Departamento de Informática

PROYECTO FIN DE CARRERA

De la teoría a la práctica en el cumplimiento de la LOPD y en el desarrollo de la seguridad

Autor: Jorge Delgado Espino
Tutor: Miguel Ángel Ramos

Leganés, Julio de 2012

Título: De la teoría a la práctica en el cumplimiento de la LOPD y en el desarrollo de la Seguridad.
Autor: Jorge Delgado Espino
Director: Miguel Angel Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día _26_ de ____Julio___ de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Somos la suma de los momentos que
hemos experimentado, con cada una
de las personas que hemos conocido…

Por lo que a todos vosotros, GRACIAS.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

1. Introducción

La seguridad de la información es algo fundamental que ninguna empresa debe llegar a descuidar.

Cuando fui becario y luego trabajador de una gran empresa privada de este país, me concienciaron mucho desde el primer día de lo que era la seguridad, y de cómo llevarla a cabo en el día a día.

Con Seguridad de la Información no nos referimos únicamente, como la mayor parte de la gente piensa, a tener un buen antivirus instalado en nuestro ordenador. Para preservar la seguridad y confidencialidad de los datos hay que tener en cuenta muchísimas más cosas, tales como el soporte donde se encuentra esa información, las medidas de seguridad que lo rodean, las personas con acceso a esa información sensible, el tratamiento que se le da, etc… sin olvidarnos nunca, de la forma en la que destruiremos dicha información llegado el momento, pues no nos vale con arrojar un montón de documentos a la papelera, existen métodos y dispositivos específicos para destruir esta información.

A raíz de todo esto, surgió la idea y la necesidad de escribir este proyecto de fin de carrera sobre la Seguridad en los Sistemas de Información, donde se recojan y detallen todos los pasos y pautas mínimos a seguir por las empresas para dar un correcto tratamiento de lo que denominamos como información sensible, centrándonos sobre todo en los datos de carácter personal. Dicho datos vienen amparados por la ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal (en adelante LOPD), la cual usaremos como base para este documento, aparte de otros tantos reglamentos y normas universales (ISO).

Por lo que analizaremos los conceptos de seguridad de la información, sus tipos, como abordarla y como protegerla y preservarla. Estudiaremos las leyes que nos afectan, las ISO's que intervienen y de qué manera; así como también, analizaremos los casos en los que nos encontramos con una mala seguridad y algunos ejemplos de proyectos donde se alcanza una seguridad mínima recomendable.

Vamos a ver a continuación un pequeño resumen sobre los distintos puntos que vamos a tratar a continuación:

- ¿Qué es la Seguridad?

  Primeramente, en este apartado, definiremos qué es lo que estamos pretendiendo proteger cuando hablamos de seguridad. Así también, definiremos aquí lo que entendemos como seguridad de los sistemas de información, dentro del amplio concepto de lo que es seguridad; incluyendo un par de definiciones específicas; así como, objetivos y alcances.

- Tipos de Seguridad

  Estudiaremos los diferentes tipos de seguridad existentes destacando sobre todo aquellos usados para potenciar la seguridad en los sistemas de información de las empresas, y centrándonos en los sistemas que se encargan del tratamiento de los datos de carácter personal.

- Datos personales.

  Intentaremos ver aquí lo que se entiende por datos personal, y las distintas formas en las que se recogen y tratan, así como los derechos que nos asisten.

- ¿Por qué es necesaria la seguridad en los Sistemas de Información?

La información es un activo muy importante para cualquier empresa u organización. Definir, lograr y mantener la seguridad de la información puede ser esencial para mantener una ventaja competitiva y así que la empresa pueda alcanzar una posición mucho más destacada dentro del mercado.

- Amenazas a la Seguridad

Las organizaciones enfrentan amenazas de seguridad de un amplio rango de fuentes, de ahí la necesidad de intentar conocerlas todas y así, llegar a prevenirlas y evitarlas.

Existen diversos tipos de amenazas a la seguridad, dependiendo de su origen, su actuación o su importancia. En este apartado trataremos de dar una pincelada sobre las más importantes y que así el lector coja unas nociones básicas sobre todo lo que se puede encontrar. Siempre centrándonos en las relativas al tratamiento de los datos de carácter personal.

- Ámbitos donde se aplica

La seguridad la podemos aplicar a distintos sistemas de información y en distintos ámbitos empresariales, y no todos ellos tienen porque ser informáticos. En este punto trataremos la seguridad en los Sistemas Informáticos (cifradores de datos, firmas electrónicas, autenticación mediante tarjetas o claves,…) no sólo como meras herramientas informáticas, también como protocolos que nos ayuden a una buena gestión para mantener dicha seguridad.

Además trataremos la seguridad en los sistemas audiovisuales (grabación mediante cámaras de seguridad o grabación de llamadas telefónicas) y la seguridad en los archivos físicos (control de accesos y

la correcta destrucción de los documentos), teniendo siempre presente las leyes, RD, ISO's y normas que los rigen.

- Aspectos jurídicos y legislación vigente

Analizaremos 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, en especial el Título VIII así como alguna ISO de la familia de las 27000, las cuales forman el sistema especializado para la estandarización mundial sobre la seguridad de la información.

- Casos

En este apartado analizaremos algunos casos de ejemplos de lo que sería una mala seguridad en los sistemas de información, indicando los puntos fuertes y los no tan fuertes, que hayan sido elegidos para gestionar dicha seguridad en ese ámbito empresarial. Así también, indicaremos las medidas básicas necesarias que debería tomar cualquier empresa para estar mínimamente protegida contra intrusiones y otro tipo de amenazas a la seguridad de sus datos.

2. Objetivo y alcance

La información es, a día de hoy, uno de los activos más preciados de los que disponemos, de ahí la importancia de protegerla y conservarla.

La verdad es que estamos en un mundo en constante evolución donde las tecnologías nunca dejan de sorprendernos y avanzar, sobre todo las tecnologías de la información. Esto conlleva un desarrollo de nuevas herramientas tanto para vulnerar la seguridad de los sistemas de información, como para avanzar en la protección de los mismos.

Un sistema que durante un año es óptimo, al siguiente puede quedarse completamente obsoleto, ampliando así las probabilidades a exponernos a un riesgo innecesario para la seguridad. Por todo esto, es preciso estar reciclándonos constantemente e ir revisando y avanzando en los distintos métodos que se desarrollan para preservar la seguridad de los sistemas de las organizaciones; y con ello, mantener la ventaja competitiva que el año anterior tenía la empresa en el mercado.

Mi principal motivación para la realización de este proyecto fue mi propia experiencia personal y profesional. En los primeros meses de mi vida laboral, todo el mundo me decía: -*Tienes que hacer esto, pero cuidado que esta información es muy sensible*.- o – *Ten cuidado con estos datos, y si te los piden nunca los des pues va en contra de la ley de protección de datos de carácter personal*.- Todo el mundo te contaba cosas, pero nadie se detenía ni diez minutos a explicarte el porqué se hacía así, o qué conllevaba el no hacerlo de esa manera. Todo eran reglas o protocolos que los trabajadores habían ido aprendiendo con el paso de los años, pero nadie se las explicaba a los trabajadores noveles, pues o no le daban la suficiente

importancia, o había gente que las daba por hecho, como si eso fuera parte del *know-how* de tu trabajo.

Debido a esta falta de información, o falta de organización en algunos ámbitos empresariales, es de donde nació mi interés por desarrollar este proyecto. Un documento donde poder encontrar las políticas, leyes y códigos de buenas conductas sobre seguridad donde se enmarcan las medidas de actuación, así como las normas o consejos mínimos que cualquier empresa debería seguir para estar protegidos y tener una buena seguridad en sus sistemas de información. También analizaremos las acciones a realizar por los responsables de su desarrollo, implantación y gestión, tales como el análisis de los posibles riesgos y resultados de futuras auditorías. Sobre todo preservando la seguridad de los datos haciendo hincapié en aquellos de carácter personal, comprobando así, si los distintos sistemas cumplen con el rendimiento esperado para las empresas.

Cabe recordar también que esta necesidad de una guía donde se recopile toda esta información, viene reflejada por el Consejo Superior de Administración Electrónica:

"Es necesaria la existencia de un conjunto articulado, sistemático, estructurado, coherente y lo más completo posible de normas que sirvan de vocabulario y lenguaje común, de unificación de criterios, de modelo, especificación y guía para su uso repetido que permitan satisfacer las necesidades y expectativas de la sociedad en materia de construcción, mantenimiento y mejora de la seguridad de la información y de los sistemas que la soportan, aportando a la vez racionalización, disminución de costes, mejoras en competitividad y calidad e incluso nuevas oportunidades." [NSTI]

Destacaremos que no existe un modelo único estándar de seguridad, éste variará en función del tamaño de la empresa o entidad, del volumen y tipo de recursos que posea, de los Activos a proteger y del nivel tecnológico que poseamos; pues no son iguales las medidas de seguridad que debería adoptar una PYME (Pequeña y Mediana Empresa), a las que puede adoptar una gran empresa de nivel nacional.

3. ¿Qué es la seguridad?

Antes de meternos a fondo con lo que es la seguridad intentemos definirla; explicaremos brevemente qué es lo que pretendemos proteger en las empresas, cuál es el activo sobre el que recae casi todo el esfuerzo.

Como ya hemos dicho anteriormente (y repetiremos bastante a lo largo de esta memoria), la información es uno de los activos más preciados de los que disponemos, no sólo en el ámbito laboral (empresas o administraciones públicas) sino también en el social, pues hoy en día nos encontramos en la **Sociedad de la Información**; de ahí la importancia de protegerla y conservarla.

Podemos clasificar la información en tres categorías diferentes, en función de los tipos de persona que tengan acceso a ese activo:

- Información de tipo *pública*: Este tipo de información se encuentra al alcance de todo el mundo. No suele tratar ningún tema crítico, pues es accesible a toda persona, interna o ajena a la organización. Un buen ejemplo sería Internet, un volumen de información altísimo al alcance de cualquiera.

- Información de tipo *interna*: Esta información se distribuye únicamente entre el personal de la empresa. Suele ser un tipo de información más sensible. Entre este tipo de información se encuentran los datos de carácter personal. Este tipo de información puede verse reflejado en las Intranets de las empresas, en correos internos o también en los boletines de cada organización.

- Información de tipo *confidencial*: Información que no puede ser divulgada a individuos no autorizados, pues podría causar un impacto muy negativo en la institución. Dentro de este tipo de información están las claves privadas, información de áreas de negocios, datos económicos, decisiones estratégicas, datos personales relativos a la salud de empleados, pacientes de un hospital, etc.…

Toda la información puede llegar a ser sensible en función del ámbito empresarial donde se trate, en especial los Datos de carácter personal. Por ejemplo, los datos que nosotros podamos facilitar o que posea el banco, puede que no nos interese dárselos a nuestra compañía de gas, o que estos sean conocidos por cualquier persona con acceso a Internet, o mismamente que una persona de la empresa tenga acceso a esa información, cuando en verdad no le concierne en absoluto.

Debido a toda esta cantidad de información que está circulando existen leyes que nos amparan y protegen nuestros datos personales. En especial, la **LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**, cuyo artículo 1 (objeto) define concretamente el alcance y propósito de la misma.

"*Articulo 1. Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar." [LOPD]

Pero, ¿qué entendemos por dato de carácter personal? La ley de protección de datos nos define en su Artículo 3, los datos de carácter personal como "*cualquier información concerniente a personas físicas identificadas o identificables*." [LOPD]

Esta ley, también recoge que todos estos datos deben almacenarse en un fichero (*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*, [LOPD]) y bajo la custodia de un responsable del fichero o tratamiento (*persona física o jurídica, de naturaleza pública o privada. u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*, [LOPD]), de tal forma que, según el Artículo 10 de la ley antes citada, se preserve el deber de secreto tanto del responsable del fichero como de todo aquel que intervenga en el tratamiento de dicha información, incluso después de que termine la relación con el titular del mismo.

Tras esta breve introducción sobre qué es lo que queremos proteger, comenzaremos a hablar sobre la seguridad, y comenzaremos con alguna definición que se nos ajuste mejor, pues la verdad es que existen mil y una definiciones distintas de Seguridad. A continuación, vamos a ver un par de ellas:

Según la RAE: "*Cualidad de seguro o la calidad de estar libre y a cubierto de todo riesgo*".

Según la Wikipedia: "*Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien*".

Según Alegsa (un portal de Internet, informática y tecnologías de la información) se define la seguridad cómo: "*La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios."* [ALEG]

El estándar internacional nos da otra definición de lo que podemos entender por seguridad de la información: "*La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales*." [ISO27002]

Como bien hemos visto por estas definiciones, podríamos extraer nuestra propia definición de lo que entendemos por Seguridad, que sería como: **LA CAPACIDAD DE ESTAR SEGURO Y PROTEGIDO DE TODO RIESGO.**

Aunque la verdad es que la seguridad absoluta es imposible de alcanzar, pues no existe un sistema informático que sea cien por cien seguro. Pero hoy en día está tan desarrollado el tema de la seguridad en las empresas, que prácticamente podemos hablar de entornos seguros.

Los principales **objetivos de la seguridad** de la información se centran en el mantenimiento de las tres siguientes características que vamos a enumerar:

- ***Confidencialidad, integridad y disponibilidad***.

A continuación vamos a explicarlas brevemente.

Confidencialidad: se trata de proteger la información de ser leída o copiada por personas no autorizadas.

Integridad: se trata de proteger la información de ser modificada o borrada, sin autorización expresa del autor o del responsable de ella. Pues hay amenazas a la seguridad que no sólo se encargan de destruir la información. Muchas veces, alterar dicho activo puede ser más dañino que su mera destrucción.

Disponibilidad: toda información debe estar disponible en todo momento para las personas autorizadas. Disponer de la información, pero no poder acceder a ella en un momento concreto, es algo contraproducente.

En definitiva, la seguridad de la información debe encargarse de velar para que dicha información sólo sea accesible por aquellos usuarios que

estén autorizados, que sea una representación fiel de la realidad y que esté disponible para su uso.

En función de estas tres características principales que componen la seguridad podemos identificar las siguientes posibles amenazas o riesgos:

Posibles Amenazas en función de las características			
	Confidencialidad	**Integridad**	**Disponibilidad**
Hardware			*Robo de equipos o eliminación de los servicios.*
Software	*Realización de copias no autorizadas.*	*Alteración de un dato o programa propiciando que falle.*	*Negación de acceso o eliminación de programas.*
Archivos	*Acceso a datos no autorizados.*	*Modificación de archivos.*	*Eliminación de archivo.*
Comunicaciones	*Lectura de mensajes privados.*	*Mensajes modificados o retardados.*	*Eliminación de mensajes.*

Tabla 1. Amenazas en función de las características

4.¿Por qué es necesaria la Seguridad en los SI?

Ésta es una pregunta típica que se nos puede plantear en varias ocasiones a lo largo de nuestra carrera profesional. En la constitución del año 1978 se establece en su artículo 18.4 que: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*" [CONST]

En la mayoría de empresas u organizaciones nos solemos encontrar, como regla general, que exista un único Sistema de Información, aunque en algunos casos de organizaciones muy grandes también nos encontramos con distintos sistemas auxiliares pero con conexiones al sistema básico.

Este sistema, será uno de los pilares fundamentales de nuestra entidad, pues la estructura de datos de la empresa es un fiel reflejo de la actividad de negocio de la misma, de ahí que sea responsabilidad de la alta dirección el dar las directrices oportunas para preservar su seguridad e integridad.

Esto último viene especificado en el Artículo 79, del Título VIII, del Real Decreto 1720/2007 (es el reglamento de desarrollo de la LOPD), el cual nos dice: "*Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.*". [RD1720]

Es muy importante la implantación de las oportunas medidas de seguridad, pues como vemos, la ley hace responsable al que sea el responsable del fichero o del tratamiento y al posible encargado del tratamiento del fichero de implantar las medidas correspondientes de seguridad que la garanticen.

Al tratar la información como un activo valioso, muchas veces no sólo tenemos que preocuparnos por ataques externos, sino también por los internos. Una de las causas más comunes suelen ser los empleados desleales que pueden intentar hacerse con dicha información sensible para venderla o utilizarla en contra de los interesados, para lo cual suelen existir en las empresas los contratos de confidencialidad, que obliga a los trabajadores, aparte de al responsable del fichero, a guardar el deber de secreto, deber que también viene recogido en el Artículo 10 de la Ley Orgánica de Protección de Datos de Carácter Personal [LOPD].

> *"Artículo 10. Deber de secreto.*
>
> *El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

La LOPD obliga a las empresas a custodiar y proteger de manera que no pueda ser consultada ni accedida por terceros no autorizados a tal fin. Es importante considerar también, que la ley no hace distinción entre pequeñas y grandes empresas, por muy pequeña empresa que seamos, si almacenamos datos personales de manera incorrecta o los usamos para un fin distinto para el que se recopilaron también estamos infligiendo la ley. Y es que debemos recordar, que el desconocimiento de una ley, no exime de su cumplimiento.

Para mantener la seguridad se elaborará un documento donde se recojan todas las medidas adoptadas y a seguir por los empleados, dicho documento será redactado por el responsable del fichero y será de obligado cumplimiento para todos lo que tengan contacto con el Sistema de información. Esto lo podemos ver reflejado en el Artículo 88 del RD 1720/2007.

"Artículo 88. El documento de seguridad.

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

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión, y respuesta antes las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de

la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenido en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de Diciembre, con especificación de los ficheros o tratamientos afectados.
En tal caso, se entenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal."

5. ¿Qué es un Dato Personal?

En la sociedad actual, para cualquier tipo de actividad, nos solicitan información. Cada vez que abrimos una cuenta en un banco, reservamos un vuelo, o simplemente participamos en un concurso estamos dando nuestros datos personales. El nombre, los apellidos, el teléfono, el correo electrónico, la dirección, el DNI, la matrícula de nuestro coche, todos esos datos que estamos acostumbrados a facilitar a diario sin la mayor importancia constituyen una información muy valiosa, pues permiten identificar, tanto directa como indirectamente, a una persona.

Hay que ser conscientes de que toda esa cantidad de información es capaz de decir mucho acerca de nosotros; nuestros gustos, capacidades, habilidades, aficiones, nuestro historial clínico, las redes sociales, hasta una simple imagen puede considerarse dato personal (pues en determinados contestos permite la identificación parcial o total de la persona); con lo cual debemos ser celosos de ella.

A toda esa cantidad de información es a la que se le denomina ***DATO PERSONAL***, por lo que todas las medidas de seguridad vendrán encaminadas a protegerlos y salvaguardarlos.

5.1. ¿Cómo se recogen los Datos?

Para que se puedan empezar a tratar los datos, previamente se necesita haberlos recogido. Lo que puede hacerse de varias formas:

- Por escrito: Cuando rellenamos un parte de alta, una suscripción o cualquier otro impreso de solicitud estamos entregando una serie de datos para identificarnos.
- De palabra: Cuando hacemos una portabilidad mediante vía telefónica, o si confirmamos el borrador de la declaración de la renta a través del teléfono, estamos entregando una serie de datos para nuestra identificación.
- Vías alternativas: Podemos llegar a considerar también la recogida de datos a través de Internet o mediante videocámaras de seguridad.

En cualquier caso, cada vez que se produce una recogida de datos, el afectado tiene como derecho, y el responsable de la recogida como obligación, el informar y solicitar el consentimiento.

Derecho de información: Toda persona, de la cual se recojan los datos, tiene el derecho de saber cómo y para qué serán usados dichos datos. En el caso de que dicha recogida de datos, no se llevase a cabo directamente de la persona, el responsable del fichero dispondrá de un período no superior a tres meses para comunicárselo. La Ley de Protección de Datos, en su artículo 5, establece:

> "*Artículo 5. Derecho de información en la recogida de datos.*
> *1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

…"

Derecho de Consentimiento: En determinadas excepciones, la ley exime de necesitar el consentimiento del afectado para la recogida de datos (tipo Administraciones públicas, cuando se refieran a las partes de un contrato laboral, cuando dichos datos figuren en fuentes de acceso públicas, etc.), para el resto de casos es **obligatorio** dicho consentimiento, lo que viene expresado en el artículo 6 de la misma ley.

"Artículo 6. Consentimiento del afectado.
1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

…"

5.2. Tratamiento de los Datos

Después de la recogida de datos por parte de la empresa, entidad o responsable del fichero, está su posterior tratamiento e informatización (en el caso de que se incluyan en un fichero informático para su automatización).

Para un correcto tratamiento de los datos dentro de las entidades, deben cumplirse tres principios o requisitos mínimos: Calidad, Seguridad y Secreto. Procederemos a explicarlos a continuación uno a uno.

- Calidad: Para un correcto funcionamiento de todo el sistema, se presupone la calidad y exactitud en los datos, ya que muchas veces determinadas decisiones dependen de dichos datos (la concesión de una beca, una notificación a nuestro domicilio, etc.).

El Artículo 4 de la LOPD, establece que los datos de carácter personal serán lo más exacto posibles y se mantendrán actualizados, de forma que reflejen siempre la situación actual del afectado. En el caso de que se sepa que los datos son inexactos o falsos, deberán cancelarse de inmediato.

Otro apartado del mismo artículo, y en relación con este principio de calidad, establece que los datos deberán de ser cancelados cuando hayan dejado de ser necesarios o haya terminado la finalidad con la que fueron recabados.

- Seguridad: Este principio es uno de los más importantes, y es al que dedicaremos más páginas de este documento.

  La seguridad de los datos, y por ende del fichero, recaerá sobre el responsable del fichero; el cual, tendrá la obligación de tomar las medidas necesarias para protegerlo y evitar un mal uso, así como todas las personas que tengan acceso al mismo.

  Dentro de la Ley Orgánica de Protección de Datos, se establece su artículo 9 dedicado a la seguridad. El cual citamos a continuación:

  "Artículo 9. 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.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley. "

- Secreto: Obviamente al existir el derecho a la protección de datos, debe existir también la obligación al secreto. Este deber, afecta a las personas con acceso a la información, y viene recogido en el Artículo 10 de la LOPD.

  "Artículo 10. Deber de secreto.

  El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

  Es por esto, que muchas veces cuando llamamos a determinados servicios telefónicos, como el 1004, te suelen preguntar el DNI o algún otro tipo de dato para probar la identidad de la persona que realiza la llamada, o por ejemplo, que no nos den información sobre una persona mayor de edad, aunque sea familiar directo nuestro, a no ser que aportemos algún documento donde expresamente nos haya dado representación."

Cuando la empresa tiene contratados los servicios de una gestoría u otro tercero, y hay necesidad de que se le transfieran algunos datos para su tratamiento, es importante que el afectado otorgue también su consentimiento para este fin. Es importante recordar que el consentimiento que se facilita es revocable, así como que si queremos ceder nuestros datos para alguna otra finalidad, la casilla que aparece en los contratos debe de estar claramente visible y no venir premarcada.

Cabe también mencionar que a la hora de tratar los datos de los menores de edad, existe una normativa totalmente ajena a la LOPD, la cual viene recogida en la Ley Orgánica 1/1996, de 15 de Enero, de Protección Jurídica del Menor. Que en tema de protección de datos se aplica el Artículo 13.

> *"Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.*
> *1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*
> *2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.*
> *3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.*
> *4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la*

autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."

5.3. Derechos que nos asisten

Como usuarios afectados por el tratamiento de datos nos asisten una serie de derechos amparados por la ley, conocidos como los derechos ARCO, que son los derechos de Acceso, Rectificación, Cancelación y Oposición a los datos recabados.

Los conocidos como derechos ARCO son los que conforman el derecho fundamental a la protección de datos. Mediante estos derechos, el afectado podrá ejercer un control sobre el tratamiento que reciben sus datos de carácter personal. Ninguno de estos cuatro derechos se puede denegar, y en caso de que así pasase, se puede invocar la tutela de la Agencia Española de Protección de Datos.

El ejercicio de estos derechos ha de ser sencillo, gratuito, personal e instransferible, y debe ser ejercitado directamente por la persona afectada, acreditando su identidad mediante su DNI correspondiente.

- Derecho de ACCESO: Este derecho nos permite acceder de forma gratuita a nuestros datos sometidos a tratamiento. Aunque sólo podrá ser ejercitado a intervalos de 12 meses como mínimo, salvo justificación explícita. No debe de existir más de un mes, desde que se solicita el acceso hasta que se recibe respuesta por parte del responsable del fichero.

- Derecho de RECTIFICACIÓN: Previamente se supone que ha debido de haber un acceso, tras el cual, se solicita rectificar un dato para que así esté actualizado por si se necesitase. En la solicitud de rectificación, deberá indicarse qué dato se desea actualizar y la acreditación que lo justifique. Se

deberá dar contestación en el plazo máximo de 10 días por parte del responsable.

- Derecho de CANCELACIÓN: Este derecho permite al afectado cancelar los datos o suprimirlos, de manera que no sean accesibles ni aptos para su tratamiento, a excepción de las Administraciones públicas y Tribunales. Transcurrido el plazo legal deberá procederse a la supresión de los datos. Al igual que en el caso anterior, una vez presentada la solicitud, deberá de obtener respuesta el afectado en el plazo máximo de 10 días.

- Derecho de OPOSICIÓN: Nos permite mostrar nuestra oposición en el caso de que no queramos que nuestros datos sean tratados ni mostrados de forma pública. La diferencia es que la oposición no necesita motivo alguno, basta con que manifestemos nuestro derecho a oponernos para que así nuestros datos no sean tratados.

6. Amenazas a la Seguridad

La tecnología avanza a un ritmo asombroso. Estos avances no sólo se notan en los sistemas informáticos o en el desarrollo de medidas de seguridad, también se notan en el desarrollo de las amenazas y riesgos que la intentan vulnerar.

Definimos riesgo como un *evento que en caso de ocurrir, tiene consecuencias o impacta en los proyectos de forma negativa*.

La mayoría de las amenazas se centran en recabar información, ya sea en forma de datos personales o económicos, pero un tipo de información muy sensible. Y es que ya lo dice un refrán: "*La información es poder.*" Y en determinadas manos, algunas informaciones pueden resultar muy destructivas. De ahí, la creciente ola de intentos de asaltar los sistemas para hacerse con información, que al que la sustraiga le conferirá un poder que en otras ocasiones no debería tener.

Según los laboratorios Kaspersky en el año 2009 casi 7 de cada 10 empresas sufrían algún tipo de ataque informático. Si según el INE hay en España más 3 millones de empresas/empresarios, esto supone más de 2 millones de ataques. Entre los más frecuentes en las PYMES son: la denegación de servicios (89,9%), los virus del tipo troyano (77,3), la recepción de correo no deseado o spam (58,7%), otros virus informáticos (42,7), la instalación de software espía (19,5%), las intrusiones remotas en el ordenador (13,4%) y las intrusiones en el correo electrónico (9,7%).

Este incremento de los ataques, lleva cada vez más a las empresas a adoptar las medidas de seguridad necesarias para proteger los datos más sensibles de que dispongan, en concreto los datos de carácter personal.

Debido a todas estas amenazas emergentes o evolucionadas, surge la creciente necesidad de intentar conocerlas todas y así poder evitarlas, o por lo menos, poner los medios para que su impacto sea minimizado.

Podemos clasificar las amenazas en función de su origen:

6.1. Amenazas accidentales

Son aquellas amenazas que se producen de manera espontánea. Son buenos ejemplos de este tipo de amenazas los errores humanos, los fallos en equipos, las radiaciones electromagnéticas, etc.…

Algunos de estos tipos de amenazas se pueden llegan a prever y así prevenir, pero hay algunos otros para los que no se puede estar preparado.

6.1.1. Errores humanos

Las más frecuentes suelen ser las amenazas por los errores humanos. Esto es debido a la gran implicación de las personas en el desarrollo, vida y mantenimiento de los productos informáticos. Por eso debemos ser conscientes de que inducido o fortuitamente el hombre se convierte en la principal amenaza de un sistema informático, al tener la capacidad de desencadenar acciones peligrosas contra el mismo.

La mayoría de estas acciones o amenazas desarrolladas por las personas pueden llegar a ser previstas, pero hay algunos accidentes, como son el caso de unos tropiezos, caídas, que se derrame un vaso con agua sobre un soporte informático, etc…. para los que nunca se está prevenido, por lo que pueden causar un gran daño al sistema.

6.1.2. Fallos de tensión

Otro tipo bastante habitual son los fallos o cortes de tensión, los cuales pueden ser debidos a fallos en el suministro eléctrico, y como consecuencia de la tensión nula (0 Voltios) en un período de tiempo prolongado, las consecuencias pueden llegar a ser desde pérdidas de datos parciales o totales hasta problemas en unidades de discos, pasando incluso por los problemas de impresión. [LANI]

6.1.3. Amenazas electromagnéticas

Y por último, aunque ya menos frecuentes, son las amenazas de tipo electromagnético, ya que pueden ser producidas por imanes, transmisores o radares.

Debemos recordar, que todo equipo informático, ya sea un ordenador, un sistema de seguridad o cualquier otro equipo tecnológico, emite una radiación al exterior. Todas estas fuentes de fuerzas electromagnéticas pueden provocar daños en equipos contiguos e incluso, en cintas magnéticas, pueden llegar a borrar todos los datos grabados.

La mejor medida de prevención para locales y espacios cerrados es el apantallamiento mediante malla metálica.

6.2. Amenazas naturales

Este tipo de amenazas también son espontáneas, pero se suelen dar a causa de fenómenos naturales. En función de las características geográficas y climáticas de cada país, habrá algunas que afecten más que otras. En el caso particular de España (la Península Ibérica) el orden en que los fenómenos naturales nos afectan son agua, fuego y calor y después los terremotos.

6.2.1. Agua

Cabe destacar que cada vez el agua está cogiendo más importancia si cabe, pues no sólo nos afecta que la Península Ibérica esté rodeada por agua en casi su totalidad, sino también nos influyen los períodos de lluvias, vapores de agua y otros tipos de factores debidos al clima mediterráneo.

Esta amenaza natural puede tener impacto tanto en sistemas informáticos, ya sean ordenadores y todo tipo de tecnología, como en el caso de ficheros físicos, pues el papel en conjunción con agua puede llegar a deteriorarse e incluso destruirse.

Para poder evitar cualquier problema de filtraciones o humedades la mejor solución pasa por una buena impermeabilización (en cuanto a equipos eléctricos). La humedad afecta menos a los archivos físicos pero en cambio, estos se ven más afectados por los problemas del agua a gran escala, tales como las inundaciones o lluvias torrenciales.

La principal medida que se puede adoptar en estos casos es de prevención y se trata de elegir bien la ubicación donde situar nuestra

instalación/empresa, pues no será igual situarnos en un clima seco que en un lugar donde las precipitaciones anuales superen la media nacional.

6.2.2. Fuego

Al contrario que el agua, el fuego y el calor están cada vez perdiendo importancia debido a las medidas antiincendios desarrolladas y a los ventiladores que ya incorporan todas las instalaciones y equipos, así como los climatizadores que se encuentran en casi todos los lugares, pues cada vez se hacen equipos más resistentes a altas temperaturas.

El fuego es una de las amenazas más destructivas, pues arrasa todo a su paso, tanto equipos eléctricos como archivos físicos o de papel. En el caso de que se produzca algún tipo de incendio la mejor medida de actuación para evitar sus consecuencias sería el uso de algún tipo de material ignífugo, que no emita gases tóxicos y así no alimentar más ese fuego, pues una vez que el fuego se haya iniciado, destruirá todo allá por donde pase.

6.2.3. Terremotos

España por suerte no es centro de mucha actividad sísmica. Los últimos grandes terremotos de gran escala, y cuyos impactos se pueden apreciar aún, son los ocurridos en la localidad murciana de Lorca y el de la isla de El Hierro.

Todos los datos de estos últimos terremotos y de otros muchos movimientos sísmicos de menos importancia, e incluso las zonas más propensas a sufrirlos, pueden consultarse en el Instituto Geográfico

Nacional [IGN], para así poder evitar aquellas zonas donde la probabilidad sea más alta, y no localizar allí nuestro centro de procesos, debido al alto riesgo que esto nos supondría.

A continuación mostramos datos del Instituto Geográfico Nacional [IGN], donde se pueden apreciar los últimos terremotos acaecidos en la Península Ibérica. Aunque debido a su baja intensidad, la mayoría han sido imperceptibles.

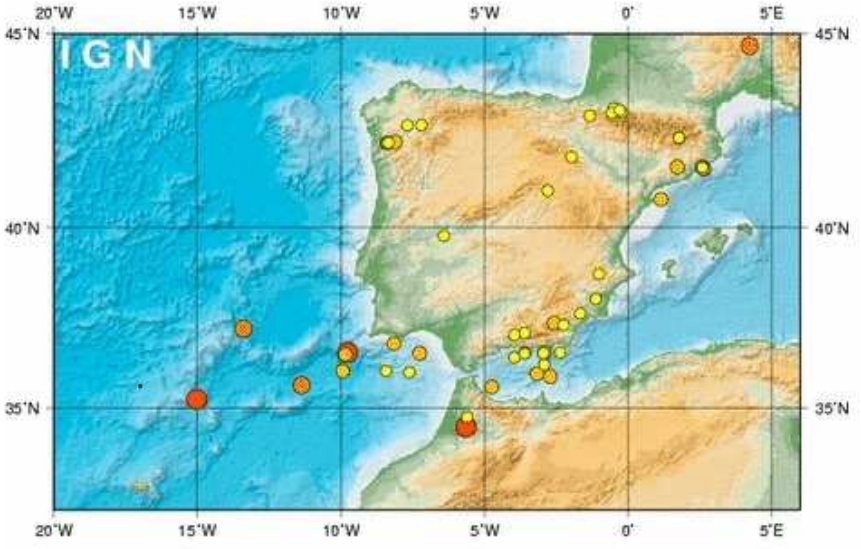


Figura 1. Últimos terremotos en la Península Ibérica.

6.3. Amenazas deliberadas o intencionadas

Son aquellas que se producen deliberadamente. Últimamente estas amenazas son las que están ganando más importancia en el mundo tecnológico. A su vez las podemos subdividir en amenazas pasivas y amenazas activas.

6.3.1. Amenazas pasivas

Son aquellas amenazas que no alteran la información, sino que únicamente escuchan, monitorizan o leen los archivos o las comunicaciones para obtener la información. Su objetivo es la intercepción de los datos que se estén transmitiendo, por lo que mayoritariamente atentan contra la confidencialidad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Dentro de las amenazas pasivas disponemos de dos tipos, las que divulgan el mensaje y las que analizan el tráfico.

Las amenazas que divulgan el mensaje o revelan contenidos son de las más comprensibles. Esto es debido al tipo de información sensible que puede ser divulgada a través de un correo electrónico, un mensaje o una simple llamada telefónica.

Las amenazas que analizan el tráfico son menos comprensibles, pues ya no se encargan de obtener la información intercambiada ya que ésta puede venir cifrada, de lo que se encargan es de su estudio. Al comprender las características de los mensajes intercambiados, tipo de frecuencia, longitud de los mensajes, localización de las máquinas, etc., se puede adivinar la índole de la comunicación que está teniendo lugar.

6.3.2. Amenazas activas

Este tipo de amenazas son más fáciles de detectar que las pasivas, pues tienen un objetivo, alterar y corromper la información. Esto pasa cuando una entidad no autorizada no sólo consigue acceder a un recurso, sino que también es capaz de manipularlo. Este tipo de ataques vulneran la propiedad de integridad. Ejemplos de estos ataques pueden ser el cambio de datos en un fichero, alterar los parámetros de un programa para que funcione de forma diferente o cambiar el contenido de un mensaje que esté siendo enviado a través de la red.

Las amenazas activas las podríamos subdividir en tres grandes grupos, las que alteran el flujo de mensajes, las que privan del servicio y las de suplantación.

La alteración del flujo de mensajes sólo significa que se altera una porción del mensaje original o que se retrasan o reordenan los mensajes.

La privación del servicio supone un uso anormal de los sistemas, pues se puede hasta llegar a impedir la comunicación entre origen y destino. Se podría dar el caso también de privar directamente de toda comunicación a una red, sobrecargándola con mensajes que inhabiliten la comunicación.

Por último, la suplantación es una amenaza que tiene como objetivo fingir que se es una entidad distinta de la original. Este tipo de ataques, por norma general, suele incluir algún tipo de las otras amenazas activas ya vistas.

El objetivo de la detección de este tipo de amenazas es contribuir también a su corrección.

6.3.3. Riesgos a los que estamos expuestos

Al igual que antes hemos comentado que no existe la seguridad absoluta, pues es imposible alcanzar, también es imposible eliminar todo riesgo, ya que siempre quedará un riesgo de tipo residual, al que estaremos expuestos.

En este punto estudiaremos los distintos riesgos a los que están expuestos nuestros sistemas. Entre ellos tenemos a las personas que los llevan a cabo como son los hackers, crackers, phreacker, y entre los programas que aprovechan las vulnerabilidades de los sistemas tenemos los virus, retro virus, hoax, gusanos, troyanos y otro tipo de fraudes, sabotajes y hurtos derivados de las amenazas anteriores.

Identificaremos una a una para saber a qué nos estamos refiriendo:

- Hacker: este término se utiliza para definir a toda persona apasionada de la informática, las cuales disfrutan accediendo, o intentando acceder, a otros ordenadores, burlando las medidas de seguridad de los sistemas; cuanto más difícil y más complejo sea el acceso, mayor será el reto. La finalidad de los Hackers es la diversión, por lo que una vez conseguido el acceso a un determinado sistema, suelen comunicárselo a la persona correspondiente para que den el aviso y así, puedan mejorar el sistema de seguridad correspondiente y conseguir un mayor reto.

- Cracker: Son personas que rompen las medidas de seguridad de los sistemas, pero con el objetivo de lograr un fin ilícito, suelen tener ideales políticos o filosóficos muy fuertes y son por los que se mueven. En algunos casos también les puede mover la arrogancia, el orgullo o incluso la ambición. Los cracker suelen investigar sobre la persona o empresa que se proponen crackear, y para averiguar claves u otro tipo de palabras claves suelen utilizar palabras muy cercanas (nombre, apellidos, nombre de la mascota, matrículas de coches, fechas de nacimiento), de ahí la importancia de elegir una clave difícil de averiguar.

- Phreacker: las personas denominadas con esta palabra, son aquellas que se sirven de los dispositivos informáticos para sondear y ejercer un control sobre los sistemas telefónicos. Aunque este tipo de atacantes cada vez tienen menos campo de acción, ya que las compañías telefónicas iniciaron el cambio desde los sistemas electromecánicos a los sistemas digitales.

- Virus: Son una combinación explosiva de gusanos, caballos de Troya, bombas lógicas, etc.… Este tipo de amenaza suele ser la más destructiva, pues al entrar en un sistema su misión es la de propagarse a otro equipos y ejecutar las funciones para las que fue diseñado (ralentización, destrucción y apagado del sistema).

- Retro virus: Este tipo específico de virus permanece en el sistema buscando fallos en el antivirus y así, poder destruirlos desde el interior.

- Hoax: No son virus propiamente dichos, puesto que no causan daños reales en el sistema. Son bulos y bromas más o menos pesadas que circulan por Internet. El perjuicio que causan es el tiempo invertido en ellos.

- Gusanos: Worm (en inglés), son un tipo de programas que se reproducen a sí mismos. Su objetivo no es producir un efecto destructivo ni atacar al sistema o a la organización, sino colapsar el ancho de banda. Suelen acompañar a un correo malicioso y tienen la capacidad de enviarse automáticamente a todos los contactos del programa gestor de correo.

- Caballo de Troya: Este tipo de programas pertenecen ocultos en el sistema. Al igual que los gusanos, no suelen producir un efecto destructivo, su objetivo es todo lo contrario, mientras permanecen en el sistema ocultos van recopilando información (passwords y otro tipo de datos personales), que envían a otro terminal. Esta es de las mayores amenazas que tienen los datos de carácter personal y la LOPD intenta regular para que la empresa se haga responsable de lo que pueda ocurrir con los ficheros.

- De los intrusos que podrían acceder a nuestro ordenador tenemos 3 tipos distintos:

  - Intruso enmascarado: Individuo que penetra en los controles de acceso para aprovecharse de la cuenta de un usuario legítimo.
  - Intruso clandestino: Aquel que sobrepasa los controles del sistema y consigue evitar la auditoría y el registro de datos de acceso.
  - Intruso transgresor: Usuario legítimo que accede a datos para los cuales no tiene autorizado el acceso, o utiliza sus privilegios de forma maliciosa.

7. Gestión de Riesgos

Debido al creciente número de amenazas que cada vez acechan más a nuestras empresas, entidades y organismos, cada vez se hace más necesario e importante un plan de gestión de riesgos, lo cual se ha convertido ya en parte integrante del sistema.

La ISO 27005 *(ISO/IEC 27005:2008 Information technology, Security techniques, Information security risk management*) sobre tecnologías de la Información, técnicas de seguridad y gestión del riesgo de la seguridad de la información, nos proporciona un marco bastante normalizado a la hora de gestionar los riesgos y las formas de actuación.

En este apartado trataremos pues de dar un enfoque sobre la gestión del riesgo, para lo cual empezaremos definiéndolo.

Entendemos la **Gestión de Riesgos** como el conjunto de procesos para identificar, analizar y responder a los riesgos, maximizando resultados positivos y minimizando consecuencias negativas.

Tras lo cual, buscaremos alguna definición sobre lo que se entiende por riesgo.

Según la RAE se define riesgo como: "*Contingencia o proximidad de un daño*".

Según la Wikipedia: "*posibilidad de daño*".

Según DefiniciónABC [DEFI]: *"Amenaza concreta de daño que yace sobre nosotros en cada momento y segundos de nuestras vidas, pero que puede materializarse en algún momento o no"*.

Aunque la definición que hace la Wikipedia llega a ser escueta y bastante precisa, intentaremos concretarla un poco más diciendo que el riesgo es *todo evento que en caso de ocurrir, tiene consecuencias o impacta en los proyectos de forma negativa*.

Para saber adoptar las medidas de seguridad necesarias, la gestión de riesgos parte de unos resultados, obtenidos previamente en un análisis para elegir, instrumentar y mantener las medidas oportunas. Este análisis de riesgos, permite identificar cuales son las mayores vulnerabilidades que tiene nuestra organización.

Con este análisis, el responsable de la seguridad ya puede llegar a considerar y evaluar qué medidas implementar, o a cuales hay que dar una mayor prioridad que a otras. Desarrollando así un plan de contingencia que defina las acciones a realizar, recursos y personal a emplear en caso de que se produzca un acontecimiento intencionado o accidental que inutilice y degrade los recursos informáticos o de transmisión de datos en una organización.

Después de esta aplicación, será necesario un control continuo o revisión, proceso por el cual verificaremos continuamente que las medidas adoptadas para la gestión del riesgo estén dando los resultados esperados.

Lo primero de todo entonces será aprender a considerar algo como riesgo, para lo cual podemos utilizar el siguiente diagrama de flujo obtenido de unos apuntes de la Carlos III, a través del cual podemos llegar a concluir si es un riesgo o no:

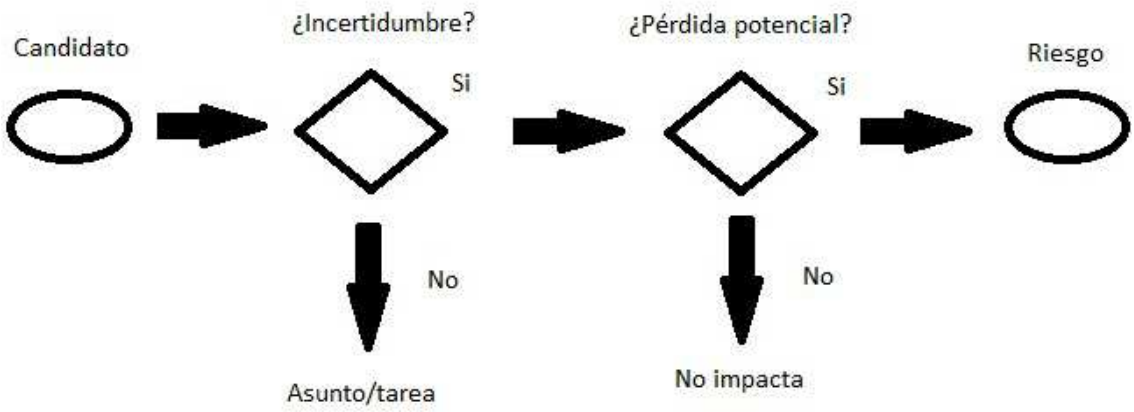


Figura 2. Consideración de riesgos.

Este grafo nos ayuda a poder decidir si consideramos riesgo a un evento que ocurra, aunque también existen otras fuentes de información que podemos usar para identificar posibles riesgos, tales como:

- Experiencia previa
- Otras personas con experiencia en la organización
- Documentos, informes, protocolos, …
- Inspecciones, auditorías internas, reclamaciones, …
- Entrevistas, encuestas, …

7.1. Análisis y evaluación de Riesgos

Como ya vimos anteriormente, es imposible alcanzar la seguridad completa y por ende la eliminación de todo riesgo.

El análisis de riesgos se centrará en estudiar las vulnerabilidades y amenazas que puedan atentar contra nuestros activos, con el objeto de evaluar el impacto que sufriría la

organización si se produjese alguno de ellos. Dicha evaluación podrá medirse de forma cualitativa o cuantitativa.

Disponemos de dos formas para analizar riesgos y evaluarlos, de forma reactiva o de forma proactiva.

- La forma reactiva se da cuando los riesgos y efectos adversos ya se han producido, por lo que nos centraremos en estudiar su "causa raíz" para averiguar cómo y porqué ocurrieron y lograr así prevenirlos para que en un futuro no vuelvan a ocurrir.

- La forma proactiva se basa en identificar y prevenir los riesgos antes de que se produzcan. Se buscarían todos los posibles fallos o riesgos, se les asignarían prioridades y se actuaría preventivamente sobre ellos. La siguiente matriz de riesgos (obtenida de unos tutoriales de la uc3m) nos proporciona una relación entre la probabilidad de que un riesgo se materialice, y la gravedad que puede llegar a alcanzar, siendo 1 el más importante y el 5 el de menos relevancia.

PROBABILIDAD

Alta	3	2	1
Media	4	3	2
Baja	5	4	3
	Bajo	Medio	Alto

IMPACTO/GRAVEDAD

Figura 3. Matriz de riesgos.

La mejor manera sería emplear ambas formas de análisis simultánea y complementariamente.

Una vez esté identificado y analizado el riesgo lo clasificaremos en varios umbrales. Pues no todos los riesgos que nos podemos llegar

a encontrar son iguales o tienen la misma magnitud, por lo que clasificaremos los umbrales de riesgo en:

Aceptable: El nivel de riesgo existente es bajo.

Tolerable: El nivel de riesgo es medio, por lo que se deben empezar a considerar medidas para reducirlo.

Inaceptable: El nivel de riesgo es alto, por lo que se deberán considerar obligatoriamente medidas para su reducción

La exposición a los riesgos va cambiando junto a la evolución que hace nuestra entidad. De ahí, la necesidad de estar en constante evolución, para que el análisis de riesgos pueda evolucionar a la par que lo hacen éstos y así no sobreexponernos a amenazas innecesarias. Para estos casos la norma ISO 27001 [ISO27001], define y establece los objetivos a alcanzar por un Sistema de Gestión de Seguridad de la Información tales como planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir con las necesidades de seguridad de la organización.

7.2. Planes de contingencia

Consideramos plan de contingencia, como el conjunto de acciones a desarrollar para la recuperación ante desastres o de continuidad de la actividad de negocio.

Se debe de definir en este plan las acciones a realizar, los recursos y el personal a emplear en caso de que se produzca un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

La definición del plan de contingencia viene determinado por el quién, qué, cómo, cuándo y dónde, en caso de que se produjese una anomalía.

Existen cinco etapas básicas en la formación de los planes de contingencia.

a) Definición del plan general: En esta etapa inicial, formaremos el marco del plan y elaboraremos un presupuesto que vaya acorde con dicho marco.
b) Determinación de las vulnerabilidades: Será necesaria la valoración de las consecuencias, identificar las aplicaciones que sean más críticas, así como los períodos máximos de recuperación.
c) Selección de recursos alternativos: Tales como recuperación manual, acuerdos alcanzados con otras instituciones, etc.…
d) Preparación detallada del plan: Documentación, acciones, personas, recursos, procedimientos, etc.…
e) Pruebas y mantenimiento: Las pruebas que se realicen no pueden alterar la función normal del departamento, por lo que las pruebas han de ser parciales y realizarse en horario nocturno o en fines de semana.

En función del tipo de riesgo que tengamos, podemos considerar cuatro tipos de respuestas o estrategias a seguir, a saber:

- Evitación o eliminación Este otro tipo de acción se produce también cuando nos encontramos con un riesgo del tipo inaceptable. Las acciones a seguir en este caso por la Organización es que se elimine toda acción que pueda causar este riesgo. Este plan de contingencia es muy drástico pues puede implicar la eliminación de algunas líneas de negocio.

- Reducción: Llegado el nivel del riesgo al umbral de tolerable, la organización se tiene que empezar a plantear medidas para su reducción. En este caso se debería iniciar el

plan de contingencia propuesto para cada caso, llevándolo a cabo para contener y reducir el posible daño.

- Traspaso: Una vez entrados en el umbral de riesgo inaceptable, la organización puede optar entre dos acciones, el traspaso o la evitación. Esta primera se produce cuando una organización decide traspasar el riesgo a otra entidad. Un buen ejemplo de esto puede ser el outsourcing, empresas que mueven las actividades que no forman parte de su negocio principal a otras empresas, con esto aparte de crear más puestos de trabajo, también consiguen derivar responsabilidades y riesgos en esta otra empresa. Otro ejemplo podría ser la contratación de una póliza de seguros que cubra el umbral del riesgo que se quiere traspasar.

- Aceptación: Se produce cuando la Organización está dispuesta a asumir el riesgo y no llevará a cabo ninguna acción para su eliminación. Obviamente, se da en casos en los que el nivel del riesgo no ha llegado aún al umbral de riesgo tolerable por lo que no sería necesario poner en marcha ningún plan de contingencia. También podría darse el caso de que tras aplicar la reducción o el traspaso, el riesgo residual que nos quedaría sería perfectamente asumible.

7.3. Seguimiento y auditorías

La importancia de las auditorías va creciendo respecto a la información como activo y los sistemas de información.

Existen tres tipos de líneas de defensa que se pueden adoptar: Control Interno (realizado por supervisores de distinto nivel, debe producirse en el día a día), auditoría interna (revisa cada departamento, centro o instalación con cierta periodicidad, sin

eliminar nunca el factor sorpresa) y auditoría externa (realiza revisiones anuales o bienales).

Según la ISO 27001 [ISO27001] en cuestión de auditorías internas del Sistema de Gestión de la Seguridad de la Información (SGSI), la organización debe realizar auditorías internas a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

- Cumplen con los requisitos de la ISO y de la legislación vigente.
- Cumplen con los requisitos de seguridad de la información identificados.
- Se implementan y mantienen de manera efectiva.
- Se realizan conforme a lo esperado.

Se debe planear un programa de auditoría, tomando en consideración los procesos a auditar, así como las auditorías previas. Las auditorías deben ser imparciales y se deben definir el criterio, alcance, frecuencia, y métodos de auditoría.

Las principales herramientas de las que dispone un auditor son la observación, la realización de entrevistas y cuestionarios, muestreo estadístico, paquetes de acceso y revisión y prueba de programas.

El informe que realice el auditor deberá reflejar una serie de puntos, los cuales la empresa deberá tener en cuenta y seguir para el correcto funcionamiento y para garantizar el bienestar de la organización. Estos puntos son:

- Objetivos
- Situación actual
- Puntos débiles y amenazas
- Revisión de los planes de riesgo y de contingencia
- Cumplimiento de los procedimientos internos
- Recomendaciones y planes de actuación

Recordemos que el auditor puede influir en las medidas que se elegirán y en los planes de actuación, pues su labor siempre será la de informar a los responsables y recomendarles, como el comité de seguridad informática o el administrador de seguridad, y después serán ellos, los que basándose en la información recibida por el auditor, tomarán las medidas oportunas.

Las labores de seguimiento también las puede llevar el mismo auditor. Recordemos que **auditoría es comparar lo que se hace con lo que se debería hacer**, así pues servirá para comprobar que las medidas elegidas para prevenir o corregir los daños se estén llevando a cabo de la manera correcta, y que estén siendo efectivas. Estas revisiones periódicas pueden realizarse utilizando la misma metodología empleada en el primer análisis, aunque se deberá definir la nueva dotación de recursos técnicos, humanos y económicos.

Para llevar a cabo este seguimiento, se pueden utilizar las tres líneas de defensa antes citadas (control interno, auditoría interna o auditoría externa) e incluso la utilización de informes, entrevistas, checklist, registros de usuarios, etc.…

8.Tipos de Seguridad

El propósito de toda medida de seguridad es disminuir los riesgos asociados a un determinado activo, tales como amenazas y vulnerabilidades.

Según cita la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, en su Artículo 9 sobre seguridad de los datos, se establece la responsabilidad del fichero en el que sea el responsable del mismo y en su caso en el encargado del tratamiento:

> "*Artículo 9. 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.*
>
> *3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el*

tratamiento de los datos a que se refiere el artículo 7 de esta Ley." [LOPD]

Debido a este artículo donde se establece la responsabilidad de los ficheros surge la necesidad de mantener dicha seguridad por las organizaciones.

Existe un amplio abanico de medidas de seguridad que toda empresa o Administración pública puede considerar utilizar para proteger su organización. Hay distintos marcos de referencia y códigos de buenas prácticas (por ejemplo Cobit 4.1 de ISACA, RD 1720/2007, ISO 20000, ISO27002, etc.…) que contienen numerosas medidas de seguridad que se pueden adoptar.

Normalmente disponemos de un presupuesto limitado como para poder llegar a adoptar todas las medidas recomendadas por estos marcos y códigos. Debido al elevado coste y la imposibilidad técnica que supondría implementarlas todas, se exige a los responsables de la Seguridad de la Información de las organizaciones que prioricen las medidas de seguridad a implementar.

En concreto 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 [RD1720], nos facilita un buen marco de referencia en cuanto a la seguridad en el tratamiento de los datos de carácter personal en su Título VIII.

El Real Decreto, en su Artículo 80, define tres niveles de seguridad: "*Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.*".

Para lograr una correcta seguridad en torno a nuestra organización, las distintas medidas que podemos adoptar las subdividiremos a su vez en una serie de niveles de protección, los cuales nos garantizarán una correcta protección de nuestro sistema en función del ámbito donde se apliquen.

8.1. Niveles de protección

Se pueden adoptar distintos niveles de protección en nuestras organizaciones. Estos son: nivel físico, nivel técnico, nivel adm./organizativo y por último el nivel legal y social.

Dichos niveles nos garantizan una correcta seguridad sobre nuestro sistema de Información. Dentro de cada uno de estos niveles de protección podemos adoptar las medidas de seguridad que creamos necesarias.

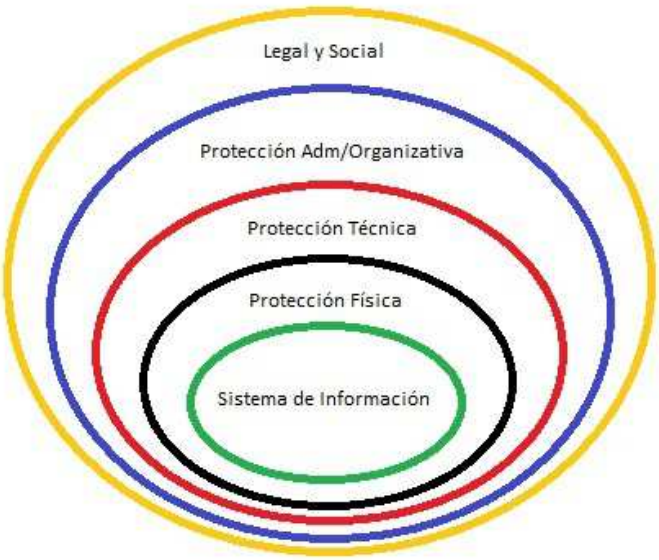


Figura 4. Seguridad en los Sistemas de Información [Apuntes uc3m]

Como se puede ver en la figura superior, estos niveles son capas concéntricas que van englobando a la capa anterior, lo que confiere una completa seguridad a nuestro sistema. Conforme nos alejemos del sistema de información, las medidas de protección irán aumentando en responsabilidades y costes, y serán llevadas a cabo por personas con unos rangos distintos dentro de la organización.

Vamos a analizar los distintos niveles para ver algunas características globales de los mismos.

8.1.1. Nivel físico

Las medidas adoptadas en el nivel físico son las primeras en llevarse a cabo. Normalmente disponen de una implementación que puede ser llevada a cabo por dispositivos electrónicos cuyo coste asociado no suele ser muy excesivo. Son medidas que disponen de una sencilla instalación y mantenimiento, lo que les confiere un buen desarrollo e implementación.

Tratan de compensar las amenazas de tipo físico. Afectan al ordenador y a su entorno, imprescindible para su funcionamiento (ubicación, condiciones, equipos, soportes, redes, instalaciones de aire acondicionado, potencia,…)

- Sistemas de detección y extinción de incendios.
- Impermeabilización de techos contra las lluvias.
- Un segundo suelo contra inundaciones.
- Sistemas de alimentación, o generador de reserva para evitar posibles cortes de energía.

8.1.2. Nivel técnico

Este nivel ya va más encaminado a la protección de software y de los datos. Su implementación suele llevarse a cabo mediante dispositivos hardware o con productos software. A diferencia de todas las demás, estas actúan dentro del mismo sistema.

- Identificación y autenticación

- Control de accesos
- Control del flujo de información
- Confidencialidad
- Integridad
- No repudio
- Notarización
- Auditoría

8.1.3. Nivel Adm./Organizativo

Este nivel sube un rango más en cuanto a la escala jerárquica dentro de nuestra entidad. Se suele encargar de elaborar las políticas de seguridad y velar por que se cumplan. También se encarga de configurar los planes de contingencia, los análisis de riesgos y las posteriores auditorías. En definitiva, se encarga de gestionar la seguridad.

- Clasificación de la información
- Establecer las políticas de seguridad correspondientes
- Asignar y requerir responsabilidades cuando sea necesario
- Formar y sensibilizar a los trabajadores.

8.1.4. Nivel Legal

Este nivel queda ya un poco más alejado del entorno de la organización, pues no viene realizado por ella, aunque debe velar porque se cumpla. Trata de proteger nuestros activos mediante la elaboración de leyes, códigos penales, reales decretos, directivas europeas, etc.… Suelen ser adoptadas por los poderes legislativos.

- LOPD

- Código Penal
- RD 1720/2007
- Derechos ARCO

8.2. Medidas según su actuación

Los tipos de medidas de seguridad que podemos adoptar siempre se centrarán más en las vulnerabilidades de los sistemas de información, y los podemos clasificar según su forma de actuación.

Según su forma de actuación existen distintos tipos de medidas de seguridad que nos podemos encontrar tales como:

- Medidas de prevención: La finalidad de este tipo de medidas es prevenir una amenaza antes de que ocurra.

- Medidas de detección: Son las que nos avisan que se está produciendo un ataque en estos momentos. Su única finalidad es la de informar, no realizan ninguna acción.

- Medidas de corrección: Estas medidas tienen como misión corregir los resultados de los ataques que ya se hayan producido.

- Medidas de recuperación: Suelen utilizarse para restaurar un sistema a un estado anterior, ya que el daño producido puede ser irreparable.

Por ver un ejemplo de las medidas de actuación. En el caso del fuego la mejor medida de prevención es el uso de materiales ignífugos, para que en el caso de que se desarrolle un fuego evitemos que este se extendiera. Las clásicas medidas de detección serían usar las correspondientes alarmas contra incendios o incluso los detectores, tanto de humo como de calor, aunque también hay los

equipos de detección de iones que están ganando importancia y eficacia en la actualidad. Para su corrección o extinción del fuego dependerá de la magnitud del mismo, si es un fuego pequeño o conato bastará con que utilicemos un extintor, en caso de que el incendio alcance magnitudes superiores no deberemos hacer nada y avisaremos a los bomberos para que se encarguen de ello. También podemos tener un sistema de extinción automático tipo Inergen… En el caso del fuego no disponemos de medidas de recuperación, pues no es como un error en un sistema que podamos recuperarlo con un backup, el fuego allá por donde pasa destruye todo, por lo que lo recomendable es tener una copia de seguridad en otro lugar distinto.

Recordaremos que para que exista una buena seguridad en nuestro sistema o nuestra empresa, no sólo basta con disponer de un tipo de medida, lo bueno sería tener una combinación de todas ellas para brindar una correcta seguridad en nuestro entorno.

Existen algunos mecanismos y estrategias a seguir para mantener una adecuada seguridad informática, y es a lo que llamamos Principios básicos de Seguridad Informática: [ECUR]

Principio de mínimo privilegio: se deben otorgar los permisos de acceso estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado.

Eslabón más débil: la seguridad de un sistema es tan fuerte como su parte más débil. Un atacante primero analiza cual es el punto más débil del sistema y concentra sus esfuerzos en ese lugar o punto de acceso.

Proporcionalidad: las medidas de seguridad deben estar en consonancia con lo que se protege y con el nivel de riesgo existente. No sería lógico proteger con múltiples recursos un activo informático que no posee valor o que la probabilidad de ocurrencia de un ataque sobre el mismo es muy baja.

Dinamismo: la seguridad informática no es un producto, es un proceso. No se termina con la implementación de los medios tecnológicos, se requiere que estén en constante monitorización y mantenimiento.

Participación universal: la gestión de la seguridad informática necesita de la participación de todo el personal de una institución. La seguridad que puede ser alcanzada mediante medios técnicos es limitada y debiera ser apoyada por una gestión y procedimientos adecuados, que involucren a todos los individuos.

Tras ver los distintos tipos de medidas de seguridad de que disponemos, procederemos a hacer un estudio sobre cada una de ellas, profundizando en algunos ejemplos.

8.2.1. Medidas de prevención

La mejor manera de evitar que una amenaza se nos materialice es previniéndola. Para esto hay que estudiar las distintas amenazas que pueden poner en riesgo nuestra información (posibles virus, crackers, empleados desleales, un mal tratamiento de la información).

Este tipo de medidas son proactivas, pues lo que pretenden es identificar los riesgos antes de que ocurran, para así poder prevenirlos y estar preparados para ellos en caso de que ocurran.

8.2.2. Medidas de detección

Estas medidas sólo nos avisan, pero no ejecutan ninguna acción contra ellas, por lo que siempre tendrán que venir acompañadas de otro tipo de medida de seguridad. Un ejemplo típico son las alarmas por incendio; nos avisan que hay fuego, pero no realizan ninguna acción al respecto.

8.2.3. Medidas de corrección

El objetivo de este tipo de medidas es corregir los resultados de los ataques. Son medidas del tipo reactivas, pues no saltan hasta que se haya producido el riesgo. Este tipo de medidas llevan consigo asociada una herramienta cuyo objetivo es encontrar la causa raíz, para así localizar qué la propició y poder evitarla en un futuro. Con esto conseguiríamos convertir esta medida de corrección en una medida de prevención.

8.2.4. Medidas de recuperación

El objetivo de este tipo de medidas es alcanzar el estado anterior al ataque. Se lleva a cabo mediante backups y discos de reinicio. Se suelen utilizar cuando ya no hay forma de arreglar el daño causado y es preferible regresar a un estado anterior, aunque se pierda parte de la información. Normalmente los

backups suelen estar en un sitio distinto para proceder a su arranque, ya que si todo es quemado no habría posibilidad ni de recuperación.

Una vez vistos los distintos niveles de protección de que disponemos y las variantes de medidas de seguridad según su actuación, procederemos en el siguiente punto a hablar sobre las medidas de seguridad que se pueden tomar para llegar a prevenir las amenazas y riesgos.

9. Mecanismos de seguridad

Ya hemos visto las amenazas que ponen en riesgo nuestra seguridad y nuestro activo más preciado, la información. Es momento pues, de ver los distintos mecanismos que nos pueden ayudar a preservarla.

Debido a la innumerable cantidad de mecanismos que nos podemos encontrar en una organización, la verdad es que nos sería imposible nombrarlos a todos, es por esto que nos centraremos en una amplia gama de los más comunes. Para facilitar su comprensión los iremos mencionando, indicando para cada uno de ellos cual se entiende que es su principal función.

Encontramos numerosa información sobre distintos mecanismos de seguridad que irán siendo analizados y adaptados a nuestros propósitos por el autor del PFC, tanto en sitios especializados en seguridad como Inteco, o en revistas o artículos informativos [FIRDIG] [10CONSEJ].

9.1. Contraseñas seguras

A lo largo de toda nuestra vida como usuarios nos tendremos que registrar en múltiples plataformas a través de nombres y contraseñas que nos identifiquen como usuarios del mismo. La elección del nombre de usuario que escojamos es más trivial, no en cambio la de la contraseña, ya que en algunos casos el usuario será

visible por todos, mientras que la contraseña nos permitirá autenticarnos.

Debido a la gran importancia en la elección de una buena contraseña, a continuación, daremos una serie de pasos a seguir para la elección de una segura y fácil de recordar, pero difícil de averiguar por otros.

Cuando queremos elaborar o intentar complicar un poco más las contraseñas para que sean más difíciles de adivinar, las basamos, incluso de modo inconsciente, en referencias o fechas simbólicas como nuestro cumpleaños, la matrícula del coche, el cumpleaños de nuestros hijos o nuestro aniversario de boda. Según un artículo de la página *The Next Web* la contraseña más utilizada en móviles es el 1234, una contraseña típica que facilita de manera considerable las opciones de acceder al móvil y saltarnos así la primera barrera de seguridad [THEN], así también el uso de nombres de mascotas o fechas de cumpleaños, se lo pone relativamente sencillo a los que quieran introducirse en nuestro sistema. También así se lo ponemos fácil a los hackers, pues simplemente con piratearnos el Facebook o entrar en alguna página web e investigarnos un poco, podrán ver alguno de estos datos y, a partir de ellos, buscar la combinación de entrada a nuestros servicios.

Respecto a la elección del nombre de usuario, los hackers saben que casi todos los usuarios utilizan el mismo nick que tenemos en la dirección de correo electrónico. Conviene, por lo tanto, no caer en los tópicos ni en lo trivial e intentar ser mucho más inteligentes y blindar lo que ahora tenemos casi como un libro abierto.

Veremos ahora los 10 consejos básicos en los cuales nos podemos basar para la elección de una buena contraseña, obtenidos de una página web, y adaptados posteriormente:

1. **Buscar siempre claves que tengan más de ocho caracteres**. En función del número de caracteres que tenga una clave así serán las distintas combinaciones posibles, y por lo tanto más fácil será romperla para un hacker. Se consideran débiles las combinaciones menores de ocho caracteres, que pueden identificarse con programas generadores de combinaciones aleatorias -llamados robots-, lo que se conoce como "la fuerza bruta".

2. **Nunca usar solo números**. Aunque pongamos claves de ocho o más dígitos, si usamos solo números, es cuestión de tiempo que un programa informático encuentre la contraseña y entre en nuestras páginas.

3. **Tampoco usar solo letras ni palabras**. Las letras se pueden combinar con robots hasta dar con la clave. Respecto a las palabras, siempre tienen una conexión simbólica con nuestro subconsciente, por lo que alguien que nos conozca un poco puede adivinar las claves si piensa en el nombre de nuestra pareja, nuestros hijos o nuestras mascotas.

4. **Optar siempre por combinaciones alfanuméricas**. Mezclar letras y números es la solución más segura porque se mezclan dos sistemas de clasificación, lo cual amplía mucho las combinaciones posibles. De todos modos, un hacker que tenga algunos datos personales sobre nosotros y mucha psicología puede adivinar las claves si no nos hemos esmerado en confeccionarlas. Debemos ser conscientes de que, de modo automático, siempre buscamos combinaciones fáciles de recordar y relacionadas con personas y fechas importantes. Por lo tanto, lo mejor después de escribir la contraseña es revisar que no contenga señales personales.

5. **Intercalar signos de teclado**. Un truco que nos permitirá usar letras y números relacionados con nuestra vida sin peligro es intercalar símbolos como "#", "$", "&" o "%" aleatoriamente entre los caracteres de la contraseña. La presencia de estos caracteres es mucho más difícil de descubrir para hackers y robots.

6. **Lo mejor son las claves aleatorias**. Si podemos usar un programa generador de claves aleatorias, estaremos mucho mejor protegidos. La página Clave Segura ofrece de manera gratuita un generador de claves en el que se puede escoger tanto la longitud de la contraseña como la cantidad de caracteres alfanuméricos que usamos. Otros servicios como Passwordmeter miden el nivel de seguridad de las contraseñas que confeccionamos.

7. **No utilizar la misma contraseña para todo**. Parece una obviedad, pero es lo que hacemos la mayoría de los usuarios. Hay que tener una contraseña distinta para cada servicio. También es recomendable cambiar las contraseñas cada cierto tiempo. En la mayoría del mundo empresarial por ejemplo, el sistema te obliga a cambiar bianualmente la contraseña.

8. **Guardar las claves en un documento de texto**. Como las claves seguras son muy difíciles, por no decir imposibles, de recordar, lo lógico es guardarlas escritas en un documento de texto, que utilizaremos para almacenar las contraseñas de todos nuestros servicios. Cada vez que debamos entrar a un servicio, tendremos que recurrir a este documento, que debemos proteger. Puede que sea pesado, pero es más seguro. La verdad que este documento supondría un arma muy valiosa si se nos olvidase en el ordenador y nos lo hackearan, por lo que

la recomendación es que se encuentre siempre en una memoria flash extraíble, o escrito en algún documento físico.

9. **Guardar el documento en un lugar seguro**. Hay varias opciones para guardar el documento con nuestras claves. La primera es usar una memoria USB separada físicamente del ordenador y que solo enchufemos cuando queramos abrir el documento con nuestras claves. Debemos ser conscientes de que podemos tener el ordenador monitorizado por algún software malicioso -ocurre con mucha más frecuencia de la que creemos- o que alguien puede acceder a través de la conexión wifi si esta no es lo bastante segura. La segunda alternativa es guardar el documento en una copia de seguridad en un servidor de la red, con protocolos de cifrado de 128 bits o más. Podemos guardarlo en plataformas diseñadas para tales usos, como Clipperz. Bastará con abrir este servicio y acceder al documento. Eso sí: la contraseña de acceso a Clipperz tiene que ser altamente compleja, deberemos tenerla escrita en una libreta, guardarla en un cajón y saber que si la perdemos también perderemos el resto de contraseñas.

10. **Cerrar la sesión de los servicios a diario**. Cuando apaguemos el ordenador por la noche o al salir de casa, la mejor opción es salir de todos los servicios de uso habitual, ya sean el correo electrónico, las distintas redes sociales donde participemos o las plataformas donde guardamos documentos para sincronizarlos, etc. Si alguien encendiera nuestro ordenador y no los hubiéramos cerrado, podría acceder fácilmente a tales servicios, ya que el navegador guarda las contraseñas si no le indicamos lo contrario. Por lo tanto, hay que indicar en el apartado de "Seguridad" de nuestro navegador que no recuerde ninguna contraseña. Al volver a usar el ordenador habrá que introducir todas las claves, pero evitaremos disgustos. En caso de que no cerremos todos los servicios cada vez que apaguemos el ordenador, lo más útil y eficaz sería

proteger nuestra sesión de usuario en el ordenador, con una contraseña, lo más potente posible.

Encontramos un par de ejemplos perfectos de cómo crear una buena contraseña, en la guía sobre la seguridad de la Carlos III [UC3MSEG].

Ejemplo: Un buen sistema para elegir nuestra clave es utilizar frases que tengan sentido para nosotros y que estén formadas por grupos de letras y números. Un ejemplo sería:

Frase: "*Yo, tengo 2 hermanas y 1 hermano*"

Clave:*Y,t2hy1h*

Esta clave es fácil de recordar y sin embargo forma un conjunto de caracteres difícil de adivinar por un programa crackeador de claves.

O "Volverán Las Oscuras Golondrinas En Tu Balcón Sus Nidos A Colgar", daría VLOGETBSNAC. Ahora modificaríamos la contraseña para que tenga minúsculas, números y signos. Por ejemplo podemos sustituir las letras LO por los números 10, insertar una coma tras la G y pasar a minúsculas la V inicial, con ello la contraseña elegida sería v10G,ETBSNAC, fácil de recordar, pero difícil de adivinar.

9.2. Firma digital

El desarrollo de la era digital y con ello todas las medidas de comunicación telemáticas y de Internet ha facilitado el intercambio de mensajes de todo tipo, incluidos aquellos de contenido administrativo, entre distintas personas, organismos, países, etc.

Debido a esto es necesario, y cada vez más, la firma y autenticación de documentos, los cuales se vienen solventando con la firma digital o electrónica, ya que equivale, a todos los efectos, a la firma autógrafa, puesto que identifica fehacientemente la autoría del mensaje.

Físicamente hablando, la firma digital se constituye sobre la criptografía y puede ser expresada como una secuencia de bits (datos electrónicos) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétrico o de clave pública.

Estos sistemas se encargan de cifrar los mensajes mediante la utilización de dos claves distintas, una privada y otra pública. La clave privada es conocida únicamente por la persona a quien pertenece la firma o el par de claves. La pública, a su vez, puede ser conocida por cualquiera, para que se puedan descifrar los mensajes cifrados o firmados con la privada, pero no existe una relación matemática que nos permita obtener la clave privada a través de la pública.

La utilización de la firma digital asegura que ambos interlocutores, el emisor y el receptor del mensaje (ya sean dos empresarios, un empresario y un consumidor o un ciudadano y la Administración) puedan realizar una transacción fiable, garantizando la autenticidad de cada interlocutor. Para ello esos mensajes firmados electrónicamente tienen las siguientes características:

1º.- Sirven para atribuir de forma irrefutable la identidad del signatario.

2º.- Garantizan la integridad del mensaje, es decir, que el documento recibido sea exactamente igual al emitido, sin que haya sufrido ninguna modificación durante su transmisión.

3º.- Aseguran el origen del mensaje de forma que el emisor no pueda repudiarlo o negar en ningún caso que el mensaje ha sido enviado por él mismo.

4º.- Y por último, son confidenciales, es decir, el mensaje no ha podido ser leído por terceras personas.

Para obtener las claves pública y privada que se usan para firmar digitalmente estos mensajes es necesario dirigirse, bien personalmente o por medio de Internet, a una empresa o entidad que tenga el carácter de "Prestador de Servicios de Certificación", para solicitar el par de claves y su certificado digital correspondiente.

El que se encargue de ser el prestador de servicios de certificación de firma electrónica deberá encargarse de comprobar la identidad del solicitante, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), y entregará una tarjeta con una banda magnética en la que están grabados tanto el par de claves como el certificado digital. Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a un ordenador personal, se podrá utilizar la información de la tarjeta para firmar digitalmente los mensajes electrónicos.

En España existen varias autoridades certificadoras. La primera fue la Fábrica Nacional de Moneda y Timbre y luego se han ido sumando otras muchas, como ACE (Agencia de Certificación Electrónica), que está formada fundamentalmente por la banca, y FESTE (Fundación para el estudio de la Seguridad de las Telecomunicaciones), que está constituida por notarios, registradores, etc. Todas ellas emplean unos medios de identificación reconocidos jurídicamente y muy seguros.

9.2.1. DNI Electrónico

La principal utilización de la firma digital en España es el DNI Electrónico, el cual aporta seguridad, rapidez, comodidad y la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos. Hoy en día, está muy extendido el uso de los DNI

electrónicos, pues aportan una gran ventaja a la hora de realizar trámites en la administración pública para poder identificarse. Simplemente hace falta un pequeño lector de tarjetas conectado a un ordenador, para poder usarlo en cualquier emplazamiento.

El DNI electrónico es una tarjeta de policarbonato que incorpora las más sofisticadas medidas de seguridad que harán virtualmente imposible su falsificación.

El Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica dice en su artículo 1.4: *"Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de Diciembre, de firma electrónica."*

9.3. Tarjetas de identificación

El propósito del sistema de tarjetas de identificación es controlar la entrada de una persona a un recinto determinado. Todo esto estará controlado por un sistema electrónico de apertura a través de la tarjeta.

Las tarjetas de identificación pueden ser utilizadas para distintas tareas, desde controlar la presencia de un individuo en una estancia determinada, llevar el control del tiempo que permanecen los empleados en la empresa o hasta llevar el control de accesos de personas a instalaciones. De todas maneras el sistema de control de presencia, se puede llevar a cabo a través de los otros, pues obviamente, si una persona ha entrado en un recinto y no ha salido, podemos concluir que sigue ahí.

El sistema de control de accesos aumenta considerablemente la seguridad de unas instalaciones, no sólo por el hecho de permitir la entrada al recinto o denegarla, sino también porque podemos restringir el acceso a determinadas áreas a algunos empleados.

Este sistema de control de accesos mediante las tarjetas de identificación ha ido evolucionando hasta llegar más recientemente al control por medio del chip de proximidad (radiofrecuencia, RFID). Este sistema de control de accesos mediante tarjetas plásticas permite, previa lectura del dispositivo, accionar la apertura de la puerta o torniquete quedando registrados en el sistema de seguridad los movimientos del portador de la tarjeta (entradas, salidas, movimientos internos en zonas restringidas, etc.). Lo que permite un completo conocimiento de qué ha hecho el usuario, a qué áreas ha entrado, etc.…

Estas tarjetas sirven también para identificar a los usuarios pues son tarjetas que por lo general llevan la fotografía y datos particulares impresos, ya que la finalidad de las tarjetas de control de presencia es mantener identificado en todo momento al portador de la misma.

No son exclusivas de los usuarios o trabajadores permanentes, también existen tarjetas para los visitantes en tránsito, a los cuales se les genera una tarjeta “in situ” ya que existen equipos de sobremesa que personalizan en un tiempo corto.

En general, su uso y aplicaciones están muy extendidos debido a las grandes ventajas que aporta, tales como:

- Sistema de identificación relativamente económico.

- Aumenta considerablemente la seguridad en las instalaciones.

- Conocimiento detallado y control de los datos de accesos de clientes, empleados y otras personas a las instalaciones (número de entradas, tiempos de permanencia...) ahorrando tiempo en la obtención de dichos datos.

Este tipo de tarjetas plásticas para el control del acceso están muy difundidas en: bibliotecas, universidades, hospitales, empresas, transporte, instalaciones deportivas, cadenas hoteleras, banca y por lo general en todas aquellas instalaciones que sea necesario unas medidas de seguridad y un control de los accesos.

9.4. Escáneres biométricos

Estas tres medidas vistas anteriormente, permiten la identificación mediante algo que se sabe (una contraseña) o algo que se posee (la tarjeta de identificación), pero estas medidas de identificación cada vez son más sencillas de frustrar o de falsificar, pues las contraseñas se pueden adivinar y las tarjetas se pueden sustraer o replicar. Debido a todo esto surgió el desarrollo y posterior implantación de las medidas de control por sistemas biométricos, las cuales garantizan en gran medida, que la persona que accede al sistema es la que de verdad está acreditada para hacerlo.

Hoy en día cada vez hay más empresas y organizaciones que tienen como sistema de control de accesos los de reconocimiento biométrico debido a su gran tasa de eficacia y a su bajo nivel de falsificaciones. La siguiente información ha sido sacada y adaptada por el autor del PFC de la bibliografía consultada del portal inteco.

9.4.1. Huella dactilar

Sin lugar a dudas, el más famoso y usado sistema biométrico de seguridad de los últimos años es la identificación basada en huellas dactilares. Esto es debido a que la mayoría de la población tiene huellas dactilares únicas e inalterables,

incluso los gemelos o trillizos suelen tenerlas distintas (aunque rara vez se ha dado algún caso de gemelos con huellas iguales).

Es el rastro biométrico más utilizado, esto es así ya que tiene una alta tasa de precisión y que habitualmente los usuarios tienen conocimientos suficientes sobre su utilización. Aparte de esto, el pequeño tamaño de los receptores y su fácil integración a los teclados o en las puertas, convierten a la huella dactilar en una tecnología muy útil y sencilla para su implantación y posterior uso en la seguridad de oficinas y hogares.

9.4.2. Reconocimiento facial

Otra técnica pero ya menos implantada, es la de reconocimiento facial, mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para lo cual, se utilizan determinados programas capaces de analizar las imágenes de rostros humanos. Entre otros parámetros estos programas se encargan de analizar la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula. Lo bueno de este sistema es que no solo se puede usar para el reconocimiento, sino también para la vigilancia en general mediante cámaras de video. El principal inconveniente de este sistema, es que hay que tener en cuenta que la cara envejece y cambia, al igual que es muy fácil alterarla poniéndose unas gafas o dejándose crecer la barba.

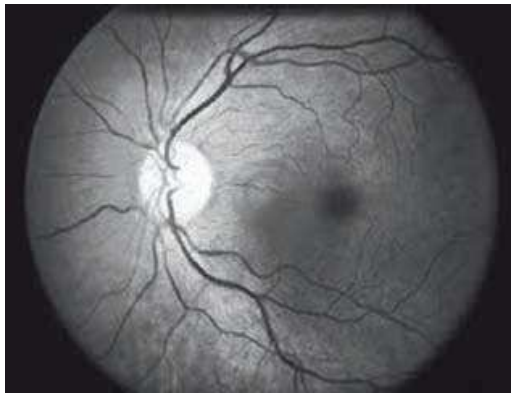
9.4.3. Reconocimiento de Iris

También existe la posibilidad de identificar la identidad del individuo a través del iris humano. Los patrones del iris vienen marcados desde el nacimiento y rara vez cambian. El escaneado del iris se basa en una fotografía de alta resolución y en tan sólo unos segundos se puede verificar.

Cabe resaltar que este procedimiento es inocuo para el ojo, aparte de que se trata de una de las tecnologías biométricas más resistentes al fraude.

9.4.4. Reconocimiento de retina

Otro tipo de escáner ocular, es el de la retina, que se basa en analizar los patrones de los vasos sanguíneos contenidos en ella. El hecho de que cada patrón sea único (incluso para gemelos idénticos) y que se mantenga invariable a lo largo del tiempo, hace de este sistema el idóneo para entornos de alta seguridad.



9.4.5. Reconocimiento de la geometría de la mano

El último método, y la verdad el menos fiable, es el reconocimiento de la morfología de la mano. A través de determinados programas de análisis en 3D, se analizan la longitud y forma de los dedos, así como el tamaño de las articulaciones y demás características que definen la complexión de la mano. El inconveniente es que a cada cicatriz que se pueda producir, herida o inflamación, esta morfología puede variar, por lo que no resulta fiable al 100%.

9.5. Control de accesos

Como dijimos anteriormente, por norma general, suele existir un único sistema gestor central y por el contrario nos encontramos con una multitud de empleados con distintas jerarquías en las empresas los cuales, obviamente, no tendrán los mismos permisos de acceso al sistema.

De ahí, surge la necesidad de decidir entre los distintos permisos que debemos aplicar a las jerarquías. Por poner un ejemplo: en un entorno bancario, todos los empleados tienen acceso al sistema central para consultar el saldo de una cuenta, pero no desempeñarán las mismas funciones el personal de caja, que el director de la sucursal o que el jefe de área; cada uno tendrá un perfil de acceso distinto en función de las funcionalidades que su puesto requiera.

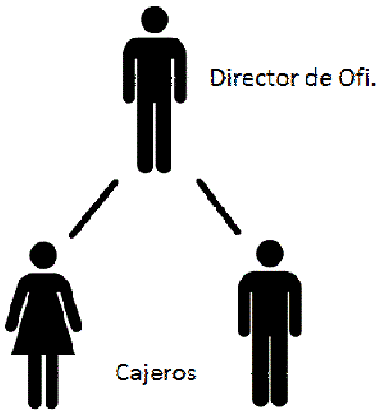


Figura 5. Ejemplo de herencia jerárquica

Este sistema de jerarquía debe permitir la herencia entre los perfiles, pues, volviendo al entorno bancario, un director de oficina podrá realizar exactamente las mismas operaciones que un cajero, a parte de las suyas propias, aunque un cajero no podrá desempeñar todas las funciones del director.

Uno de los mejores sistemas de gestión y control de accesos es el basado en roles, el cual veremos a continuación, aunque para verlo con mayor profundidad pueden consultar el portal de INTECO.

9.5.1. Control de accesos basado en roles

La mejor alternativa para gestionar el control de accesos a gran escala es el sistema basado en roles o RBAC (Role Based Access Control).

Es una tecnología que ha tenido un gran auge ya que combina varias características principales de sus antecesores (listas de control de acceso, control de acceso discrecional y control de acceso obligatorio). Básicamente, el éxito de este tipo de control de accesos se basa en la forma jerárquica de funcionar que tienen los roles, ya que es más fácil administrar

un sistema con roles asignados, y así poder llevar una administración de la seguridad más confiable y de menor coste.

La ventaja de este tipo de sistema es que es el propio administrador o propietario del sistema quien maneja los datos y asigna los roles, pudiéndose ajustar al máximo a las necesidades de la empresa.

Los permisos se encuentran asociados con los roles y los usuarios son miembros de esos roles. Los roles son creados en función de los distintos puestos que requiera la organización, y a los miembros se les podrá mover entre distintos roles, con lo que variarán sus permisos para adaptarse a las necesidades actuales de la entidad. Para ampliar la eficiencia de este sistema, nos encontramos con la herencia de roles, ya que un usuario podrá heredar los roles de otro usuario que esté a un nivel inferior.

El uso de este tipo de tecnología permite obtener una serie de beneficios, tales como:

- Administración simplificada
- Mejora de la productividad
- Ayuda a la hora de asignar roles a los nuevos empleados, ya que estos vendrán prefijados.

9.6. Cortafuegos (*FIREWALLS*)

Los cortafuegos constituyen uno de los mecanismos de seguridad básicos en los entornos informáticos. Son programas que se integran en el sistema operativo o bien, pueden ser instalados en

los mismos y permiten controlar las conexiones que se producen entre dispositivos, ya sea vía Internet o a través de otro sistema.

Para los no muy versados en la materia, el intercambio de información entre clientes o servidores se produce a través de Internet y usando unos determinados protocolos y puertos. Los cortafuegos son como unos semáforos que dejarán establecer la conexión o no, por lo que se encargan de vigilar y controlar dichos puertos y conexiones para saber si permiten el flujo de datos o lo deniegan y así evitar envíos no deseados de información o conexiones entre clientes y servidores o a determinadas páginas que no queramos que se produzcan.

Podemos encontrar múltiples firewall distintos, además de que existen máquinas específicamente creadas para realizar las funciones de cortafuegos. Pero nosotros nos centraremos en dar algunas nociones sobre los de tipo personal, que son aquellos que, por regla general, ya vienen integrados en el sistema operativo.

El Firewall personal es el programa que se encuentra en la frontera entre nuestro sistema operativo y las aplicaciones de red, por lo tanto será el encargado de, tras comprobar una serie de parámetros, permitir o denegar el acceso. El sistema operativo si tiene instalado un firewall, le dejará a este por completo la elección de a qué programas se les permite el acceso y a cuales no.

Los cortafuegos de tipo entrante controlan los intentos de conexión que pretenden entrar en nuestro sistema, están pensados para controlar desde dónde se quiere acceder a un determinado servidor. Y los cortafuegos salientes son mucho más seguros, aunque por el contrario son los menos implantados y los menos usados. Su misión es controlar las conexiones que se realizan a otro servidor. Está pensado para comprobar a qué IP nos queremos conectar.

9.7. Medidas de seguridad físicas

Contra las amenazas naturales vistas anteriormente existen multitud de medidas que podemos tomar en consideración. En este apartado nombraremos algunas básicas que siempre debemos tener en cuenta.

Uno de los problemas más comunes que nos podemos encontrar en entornos tecnológicos son los problemas debidos a campos electromagnéticos y a posibles fallos de tensión. Todo equipo eléctrico produce un campo magnético que puede afectar a los equipos contiguos, ocasionando en algunos casos, pérdidas de datos relevantes. La mejor solución que podemos encontrar para minimizar al máximo este problema es el apantallamiento de los equipos a través de una malla metálica. En el caso de los fallos de tensión o pérdidas de la tensión pueden llegar a ocurrir que se pierdan los datos si nos falta la corriente durante un periodo considerable de tiempo. Una opción que encontramos cada vez en más empresas y administraciones públicas es la incorporación de un generador auxiliar o equipos compensadores que en caso de que falte la corriente o haya un fallo de tensión, el generador continuará con el suministro para que no se produzca ningún daño en los equipos o pérdida de datos.

Para solucionar posibles problemas de agua la mejor solución sería la impermeabilización, pero aun así para problemas de agua con mayor envergadura nos encontramos con que eso puede que no sea suficiente, en cuyo caso lo mejor sería tener siempre una copia de seguridad, tanto de los ficheros físicos (que obviamente deberán estar en otro emplazamiento), como de los ficheros digitales que podrán estar copiados en otro lugar o subidos a alguna web. Aunque, para garantizar una buena evacuación del agua, será imprescindible contar con una buena ubicación y disponer de desagües y canales para poder evacuarla en caso de inundación o similar.

Algo parecido nos encontramos con el fuego o los terremotos. Para un fuego pequeño nos valdría con tener el fichero recubierto de

algún material ignífugo que no emitan gases tóxicos para que así no alimenten el fuego o disponer de almacenes aislados. En cambio, para fuegos de una magnitud considerable, lo recomendable sería, debido a la fuerza destructiva del fuego, poseer copias de seguridad en otro lugar, o si se trata de archivos físicos, digitalizarlos y subirlos a algún servidor web.

Para terremotos o seísmos de baja escala en los que no haya consecuencias físicas tampoco serían necesarias demasiadas medidas de seguridad, aunque si nos encontramos en zonas donde haya una gran presencia de temblores o posibilidad de que ocurran con una magnitud fuerte dentro de la escala de Mercallí o de Reigter, sí sería recomendable o desplazar nuestro emplazamiento, o en su defecto realizar copias de seguridad con cierta periodicidad y mandarlas a otro lugar, menos sensible a los movimientos sísmicos.

9.8. Antivirus

Los virus son programas informáticos cuya única finalidad es ejecutarse en un ordenador y corromper el resto de programas, ya sea destruyendo información, copiándola a otro ordenador, etc.

Debido al auge que experimentó este tipo de programas, surgieron los antivirus. Programas cuya función básica es detectar y eliminar los virus informáticos que se encuentren a su paso, así como todo tipo de programa malicioso.

Las funciones básicas que realiza un antivirus son: analizar los programas y archivos de nuestro ordenador y compararlos con una base de datos, donde se encuentran todos los códigos de los virus. De ahí, la importancia de tener nuestro antivirus actualizado, para disponer de la última versión de esa base de datos, no sea que en una comparación un virus relativamente nuevo no sea detectado.

Normalmente los antivirus cuentan también con componentes que se cargan en memoria y comprueban todos los archivos abiertos, creados o modificados en tiempo real, así como los archivos adjuntos de los correos electrónicos, scripts, etc.

Junto con los antivirus nos encontramos con los centinelas. Programas de pequeña envergadura que siempre acompañan a los antivirus, y que se encargan de controlar todos los ficheros con los que trabajas en tu ordenador, alertándote en caso de encontrar algo que ponga en riesgo la seguridad de tu equipo.

Softonic realizó un estudio donde analizaron los antivirus comerciales y elaborando un ranking con los 5 mejores del mercado del 2012. El ranking queda de la siguiente manera:

1.- Norton Antivirus 2012. Es el número 1 del ranking debido a su usabilidad y funciones, así como a su rapidez y potencia.

2.- Panda Antivirus Pro 2012. Poseen una eficacia y velocidad sobresalientes, además de su inteligencia colectiva y las vacunaciones de los USB de que dispone.

3.- ESET NOD32 Antivirus. Se destaca del ranking debido a su alta eficacia y el buen escaneo del malware que proporciona.

4.- Kaspersky Antivirus 2012. Se caracteriza por sus 4 escudos en tiempo real, su Widget en el Escritorio y por una inmejorable tasa de detección.

5.- McAfee Antivirus Plus 2012. Destacado por su Limpiador de Huellas, su Cortafuegos y el Anti-phishing.

Podemos encontrar el video con el ranking en el siguiente enlace (http://www.youtube.com/watch?v=d36U3kCRMpk).

9.9. Monitorización de ordenadores

Normalmente las funciones de monitorización de ordenadores son llevadas a cabo por agentes (programas) que se encargan del seguimiento y registro de la actividad.

Como nunca sabemos si el peligro viene desde fuera de la empresa o dentro (pueden darse casos de empleados desleales), la organización puede elegir qué actividades monitorizar. Éstas pueden ser:

- Ejecución de copias de archivos.
- Entradas y salidas de usuarios en la red.
- Arranque de determinadas aplicaciones o programas.
- Registro de cambios relevantes producidos.

En función de la necesidad o la frecuencia con que ocurran los hechos, podremos programar que se nos avise de una forma u otra, ya sea mediante mensajes al móvil, envíos de correos electrónicos o que se almacenen estos avisos en un archivo para su posterior control y análisis.

La información que recabaríamos sería la siguiente:

Contenido de un Registro de Auditoría	
Sujeto	Persona que realiza la acción o terminal que actúa de parte de un usuario.
Acción	Operación realizada por el Sujeto utilizando un objeto.
Objeto	El que recibe la acción directa realizada por el Sujeto.
Condiciones de excepción	
Utilización de Recursos	Una lista de todos los elementos usados o afectados.
Sello de tiempo	Identificador del momento en que se realizó la acción. Se debe especificar fecha y hora.

Tabla 2. Registros de Auditoría

9.10. Acceso a terceros desde ordenadores externos (Token RSA)

Debido a la gran expansión que sufren algunas organizaciones cada vez se hace más necesario el uso de la intranet de la empresa o administración desde cualquier ordenador externo a la red, con el inconveniente de que las medidas de seguridad se verán mermadas al acceder desde un ordenador personal o desde cualquier otro terminal que no sea uno de la misma entidad.

Para lograr un acceso eficaz y fiable los usuarios tendrán que identificarse con dos factores exclusivos, algo que saben y algo que conocen, antes de permitirles el acceso.

Este tipo de tarjetas inteligentes fueron desarrolladas y explotadas por *RSA Security* que las incluyeron con la clave simétrica y su pin protegido. Además les aportaron las credenciales correspondientes y las hicieron soportar un registro único con RSA.

Este tipo de sistema de autenticación ofrece una alta seguridad frente a otros sistemas ya que tienen una clave simétrica que se combina con el algoritmo para generar el código de un solo rol cada 60 segundos. Que el código varíe cada 60 seg. hace de este sistema algo extraordinario, pues sería muy difícil que alguien que quiera acceder al sistema de forma ilícita, averigüe la clave en menos del minuto que dura, antes de que cambie.

Otra de las grandes ventajas de estos dispositivos es que debido a su utilidad pueden ser utilizados por empleados, personal asociado a la entidad, comerciales y clientes, los cuales las pueden

llevar siempre encima debido a su pequeño tamaño y acceder siempre así al sistema.

9.11. Borrado seguro

Recordemos que las empresas son las encargadas de gestionar todos nuestros datos, no sólo en el momento en que sean recopilados y utilizados, también se deben encargar, a la hora de ser destruidos, de velar porque se haga de forma adecuada.

Aunque la verdad que esta destrucción de la información nunca suele llevarse de manera eficaz, pues siempre puede quedar algún tipo de residuo de información recuperable que vulnere la ley de Protección de Datos de Carácter Personal. De manera que veremos algunos tipos de borrado, en función del tipo de soporte que tengamos para la información, que garanticen un correcto borrado evitando así que los datos sean recuperados.

9.11.1. Desmagnetización

Este tipo de borrado sólo se puede aplicar a dispositivos magnéticos, tales como disquetes o cintas magnéticas. Se basa en la exposición de los dispositivos a un campo magnético que borre todos los datos contenidos en el dispositivo.

El tipo de campo magnético al que tengamos que exponer el dispositivo variará en función del soporte que se pretenda borrar, así como de su tamaño y forma, para así asegurar una correcta polarización de todas las partículas, y un correcto borrado.

Tras un proceso de esta envergadura hay determinados dispositivos que pueden no funcionar correctamente, lo que ocasiona un inconveniente, y es que dificulta la posterior comprobación de que todos los datos hayan sido borrados. Otra contraindicación es que por norma general, se suele optar por aplicar la potencia más alta del campo magnético en vez de estudiar la intensidad adecuada, lo que supone un desperdicio de energía.

9.11.2. Destrucción física

El objetivo de este proceso es la completa destrucción del medio de almacenamiento. Nos podemos encontrar con diferentes métodos que garanticen esta correcta inutilización del soporte, tales como:

- Fusión e incineración: Se suelen llevar a cabo en fundiciones o en plantas de incineración, y destruyen por completo el medio físico de almacenamiento.

- Trituración: Se suele usar cuando el medio físico donde se encuentra la información es el papel. La trituración se lleva a cabo por máquinas trituradoras especiales. El tamaño de la información de los residuos será directamente proporcional a la confidencialidad de los datos, cuanto más sensibles sean los datos más pequeños serán los pedazos. Los soportes de tipo óptico, como los CD o DVD, deben destruirse mediante pulverización o incineración, en destructoras determinadas.

Para la destrucción física es necesario algún tipo de certificación que garantice que la operación de destrucción se ha llevado a cabo correctamente, y no es posible acceder a la información eliminada. Este tipo de destrucción obliga en la

mayor parte de las ocasiones, al transporte de los dispositivos hasta el centro de reciclaje, extremando además las medidas de custodia durante el traslado, lo que aumenta el coste.

9.11.3. Sobre-escritura

Normalmente, con el borrado lógico no se borran los registros, sino que lo que se suele hacer es poner el indicador de registro a cero, aunque la información se suele seguir conservando, esto permite un posible acceso futuro a la información que ya creíamos borrada. Para evitar esta situación, utilizamos el método de sobre-escritura, basado en escribir un patrón de datos (todo ceros, o ceros y unos o algo similar) sobre los datos que queramos eliminar.

Este método es tremendamente útil para aquellos dispositivos regrabables, pero ineficaz en los no regrabables como los CD y DVD, para los cuales tendremos que usar otro método de eliminación de la información como la destrucción de los propios soportes. Además, otras ventajas con las que contamos es que este proceso se puede desarrollar dentro de las empresas, eliminando el coste del transporte, y se puede verificar también la efectividad del borrado accediendo al dispositivo.

Veremos ahora una tabla obtenida del portal INTECO (*www.inteco.es*), modificada y ampliada por el autor del PFC, donde se detallan los distintos tipos de borrados seguros que podemos usar, en función del dispositivo que tengamos.

Métodos de borrado en función del dispositivo				
Soporte	**Tipo**	**Desmagnetización**	**Destrucción Física**	**Sobre-escritura**
Discos duros	Magnético	✓	✓	✓
Discos flexibles	Magnético	✓	✓	✓
Cintas de Backup	Magnético	✓	✓	✓
CD	Óptico	×	✓	×
DVD	Óptico	×	✓	×
Blue-Ray	Óptico	×	✓	×
Pen Drive	Electrónico	×	✓	✓
Tarjetas de Memoria (SD)	Electrónico	×	✓	✓

Tabla 3. Tipos de borrado segudo

10. Videovigilancia. ¿Qué es? ¿Qué derechos nos asisten? y ¿Cómo tratarla?

*Partes extraídas de Inteco [VVIG], y ampliadas por el autor del PFC

La videovigilancia consiste en la captación y el tratamiento de imágenes de forma que se garantice la seguridad del objeto a proteger, normalmente personas o bienes inmuebles. Aunque también es verdad, que últimamente han proliferado este tipo de sistemas en el entorno empresarial, con el fin de efectuar un control laboral y comprobar que los empleados están cumpliendo con sus obligaciones como trabajadores. Pero, ¿dónde está el límite entre el mero control e invadir la intimidad de cada uno?

La Constitución Española, en el artículo 18.1, desarrolla el derecho a la intimidad, honor y propia imagen contra las intromisiones ilegítimas en los mismos. En estas imágenes grabadas pueden aparecer personas y su posible identificación, este hecho puede ocasionar una vulneración del derecho a la intimidad de estos individuos y el incumplimiento de la protección de datos de carácter personal.

Existe un derecho genérico de las personas no conocidas a no ser grabadas en lugares públicos a no ser que dicha grabación se encuentre cubierta por el derecho fundamental a la libertad de información, aunque impidiendo la explotación comercial sin el consentimiento del particular. Esto es debido a que la grabación de la vía pública y de las personas que circulan por ella está permitida en determinadas ocasiones por motivos de seguridad, aunque la

captación de imágenes de una persona reconocible, constituye un dato de carácter personal y por tanto, tiene que ser tratado acorde a la legislación vigente en materia de protección de datos, siempre que se utilicen medios técnicos para grabar, captar, almacenar y reproducir las imágenes de personas identificables, ya sea en tiempo real o diferido..

Obviamente, está prohibida la grabación de imágenes en determinados espacios reservados, tales como: vestuarios, baños, probadores, etc. pues vulnera el derecho a la intimidad.

Quedan exentas del derecho de protección de datos aquellas imágenes tomadas dentro del ámbito familiar (cabe recordar que la difusión de imágenes por Internet supone traspasar dicho ámbito doméstico).

Tratamiento de imágenes:

A la hora de realizar un correcto tratamiento de las imágenes de videovigilancia es importante tener en cuenta varios principios. Los más importantes son:

El principio de proporcionalidad. Este principio establece que el responsable debe ponderar el objetivo buscado, de tal forma que no exista un medio menos invasivo que cumpla la misma finalidad perseguida.

El principio de información. Las personas que vayan a ser grabadas por cámaras de videovigilancia deberán recibir la oportuna notificación antes de que se produzca, para que estos puedan decidir si acceder o no al lugar de grabación, así como ejercer sus derechos ARCO.

El deber de secreto. Todas las personas que intervengan en el tratamiento de dichas imágenes grabadas mediante sistemas de videovigilancia, están obligadas a guardar la confidencialidad. Dicho deber no finaliza, aunque hayan terminado las relaciones entre empresa y trabajador.

Obviamente, toda empresa de seguridad, o la entidad que sea la encargada de llevar a cabo las labores de grabación, deberán establecer también las correspondientes medidas de seguridad para proteger aquellas imágenes, las cuales pueden llegar a considerarse como dato personal en la mayoría de ocasiones.

Las empresas u organizaciones deberán preservar la confidencialidad y dotar las instalaciones de las medidas de seguridad oportunas para preservar dicho derecho. Para ello, deberían de dotarse todas las instalaciones de las mismas medidas de seguridad que si se tratase de un sistema informático (Punto 13.1 de este documento).

Recordar también que se debe permitir a los afectados que ejerzan sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), poniendo especial interés en la cancelación, de manera que se efectúe un borrado seguro de la información o el correspondiente bloqueo.

A la hora de tratar las imágenes, o mejor dicho de tomarlas, es muy importante que al ejercer nuestro derecho para videovigilar no estemos vulnerando el derecho de otra persona a su intimidad. Hay un caso muy ilustrativo de este matiz, que lo podemos ver recogido en una sentencia del Tribuna Supremo de hace un par de años:

"Sentencia del TS:

En el ámbito de la videovigilancia, el Tribunal Supremo (STS 7549/2010) resolvió que la instalación de cámaras de seguridad que permitían visualizar y grabar tres puertas de una vivienda colindante y, por tanto, las entradas y salidas de los vecinos, vulneraban el derecho a la intimidad de éstos. Esta sentencia, confirmó una anterior de la Audiencia de Santa Cruz de Tenerife que apreció la vulneración del derecho a la intimidad del vecino y condenó al demandado a retirar las cámaras de filmación y a indemnizarle por daños morales. En aplicación de la doctrina del Tribunal Constitucional sobre el

juicio de proporcionalidad en la restricción de derechos fundamentales, el TS concluyó que la medida adoptada no era proporcionada para el fin pretendido de seguridad, pues para garantizarla se invadía la intimidad de otra persona."

11. Aspectos jurídicos y legislación vigente

Debido a la vertiginosa evolución que sufren hoy en día los sistemas informáticos es completamente necesario e imprescindible estar al tanto de toda la normativa legal vigente por la que nos regimos.

Aunque disponemos de multitud de leyes y reales decretos que se van creando para ir delimitando el marco de actuación, hemos escogido una serie de leyes o normativas que mejor nos pueden ayudar e ilustrar sobre nuestra misión en la empresa.

11.1. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal

Esta ley es muy amplia y abarca muchos otros ámbitos, por lo que aquí sólo citaremos un par de artículos, los más relevantes al tema de la seguridad. Para consultar el resto de la citada ley, les remitimos al BOE.

*"**Artículo 9. 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.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo." [LOPD]

11.2. Modificación de la LOPD

En el Boletín Oficial del Estado del 5 de Marzo de 2011 se publicó, entre otras muchas normativas, la modificación de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), donde las principales modificaciones se hicieron en lo relativo a las sanciones por el incumplimiento de la misma. (A continuación citaremos del BOE dichas modificaciones de

los artículos, las cuales afectan sobre todo a la diferenciación entre infracciones leves, graves o muy graves.)

*"**Son infracciones leves**: (Las infracciones leves serán sancionadas con multa de **900 a 40.000 euros.**)*

a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

***Son infracciones graves**: (Las infracciones graves serán sancionadas con multa de **40.001 a 300.000 euros**.)*

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín oficial del Estado" o diario oficial correspondiente.

b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.

c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo

desarrollan, salvo cuando sea constitutivo de infracción muy grave.

d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

j) La obstrucción al ejercicio de la función inspectora.

k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

***Son infracciones muy graves**: (Las infracciones muy graves serán sancionadas con multa de **300.001 a 600.000 euros**.)*

a) La recogida de datos en forma engañosa o fraudulenta.

b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

c) No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Finalmente se añade un nuevo artículo, al que se ha numerado como 45.6 desplazando a los anteriores 45.6 y 45.7 que pasan a ser respectivamente 45.7 y 45.8).

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no fuera

atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.“ [MODLOPD]

11.3. Cómo redactar un documento de Seguridad

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, establece en su punto 1 que *“El responsable del fichero, … deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal”.* [LOPD]

Con el objeto entonces de facilitar a los encargados del tratamiento de los ficheros la adopción de las disposiciones del Reglamento de Seguridad de la AEPD (Agencia Española de Protección de Datos) se pone a disposición de las entidades el modelo de Documento de Seguridad, para servir de guía sobre la normativa de protección de datos.

El contenido principal de este Documento quedaría estructurado de la siguiente manera (el siguiente esquema ha sido obtenido del modelo de documento emitido por la Agencia Española de Protección de Datos):

I. Ámbito de aplicación del documento.
II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
III. Procedimiento general de información al personal.

IV. Funciones y obligaciones del personal.
V. Procedimiento de notificación, gestión y respuestas ante las incidencias.
VI. Procedimientos de revisión.
VII. Consecuencias del incumplimiento del Documento de Seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros.

Anexo I a. Aspectos relativos al fichero <nombre del fichero a>

Anexo I b. Aspectos relativos al fichero <nombre del fichero b>

.....

Anexo II. Nombramientos

Anexo III. Autorizaciones firmadas para la salida o recuperación de datos

Anexo IV. Inventario de soportes <si se gestiona en papel>

Anexo V. Registro de Incidencias <si se gestiona en papel>

Anexo VI. Contratos o cláusulas de encargados de tratamiento <si existen, de acuerdo con lo indicado en el artículo 12 de la LOPD>.

Anexo VII: Registro de entrada y salida de soportes

Este Documento deberá mantenerse permanente actualizado, y cualquier modificación, total o parcial, de los ficheros o personas responsables del tratamiento, deberá ser modificada en el documento.

11.4. 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

Más que la Ley de Protección de Datos de carácter personal, el reglamento por el que más nos vamos a regir y el cual crea un buen marco con las medidas de actuación es el Real Decreto 1720/2007, el cual nos desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

Como este documento llega a ser muy extenso, citaremos el índice y a continuación procederemos a hacer un pequeño estudio sobre los artículos más importantes relativos a la seguridad y tratamiento de ficheros.

Adicionalmente, y relacionando dicho artículo con la ISO 27002, sobre Tecnologías de la Información, Técnicas de seguridad y Código para la práctica de la gestión de la seguridad de la información, añadiremos después de cada artículo el punto con el cual se asemeja o el cual aplica en lo concerniente a las medidas de seguridad en el tratamiento de los datos de carácter personal.

A continuación citaremos artículos del Real Decreto por el que se aprueba la Ley Orgánica de Protección de Datos y los iremos analizando para ver la mejor forma de implementarlos o tenerlos en cuenta en nuestras organizaciones.

11.5. Niveles de seguridad (RD 1720/2007)

En el Artículo 81 de este Real Decreto se define la aplicación de los distintos niveles de seguridad, para tener así el marco de referencia de cuando aplicar el nivel básico, el medio o el alto. Citamos a continuación parte de este Real Decreto [RD1720].

"Artículo 81. Aplicación de los niveles de seguridad. (Aplica en los puntos 7.1.1, 7.2.1, 7.2.2 y 15.1.4 de la ISO 27002)

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de Diciembre.

c) Aquellos de los que sean responsables administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los

que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medias de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquellos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad."

11.5.1. Medidas de seguridad aplicables a ficheros y tratamientos automatizados (RD 1720/2007)

"Sección 1. Medidas de seguridad de nivel básico.

Artículo 89. Funciones y obligaciones del personal. (Aplica en los puntos 7.1.3, 8.1.1, 8.1.3, 8.2.1., 8.2.2. y 8.2.3 de la ISO 27002)

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

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

(Es importante tener bien recogidas en un documento las personas con acceso a la información sensible, así como sus permisos de acceso y consulta a datos, para así en caso de mal uso, tener registrado quienes tenían acceso y en su lugar, quienes son los responsables.)

Artículo 90. Registro de incidencias. (Aplica en los puntos 12.6.1, 13.1.1, 13.1.2 y 13.2.1 de la ISO 27002)

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso. (Aplica en el punto 9.1.2 de la ISO 27002)

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

(Para poder controlar los accesos y que no todas las personas puedan acceder a la misma información, se establecerá un sistema de roles. Dicho sistema se basará

en contraseñas y/o tarjetas de acceso para verificar la identidad a través del ordenador de la persona que está intentando acceder y así, permitirle el acceso sólo a la información necesaria.)

Artículo 92. Gestión de soportes y documentos. (Aplica en los puntos 7.2.2 y 9.2.6 de la ISO 27002)

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.
Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejados a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

(Uno de los puntos más importantes en toda seguridad, es la destrucción de los documentos que ya no sirven, pues pueden seguir teniendo información de carácter confidencial. De ahí que en el punto 92.4 se recoja la necesidad de efectuar un borrado seguro de la información, o una correcta destrucción del soporte donde se encuentra.)

Artículo 93. Identificación y autenticación. (Aplica en el punto 6.2.2 de la ISO 27002)

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que,

mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación. (Aplica en el punto 10.5.1 de la ISO 27002)

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales previamente deberá haberse realizado una copia de seguridad.

(Las copias de seguridad, backups, son algo fundamental en cualquier empresa u organización. A menudo se borran por accidente o se modifican documentos sin querer y no hay posibilidad de recuperarlos; con el backup conseguimos restaurar nuestro sistema o fichero al estado anterior a que esto hubiera pasado, como si nada hubiera ocurrido. Es muy frecuente que las copias de seguridad se realicen con una recurrencia semanal.)

Sección 2. Medidas de seguridad en el nivel medio.

Artículo 95. Responsable de seguridad. (Aplica en el punto 6.1.3 de la ISO 27002)

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.
Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

(Esta figura es fundamental en todas las empresas. Normalmente en todos los departamentos, suele existir un equipo de soporte o algo parecido, donde se encuentran los técnicos de información que dan asistencia a los analistas; pues dentro de ese equipo, uno de los responsable debería ser el titular de los ficheros,

controlarlos y manejarlos, así como dar los permisos necesarios y mantenerlos.)

Artículo 96. Auditoría. (Aplica en los puntos 6.1.8 de la ISO 27002)

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.
Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos. (Aplica en el punto 10.8.1 de la ISO 27002)

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

(Utilizando un software para hacer un login y validar contraseñas, se puede establecer un máximo de tres intentos, y una vez superados, bloquearse el sistema para ese usuario.)

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se

hallen instalados los equipos físicos que den soporte a los sistemas de información.

(Para implementar el control de accesos nos podemos decantar por el sistema más barato, eficaz y con mayor usabilidad, las tarjetas de identificación. Dichas tarjetas se suelen usar a través de tornos en la entrada de los sitios donde estén emplazadas nuestras organizaciones, para controlar las personas que acceden.)

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3. Medidas de seguridad de nivel alto.

Artículo 101. Gestión y distribución de soportes. (Aplica en los puntos 10.7.1, 10.8.1 y 10.8.3 de la ISO 27002)

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 102. Copias de respaldo y recuperación. (Aplica en el punto 10.5.1 de la ISO 27002)

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos. (Aplica en el punto 10.10.1 de la ISO 27002)

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones. (Aplica en el punto 10.9.2 de la ISO 27002)

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

(Muy importante el cifrado de datos. En la mayor parte de empresas se transfiere información entre correos electrónicos de forma que puede ser vulnerada la LOPD con mucha facilidad, para lo que habrá que habilitar un sistema de cifrado de datos que proteja ese intercambio de información.)”

11.5.2. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (RD 1720/2007)

"Sección 1. Medidas de seguridad de nivel básico.

Artículo 105. Obligaciones comunes. (Aplica en el punto 15.1.5 de la ISO 27002)

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:
a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

(Si nuestro mecanismo se trata de archivos físicos de almacenamiento de información, estos deberán de protegerse para que no sean accesibles por personal no autorizado, tipo cerraduras o algún sistema que impida el acceso. Además habrá que equiparlos con un etiquetado críptico, de manera que para los usuarios con acceso autorizado les resulte fácil la identificación del contenido, pero que dificulte la identificación para el resto de personas.)

Artículo 108. Custodia de los soportes. (Aplica en el punto 15.1.5 de la ISO 27002)

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2. Medidas de seguridad de nivel medio.

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3. Medidas de seguridad de nivel alto.

Artículo 111. Almacenamiento de la información. (Aplica en el punto 15.1.5 de la ISO 27002)

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro

dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción. (Aplica en el punto 15.1.5 de la ISO 27002)

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de

acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

(Cuando hablamos del traslado de documentos hay que extremar mucho las precauciones, pues no es como si se tratase de perder un CD, donde la información está cifrada. Si perdemos, perdemos uno de los pocos originales que pueda haber y con la información accesible a cualquiera.)”

12. Casos de una mala Seguridad en los SI

No en todas las empresas nos encontramos con un entorno modélico donde no haya errores de gestión de los datos personales. Estos son los errores más comunes que nos podemos encontrar:

1. Cuando recibimos los curriculums de los candidatos a un puesto, el hecho de archivarlos (aunque sea en un cajón) y no comentar a los candidatos que van a ser conservados ni de sus derechos ARCO (acceso, rectificación, cancelación y oposición), conlleva un grave error.
2. Facilitar los datos personales de una persona a una gestoría, o cualquier otra empresa subcontratada, sin que medie un contrato de regulación de responsabilidades en materia de protección de datos.
3. Felicitar a sus trabajadores por su cumpleaños (aunque parezca una tontería, pero sus trabajadores no le han facilitado su fecha de nacimiento con ese fin, por lo que sería también una infracción si no tiene el consentimiento para esa finalidad).

Es importante realizar tres ejercicios/tablas, para tener presentes los puntos donde más debemos enforcar nuestro sistema. (Dichas tablas han sido extraídas de la guía *Small Business Information Security: The Fundamentals,* de Richard Kissel.)

- La primera tabla la usaremos para conseguir las principales prioridades en cuanto a tipos de información que tratemos:

Table 1 The 5 Highest Priority Information Types In My Organization

Priority	Type of Information	Stored On Which System?
1		
2		
3		
4		
5		

Tabla 4. Ejercicio 1

Como vemos, realizaremos un "Top 5", identificando los cinco tipos de información que utilizamos en nuestra organización, considerando tanto el tipo de organización, como el sistema donde se localiza.

- Mediante la realización de la segunda tabla se trata de intentar conseguir identificar la protección que podemos llegar a necesitar para proteger la información de la que disponemos en nuestra organización.

Table 2 The Protection Needed By The 5 Highest Priority Information Types In My Organization

Priority	Type of Information	C	I	A
1				
2				
3				
4				
5				

Tabla 5. Ejercicio 2

En esta tabla, se trata de introducir los cinco mayores tipos de información que vamos a proteger, especificando las necesidades: C-Confidencialidad, I-Integridad y A-Disponible (del original *Availability*), si las necesitamos o no para nuestro tipo de información referenciado.

- La tercera y última tabla que vamos a realizar, la utilizaremos para ayudarnos a medir los costes de un error, derivados de una mala gestión.

Se trata de introducir como siempre nuestros mayores tipos de información que nos podemos encontrar en nuestro negocio. Introducimos también los costes estimados para cada categoría. Con lo cual llegaremos al coste total en el caso de que la información sea borrada, modificada o perdida.

Table 3 The Highest Priority Information Type In My Organization and an estimated cost associated with specified bad things happening to it.

	<data type name> Issue: Data Released	<data type name> Issue: Data Modified	<data type name> Issue: Data Missing
Cost of Revelation			
Cost to Verify Information			
Cost Of Lost Availability			
Cost of Lost Work			
Legal Costs			
Loss of Confidence Costs			
Cost to Repair Problem			
Fines & Penalties			
Other costs- Notification, etc			
Total Cost Exposure for this data type & issue	$	$	$

Tabla 6. Ejercicio 3

12.1. ¿Quién regula todo?

El órgano que se encarga de velar porque se cumpla toda la legislación sobre protección de datos y controlar su aplicación es la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS [AEPD].

La cual será representada por su director. Consta de un registro de todos los ficheros, tanto públicos como privados. Se encarga de notificar a las distintas organizaciones de su deber de poner en conocimiento de los afectados, que sus datos serán incluidos en un fichero para su tratamiento automático.

La AEPD también se encargará (en concreto su director) de aprobar la transferencia internacional de datos a países que no cumplan con los requisitos mínimos de seguridad, sin la previa autorización de su director.

12.2. Casos públicos de mala gestión.

Hoy en día, el hecho de llevar a cabo una mala gestión de los datos de carácter personal, puede llevar a determinadas empresas a ser denunciadas y obligadas a pagar una indemnización a los afectados. No suelen ser casos muy sonados, pero indagando en Internet nos podemos encontrar con claros ejemplos:

- Multa de 40.000 € a Endesa, por vulnerar la LOPD. La empresa fue sancionada por constituir un contrato de alta sin el consentimiento del cliente.
- Multa de 60.101,21 €, rebajada a 3.000 €, a un abogado por tener compartida en el emule una base de datos con información de 1.500 clientes.
- Multa de 60.101,21 €, rebajada a 6.000 €, al BBVA por dejar depositadas en la basura siete cajas con información de clientes.
- Multa de 50.000 € a un banco nacional, por incluir en la lista de morosos a un cliente sin haberle requerido previamente el importe de la deuda (se vulneró el principio de la calidad del dato).

13. Guía de aplicación en los distintos entornos

A continuación veremos los pasos a seguir y todos los factores a tener en cuenta para mantener una buena seguridad dependiendo de los distintos entornos, y según como se base nuestro sistema de información, ya que podemos hablar de entornos enteramente digitales, o por el contrario podemos encontrarnos con entidades donde todo el soporte de la información se maneje en formato papel.

13.1. Sistemas Informáticos

En el caso de que nos encontremos con una entidad, ya sea empresa u organización pública, cuyo soporte para el manejo de la información de tipo digital se base en sistemas informáticos deberemos tener en cuenta una serie de pautas o directrices que nos ayudarán a mantener una correcta seguridad en nuestro sistema y así evitar cualquier tipo de vulnerabilidad.

- Lo primero de todo es asegurarnos de que hemos realizado una buena elección del entorno. Para conseguir evitar desastres innecesarios, lo recomendable será hacer un estudio para evaluar la zona en la que ubicaremos la sede de la entidad, para así conseguir evitar tanto las posibles amenazas naturales (como el agua, fuego o los terremotos),

como las amenazas accidentales posibles (fallos de tensión, sobreexposición a campos magnéticos, etc.…).

Nunca deberemos localizar nuestra central muy cerca de un río o sus afluentes, pues con las lluvias o los deshielos su caudal puede aumentar de forma considerable y anegar las zonas cercanas.

De la misma manera, tampoco será recomendable ubicarla cerca de zonas con altas probabilidades de sufrir un terremoto. Debido a la tectónica de placas, la fricción entre ellas es la que genera los movimientos, y da la casualidad de que por el estrecho de Gibraltar pasa una línea de falla que es la que divide Europa de África, de ahí que la zona de la península más meridional sea más propensa a sufrir algún tipo de temblor.

De los fallos de tensión es más difícil protegerse, a no ser que dispongamos de un sistema auxiliar generador de energía, pues en todo momento puede haber algún tipo de fallo que imposibilite el suministro y nos quedemos sin energía, con el perjuicio que supondría el apagón eléctrico de forma repentina.

Otra cosa que debemos tener en cuenta a la hora de elegir ubicación, es tener en cuenta los campos magnéticos. Toda bobina por la que circule electricidad genera un campo magnético, esto será proporcional a la cantidad de corriente que la atraviese y al tamaño de la bobina, por lo que sería recomendable evitar emplazarnos en lugares cercanos a estaciones eléctricas, sistemas de suministros, o cualquier otro tipo de fábrica donde podamos intuir que exista riesgo magnético.

- Una vez elegido el emplazamiento que más nos beneficie, deberemos dotar a nuestro edificio de las correctas medidas de seguridad.

  Empezaremos por las medidas de seguridad para restringir accesos al personal ajeno a nuestra organización, para lo cual sería recomendable disponer de **tarjetas de identificación**. Dichas tarjetas lo que nos permiten es tener identificados a los empleados, ya que esas tarjetas pueden

llevar una fotografía junto con los datos personales para una mayor identificación de la persona. Al dotarlas de un chip, son perfectas para garantizar el acceso al edificio o determinadas áreas. En el caso de que haya tornos en la entrada de acceso al edificio, estas tarjetas permitirán hacer un filtro para que sólo entren los empleados con acceso al mismo. En el caso de visitantes o personal externo a la organización se les podrían expedir tarjetas de visita.

Para evitar que alguien salte los controles o se cuele en la empresa, consiga sacar información y salir tan airosamente del recinto, sin que nadie se inmute o se fije en alguien nuevo que lleva documentación de un lado a otro, algunas empresas suelen obligar a sus empleados a llevar colgadas al cuello las tarjetas de identificación. Esto supone un control pasivo entre todos los compañeros, pues al ver a alguien sin la tarjeta de identificación colgada al cuello, levantará alertas y hará que el sospechoso no se pueda pasear tan tranquilamente por las instalaciones.

En el caso de trabajadores fijos, y si consideramos que nuestra empresa se dedica a un tratamiento de información bastante sensible, podemos llegar a pensar incluso en dotar a los tornos de entrada de un sistema de huellas dactilares, debido a la gran ventaja que estos poseen de verificar la identidad de las personas, ya que las tarjetas de identificación se pueden perder, olvidar e incluso robar.

Como en este caso nuestra empresa se centra en un sistema que gestiona sobre todo información en formato electrónico, se supone que encontraremos muy poca información en formato papel, y todo nuestro núcleo de gestión de la información se centrará en los ordenadores por lo que sería recomendable también, restringir el acceso a ellos de alguna manera, aparte de la típica contraseña de inicio de sesión, estaría bien usar la tarjeta de identificación que hemos usado para entrar en el edificio como medio para encender el ordenador y permitir el acceso. Dependiendo de los medios de que dispongan las empresas, podremos encontrar dos tipos de tarjetas, las más sencillas

serán aquellas que tendremos que insertar en nuestro teclado para que sean reconocidas, y las otras serán aquellas que se lean por proximidad al terminal.

- En el caso de que seamos un empleado externo o comercial que quiere acceder a los servicios de la empresa a través de Internet, aparte de utilizar las tarjetas Token explicadas anteriormente que nos dan una clave aleatoria cada minuto, sería recomendable usar algún otro tipo de seguridad. La verdad es que últimamente se ha desarrollado mucho la tecnología consistente en capturadotes de teclado, que en tiempo real consiguen averiguar qué teclas estás pulsando. Mediante la instalación de un virus que se introduce en la memoria del ordenador y que permite capturar los números que se introducen en el teclado cuando éste accede a páginas que requieren identificación.

  Este virus es introducido en el ordenador de forma oculta mediante la instalación de otros programas que aparentemente tienen otros fines, como juegos o tarjetas de felicitación o enlaces. Una vez capturados los datos, la información se envía a direcciones de correo controladas por los atacantes, quienes finalmente suelen vender la información para que otros puedan operar sin restricciones sobre la cuenta usuaria. Normalmente con el fin de evitar este tipo de fraude y amenaza algunas entidades se preocupan en introducir en sus páginas un sistema para introducir los dígitos que componen la firma electrónica, mediante el cual se evita que el usuario introduzca las claves a través del teclado. De esta forma, la inserción del código ha de hacerse a través de un teclado virtual, utilizando en todo caso el puntero del mouse.

- Si accedemos sobre la Web, deberemos cerciorarnos de que lo hacemos a través de una página segura, y que dicha página no es un fraude que lo único que busque sea la obtención de nuestra clave. La verdad es que hoy en día, han proliferado gran cantidad de páginas Web falsas y correos electrónicos falsos cuya única finalidad es hacerse

con nuestras claves y con eso, conseguir acceder a todo tipo de información personal o confidencial, para lo cual sería óptimo dotar a nuestra página corporativa de algún tipo de certificado (existen muchos tipos de entidades que nos facilitan un certificado y con ello una garantía de seguridad, tipo Verisign, etc.)

Verisign [Verisign] es una empresa que ofrece servicios de autenticación y ayuda tanto a otras empresas y organizaciones, como a personas particulares, a establecer relaciones a través de Internet de una forma cómoda y segura garantizando la identidad de los participantes de la relación comercial. La verdad es que Verisign ofrece una protección mediante un cifrado SSL, lo cual da una credibilidad y proyecta una confianza considerable. La forma de identificar si un sitio Web está protegido mediante servicio, es fijándonos en la barra de direcciones y ver que aparece al principio la letra "s" junto con un candado cerrado.

- Otra recomendación básica a utilizar en nuestros ordenadores corporativos es el uso de los cortafuegos, antispyware y antivirus. Dichas herramientas son básicas en el día a día del uso de ordenadores. La primera, los cortafuegos, en líneas generales sirven para restringir las conexiones que se puedan recibir a través de la red, esto nos ayudará a estar seguros y protegidos de que intenten acceder a nuestro ordenador a través de Internet. Si utilizamos el sistema operativo Windows, ya nos suele venir uno instalado, pero habrá que chequear que esté funcionando correctamente. Los antivirus nos ayudan a proteger nuestros equipos, no sea que venga algún archivo infectado y se pueda propagar por todo el sistema; el antivirus lo detectará y nos avisará para que estemos sobre aviso. Lo normal es que los antivirus comprueben los ordenadores en horario nocturno, para no interrumpir en el trabajo diario. Determinados empleados se suelen llevar el

trabajo a casa, y desarrollan en equipos domésticos sus actividades laborales, por lo que sería preferible que estos también estuvieran cubiertos.

- Es importante también que los usuarios tengan en cuenta que no deben abrir correos electrónicos a no ser que los estén esperando con ese asunto y conozcan al remitente.

- También es desaconsejable pinchar en un link que nos manden, pues muchos de ellos pueden desencadenar algún tipo de amenaza o una puerta para que un virus entre en nuestro ordenador. Evitar entonces pinchar en ellos, a no ser que sepamos a donde nos va a llevar y/o confiemos completamente en la persona que nos lo remite.

- Para hacer negocios seguros y transacciones bancarias seguras, las entidades financieras ponen a nuestro servicio páginas seguras, pero después suelen quedar restos del historial y demás información en nuestro ordenador y nuestra carpeta temporal que puede llegar a ser peligrosa si nos entrase algún tipo de malware.

- Hasta ahora hemos visto algunas medidas de seguridad para protegernos contra ataques externos, pero sería muy conveniente tener en cuenta que también nos podemos encontrar con algún caso de deslealtad dentro de la empresa, para lo que crearemos distintos perfiles de empleados. Para garantizar un correcto tratamiento y seguridad de la información personal deberán de recogerse en un documento, que describiremos con posterioridad, las funciones y obligaciones de los empleados en cuanto al control de accesos y tratamiento de la información de carácter personal se refiere, así como las repercusiones en caso de incumplimiento. La forma de conseguir esto es a través de los privilegios informáticos; asignaremos usuarios en función del rango, y obviamente, una persona con un rango muy bajo dentro de la empresa casi no tendrá acceso a información confidencial, mientras que según vayamos

ascendiendo en la pirámide jerárquica irán aumentando dichos privilegios, tales como consultar, grabar, actualizar, agregar, suprimir o modificar datos de carácter personal. Estos rangos se irán modificando en función del cargo y funciones desempeñadas, así como de años dedicados a la empresa y la vinculación que se muestre con ella.

Otro aspecto a tener en cuenta, en cuanto a gestión y protección de la confidencialidad se trata, es la relación de nuestra empresa con personajes conocidos o altos cargos. Ej.: Hoy en día, toda persona relevante, ya sea un actor, político, o cualquier personaje público, tiene una cuenta en un banco, una alarma de seguridad en su domicilio, etc., ello implica que en determinadas empresas habrá empleados con acceso a datos de cierta sensibilidad para los que se deberá llevar un control especial. Con esto no se quiere decir que se restrinjan dichos accesos, puesto que habrá empleados que ciertamente deban tener acceso a esta información constantemente, pero sí se debería crear alguna especie de alarma interna o control de seguimiento para controlar los empleados que acceden y qué tipo de información consultan, lo que deberá ser reportado a un cargo superior para que lo verifique y apruebe.

- Para evitar posibles pérdidas de información debido a fallos de tensión, errores humanos, etc. la mayoría de las entidades cuentan con los mecanismos necesarios para realizar periódicas copias de seguridad (backups). Lo recomendable es que las copias se produzcan al menos de forma semanal, aunque en función de la información o las necesidades, se pondrán elegir otro tipo de periodicidades, como copias diarias o incluso varias veces al día. Aparte de estas copias de seguridad, que normalmente sólo incluyen archivos, sería recomendable que una vez al mes se hiciera una copia del sistema completo y almacenarla fuera de la localización de la oficina. Cabe destacar que dichas copias deberán guardarse en lugar seguro, custodiadas por el

responsable del fichero y bajo las medidas de seguridad que garanticen su confidencialidad. La recomendación de que se realicen copias como mucho semanales es lo recomendable, puesto que día a día no se suelen producir los suficientes cambios significativos como para realizar un backup, aunque si nuestros recursos nos lo permiten (capacidad para almacenar tantas copias de seguridad) y no interfiere lo suficiente con nuestro trabajo del día a día, se podrían hacer las copias de seguridad diarias. También nos veremos influidos en función del sector de actividad, pensemos por ejemplo en una entidad con muchas operaciones al día como un banco.

La mayoría de las empresas tienen personal informático o del equipo de tecnología que se encarga de realizar las copias de seguridad en red. Si nosotros somos una pequeña empresa, realizar las copias de seguridad sería tan sencillo como adquirir un disco extraíble lo suficientemente grande (500 GB o 1 Tera) y realizar una a una las copias de los ordenadores de nuestra empresa, e ir almacenándolas en el disco extraíble en subcarpetas nombradas con la fecha y el ordenador al que corresponden.

- En el caso anterior deseábamos protegernos de un borrado accidental o una posible pérdida de información, en este caso intentaremos ver la mejor forma de hacer un borrado a conciencia, un borrado seguro que no permita recuperar la información. Normalmente en las oficinas existe información la cual nos interesa destruir, porque ya no nos sirva, sea errónea o se haya quedado obsoleta. Para tratar todo este borrado de información y asegurarnos que es totalmente destruida sin posibilidad de recuperación deberemos de tener en cuenta el soporte en el que se encuentre. Normalmente, todo el grueso de la información que se trata en las empresas y entidades de hoy en día se encuentra en formato electrónico, donde el soporte más encontrado es el disco duro, el cual dispone de los tres tipos de borrado: desmagnetización, destrucción física y

sobreescritura (ver cuadro del punto 9.11.3 para consultar los tipos de borrado), con lo cual podremos usar cualquiera de los tres tipos mencionados para destruir la información. En el caso de que debamos transportar información fuera de las oficinas como esto se suele realizar en CDs, DVDs o memorias flash, se deberá de tener en cuenta el tipo de borrado para este soporte (sólo se pueden destruir mediante la destrucción física).

- Algo básico que todas las empresas y organizaciones deben tener es el Documento de Seguridad. Dicho documento viene regulado por lo establecido en el Reglamento de Desarrollo de la LOPD. El documento en cuestión, deberá de contener una serie de temas o aspectos básicos tales como: definir el ámbito de aplicación del documento donde se recojan los recursos a proteger, definir las medidas de seguridad tomadas así como los procedimientos de actuación para garantizar el nivel de seguridad óptimo, recoger las funciones y obligaciones del personal de la organización, definir la estructura de ficheros que tratan la información de carácter personal, así como las medidas de notificación y respuesta en caso de que se produzca alguna incidencia y los procedimientos para la realización de copias de seguridad así como las medidas de seguridad en caso de transporte de soportes y documentos. Este documento es de gran importancia, ya que su misión es dar a conocer a los usuarios de los ficheros las medidas de seguridad adoptadas por la empresa, esto es un dato importante ya que cada empresa tiene una organización distinta.

  En el documento deberán recogerse también los equipos informáticos usados en su tratamiento (servidores, ordenadores, etc.), aplicaciones usadas para el tratamiento (bases de datos, hojas de calculo,…), una descripción de la red de comunicaciones y los locales donde se aplicará la normativa elegida. En este documento también se recogerán tanto las normas de acceso físico a los locales u oficinas, como las normas de utilización de las aplicaciones

informáticas o los procedimientos a través del acceso a la red; deberán también de incluirse las pautas concretas para el uso de aplicaciones especificas como el correo electrónico, generación de contraseñas, etc.…

Junto al documento de seguridad, deberá incluirse un anexo, donde se recoja un listado de todas las personas con acceso a la información, y su rango dentro de la empresa, especificando a los niveles de información que tiene acceso en función de su posición.

- Obviamente, todas estas recomendaciones, son medidas de seguridad y aspectos básicos a tener en cuenta a la hora de diseñar un plan de seguridad para una entidad. Aunque estas medidas suelen ser tomadas por la organización, lo normal es que en los primeros días en los que un trabajador se incorpora, se le informe de las costumbres sobre seguridad que allí se siguen, así como de las políticas de empresa para evitar brechas en la seguridad. Aunque, si nuestra entidad dispone de los suficientes recursos, se podrían incrementar todos los sistemas hasta hacer una organización totalmente blindada frente a ataques.

13.2. Archivos físicos

Antes hemos visto las posibles recomendaciones mínimas para una empresa cuyo grueso de la información se trate en soporte electrónico. Ahora intentaremos ver algunas recomendaciones para el caso de empresas y organizaciones donde el soporte más manejado sea el de tipo papel.

Dos casos muy típicos de este tipo de empresas son las gestorías y notarías, empresas que se basan en la gestión y custodia

de documentos originales rubricados y con sello notarial, los cuales merecen una especial seguridad.

- Por regla general, el tipo de empresas antes mencionadas (gestorías o notarías) no suelen ser macro empresas o multinacionales, se catalogan en el rango de PYMES (Pequeñas y Medianas Empresas).

- Las recomendaciones a la hora de elegir el emplazamiento para nuestra entidad serían básicamente las mismas que para el otro tipo de empresa, poniendo un especial interés en dos amenazas concretas (fuego y agua), las dos con mayor potencial de destrucción de nuestro soporte en papel. Para lo cual tendremos especial cuidado en no elegir nuestra sede cerca de ningún río, mar o lago, y tomaremos las medidas de extinción de incendios necesarias para evitar cualquier incidente.

- Para todo el tema de control de accesos de personas físicas al lugar, así como su identificación, podemos tener en cuenta las mismas consideraciones que en el caso anterior.

- Para el tema de copias de seguridad se nos complica un poco la cosa con respecto a los sistemas informáticos, pues no podemos hacer copias de los documentos de forma semanal para preservarlos. Por norma general siempre se suele tener una copia del documento, dos a lo sumo, las cuales deberemos de custodiar nosotros pues no podremos realizar todas las copias que se quieran. Además, del inconveniente de que a cada copia que se realiza, más espacio físico que se ocupa.

- En el caso de empleados desleales la cosa se nos complica más aun. Puesto que en formato digital podemos tener mayores medidas de seguridad de las que nos encontramos en soporte papel.

En el caso de que un empleado se proponga destruir información (y lo consiga), con un sistema de información digital el mal es menor, debido a la gran cantidad de copias de seguridad que se hayan podido ir creando a lo largo del tiempo; pero si destruyera las dos o tres copias de un documento único, no habría posibilidad de recuperar dicha información, con todos los inconvenientes que ellos supondría.

- Para una destrucción segura de la documentación de que dispongamos en nuestra entidad, existen diversas empresas que nos proporcionan un servicio donde se nos garantiza la completa destrucción de la información y la confidencialidad. Dichas empresas te proporcionan la recogida y el transporte de la documentación hasta las instalaciones donde será destruida. El método más común es la trituración o la incineración del papel en trozos tan pequeños que resulta imposible su recuperación. Después de la destrucción se produce una compactación del papel para su posterior reciclaje en empresas de recuperación. Las empresas a su vez te permiten estar presente en el momento en el que se produzca la destrucción del papel, así como llegado el momento, te emiten un certificado de destrucción conforme a la documentación triturada.

14. Presupuesto

El objetivo del proyecto es desarrollar un documento donde se recogieran las principales amenazas a la seguridad y las posibles medidas que se pueden adoptar para mantenerla y preservarla.

El desarrollo del proyecto consistió en una búsqueda continua de documentación, la realización de un análisis exhaustivo, y la posterior consolidación de la información en el proyecto.

Las primeras fases de desarrollo de proyecto consistieron en establecer un índice, para saber qué puntos clave íbamos a tocar, y buscar información y documentación en internet, documentos y libros de la universidad, páginas webs específicas sobre seguridad, etc., para empaparnos bien y recopilar información al respecto del tema.

Cada cierto tiempo, mandaba una copia del proyecto a mi tutor del mismo, para su supervisión y que me fuera orientando en cuanto al estilo, forma, formato y contenidos del documento. Ese par de días en los que el se revisaba el trabajo, yo no paraba de buscar información y seguir redactando el documento.

Una vez él me contestaba con sus indicaciones, las plasmaba en el pfc y seguía con su desarrollo, hasta alcanzar otro momento en el que se lo volvía a mandar para su revisión, y repetíamos este último ciclo.

Cuando ya consideramos que el proyecto había alcanzado su fín, nos pusimos a organizar los remates, y demás cuestiones de última hora.

Adjuntamos un pantallazo del Gantt del proyecto para que se pueda observar mejor su desarrollo.

	Nombre de tarea	Duración	Comienzo	Fin	Pred	Nombres de los recur
0	**PFC**	**237,2 días**	**lun 12/12/11**	**jue 05/07/12**		
1	Inicio	0 días	lun 12/12/11	lun 12/12/11		Autor;Ordenador
2	Elegir y definir los límites c	3,4 días	lun 12/12/11	mié 14/12/11	1	Autor;Ordenador
3	Buscar documentación	13 días	mié 14/12/11	lun 26/12/11	2	Autor;Ordenador
4	Analizar la documentació	8 días	lun 26/12/11	lun 02/01/12	3	Autor;Ordenador
5	Escribir esquema del PFC	38,6 días	lun 02/01/12	vie 03/02/12	4	Autor;Ordenador
6	**Revisiones**	**8,4 días**	**vie 03/02/12**	**vie 10/02/12**		**Autor;Ordenador**
7	Revisión por el tutor	2 días	vie 03/02/12	lun 06/02/12	5	Autor;Ordenador
8	Aplicar modificaciones	4 días	lun 06/02/12	jue 09/02/12	7	Autor;Ordenador
9	Revisión por el tutor	2 días	jue 09/02/12	vie 10/02/12	8	Autor;Ordenador
10	Redacción del pfc	21 días	vie 10/02/12	mié 29/02/12	9	Autor;Ordenador
11	**Revisiones**	**7,8 días**	**mié 29/02/12**	**mié 07/03/12**		**Autor;Ordenador**
12	Revisión por el tutor	5 días	mié 29/02/12	lun 05/03/12	10	Autor;Ordenador
13	Aplicar modificaciones	3 días	lun 05/03/12	mié 07/03/12	12	Autor;Ordenador
14	Buscar más documentaci	10 días	mié 07/03/12	jue 15/03/12	13	Autor;Ordenador
15	Redacción del pfc	18 días	jue 15/03/12	vie 30/03/12	14	Autor;Ordenador
16	**Revisiones**	**8,8 días**	**vie 30/03/12**	**lun 09/04/12**		**Autor;Ordenador**
17	Revisión por el tutor	5 días	vie 30/03/12	mié 04/04/12	15	Autor;Ordenador
18	Aplicar modificaciones	4 días	mié 04/04/12	lun 09/04/12	17	Autor;Ordenador
19	Redacción del pfc	20 días	lun 09/04/12	jue 26/04/12	18	Autor;Ordenador
20	Modificar el esquema inici	4 días	jue 26/04/12	mar 01/05/12	19	Autor;Ordenador
21	Buscar más documentaci	10 días	mar 01/05/12	mié 09/05/12	20	Autor;Ordenador
22	Redacción del pfc	27 días	mié 09/05/12	vie 01/06/12	21	Autor;Ordenador
23	**Revisiones**	**21 días**	**vie 01/06/12**	**mié 20/06/12**	**22**	**Autor;Ordenador**
24	Revisión por el tutor	8 días	vie 01/06/12	vie 08/06/12		Autor;Ordenador
25	Aplicar modificaciones	13 días	vie 08/06/12	mié 20/06/12	24	Autor;Ordenador
26	Repaso general	15 días	mié 20/06/12	mié 04/07/12	25	Autor;Ordenador
27	Impresión y encuadernad	1 día	mié 04/07/12	jue 05/07/12	26	Autor;Ordenador
28	Fin	0 días	jue 05/07/12	jue 05/07/12		Autor;Ordenador

Figura 6. Tareas del Diagrama de Gantt

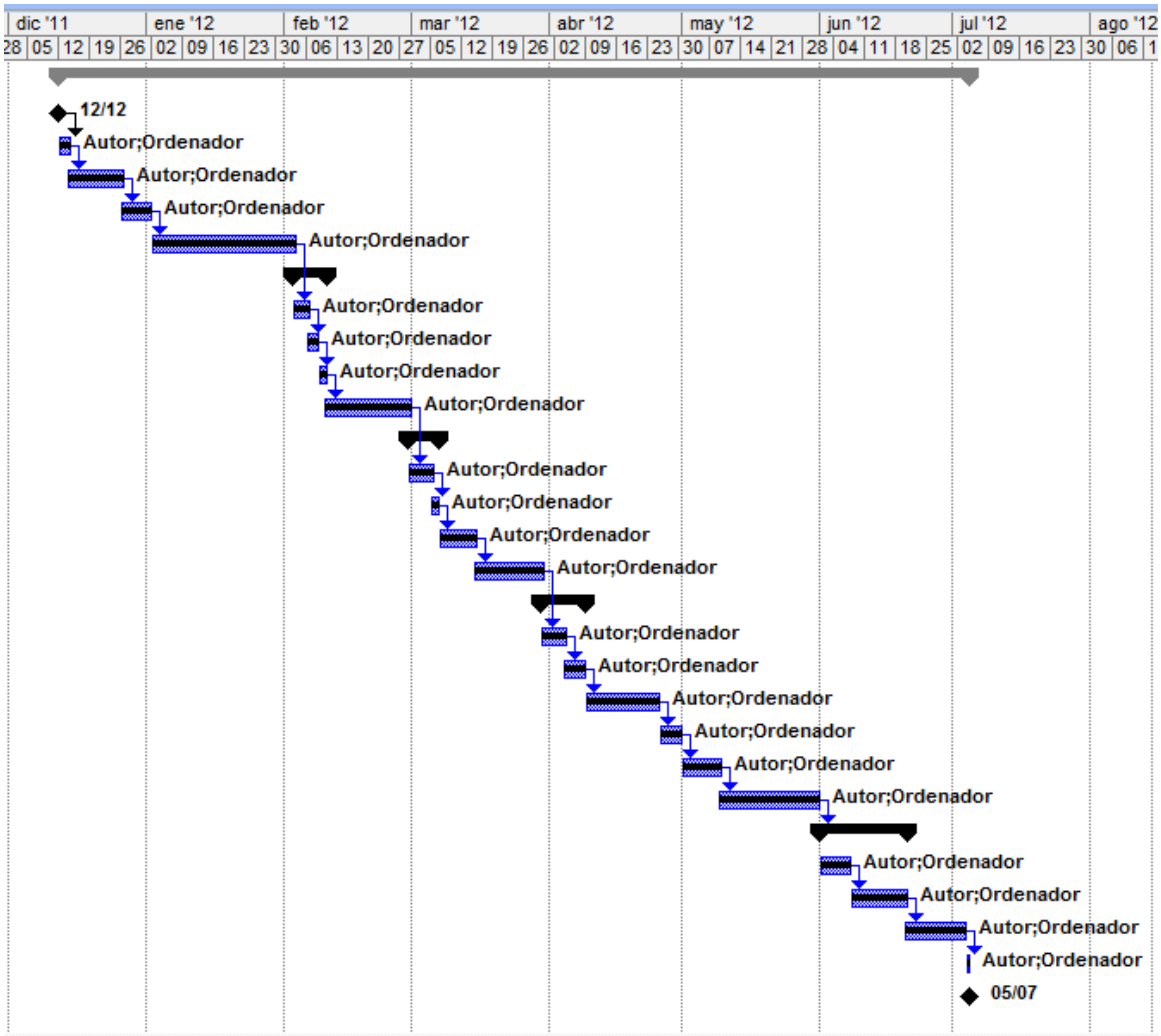


Figura 7. Diagrama de Gantt

Siendo objetivos, el desarrollo del proyecto se ha podido de considerar de "bajo" coste. En cuanto al coste personal sólo ha intervenido una persona (el autor), y siempre a media jornada, por lo que el coste en sueldo que podría tener es de unos 800 €/mes. En lo relativo al coste de material y otros recursos, debido a la necesidad de proveernos de un ordenador donde poder desarrollar este documento, el coste asociado ascendería a unos 400 €, por la adquisición del portátil. Además debemos considerar el gasto de internet, básico para estar conectados constantemente a la red y facilitarnos así la tarea de búsqueda de

información (60 €/mes) y un presupuesto de unos 20 € en total para fotocopias, en caso de necesidad de copiar algún documento de alguna biblioteca para su posterior análisis.

Desarrollo de los gastos:

800 €/mes * 8 meses = 6.400 € sueldo autor.
400 € por el portátil.
60 €/mes * 8 meses = 480 € internet.
20 € por fotocopias.

El presupuesto total de este proyecto asciende a la cantidad de 7.300 EUROS.

Leganés a 26 de Julio de 2012

El ingeniero proyectista

Fdo. Jorge Delgado Espino

15. Glosario

- **Activo:** *Todo elemento necesario o valioso para que la Organización cumpla sus objetivos.*

- **Afectado o interesado:** *Persona física titular de los datos que sean objeto del tratamiento [LOPD]*

- **Amenaza:** *Causa potencial de un incidente que puede resultar en un daño a un sistema u organización [ISO27002]*

- **Arco:** *Derecho de Acceso, Rectificación, Cancelación y Oposición para el almacenamiento de los datos de carácter personal.*

- **Auditar:** *Consiste en comparar lo que se hace con lo que se debería hacer.*

- **Certificado:** *Documento digital mediante el cual un tercero certifica la vinculación entre un sujeto y su clave pública.*

- **Clave privada:** *Pertenece a un sistema de identificación basado en clave pública y privada. La privada es con la que yo cifro (firmo) para que los demás puedan verificar su autenticidad.*

- **Clave pública:** *Pertenece a un sistema de identificación basado en clave pública y privada. La pública es la clave con la que todo el mundo puede descifrar algo que yo he cifrado.*

- Consentimiento: *Manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de los datos personales que le conciernen.*

- Datos de carácter personal: *Cualquier información concerniente a personas físicas identificadas o identificables [LOPD]*

- Evaluación cualitativa del riesgo: *Evaluación en la que los resultados sobre la probabilidad de que ocurra el incidente y la magnitud de las posibles consecuencias se expresan en términos cualitativos como "insignificante", "baja", "media" o "alta".*

- Evaluación cuantitativa del riesgo: *Los resultados de la evaluación del riesgo y sus posibles consecuencias se expresan en cifras.*

- Fichero: *Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso [LOPD]*

- Gestión del Riesgo: *Proceso de identificación, selección y aplicación de las medidas que permiten reducir el nivel de riesgo.*

- Malware: *Todo programa malicioso para nuestro equipo o sistema.*

-Propietario: *Este término, identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. Aunque no significa que la persona tenga en realidad derechos de propiedad sobre el activo.*

- Responsable del fichero: *Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. [LOPD]*

- Riesgo: *Evento que en caso de ocurrir, tiene consecuencias o impacta en los proyectos de forma negativa.*

- Widget: *Punto de interacción del Usuario con un programa. Suelen encontrarse en el escritorio para su directa manipulación.*

16. Referencias

[10CONSEJ] Diez consejos para la elaboración de una clave segura. Tú canal de Tecnología, Eroski Consumer. Internet.
<http://www.consumer.es/web/es/tecnologia/internet/2011/07/11/201596.php>

[AEPD] Agencia Española de Protección de Datos.
< http://www.agpd.es/portalwebAGPD/index-ides-idphp.php>

[ALEG] Definición de Seguridad informática. Alegsa, Portal de Internet, informática y tecnologías de la información. [Internet]
<http://www.alegsa.com.ar/Dic/seguridad%20informatica.php>

[CONST] Constitución española de 1978.
<http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCASTELLANO.pdf>

[DEFI] DefiniciónABC. Página dedicada a la búsqueda de definiciones. Disponible en Internet.
< http://www.definicionabc.com/general/riesgo.php>

[DOCSEC] Como redactar un documento de seguridad para las empresas. Por la Agencia española de Protección de Datos. Disponible en Internet.
<http://www.gli.es/rrhh/lopd/seguridad.pdf>

[ECUR] Ecured. Seguridad Informática. Disponible en Internet.
http://www.ecured.cu/index.php/Seguridad_Inform%C3%A1tica#Principios_b.C3.A1sicos_en_la_Seguridad_Inform.C3.A1tica.

[FIRDIG] Firma Digital. Disponible en Internet.
<http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php>

[IGN] Instituto Geológico Nacional. Ministerio de Fomento. Disponible en Internet.
< http://www.ign.es/ign/layout/sismo.do>

[ISO27001] Estándar Internacional ISO 27001. Disponible [Internet]
<http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf >

[ISO27002] Estándar Internacional ISO 27002. Disponible [Internet]
< http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html>

[LANI] Laninfor. Rumbo a la seguridad informática. Disponible en Internet.
< http://www.laninfor.com/index.asp?IdContenido=1>

[LOPD] Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de carácter personal.
<http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1999-23750>

[MODLOPD] Modificación de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de carácter personal.
<http://marketingpositivo.blogspot.com/2011/03/entrada-en-vigor-de-la-reforma-de.html>

[NSTI] Normalización en Seguridad de las tecnologías de la Información. Ministerio de Hacienda y Administraciones Públicas. Disponible [Internet].
<http://www.csi.map.es/csi/pg3441.htm>

[RD1720] 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.
http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

[THEN] 1234 The most common password. The next web. Artículo disponible en Internet.
<http://thenextweb.com/apple/2011/06/13/1234-is-the-most-common-iphone-passcode-app-developer-reveals/>

[UC3MSEG] La seguridad informática también es cosa tuya. Folleto informativo. Universidad Carlos III de Madrid.

[VERISIGN] Verisign, empresa de certificación web.
<www.verisign.es>

[VVIG] Guía de Inteco sobre Videovigilancia. Disponible en Internet.
<http://www.inteco.es/Seguridad/Observatorio/guias/guia_videovigilancia_2011>

17. Bibliografía consultada

Estrategia y Sistemas de Información. Ed. McGraw-Hill. Autores: Rafael Andréu, Joan E. Richard y Josep Valor

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. (BOE)

LEY ORGÁNICA 15/1999, de 13 de Diciembre, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. (BOE)

Apuntes UC3M, Gestión de proyectos. Profesor Miguel Recio Segoviano

Apuntes UC3M, Auditoría Informática. Profesor Miguel Ángel Ramos

Apuntes UC3M, Seguridad y Protección de la Información (ITIG).

La seguridad informática también es cosa tuya. Folleto informativo. Universidad Carlos III de Madrid.

Guía sobre las tecnologías biométricas aplicadas a la seguridad. Inteco. Disponible en Internet.
< www.inteco.es/file/ncKsGyFaqPdQ7ms3m2eDeA>

Página de la Agencia española de Protección de Datos.

Página de RSA, security
<http://www.rsa.com/go/gpage.aspx?id=42&activity_id=16701&division=rsa&gclid=COPxy_2chK8CFUcntAoddQlf0Q>