficheros propiedad del Servicio Aragonés de Salud, exigiéndosele por ello las siguientes

OBLIGACIONES

1.- El abajo firmante se compromete a tratar dichos datos personales observando los principios exigibles por la legislación en materia de protección de datos, en particular los relativos a la calidad y seguridad de los datos y al deber de secreto.

2.- El firmante se compromete a tratar dichos datos conforme a las concretas instrucciones recibidas del Centro de Gestión Integrada de Proyectos Corporativos del SALUD, no aplicando o utilizando dichos datos con finalidades distintas a las especificadas.

3.- El firmante se compromete a observar el secreto profesional respecto de los datos personales objeto de tratamiento, manteniendo absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento de los servicios prestados, no comunicando a ningún tercero, ni siquiera para su conservación, los datos facilitados por el SALUD como responsable del fichero. Esta obligación subsistirá aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

4.- En el supuesto de que el firmante, destine los datos a finalidad distinta de la estipulada, los comunique o utilice incumpliendo las instrucciones fijadas en el presente contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido.

5.- Como encargado del tratamiento, el firmante se compromete a la observancia de las medidas de seguridad correspondientes al tratamiento de los datos personales del SALUD a los que tiene acceso, de acuerdo al nivel de protección que corresponda a los datos facilitados establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal o en cualquier otra norma que lo sustituya.

6.- El firmante se compromete a, una vez cumplida la prestación asociada al acuerdo, devolver al Centro de Gestión Integrada de Proyectos Corporativos del SALUD los datos objeto de tratamiento, soportes o documentos en que estos consten, así como a destruir aquellos según las instrucciones del responsable de tratamiento.

7.- El firmante se compromete a, una vez cumplida la prestación asociada al acuerdo, informar al Centro de Gestión Integrada de Proyectos Corporativos del SALUD para que este proceda a eliminar cualquier posibilidad de acceso a los datos por parte del mismo.

En prueba de conformidad, se suscribe de mutuo acuerdo el presente documento en la fecha indicada en su encabezamiento.

Como responsable del fichero,
EL DIRECTOR GERENTE
DEL SERVICIO ARAGONÉS DE SALUD,

Fdo.: D.

Como responsable del acceso y tratamiento de datos personales,

Fdo.: _____

NIF: _____

Mail: _____

ANEXO II

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad privada
SOLICITUD DE INSCRIPCIÓN

NOTIFICACIONES TELEMÁTICAS A LA AEPD

Tipo de solicitud

1 Inscripción de creación de fichero o tratamiento C
0 Inscripción de modificación de fichero M
0 Inscripción de supresión de ficheros S

Código Inscripción

Datos de registo de entrada (A consignar en la Agencia Española de Protección de Datos).

Soporte de la solicitud y modo de presentación

Número de envío B0000000011c2012120828

0 **Persona física que actúa en representación del responsable del fichero ante la AEPD**

Datos del responsable del fichero (del Apartado 1)

Razón Social o Nombre y Apellidos

CIF/NIF

Declarante

Nombre | Primer Apellido | Segundo Apellido

NIF | Cargo o condición del firmante en relación con el responsable del fichero

Dirección a efectos de notificación

Apellidos y Nombre o Razón Social

Dirección postal

Localidad | Código Postal | Provincia | País

Teléfono | Fax | Correo electrónico

Medio de notificación | Dirección electrónica servicio Notificaciones

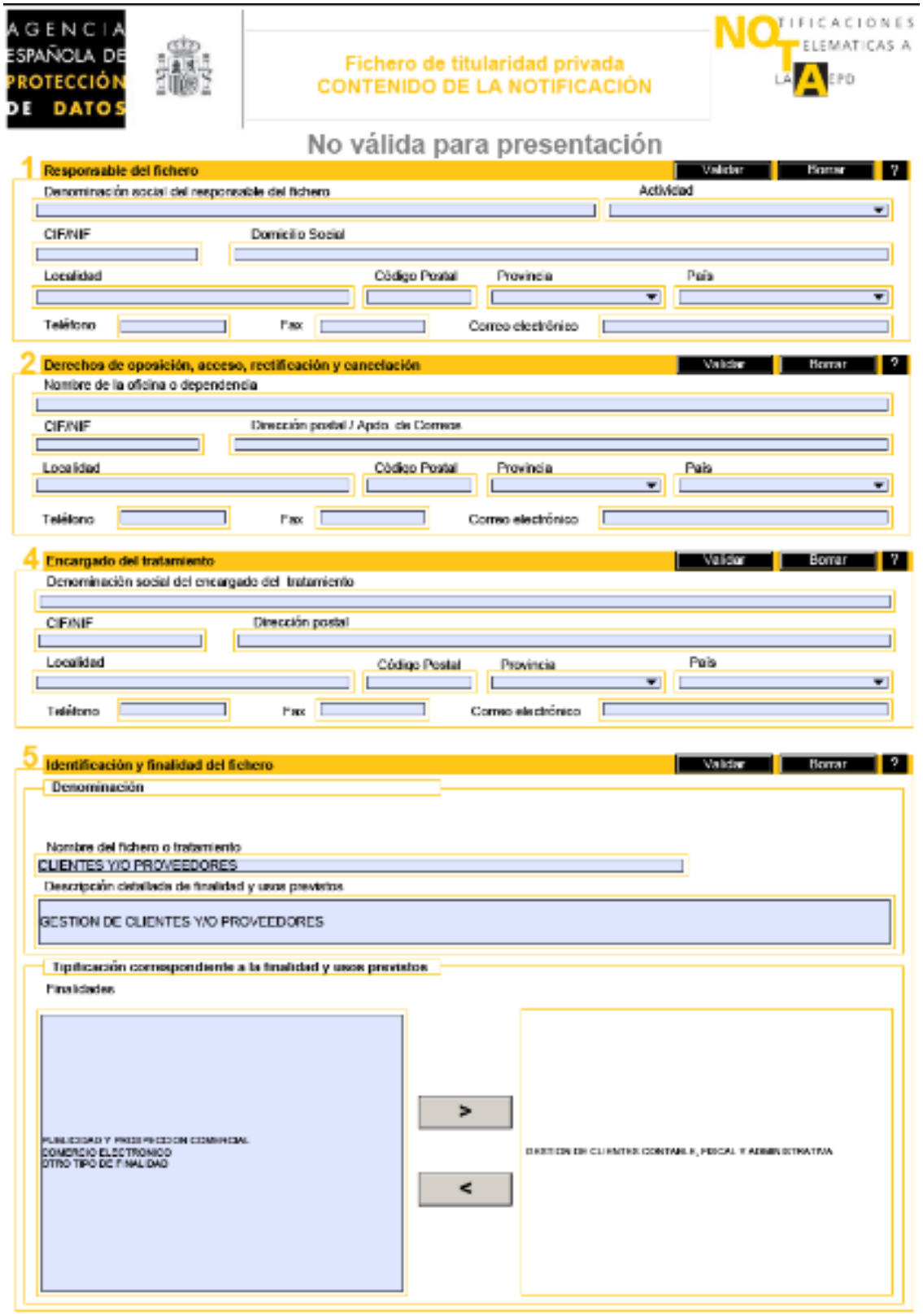
De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, solicito la inscripción en el Registro General de Protección de Datos de los ficheros de datos de carácter personal descritos en el formulario de notificación adjunto. Así mismo, bajo mi responsabilidad manifiesto que dispongo de representación suficiente para solicitar la inscripción de estos ficheros en nombre del responsable del fichero y que éste está informado del resto de obligaciones que se derivan de la LOPD. Asimismo, declaro que todos los datos consignados son ciertos y que el responsable del fichero ha sido informado de los supuestos legales que habilitan el tratamiento de datos especialmente protegidos, así como la cesión y la transferencia internacional de datos.

La Agencia Española de Protección de Datos podrá requerir que se acredite la representación de la persona que formula la presente notificación.

En a de de Firma de la persona que efectúa la notificación

Conocimiento de los deberes del declarante

ANEXO III


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÒN
NOTIFICACIONES TELEMATICAS A LA AEPD
No válida para presentación
1 Responsable del fichero
Validar
Borrar
Denominación social del responsable del fichero
Actividad
CIF/NIF
Domicilio Social
Localidad
Código Postal
Provincia
País
Teléfono
Fax
Correo electrónico
2 Derechos de oposición, acceso, rectificación y cancelación
Nombre de la oficina o dependencia
Dirección postal / Apdo. de Correos
4 Encargado del tratamiento
Denominación social del encargado del tratamiento
Dirección postal
5 Identificación y finalidad del fichero
Denominación
Nombre del fichero o tratamiento
CLIENTES Y/O PROVEEDORES
Descripción detallada de finalidad y usos previstos
GESTION DE CLIENTES Y/O PROVEEDORES
Tipificación correspondiente a la finalidad y usos previstos
Finalidades
PUBLICIDAD Y PROSPECCION COMERCIAL
COMERCIO ELECTRONICO
OTRO TIPO DE FINALIDAD
>
<
GESTION DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA