Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID

ESCUELA DE INGENIERIAS INDUSTRIALES

GRADO EN INGENIERÍA DE ORGANIZACIÓN INDUSTRIAL

ANÁLISIS DE MAGERIT Y PILAR

Autor:

De Santiago Bartolomé, Iván

Tutor:

Gonzalo Tasis, Margarita

Departamento de Informática.

Valladolid, julio de 2019.

Resumen:

El principal objetivo de este Trabajo Fin de Grado (TFG) es el análisis de MAGERIT, una metodología sistemática para el análisis y gestión de los riesgos que derivan del uso de la información, y Pilar, que consiste en una herramienta diseñada para analizar los riesgos de un sistema siguiendo la metodología de MAGERIT, con la intención de mejorarlas añadiendo propuestas, cambiando, modificando o eliminando procesos ya implantados, y asegurando el cumplimiento de todas las normas requeridas en el ámbito de la seguridad de la información.

Palabras clave:

Seguridad, información, análisis, ISO 27000.

Abstract:

The main objective of this End of Degree Project (TFG) is the analysis of MAGERIT, a systematic methodology for the analysis and management of the risks arising from the use of information, and Pilar, which consists of a tool designed to analyze the risks of a system following the MAGERIT methodology, with the intention of improving them by adding proposals, changing, modifying or eliminating already implemented processes, and ensuring compliance with all the standards required in the field of information security.

Keywords:

Security, information, analysis, ISO 27000.

ÍNDICE

INTRODUCCIÓN

Contexto y justificación del proyecto

Hoy en día, la seguridad informática es una de las principales inquietudes de toda organización, y con el creciente uso de las TIC, se hace más complicado mantener la información bajo protección debido a que cada vez hay más ataques cibernéticos y cada vez son más sofisticados. Estos ataques pueden provocar importantes daños, tanto personales como económicos, para la empresa y para los propietarios de la información robada.

Por tanto, se hace necesario prevenir estos y otros ataques que pueden afectar a la información privada de una empresa.

Debido a esta necesidad de protección, el Consejo Superior de Administración Electrónica del gobierno español elaboró una metodología para el análisis y la gestión de los riesgos de los sistemas de información, MAGERIT.

MAGERIT consiste en un método sistemático para el análisis y gestión de los Riesgos que derivan del uso de la información. Su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos. Su herramienta para aplicar esta metodología se llama Pilar “Procedimiento Informático-Lógico para el Análisis de Riesgos”.

Este método y su herramienta buscan proteger la misión de la Organización mediante un procedimiento sistemático que ayude a los sistemas de información a proteger el sistema con un nivel de confianza adecuado para proteger a la organización de cualquier accidente (ya sea voluntario o malintencionado) que comprometa la confidencialidad, disponibilidad e integridad de los datos y servicios de los que dispone la organización.

Objetivos

El objetivo de este Trabajo Fin de Grado (TFG) consiste en el análisis de la metodología MAGERIT y de la herramienta que utiliza esta metodología para analizar y gestionar riesgos de los sistemas de información, Pilar.

Se estudiará la metodología actual y, se intentará optimizar, de manera que resulte más sencillo trabajar con ella, se consiga una mejora del análisis y gestión de los riesgos y, por consiguiente, se consiga aumentar el nivel de protección en los sistemas de información que utilicen esta metodología.

Estas posibles modificaciones seguirán asegurando el cumplimiento de toda la normativa que requiere la seguridad de la información.

Estructura de la memoria

Introducción: El trabajo comienza con una breve explicación de la necesidad de proteger la información y los objetivos a los que se pretenden llegar con este informe.

Capítulo 1: Seguridad de la información. Se explica qué es la seguridad de la información y se justifica por qué es necesaria dentro de las empresas.

Capítulo 2: Sistema de gestión de la seguridad de la información. Se explica cómo se debe gestionar la seguridad de la información.

Capítulo 3: Normativa. Se definen las diferentes leyes que tratan sobre la seguridad de la información.

Capítulo 4: MAGERIT. Se describe la metodología que se quiere estudiar paso a paso y se detallan otros procedimientos similares.

Capítulo 5: Aplicación de MAGERIT con PILAR. Se realiza un caso práctico en el que se utilizan la metodología MAGERIT con su herramienta para analizarlas.

Capítulo 6: Propuestas de mejora: Se realiza un informe con propuestas para mejorar tanto la metodología MAGERIT como su herramienta PILAR.

Conclusiones: Se hace un juicio sobre el estudio una vez realizado el análisis.

Bibliografía: Lista de aquellos documentos consultados como apoyo para la realización del trabajo.

CAPÍTULO 1: SEGURIDAD DE LA INFORMACIÓN

1.1. Introducción

En la actualidad, han ocurrido recientemente ataques informáticos a organizaciones importantes, tanto públicas como privadas. Estos ataques contra la información de las empresas afectan desde los clientes hasta los accionistas de estas empresas pasando por todas las personas y organizaciones que están relacionadas directa o indirectamente con la empresa. En algunos casos muy extremos pueden afectar incluso a la seguridad del país.

Cualquier empresa con vistas a ser competitiva en estos tiempos, debe contar con unos sistemas de seguridad que den cierta confianza a los clientes y les asegure que sus datos privados no van a ser utilizados sin su permiso. [1]

Ejemplo: En el caso de que se vulnere el sistema de seguridad informático de un banco y sean robados los datos de clientes, podría ser conocida la situación económica de los clientes, sus direcciones, su edad, sus números de teléfono, etc. Esto puede ayudar a los posibles atracadores a fijar un determinado objetivo. Por parte del banco, además de lo costoso que puede ser reparar el sistema, posiblemente se tendría que enfrentar en juicios contra sus clientes, lo que conllevaría una pérdida de confianza de éstos. Por esta razón, un banco con unos sistemas de seguridad más avanzados que los de su competencia, tendrá mayor ventaja competitiva. [2]

En este tipo de casos, es necesario implantar un sistema de gestión de la seguridad de la información que opere de una manera sistemática y sea práctico. Este sistema de gestión tiene que asegurar que las medidas que se van a sacar de él, tanto las preventivas como las reactivas, van a ser capaces de resguardar y proteger la información de posibles ataques.

1.2. Seguridad de la información

La seguridad consiste en tener la certeza de estar protegido de algún riesgo o amenaza.

Consideramos información a todos aquellos datos que están en poder de una organización y tengan cierto valor para ésta, sin importar su origen (procedente de la propia entidad o de fuentes externas), cómo se almacena, cómo se transmite (escrita, oral, impresa, enviada por correo, etc.) o la fecha en que se obtuvo.

Se suele interpretar la seguridad informática y seguridad de la información como sinónimos, sin embargo, son ideas distintas pero relacionadas entre sí.

La **seguridad de la información** abarca a todas aquellas medidas y controles que previenen que se divulgue información de personas o sistemas. Tiene tres principios básicos: impedir el acceso a la información a usuarios no autorizados (Confidencialidad), proteger los datos de ser modificados de manera no autorizada (Integridad) y estar a disposición de quien tiene que utilizarla cuando tenga que utilizarla (Disponibilidad).

Cualquier vulnerabilidad en alguna de estas tres características de la seguridad de la información conllevará una amenaza para la entidad. Una buena seguridad de la información reducirá las posibles amenazas, y por consiguiente los posibles riesgos, y, además, hará que la imagen de la empresa sea más competitiva.

En los sistemas de información es muy difícil hablar de seguridad ya que no se puede determinar si un sistema es seguro debido a la gran cantidad y variedad de amenazas que puede haber en un sistema. En este caso hablaremos más de las vulnerabilidades que puede tener un sistema y catalogaremos el sistema según los tipos de ataques que puedan dañarlo.

En cambio, la **seguridad informática** es una rama de la seguridad de la información que trata sobre la prevención, detección y protección de los sistemas informáticos ante usos no autorizados. Abarca medidas de seguridad tales como antivirus o firewalls, con el fin de evitar intentos de conexión entre los equipos y la red no autorizados, etc.

Estos ataques pueden provocar daños en el sistema, comprometer datos confidenciales, dañar la información, disminuir el rendimiento del sistema...

Implantar medidas de seguridad en los sistemas informáticos conlleva un coste extra. Hay cuatro tipos de medidas de seguridad en los sistemas informáticos: Legales, administrativas, físicas y lógicas.

Las medidas físicas y lógicas son las encargadas de evitar los ataques, las administrativas se encargan de asignar responsabilidades y las legales ayudan a

los administradores a decidir contra qué tipo de acciones se ha de proteger al sistema.

Los sistemas informáticos como norma general, deben llevar incorporados ciertos mecanismos o subsistemas que aporten a los usuarios unos determinados servicios de seguridad. [3]

La Seguridad Informática se entiende como un proceso cíclico:

Figura 1. *La seguridad informática como proceso y no como producto* Fuente: [3]

1.2.1. Funciones de la seguridad de la información

Se pueden encontrar tres criterios indispensables para establecer la seguridad de la información: [3]

- Confidencialidad: La información solo puede ser utilizada por aquellos usuarios autorizados y que tengan el derecho legal a usarla, ya sean personas, programas, entidades…

  Ejemplo: En una compra por internet, el comprador tiene que introducir el número de la tarjeta de crédito, así como la fecha de caducidad y el código de verificación de la tarjeta. Una vez introducido, el sistema se encarga de cifrar los datos para asegurar que ningún tercero pueda hacerse con ellos. En caso de que un tercero no autorizado sea capaz de obtener estos datos, se habrá vulnerado la confidencialidad de la información.

- Integridad: La información no puede ser falseada, y se debe asegurar que lo que envía un emisor es lo mismo que recibe el receptor.

Ejemplo: El director de un banco recibe los informes de su subdirector sobre la contabilidad del banco, y tiene que asegurar que la información no va a ser modificada. Puede ocurrir que un empleado del banco que pueda disponer de esos datos, falsifique los datos de la contabilidad para transferirse dinero a él mismo. En ese caso se habría vulnerado la integridad de la información. Para proteger la integridad, se puede hacer uso de una clave de manera que sólo las personas que tuvieran esa clave pudieran modificar el documento.

- Disponibilidad: Esta propiedad indica quién puede tener acceso a la información y en qué momento puede acceder a ella. Se debe tener la seguridad de que aquellos usuarios no autorizados no van a poder llegar a obtener la información, y asegurar que los usuarios sí autorizados puedan disponer de la misma.

Ejemplo: Una universidad que imparte cursos por internet tiene que estar siempre disponible para sus usuarios, en caso de que sufra un ataque y tengan que cerrar la página web temporalmente, se habrá vulnerado la disponibilidad de la información.

Las normas ISO y CCITT en materia de servicios de seguridad de redes de datos aportan dos características necesarias en cualquier sistema de información:

- Imposibilidad de rechazo: la cual asegura que cualquier usuario que envíe o reciba información no puede demostrar que no la envió o recibió. Para esto se utilizan métodos como el correo electrónico certificado. Hay dos posibilidades: imposibilidad de rechazo en el origen (por el que el emisor no puede negar el envío de un mensaje) e imposibilidad de rechazo en el destino (por el que el receptor no puede negar que ha recibido un mensaje)

Ejemplo: En una compra por internet, para asegurar que, tanto el comprador ha pagado el servicio y ha recibido el servicio, como que el vendedor ha recibido el pago y ha proporcionado el servicio, se certifica que ambos han cumplido con sus partes con un certificado digital

- Autenticidad: por la que se tiene la certeza de conocer el origen y el destino de la información con métodos como la firma electrónica, la validación del correo electrónico, etc.

Ejemplo: El director de un banco recibe los informes de su subdirector sobre la contabilidad del banco, y tiene que asegurar que la información ha sido enviada por su subdirector y no por otra persona. Para proteger la

autenticidad, se puede hacer uso de la firma electrónica, de manera que el director no tendrá duda de quién ha enviado el informe.

Estas cinco características basadas en las 4 normas ya comentadas, deben estar interrelacionadas, y todas ayudan en la implantación de las medidas de seguridad que salvaguardarán al sistema de información.

Además de estas cinco características indispensables en todo sistema de seguridad de la información, hay muchas más funciones que debe cumplir un sistema de seguridad de la información:

- Autorización (Control de acceso a equipos y servicios): Esta función busca controlar a los usuarios que acceden a un determinado equipo o servicio del sistema informático mediante un proceso de autenticación basadas en unas Listas de Control de Acceso (ACL)

- Auditabilidad o trazabilidad: Control bajo un registro de la utilización de los recursos del sistema para registrar qué usuarios y en qué momento los han utilizado. Así se puede, además de controlar comportamientos extraños de los usuarios, controlar otros datos útiles para la organización (rendimiento, número de transacciones realizadas por cada empleado…)

- Reclamación de origen: Función utilizada para conocer con certeza quién ha creado un archivo.

- Reclamación de propiedad: Útil para conocer el usuario de un archivo protegido por derechos de autor, y asegurar que es ese usuario el que tiene la titularidad de los derechos de autor.

- Anonimato en el uso de los servicios: Función utilizada en algunos servicios en los que es conveniente asegurar al usuario su anonimato de manera que su privacidad quede siempre preservada. Este servicio de seguridad puede entrar en conflicto con algún otro, por lo que cada vez este servicio está siendo más restringido.

- Protección a la réplica: Esta función evita los llamados “ataques de repetición” por los que un usuario con malas intenciones puede interceptar y reenviar un mensaje con intenciones de vulnerar el sistema. Son protegidos con números de secuencia o sellos temporales de manera que se puedan detectar posibles mensajes repetidos.

- Confirmación de la prestación de un servicio o de la realización de una transacción: Asegura que se ha producido una operación indicando los usuarios que han intervenido.

- Referencia temporal: Este servicio certifica la fecha en las que se ha llevado a cabo una operación.

- Certificación mediante terceros de confianza: Utilización de terceros para certificar y avalar la identidad de los interesados.

1.2.2. Política de la seguridad de la información

El objetivo primordial de esta política es la implementación, mantenimiento y mejora de un SGSI, regido por la ISO/IEC 27001.

La Dirección General de la organización es la encargada de:

- Garantizar la confidencialidad, integridad y disponibilidad de la información que trata la empresa

- Cumplir con las normas tanto nacionales como internacionales.

- Asegurar una actividad empresarial continua sin interrupciones para convencer al cliente

- Lograr una respuesta rápida ante posibles incidentes

- Asegurarse de que todos los empleados comprenden la obligación de seguir unas normas de seguridad y la responsabilidad de acatarlas.

- Garantizar que las cláusulas firmadas con los clientes se cumplen

La dirección debe proveer al SGSI de todo lo necesario para garantizar que todos sus empleados conocen esta política y que se va a cumplir siempre. [3]

1.2.3. Objetivos de la seguridad informática

Los objetivos de la seguridad informática se basan en asegurar que la utilización de las aplicaciones y los recursos del sistema es la adecuada, ser capaz de detectar

los posibles riesgos y amenazas que pueden afectar a la seguridad del sistema, limitar las pérdidas en caso de que se materialice alguna amenaza, minimizar y controlar los posibles riesgos que pueda tener el sistema de información, ser capaz de recuperar el sistema adecuadamente en caso de que se materialice alguna amenaza, y cumplir con la legalidad y con los requisitos de los clientes en cuanto a protección de datos. [3]

Para conseguir estos objetivos hay cuatro planos de actuación en los que debe trabajar la organización:

- Humano: requiere la formación, tanto de empleados como de directivos, su sensibilización, reparto de responsabilidades y obligaciones, control de los empleados…
- Técnico: trata de seleccionar, instalar, configurar y actualizar tanto el hardware como el software adecuados. Utilización de criptografía, seguridad a la hora de usar aplicaciones…
- Organizativo: consiste en la implantación de normas y procedimientos que deben conocer tanto los directivos como los empleados, en temas de trato con terceros, respuesta de incidentes…
- Legal: En cada país o conjunto de países tienen una serie de medidas de seguridad de la información a la que toda organización debe adaptarse y cumplir con ella.

1.2.4. Consecuencias de la falta de seguridad

Según varios estudios que buscaban conocer como influían las pérdidas de información en pequeñas y medianas empresas, concluyeron con que cerca del sesenta por ciento de estas empresas tenían que cerrar después de la pérdida de información. También concluyeron que más del noventa por ciento de las empresas que habían sido atacadas durante más de diez días, declaraban la quiebra en un período máximo de un año.

El daño que produce un ataque a la seguridad informática de una organización no solo abarca todos los posibles daños a los equipos y a la información, sino que hay que sumarle otros daños importantes y costosos para la organización: [3]

- Coste de mano de obra por el tiempo utilizado en la reparación y reconfiguración del sistema.

- Coste de oportunidad: pérdidas ocasionadas por no tener disponibles los recursos necesarios en el momento que debían estarlo.

- Costes debidos a posibles multas o sanciones debido a la pérdida de información confidencial.

- Posibles consecuencias económicas por no cumplir la ley de protección de datos personales.

- Indemnizaciones a terceros por la posible difusión de datos personales

- Penas civiles para aquellas organizaciones que no dispongan de medidas de seguridad necesarias

- Posibles daños físicos a personas.

- Coste debido a retrasos, pérdidas, reducción de calidad del producto…

- Daño a la imagen de la empresa con posibles pérdidas de clientes o proveedores, daño a la reputación de la empresa…

Ejemplo: En el supuesto de que un banco sea atacado por un hacker, quien consigue acceder a información de los clientes y manipular sus cuentas bancarias. Una vez robados los datos de los clientes, el hacker conocerá el domicilio de los clientes, su nivel económico, su edad, etc. Esto puede facilitar a un atracador elegir una posible víctima para un atraco

A parte del valor económico del robo, entre otras consecuencias, los clientes perderán confianza en ese banco, se dañará la imagen de la empresa de cara a posibles inversores, seguramente tendrá que pagar indemnizaciones a los afectados por la difusión de sus datos personales a un delincuente, supondrá un coste reparar los daños en el sistema y asegurarlo para que no vuelvan a ocurrir estos incidentes, puede ser que tenga que parar la actividad durante la reparación, lo que provocaría pérdidas de ingresos en esas fechas, y, en un caso muy grave, podría llevar al banco a la quiebra.

En conclusión, un ataque a un sistema informático puede provocar números daños y muy costosos para la organización. La mejor manera de prevenirlo es contar con un buen SGSI que ayudará a evitar que estos ataques se produzcan.

1.2.5. Necesidad de la protección de la información

A lo largo de la historia, siempre se ha buscado la forma más eficaz para utilizar y transmitir la información, pero esto provoca un aumento de los riesgos que puede provocar ésta.

Disponer de información que no todo el mundo conoce o puede obtener, permite poder usarla para beneficio propio. Por ello es importante salvaguardarla utilizando los métodos adecuados para protegerla de posibles ataques. Como la información privilegiada puede acarrear beneficios al que la use adecuadamente, siempre va a haber alguien que intente conseguirla.

En la actualidad, hay sistemas con los que se puede enviar y recibir grandes cantidades de información de manera instantánea. Esto adquiere una gran importancia cuando se trata de transacciones bancarias en las que se utilizan tarjetas y cuentas bancarias. Estos datos hay que protegerlos de los posibles ataques.

La dificultad de proteger la información de los posibles ataques se basa en que cada vez hay más posibles atacantes con nuevas formas de intentar conseguir la información, y además, los medios utilizados para poder atacar un sistema son cada vez más complejos.

El problema de la información es la dificultad que tiene conocer el alcance que puede tener unos determinados datos para los atacantes. Hay información que se puede saber fácilmente que es útil para los atacantes, e información que puede parecer insignificante y ser muy útil para ciertos atacantes. [4]

Tanto el hardware, como el software, como el personal que utiliza o transmite información corren el riesgo de ser atacados.

- Hardware: Los ataques recibidos por el hardware pueden ser intencionados o involuntarios (Aquellas amenazas causadas por acciones inconscientes normalmente de los usuarios, muchas veces provocadas por falta de conocimiento). Un virus puede, entre otros, dañar el disco duro del sistema reduciendo su rendimiento o su efectividad, o dañar el microprocesador. En la actualidad, se están creando equipos que resistan de manera eficaz a estos ataques.

- Software: El software necesita de grandes conocimientos para poder protegerlo. La gran variedad de ataques que puede sufrir lo hace muy vulnerable.

- Personal: Todo el personal debe estar cualificado para tratar información. Cualquier error de un empleado puede suponer un daño muy grande para la organización.

Hay cuatro grandes tipos de amenazas a la información:

- Intercepción: Se produce cuando alguien o algo logra el acceso a algún punto del sistema donde no está autorizado. Un ejemplo es la copia de una base de datos. Es difícil de detectar debido a que normalmente no provoca ningún cambio en el sistema.

- Modificación: Este caso es semejante al anterior, solo que además de tener acceso a algún punto del sistema en la que no se tiene autorización, se cambia el funcionamiento del sistema. Ejemplos: Cambiar datos en una transferencia bancaria, cambiar contenidos de una base de datos, cambiar los códigos de un programa…

- Interrupción: Esta amenaza consiste en la intervención de algún agente externo en el sistema que pueda destruir el hardware, borrar bases de datos, programas, etc.

- Generación: Consiste en la introducción de datos en una base de datos, añadir parámetros a un programa, introducir mensajes no autorizados por el programa. Ejemplo: Virus informáticos.

Por todas estas posibles amenazas, se hace indispensable contar con una política de seguridad para poder realizar análisis de riesgos íntegros y poder incluir métodos y sistemas de seguridad que permitan salvaguardar la información. [3]

1.2.6. Beneficios de un SGSI:

La implantación de un buen SGSI, evidenciará la responsabilidad de la organización en el cumplimiento de la normativa de la seguridad de la información. Esto dará a la empresa una buena imagen ante los clientes, y la proporcionará una manera metódica, fácil y estructurada de analizar y gestionar los riesgos, con ello hará que tomar decisiones sea más sencillo y que aumente la credibilidad y la confianza de los clientes, empleados, proveedores y todas las terceras partes que tengan relación con la organización. Con todo esto, se puede esperar que la actividad de la empresa aumente y, por consiguiente, aumente los beneficios. [3]

1.3. Ataques al sistema informático:

El término Malware se utiliza para referirse a todos los software que son capaces de dañar e infectar a un sistema con malas intenciones que se introducen en un sistema sin consentimiento o sin conocimiento del usuario. Son capaces, en algunos casos, de reproducirse, de almacenarse en la memoria y de pasar inadvertidos para el usuario.

Estos Malware se pueden camuflar de muchas maneras, algunas pueden parecer aparentemente inofensiva pero ser muy dañinas para la organización. Es posible contagiar a tu sistema de algún virus mediante las redes sociales, mediante páginas web infectadas, mediante descargas de archivos de internet, mediante la entrada de dispositivos (CD, DVD, USB…) infectados, mediante correos electrónicos con archivos adjuntos infectados (también llamados spam), o mediante mensajes en internet utilizados para engañar al usuario. [3]

Hay muchos tipos de Malware que pueden dañar a nuestro sistema y se clasifican según su función o según como se introducen en el sistema: [5]

- Virus de boot: Se trata de virus que afectan al sistema según se inicia el equipo. El virus se introduce en la memoria y así controla el sistema desde que se ejecuta.

- Bombas lógicas o de tiempo: Se produce al cumplirse una o más condiciones en un programa o después de un tiempo determinado, el programa baja la calidad de su funcionamiento. Pueden ser capaces, entre otras, de borrar información del disco duro, enviar correos electrónicos, apagar el equipo, destruir ficheros, atacar a la seguridad del sistema enviando contraseñas a otro equipo, etc.

- Virus de enlace: También llamados de directorio. Consisten en programas que modifican las direcciones de acceso a los archivos para provocar la infección de estos archivos.

- Virus de sobre escritura: Este tipo de virus trata de sobrescribir información sobre la información original de manera que esta se pierda.

- Gusanos: Este tipo de Malware tiene como principal característica expandirse por el sistema, más que de infectar al sistema. Al instalarse en la memoria del equipo y expandirse, consumen mucha memoria y van disminuyendo la capacidad del dispositivo.

- Troyanos: Con este Malware, presentado mediante un programa aparentemente inofensivo y legítimo, una persona ajena al sistema puede entrar en el ordenador infectado y controlarlo, robar datos y contraseñas, instalar otros programas, etc.

- Hijackers: Llamados así a aquellos programas que manipulan nuestros navegadores modificando la dirección web, impidiendo acceder a algunas páginas web o llenando la pantalla de publicidad con pantallas emergentes.

- Keylogger: Se trata de una aplicación diseñada principalmente para robar contraseñas a los usuarios del equipo registrando las pulsaciones del teclado.

- Hoax: Este Malware envía bulos al usuario y su única intención es hacer que el usuario lo reenvíe a otros usuarios e intentar llegar al mayor número de usuarios.

- Joke: Se trata de un Malware cuya función principal es ocasionar molestias al visitante, por ejemplo, introduciendo contenido pornográfico en las páginas web. No es considerado un virus y solo sirve para molestar.

- Spyware: También llamado programa espía, consiste en un programa que roba información de un ordenador y lo transmite sin el consentimiento del usuario a otro equipo externo.

- Adware: Llamado así a cualquier programa o aplicación que muestre publicidad no deseada o engañosa sin consentimiento del usuario, tiene como finalidad el lucro de sus creadores.

- Phishing: Método utilizado para intentar conseguir información personal y confidencial del usuario utilizando mensajes fraudulentos, ya sea por correo electrónico o por llamada telefónica, y haciéndose pasar por alguna persona o empresa de confianza. Normalmente es utilizado para robar información sobre tarjetas de crédito o cuentas bancarias con el fin de robar dinero al usuario.

- Estado zombie: Es producido cuando un ordenador es infectado por algún Malware, y a partir de ahí, es utilizado por una tercera persona.

- Vishing: Consiste en la realización de llamadas telefónicas para supuestas encuestas, de manera que se engaña a la víctima para sacarla información personal sin que se dé cuenta.

- Baiting: El atacante "pierde", en algún sitio donde alguna víctima pueda encontrarlo, un dispositivo de almacenamiento extraíble, como puede ser un USB o un CD, infectado con un software malicioso, de manera que cuando el usuario que lo encuentre lo introduzca en su ordenador, el atacante podrá acceder a todos los datos de ese ordenador.

- Quid pro quo: El atacante realiza llamadas telefónicas a empleados de una empresa haciéndose pasar por el soporte técnico, y con la supuesta intención de resolver un problema, intenta normalmente conseguir datos de acceso, contraseñas.

Recomendaciones de seguridad:

- No instalar softwares de fuentes no fiables. Siempre del sitio web oficial.
- Tener la última actualización siempre que se pueda del sistema operativo
- Utilizar antivirus y tenerlo siempre actualizado
- Realizar copias de seguridad de manera periódica
- Instalar dispositivos diseñados para bloquear los accesos no autorizados a la red, también llamados firewall.
- Borrar periódicamente las cookies del ordenador
- Bloquear pantallas emergentes en el navegador
- Asegurarse de que un sitio web dispone de la política de privacidad antes de introducir algún dato personal.
- Asegurarse de que, al introducir datos confidenciales, la conexión entre el navegador y nuestro equipo está cifrada. Esto se puede saber porque aparece un candado en el navegador.

1.3.1. Ingeniería social

La ingeniería social puede ser considerado otro ataque a la seguridad de la información, y abarca todas aquellas acciones que, mediante el engaño o manipulación de usuarios legítimos y autorizados para acceder a una determinada información, se obtiene dicha información para un usuario ajeno. Hay muchas

maneras de hacer que un usuario se confunda para que desvele información privada, desde aportar directamente la información, desvelar la manera de llegar a esta información o la forma de vulnerar el sistema que guarda la información.

Los ataques más comunes consisten en la invención de una situación crítica e importante para la víctima que, haciéndole creer que es legítimo, en el momento que se lo crea, haga todo lo posible por solucionarlo dando datos privados que no debería dar. Otra forma muy común de engañar a la víctima consiste en suplantar a compañeros, amigos, la policía o a cualquier persona o entidad de confianza de la víctima para conseguir información o alguna acción de la víctima.

Algunos de los ataques relacionados con la ingeniería social son: el phishing, el vishing, el baiting y el quid pro quo. [3]

Ejemplo: En agosto de 2018, Caja rural sufrió un ataque de phishing. Este fraude consistía en el envío de correos electrónicos fraudulentos de un hacker haciéndose pasar por el banco. El asunto del correo era "Asunto importante" y en el contenido del mensaje indicaba que se había cancelado la cuenta del cliente por motivos de seguridad y que debía recuperarla. Su objetivo era que la víctima fuera dirigida a una página web donde tenían que poner sus datos de acceso a la cuenta online del banco. El hacker robaba estos datos para así poder acceder a su cuenta bancaria.

1.4. Protección de datos

1.4.1. Principios de la protección de datos

La manera más eficaz de proteger los datos consiste en utilizar procedimientos criptográficos

Toda organización pública o privada que trate datos personales tiene la obligación de cumplir el reglamento general de protección de datos, en adelante RGPD.

Debe aplicarse la RGPD con independencia de la cantidad de datos almacenados y aunque los datos se traten de manera automatizada.

El almacenamiento de los datos personales también tiene que cumplir la RGPD. [6]

Toda organización debe seguir estos principios:

- Principio de calidad de los datos que establece los límites que tiene una organización para tratar los datos de carácter personal.

- Derecho de información en la recogida de datos por la que los interesados que sean propietarios de los datos podrán conocer las condiciones de la empresa a la hora de tratar los datos.

- Consentimiento del interesado por el que éste acepta el tratamiento que se va a hacer con sus datos.

- Aquellos datos que revelen información comprometida del individuo deber estar especialmente protegidos

- Los datos relativos a la salud no podrán ser cedidos a no ser que lo consienta el interesado, lo autorice una ley, se necesiten por alguna urgencia sanitaria o para realizar estudios. No siendo necesario el consentimiento del interesado para la transmisión de los datos entre distintos centros de salud.

- Obligación de proteger los datos personales que se recogen mediante las medidas de seguridad necesarias.

- Cualquier persona que haya tratado los datos tiene la obligación de secreto desde que los trata y la obligación de protegerlos de terceros no autorizados. Vulnerar este deber de secreto puede suponer un delito leve, grave o muy grave dependiendo de los datos que se revelen.

- La comunicación de datos a un tercero que no sea el interesado, debe ser consentida por éste y con fines únicamente relacionadas con el servicio que se va a realizar.

1.4.2. Tratamiento de los datos personales

El tratamiento de datos personales abarca todas las acciones que se realicen con estos desde que son recogidos. Recoger, grabar, conservar, modificar, consultar, utilizar, bloquear o eliminar datos son algunas de las acciones que están incluidas en el tratamiento de los datos personales.

Hay tres momentos fundamentales en el tratamiento de datos, la recogida de datos (en los que el usuario aporta sus datos personales), la conservación y utilización de los datos (en los que se guardan y manipulan los datos), y la comunicación (en la que se transmiten los datos a terceros). En cada momento hay unas obligaciones definidas para proteger los datos del usuario.

El reglamento general de protección de datos (RGPD), entró en vigor en mayo de 2016, y fue aprobado por el parlamento europeo para ser cumplido en todos los

estados de la Unión Europea. Tiene el objetivo de regular el tratamiento de datos y ficheros de las personas físicas, empresas, asociaciones, comunidades y organismos y administraciones públicas.

En el tratamiento de datos pueden intervenir tres sujetos: El interesado (la persona titular de los datos), el responsable del fichero (quien decide la finalidad y el tratamiento de los datos), y el encargado del tratamiento (la entidad que lleva a cabo el servicio).

Siempre que la organización cuente con más de 250 empleados, traten datos de categorías especiales o relativos a condenas y delitos penales, o traten con datos que pueden poner en peligro a los interesados, tienen que contar con un registro de actividades de los responsables y encargados. En ellos se detallarán los datos de contacto de todas las personas implicadas en el tratamiento, los fines del tratamiento, las categorías de los datos del tratamiento (básicos, especiales o penales), personas responsables de cada fichero (responsable o encargado del tratamiento), análisis de la categoría del tratamiento (si es de alto riesgo, interés público, transferencias internacionales, etc.), .y comprobación de que se cumplen los principios del tratamiento de datos. [3]

1.4.2.1. Criptografía

La criptografía es una ciencia que se basa en la seguridad de los sistemas informáticos utilizando técnicas como el cifrado y codificado de los datos, lo que hace que éstos sean inteligibles a usuarios no autorizados. [6]

Hay tres tipos de ataques posibles a un criptosistema:

- Ataque a partir sólo del texto cifrado: El atacante plantea el ataque estudiando el cifrado para intentar conseguir la clave. El sistema debe ser capaz de resistir el ataque aun cuando el criptoanalista descubra la función de cifrado.

- Ataque a partir de algún mensaje conocido: Este tipo de ataque se produce cuando el criptoanalista conoce con seguridad la posición exacta de alguna o algunas palabras, y, a partir de esas palabras, trata de descifrar la función de cifrado relacionándolas con el mensaje cifrado.

- Ataque por elección de mensaje: Este ataque se puede producir cuando el criptoanalista es capaz de introducir palabras o mensajes dentro del sistema y puede descubrir su mensaje codificado.

1.5. Plan director de seguridad

Un Plan Director de Seguridad consiste en elaborar un proyecto para minimizar todo lo posible los riesgos en materia de información que puede tener una organización. Tiene que ser un proyecto que no impida desarrollar la actividad de la organización pero incluyendo las obligaciones y responsabilidades que tendrán que cumplir los trabajadores, tanto directos como indirectos, de la organización. Además debe estar actualizándose y mejorándose continuamente. [7]

Este PDS será distinto en función de las características de la empresa

El PDS tiene 6 etapas comunes para todo tipo de metodologías de análisis de riesgos, en ellas se trata de explicar de manera básica cómo realizar un análisis de riesgos para sacarle el máximo provecho.

Etapa 1: Definir el alcance

La fase inicial para realizar un análisis de riesgos consiste en definir el alcance del estudio. El alcance del estudio puede ser de toda la organización, o un alcance más especializado en unos determinados departamentos, procesos, sistemas, etc.

Etapa 2: Reconocimiento de los recursos

Se deben distinguir los recursos o activos más importantes dentro del alcance del PDS,

Etapa 3: Identificar las amenazas

Esta etapa consiste en reconocer los peligros a los que está expuesto el sistema. Hay muchas posibles amenazas en cualquier organización, por lo que hay que seguir una metodología que sea útil para prevenir todo tipo de ataques. Además hay que realizar un análisis de estas amenazas teniendo en cuenta el posible impacto que puede causar relacionándolo con la probabilidad de que esto ocurra. En este paso, es aconsejable seguir la metodología MAGERIT que se detallará más adelante.

Etapa 4: Identificación de vulnerabilidades y salvaguardas

Con esta etapa se pretende estudiar los atributos de nuestros recursos para reconocer las debilidades que puede tener el sistema, proceso o departamento. También en esta etapa, se analizan y detallan aquellas medidas de seguridad que se van a tratar en el sistema o parte del sistema que corresponda.

Etapa 5: Evaluación del riesgo

Una vez se ha definido el alcance, se han reconocido los recursos que están dentro del alcance, se han identificado las amenazas y vulnerabilidades, y se han analizado y detallado las medidas que se van a implantar en el sistema, se evalúa el riesgo de que se materialicen las amenazas, y se tratan aquellos riesgos que sobrepasen el límite de riesgo que la organización acepta.

Para cada amenaza que afecta a un activo, se evaluará la posibilidad de que la amenaza se lleve a cabo, teniendo en cuenta las vulnerabilidades y salvaguardas, y se estudiará el daño que puede causar a la entidad.

Etapa 6: Tratamiento del riesgo

Evaluados y calculados los riesgos por la regla de:

RIESGO = IMPACTO x PROBABILIDAD

Tenemos varias opciones para tratar los riesgos dependiendo que tipo de riesgo sea:

- Repartir responsabilidades externalizando algunas partes del sistema o contratando seguros para reducir el impacto.
- Eliminar el riesgo eliminando la raíz del problema, prescindiendo por ejemplo de algún procedimiento que pueda ser causa de un problema grave.
- Aceptar el riesgo siempre que sea de manera razonable, por ejemplo en caso de que minimizar el riesgo sea demasiado costoso y no sea rentable tratarlo.
- Ejecutar medidas para moderar el impacto en caso de que se materialice la amenaza.

Finalizando este proceso, hay que tener en cuenta que las medidas que tomemos en este análisis hay que detallarlas y priorizar las más importantes.

1.6. Defensa en profundidad

Este modelo de seguridad consiste en la implantación de un sistema basado en “barreras”.

La idea de este modelo es que si puedes proteger una determinada información con más de una medida de seguridad, mejor.

De esta manera, se dispone de un sistema de seguridad por capas, donde en cada capa se aplican distintos controles. [3]

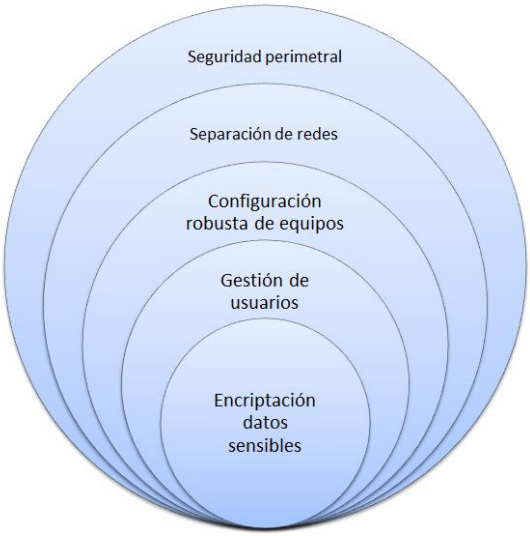

Figura 2. *Principio de defensa en profundidad*. Fuente: [8]

Con este sistema de seguridad, un atacante tendría que conseguir vulnerar todas las barreras para llegar a la información confidencial.

Ejemplo: En un caso sencillo, para acceder a un ordenador, necesitarás introducir tu usuario y contraseña, pero además de esta medida, se pueden aplicar otra como la protección a diversas aplicaciones instaladas en el ordenador para las que se necesita usuario y contraseña (distintas a las del inicio). De esta manera, para que un hacker pueda acceder a la información de esa aplicación, deberá pasar esos dos controles.

CAPÍTULO 2: SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. Sistema de gestión de la seguridad de la información

Con el fin de tener la certeza de que una organización tiene la información segura de posibles incidentes, se implanta un sistema de gestión de la seguridad de la información (SGSI).

Llamamos Sistema de Gestión de la Seguridad de la Información al conjunto de tareas y procedimientos necesarios para conseguir que una organización tenga implantada una manera de gestionar la seguridad de la información, de manera que cumpla todos los niveles de seguridad necesarios. [9]

Según la ISO/IEC 27001, un SGSI se define como *"la parte de sistema de gestión general, basada en un enfoque de riesgo empresarial que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos"*

Estos sistemas se rigen por unas políticas, las Políticas de Gestión de la Seguridad de la Información, que recogen todas las normas, reglas y procedimientos con los que se deben tratar los haberes de la organización.

La Gestión de la seguridad de la Información, podríamos dividirla en cuatro etapas:

- 1ª etapa: Etapa para asentar las medidas básicas de seguridad. En esta etapa abarcamos los controles de acceso, copias de seguridad…
- 2ª etapa: Esta etapa se centra en el cumplimiento de la legislación vigente (depende del país o conjunto de países).
- 3ª etapa: Gestión global de la seguridad de la información. En esta etapa se marcan las políticas de seguridad, el análisis y gestión de los riesgos, los planes y procedimientos de actuación, planes contra posibles ataques al sistema…
- 4ª etapa: Certificación de que las políticas utilizadas son buenas y útiles para poder garantizarlo ante terceros. La ISO 27001 marca un proceso de certificación.

2.2. Fases para la implantación de un SGSI

A la hora de implantar un SGSI, hay varias fases indispensables que todo SGSI debe cumplir:

- 1ª: Concretar las políticas de seguridad por La Dirección general y los empleados
- 2ª: Especificar el alcance del proyecto
- 3ª: Definir un Documento de Seguridad en el que se describen los puntos importantes del SGSI, se asignan responsabilidades y se asegura el cumplimiento de las leyes.
- 4ª: Crear un comité de seguridad que revise y actualice las políticas de seguridad según se vayan actualizando los posibles riesgos para la organización
- 5ª: Encargar un responsable que instaure el SGSI y que se encargue de encauzar y preservar el SGSI relacionándose con el comité de seguridad y con los responsables de la organización, y de realizar auditorías internas para controlar el SGSI.
- 6ª: Conocer y detallar los activos de la organización y asignar los responsables de ellos.

- 7ª: Analizar y gestionar los riesgos y crear un documento donde se reconozcan amenazas, vulnerabilidades y probabilidades de impacto. Así como las medidas que se han de tomar.

- 8ª: Crear un Documento de Selección de Controles de Seguridad

- 9ª: Crear un Programa de Mejora de la Seguridad siguiendo el modelo "Plan-Do-Check-Act".

- 10ª: Realizar auditorías internas y de certificación y seguir los consejos de la auditoría.

Ventajas que aporta un SGSI:

- Ayuda a conocer de manera amplia y detallada el funcionamiento de una organización

- Aporta un plan de mejora continua para la gestión de la seguridad informática.

- Reconoce vulnerabilidades y posibles amenazas para analizar riesgos y calcular su posible impacto.

- Ayuda a reducir costes previniendo posibles incidentes de seguridad.

- Asegura la continuidad del negocio.

- Ayuda a aumentar la confianza de los clientes

- Mejora la imagen de la empresa

- Permite cumplir con las leyes europeas y nacionales en relación a la protección de datos. [9]

2.3. Implementación de un SGSI haciendo uso del ciclo PDCA

El ciclo "PDCA" es una herramienta que busca mejorar continuamente una organización. Este método se puede aplicar en todos los procesos del sistema de gestión de la seguridad de la información.

Las siglas del proceso cíclico significan Plan, Do, Check, Act, en español planear, hacer, verificar y actuar.

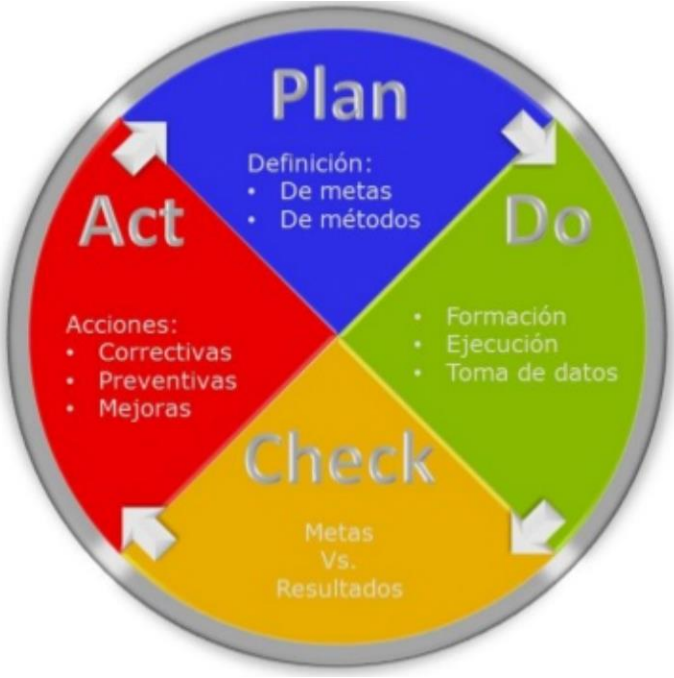

Figura 3. *Ciclo PDCA.* Fuente: [10]

Antes de iniciar un ciclo PDCA, se deben tener en cuenta las características de la organización, es decir, modelo de negocio, activos, tecnología utilizada, alcance del SGSI, etc.

Es posible implementar un SGSI, realizando un ciclo PDCA y aplicando la norma ISO/IEC 27001, sea la organización que sea ya que esta norma es muy flexible y abarca a todo tipo de organizaciones, ya sean grandes, pequeñas, cualquier tipo de negocio, etc.

Fases del ciclo:

- PLAN: En esta primera fase, se trata la planificación y el diseño del SGSI y las políticas que se van a aplicar en la organización. Se establecen las metas que se quieren conseguir, los medios que se usarán para conseguir estas metas, los activos necesarios, los procesos que se van a utilizar, los análisis de riesgos y las pautas que se seguirán para responder a posibles impactos.

  En esta primera fase del ciclo, se realizan las siguientes partes de la norma ISO/IEC 27001:

- Precisar el alcance del sistema de gestión.
- Detallar la política de seguridad
- Reconocer las vulnerabilidades y amenazas hacia los activos.
- Análisis y evaluación de riesgos
- Evaluar impactos.
- Definición del plan de tratamiento de riesgos
- Enumerar los activos necesarios
- Elegir los controles para cumplir la política de seguridad que se van a llevar a cabo

➢ DO: En esta parte del ciclo se trata de implantar las medidas planeadas en el primer paso del ciclo y poner en funcionamiento el sistema.

En esta segunda fase del ciclo, se realizan las siguientes partes de la norma ISO/IEC 27001:

- Implantar el plan de tratamiento de riesgos
- Implantar los controles necesarios para cumplir con la política de seguridad
- Asignar responsables a cada tarea

➢ CHECK: Se busca la verificación de que el SGSI cumple los requisitos que buscábamos al planearlo, y que, por lo tanto, cumple la norma ISO/IEC 27001. Se analiza el grado de cumplimiento de las políticas de seguridad y sus procedimientos, y en caso de que haya fallos, revisarlos y corregirlos. Se trata de controlar si los procesos se han ejecutado correctamente y han conseguido alcanzar los objetivos que debían alcanzar.

En esta tercera fase del ciclo, se realizan las siguientes partes de la norma ISO/IEC 27001:

- Revisión del SGSI

- Medición de la eficacia de los controles de la política de seguridad
- Elaboración de auditorías internas
- Control del funcionamiento de los activos utilizados para la seguridad del sistema.

➢ ACT: En esta fase del ciclo se trata de mantener y mejorar el SGSI, con medidas correctoras y preventivas para tener bajo control cualquier tipo de riesgo.

En esta cuarta fase del ciclo, se realizan las siguientes partes de la norma ISO/IEC 27001:

- Adoptar medidas correctoras
- Adoptar medidas preventivas
- Adoptar medidas que ayuden a mejorar el sistema

Una vez finalizada esta fase, se repetiría el ciclo otra vez comprobando los nuevos riesgos que puede haber tras llevar a cabo las nuevas medidas. El objetivo es obtener la certificación de que el sistema cumple con la normativa. [11]

2.4. Proceso de certificación

Con el fin de determinar si un sistema de gestión de la seguridad de la información es adecuado, se debe realizar un proceso de certificación, por una organización independiente, confirmado por escrito.

Esta certificación da una garantía de "calidad de la seguridad" a toda aquella organización que haya realizado un correcto SGSI. No obstante, esta garantía de calidad obtenida por las organizaciones que cumplen la norma, no aseguran de manera total la protección de la organización frente a los riesgos, pero sí ayuda a reducirlos de manera notable.

Esta certificación consta de dos pasos:

- Consultoría: Un equipo de expertos en la norma ayuda a la organización a cumplir con aquellos requisitos necesarios para obtener la certificación. También, se detallarán las medidas, tanto correctivas como preventivas, que se van a tomar en la organización.
- Auditoría: En esta etapa, un organismo experto en gestión de seguridad, revisa aquellos procedimientos requeridos por la norma y la implantación de los controles. En España, este organismo es AENOR (Asociación Española de Normalización y Certificación). [6]

CAPÍTULO 3: NORMATIVA

Con el fin de asegurar que la información va a estar bien protegida de posibles amenazas se utilizan unas normas o reglas que toda organización debe cumplir con el fin de proteger tanto a organizaciones como a clientes.

3.1. ISO/IEC 27000

La serie ISO/IEC 27000 se basa en unos estándares para proporcionar unas reglas para la gestión de la seguridad informática, formulados por ISO (International Organization for Standardization) y por IEC (International Electrotechnical Commision). Son útiles para todo tipo de organizaciones, ya sean grandes, pequeñas, públicas, privadas, nuevas, viejas… [10]

La serie ISO/IEC 27000 se compone de:

- ISO 27000: Esta primera norma establece los límites de cada una de las normas de la serie y detalla cada una de ellas, es decir, es un resumen de todas las normas de la serie. Explica la importancia de los SGSI y las etapas que hay que seguir para implantarlos, controlarlos, mantenerlos y mejorarlos.

- ISO/IEC 27001: Es considerada la norma principal y la única certificable de toda la serie, y el resto de las normas son para sustentar esta. Se basa en dos reglas principales: Una que explica como implantar, controlar, mantener y mejorar los SGSI y otra que explica el análisis y el tratamiento de los riesgos de la seguridad de la información.

- ISO/IEC 27002: Detalla los métodos para gestionar un riesgo relativo a la seguridad de la información y describe qué es lo que se quiere lograr utilizando ese control.

- ISO/IEC 27003: Detalla los puntos críticos en el diseño e implantación de un SGSI.

- ISO/IEC 27004: Explica la manera de utilizar unas técnicas de medida y como interpretar los datos obtenidos para como comprobar la eficacia de un SGSI.

- ISO/IEC 27005: Detalla distintas metodologías para llevar a cabo la gestión de los riesgos del SGSI en función del alcance de la organización.

- ISO/IEC 27006: Especifica las normas que han de seguir los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información.

- ISO/IEC 27007: Explica los procedimientos que tiene que seguir un organismo que realiza auditorías y certificaciones para llegar a tal certificación.

- ISO/IEC 27008: Explica cómo realizar las auditorías a los controles de seguridad que ya han sido implantados.

- ISO/IEC 27009: Detalla cómo se debe adaptar la ISO/IEC 27001 en sectores específicos.

- ISO/IEC 27010: Detalla qué métodos, procesos y controles hay que seguir para realizar un intercambio seguro de información.

- ISO/IEC 27011: Describe qué procedimientos prácticos se deben usar en el sector de las telecomunicaciones.

- ISO/IEC 27014: Explica como relacionar la estrategia de seguridad de la información con la propia estrategia que tenga la empresa.

- ISO/IEC 27015: Describe qué procedimientos prácticos se deben usar en el sector financiero y seguros.

- ISO/IEC 27016: Aporta información para ayudar a la toma de decisiones en relación a la seguridad de la información y ayuda a prever las consecuencias económicas de esas decisiones.

- ISO/IEC 27017: Aporta controles de seguridad en relación a la nube, pasos a seguir y recomendaciones.

- ISO/IEC 27018: Detalla los controles específicos necesarios para proteger la información personal.

- ISO/IEC 27019: Describe información detallada en relación al sector de la industria energética.

- ISO/IEC 27031: Analiza métodos y procedimientos para conocer las TIC y poder así mejorarlas dentro de una organización.

- ISO/IEC 27032: Explica la colaboración necesaria entre los miembros de una organización para evitar o reducir riesgos.

- ISO/IEC 27033: Detalla información con el fin de proteger la información que fluye por las redes.

- ISO/IEC 27034: Destinada a las aplicaciones utilizadas por las organizaciones.

- ISO/IEC 27035: Detalla controles específicos con acciones correctivas para determinados impactos.

- ISO/IEC 27036: Explica puntos fundamentales en las relaciones de la organización con los proveedores.

- ISO/IEC 27037: Esta norma trata sobre el trato que se debe dar a las pruebas digitales para investigaciones forenses.

- ISO/IEC 27038: Esta norma trata sobre la protección de ciertos documentos cuya forma de protección se basa en la eliminación de ciertas partes del documento.

- ISO/IEC 27039: Ayuda a elegir, implantar y utilizar softwares para proteger los sistemas.

- ISO/IEC 27040: Detalla cómo debe tratarse el almacenamiento de datos.

- ISO/IEC 27041: Trata sobre la investigación (métodos, procesos y procedimientos a seguir) de los incidentes de seguridad.
- ISO/IEC 27042: Trata sobre el análisis e interpretación de pruebas digitales para investigaciones forenses.
- ISO/IEC 27043: Detalla modelos de investigación para distintos escenarios en procesos forenses.
- ISO/IEC 27099: Detalla información específica para el sector sanitario.

3.2. ISO 27001:

La norma ISO 27001 es la norma principal de la serie, fue publicada en octubre de 2005 y establece los procedimientos y requisitos necesarios para los SGSI de una organización. [12]

Su estructura es:

Figura 4. *Diagrama de la estructura estándar de ISO/IEC 27001:2013. Fuente: AENOR (2014)*

Esta norma tiene dos tipos de requisitos fundamentales que se deben cumplir para conseguir un buen SGSI:

- Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI

- Requisitos para la evaluación y tratamiento de los riesgos.

Toda organización debe conocer aquellos aspectos que pueden afectarla para conseguir tener un SGSI adecuado. Para ello debe: [10]

- Definir las partes interesadas (llamado así a aquellas personas, grupos, equipos u organizaciones que están interesados en que se lleve a cabo el proyecto y/o que podrían ser afectados por alguna acción que se realice sobre el sistema de gestión de la seguridad de la información), para conocer sus condiciones o requerimientos para elaborar un buen SGSI.

Ejemplo: En una gran empresa formada en una ciudad pequeña, los interesados serán:

Los dueños del negocio, los inversores, los acreedores, los clientes, los sindicatos, las comunidades (que pueden verse afectadas por su impacto en la economía, impacto medioambiental, etc.), los clientes, los proveedores, los empleados de la empresa, los sindicatos de trabajadores… En conclusión, en toda empresa hay una gran cantidad de interesados, ya sean directos o indirectos, a los que les puede afectar una mala gestión de la seguridad de la información.

- Recoger los requerimientos y condiciones de las partes interesadas para satisfacerlas con un SGSI que se adapte a todas ellas. En algunos casos será necesario negociar con las partes interesadas para evitar posibles complicaciones, ya que puede ser imposible satisfacer a dos partes que tienen requisitos opuestos.

Ejemplo: En una empresa, un ingeniero puede considerar necesario cifrar los datos que se recojan de los pedidos que se encargan a un taller. Sin embargo, los operarios del taller no consideran este cifrado como algo importante, debido a que el volumen de pedidos no es muy grande y supondría un problema para los operarios que no disponen de los equipos necesarios para controlar ese cifrado, además del tiempo que supondría para estos llevar ese control.

Recogidos las opiniones y requisitos de ambos, se llegará a un acuerdo que satisfaga a las partes. En este caso, unas posibles soluciones serían adaptar nuevos equipos, no cifrar todos los datos, cifrar los datos mensualmente…

- Determinar el alcance del sistema a partir de sus límites y su aplicabilidad. Con esto se pretende determinar la cantidad de trabajo que se va a necesitar para conseguir los objetivos del sistema de gestión de la seguridad de la información. Se tienen en cuenta los requisitos de todas las partes interesadas, las relaciones entre los distintos procesos de la empresa y las relaciones con otras organizaciones, con la finalidad de conocer el trabajo necesario para llevar a cabo el SGSI y solo el requerido.

Ejemplo: Este SGSI cubre todos aquellos procesos, personas, información, sistemas de información, activos, y operaciones realizadas en la empresa X en la base de la ciudad Y.

En materia de liderazgo, la ISO 27001 detalla la importancia que tiene la dirección en el SGSI:

- La alta dirección tiene que asegurarse de establecer la política y los objetivos del SGSI y hacer que se puedan cumplir a la vez que los objetivos estratégicos de la organización. Además, deben garantizar que existen los recursos adecuados para realizar el SGSI.

- La dirección debe asegurarse de que la información en materia de seguridad llega a todos sus empleados

- La dirección debe mostrar liderazgo y compromiso con la organización.

- Es la encargada de asignar responsabilidades en materia de seguridad.

Para la planificación del SGSI es necesario conocer el alcance del proyecto para cumplir los objetivos del sistema de gestión de la seguridad de la información, así como los riesgos y oportunidades que hay que controlar.

Respecto a la evaluación de los riesgos:

- Hay que identificar los riesgos que actúan sobre el alcance del SGSI (por ejemplo con un análisis DAFO), así como los responsables de estos posibles

riesgos y los responsables de responder a esos riesgos identificados en el momento adecuado.

- Se deben detallar los criterios por los que se considerarán más importantes unos riesgos u otros, según su probabilidad e impacto, así como los criterios para aceptar riesgos. En caso de que no se encuentre una estrategia eficiente para mitigar un riesgo, estos riesgos se aceptan y son llamados riesgos residuales. Dependiendo del riesgo se les puede controlar, es decir, si es un riesgo importante se buscarían soluciones para intentar minimizar los daños que puede provocar.

- Todos aquellos riesgos identificados deben ser analizados y evaluados con los criterios establecidos, para conocer su importancia y poder priorizar unos sobre otros.

Una vulnerabilidad en el sistema puede ser la causa de una o varias amenazas. Es importante intentar conocer de dónde vienen los riesgos para poder combatirlos.

Ejemplo: Si se realiza una copia de seguridad y no se hace adecuadamente: podría producirse un acceso de un usuario no autorizado y robar los datos si no han sido cifrados, si el software utilizado no es el adecuado pueden aparecer virus informáticos que amenacen a la información de la copia de seguridad, podría no guardarse toda la información en la copia de seguridad, etc.

Todas estas amenazas provienen de la vulnerabilidad provocada al realizar mal la copia de seguridad, por tanto, corrigiendo los errores y llevando a cabo la copia de seguridad de manera correcta, se evitarían varias amenazas a la vez.

En cuanto al tratamiento de los riesgos:

Es necesario definir un plan para el tratamiento de los riesgos de la seguridad de la información, incluso para los riesgos residuales.

Los métodos para gestionar riesgos relativos a la seguridad de la información, así como las metas que tengan estos métodos, vienen determinados en esta norma.

Puede haber controles preventivos, correctivos y de investigación:

- Preventivos: Buscan evitar que surjan problemas.

Ejemplos: Publicar la política de seguridad para que llegue a todos los empleados de la entidad, hacer firmar contratos de responsabilidad, comunicarse frecuentemente con los empleados…

- Correctivos: Buscan actuar una vez se ha producido el impacto para corregir las consecuencias.

Ejemplo: Realizar copias de seguridad, formar a los empleados para responder ante situaciones de emergencia,

- De investigación: Busca encontrar irregularidades en el sistema

Ejemplo: Utilización de cámaras de seguridad, alarmas…

3.3. "RGPD" o Reglamento General de Protección de Datos:

El Reglamento General de Protección de Datos ha sido aprobado por el Parlamento Europeo en mayo de 2016 y puesta en vigor en mayo de 2018 con la intención de tener una normativa común para todos los Estados de la Unión Europea y su cumplimiento es obligatorio.

Este nuevo reglamento ha reforzado ampliamente la protección de datos. [13]

Los principios más importantes de este reglamento son:

- Prohibir salvo autorización: por este principio se prohíbe cualquier uso de los datos personas que no estén autorizados, sin excepción.

- Limitar la finalidad: Aquella organización que recopile y edite datos, lo tendrá que hacer con unos objetivos específicos, además de tener que documentar al poseedor de los datos del futuro de esos datos. Solo se permite modificar los objetivos en unos determinados casos.

- Minimizar los datos: Todas empresas que tengan que recopilar datos, recopilarán los mínimos datos posibles, pero los necesarios.

- Transparencia: Por este principio se da más derechos a los usuarios de los datos. Las organizaciones que recopilen datos deben comunicar los datos existentes y el uso que van a dar de ellos.

- Confidencialidad: Toda organización con datos personales, tiene la obligación de proteger los datos de sus clientes de modificaciones, robos o destrucción de dichos datos.

3.4. "LOPD GDD" o Ley Orgánica de Protección de Datos y Garantía de los Derechos personales

Esta ley, en vigor desde diciembre de 2018, sustituye a la antigua LOPD de 1999 y ratifica el reglamento general de protección de datos europeo a nivel nacional. [14]

Está compuesta por noventa y siete artículos divididos en diez títulos:

- Primero: relativo a las disposiciones generales, en el que explica los objetivos de la ley; adaptar la ley española al "RGPD" europeo, detallar el derecho de las personas a la protección de sus datos personales y garantizar los derechos digitales de la ciudadanía.
- Segundo: Principio de protección de datos
- Tercero: Principio de los derechos de las personas
- Cuarto: Disposiciones aplicables a tratamientos concretos
- Quinto: Responsabilidades y encargados del tratamiento de datos
- Sexto: Transferencia de datos internacionales
- Séptimo: Autoridades de protección de datos
- Octavo: Procedimientos en caso de vulneraciones de la normativa
- Noveno: Régimen sancionador
- Décimo: Derechos digitales

3.5. "LSSI-CE" o Ley de Servicios de la Sociedad de la información y comercio electrónico:

Aprobada en julio de 2002 y puesta en vigor en octubre de ese mismo año, esta ley se aplica a servicios que requieran de movimientos económicos en internet, es decir, comercio electrónico, información y publicidad, servicios de intermediación y contratación en línea.

Esta ley obliga a los proveedores y prestadores de servicios a informar a los clientes de las posibles amenazas de seguridad que pueden tener, las herramientas que

pueden utilizar para evitar contenidos indeseados y a informar de las medidas de seguridad que van a tomar en sus servicios. [15]

3.6. Ley de firma electrónica

Esta ley entró en vigor en diciembre de 2003.

(Art. 3.1) *"La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".* [16]

Por lo tanto, la firma electrónica permite garantizar la integridad, autenticación y la no repudiación en un sistema informático.

Características de la firma electrónica:

- Es personal y sólo el propietario de la firma la puede generar.
- Es casi imposible falsificar esta firma en la actualidad.
- Fácil de generar.
- Fácil de autenticar.
- No repudiable.
- Garantiza la integridad del documento firmado.

Se pueden distinguir dos tipos de firma:

(Art. 3.2) *"La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".* [16]

(Art. 3.3) *"Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".* [16]

Es decir, la firma reconocida es la única que es considerada como si fuera hecha a mano.

Para corroborar la firma electrónica reconocida se tiene que cumplir que:

- Identifique al firmante
- Verifique la integridad del documento firmado
- Garantizar el no repudio en el origen
- Estar basada en un certificado electrónico reconocido por el Ministerio de Industria y Comercio
- Debe de ser generada con un dispositivo seguro de creación de firma en el que las claves sean únicas y secretas

Con los cuatro primeros puntos se obtendría una firma avanzada, y si, además se cumplen los otros dos, sería una firma reconocida.

La firma con el DNI electrónico es considerada también una firma reconocida.

El ENI (Esquema Nacional de Interoperabilidad), detalla las normas y obligaciones de todos los involucrados en una firma.

El ENS (Esquema Nacional de Seguridad), define los principios y obligaciones de la política de seguridad para proteger la información y establece que tipo de firma debe aplicarse dependiendo el tipo de documento que se vaya a firmar.

CAPÍTULO 4: MAGERIT

MAGERIT "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" se centra en el punto 7 de las fases de implantación del SGSI, consiste en un método sistemático para el análisis y gestión de los Riesgos que derivan del uso de la información. Su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos.

Esta metodología se basa en cuatro objetivos principales:

- Concienciar a los responsables de la presencia de riesgos para el Sistema de Información y la necesidad de adoptar medidas para evitarlos, controlarlos o minimizar sus daños.

- Ofrecer un método común para analizar los riesgos en todas las organizaciones.

- Ayuda para la planificación de las medidas a adoptar en la organización.

- Facilitar todos los procesos relacionados con la gestión de los riesgos.

MAGERIT tiene muy presente la relación existente entre la utilización de las TICs y el control que debe hacerse sobre ellas, ya que son muy beneficiosas para las personas y entidades pero es importante también el riesgo que puede entrañar su utilización. La misión de esta metodología será minimizar estos riesgos y dar confianza a los usuarios de estos servicios.

Esta metodología tratará de medir los impactos y las probabilidades de que se materialice una amenaza y controlar así qué riesgos son más importantes y, por tanto, priorizar unos de otros. [11]

4.1. Proceso para la gestión de los Riesgos de la Información

El proceso de gestión de Riesgos consiste en el tratamiento y análisis de los riesgos que pueden afectar a una organización. [11]

- Con el tratamiento de los riesgos se pretende fabricar un plan de seguridad que permita a la dirección tener la confianza necesaria para comenzar o continuar con la actividad

- El análisis de riesgos pretende dar una aproximación de cómo de protegido está el sistema que estamos analizando.

4.2. Análisis y gestión de los riesgos de la información

La inversión en análisis y gestión de Riesgos de la información trata de prevenir los fallos y estar preparados por si estos ocurren. Lo ideal sería que no hubiera fallos pero es prácticamente imposible conseguirlo, por tanto, se acepta que va a haber fallos en los sistemas. Un buen sistema es aquel que en caso de tener un incidente informático, lo tiene bajo control, es decir, sabía que podía ocurrir, sabe lo que puede provocar y sabe arreglar el problema.

En esta nueva etapa de la sociedad en la que hay tanta dependencia y tantos beneficios de las tecnologías de la información y la comunicación, hay que tener en cuenta que estas tecnologías tienen riesgos que deben tratarse adecuadamente para dar seguridad a los usuarios de estos servicios.

Es recomendable realizar un análisis de riesgos en organizaciones que, para cumplir con su misión, utilicen sistemas de información y comunicación.

La norma [ISO 38500] indica cómo hacer un uso eficiente y adecuado de las TICS, de manera que ayudará a los responsables de las organizaciones a tener los riesgos y oportunidades bajo control en la medida de lo posible.

En definitiva, este método busca de alguna manera que todos los informes de análisis y gestión de riesgos sigan el mismo procedimiento. [11]

Figura 5. *Diagrama de análisis y gestión de riesgos. Fuente: www.ISO27000.ES*

4.3. Análisis de los riesgos

El análisis de riesgos pretende calcular el riesgo al que está sometida la organización mediante un procedimiento metódico.

Pasos:

1. Determinar aquellos elementos del sistema de información que pueden ser víctima de una amenaza y el coste que supondría que ese activo sufriera algún perjuicio.

2. Definir las amenazas que pueden causar algún perjuicio a los activos.

3. Definir las medidas de protección posibles y cómo de eficaces serían para minimizar el daño de las amenazas.

4. Evaluar el impacto, es decir, el perjuicio que provocaría al activo que una amenaza se materializara.

5. Evaluar el riesgo, es decir, el daño que provocaría a la organización que la amenaza se materializara.

Figura 6. *Diagrama análisis de riesgos. Fuente:* www.iso27000.es

1. Determinar aquellos elementos del sistema de información que pueden ser víctima de una amenaza y el coste que supondría que ese activo sufriera algún perjuicio.

Elementos que pueden ser víctimas de amenazas

Datos, servicios y equipos auxiliares, software, hardware, programas para el almacenamiento de datos, instalaciones, las redes de comunicación y las personas son componentes del sistema de información que pueden ser atacados y provocar perjuicios en la organización.

¿Cuánto costaría reparar los daños provocados en caso de que se materializara una amenaza?

- Coste de adquisición e instalación de un activo nuevo
- Coste de mano de obra utilizada para reparar el activo
- Pérdida de ingresos por la posible interrupción del servicio

- Pérdida de confianza de los usuarios que puede afectar a la demanda
- Posibles sanciones
- Daños a otros activos, personas o medioambientales.

Priorización de activos:

Valoración cualitativa: Colocando a cada activo en orden de mayor a menor importancia

Valoración cuantitativa: Valoraciones para determinar si merece la pena invertir en salvaguardas para un determinado activo, en cuánto tiempo se recupera la inversión, si es razonable tener un seguro por si ocurre alguna incidencia…

2. Definir las amenazas que pueden causar algún perjuicio a los activos:

Una amenaza se denomina a cualquier fenómeno que puede causar perjuicios a nuestro sistema de información o a toda la organización en un futuro

Las amenazas pueden ser:

- Externas
- Internas
- Naturales

Su grado de peligrosidad, se mide con dos cualidades:

- El grado de daño que provocaría sobre el activo
- La probabilidad de que la amenaza se materializara.

3. Definir las medidas de protección posibles y cómo de eficaces serían para minimizar el daño de las amenazas. A estas medidas se las llama salvaguardas.

Una salvaguarda consiste en un proceso o instrumento utilizado para actuar sobre un riesgo.

La misión de las salvaguardas es limitar la probabilidad de que se materialicen las amenazas (seguridad activa) y limitar el daño que pueden causar (seguridad pasiva)

Para definir las salvaguardas, hay que centrarse en los activos con mayor valor y que pueden provocar mayor perjuicio al sistema en caso de que fueran dañados.

Después en la probabilidad de que esa amenaza se materialice.

Y, por último, en la protección que dan a ese activo sobre esas amenazas otras salvaguardas.

Las salvaguardas pueden ser:

- Preventivas: En caso de que reduzcan la probabilidad de que se materialice una amenaza. Pueden ser preventivas, disuasorias o eliminatorias de la amenaza.

  Ejemplo: El uso de contraseñas en un sistema informático previene que un usuario no autorizado pueda acceder al sistema.

- Minimización del daño: En caso de que su misión sea minimizar, corregir o recuperar al activo en caso de ser dañado.

  Ejemplo: Una copia de seguridad no previene que se pierda la información debido a un ataque al sistema, sin embargo, reduce el impacto que puede provocar el ataque recuperando información.

- Apoyo a las demás salvaguardas: Pueden ser de monitorización, de detección, de concienciación o administrativas.

  Ejemplo: La detección de un ataque es fundamental para que puedan actuar el resto de salvaguardas. Si está sucediendo un ataque y no es detectado, no se pondrán en marcha las salvaguardas necesarias para eliminar el ataque.

Todo lo que no está protegido por las salvaguardas serán vulnerabilidades que pueden ser explotadas por una amenaza y causar daño al sistema, sin embargo, hay que aceptar algunas vulnerabilidades ya que no podemos invertir en una salvaguarda más dinero del que queremos proteger.

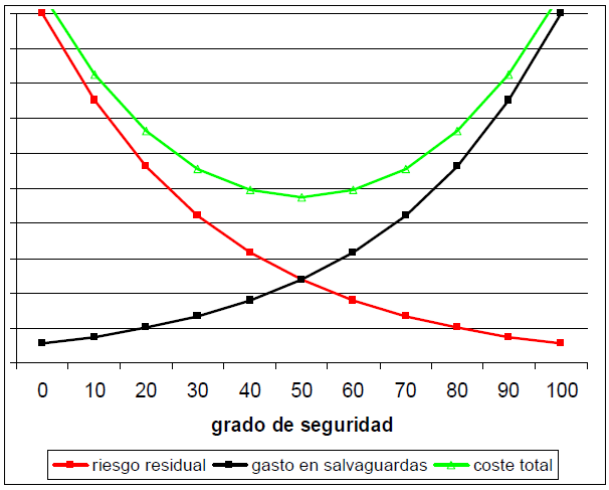

Figura 7. *Relación entre el gasto en seguridad y el riesgo residual.* Fuente: [11]

Esta gráfica explica como el coste para que un riesgo alto caiga rápidamente es bajo, y el coste de asegurar un riesgo al 100% es muy elevado. Económicamente hablando, se trata de buscar un equilibrio entre lo que se invierte en salvaguardas, y lo que se arriesga

4. Evaluar el impacto, es decir, el perjuicio que provocaría al activo que una amenaza se materializara.

Una vez realizados todos los pasos anteriores, las amenazas han pasado de tener un impacto potencial, a un impacto residual.

5. Evaluar el riesgo, es decir, el daño que provocaría a la organización que la amenaza se materializara.

Una vez realizados todos los pasos anteriores, el riesgo ahora ha pasado de ser potencial a ser residual. Se calcula usando el impacto residual y la probabilidad residual de que se lleve a cabo. [11]

4.4. Tratamiento de los riesgos

Los riesgos están determinados por el impacto que puede provocar una amenaza al materializarse y la probabilidad de que esa amenaza se materialice.

En caso de que el riesgo residual sea muy elevado, prácticamente solo se puede reducir el riesgo.

En la siguiente gráfica, se diferencian los riesgos por zonas según su impacto potencial y la probabilidad de que ocurra un perjuicio.

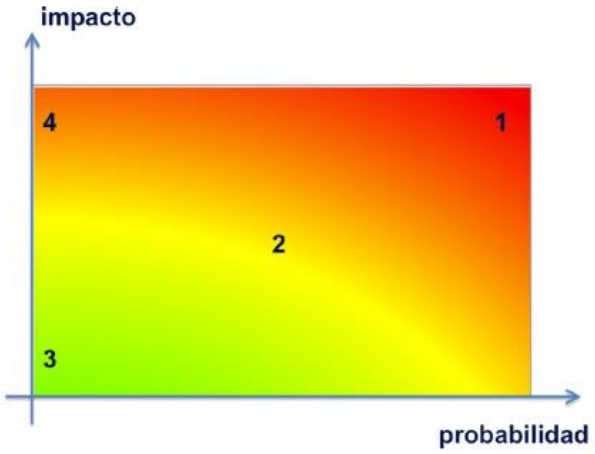

Figura 8. *Zonas de riesgo*. Fuente: [11]

- Zona 1: Los riesgos pueden provocar un fuerte impacto y son bastante probables. La solución será sacarlos de esta zona

- Zona 2: Tanto el impacto como la probabilidad son medios. Hay varias opciones que se pueden tomar.

- Zona 3: Tanto el impacto como la probabilidad son bajos. Se pueden dejar como están, o, en caso de que pudiera ser beneficioso para la organización, se podría arriesgar un poco y aumentar el riesgo a cambio de otras ventajas o posibilidades.

- Zona 4: El impacto que puede provocar un riesgo es muy alto, pero hay poca probabilidad de que esto ocurra. Lo más lógico será centrarse en salvaguardas para limitar el daño en caso de que la amenaza se materialice, además de salvaguardas para recuperar el activo.

En caso de no saber definir el posible impacto o la probabilidad de un riesgo, hay que buscar alguna manera de mejorar la previsión (consultando a expertos), intentar evitar el riesgo (cambiando alguna característica del activo o del sistema) o tener sistemas de detección temprana que permita avisar de la amenaza lo antes posible. [11]

Opciones para el tratamiento de los riesgos:

- Eliminación de la fuente de riesgo: Cuando el riesgo no es aceptable, se pueden eliminar algunos activos y sustituirlos por otros

- Mitigación: Consiste en reducir el impacto y la probabilidad de un riesgo. Se consigue mejorando las salvaguardas

- Compartición: Consiste en repartir responsabilidades externalizando algunas partes del sistema o contratando seguros para reducir el impacto.

- Financiación: Consiste en guardar unos fondos, llamados fondos de contingencia, para poder asumir los perjuicios que pueda provocar la materialización de un riesgo.

4.5. Otros procedimientos similares

4.5.1. CRAMM:

CRAMM es un procedimiento utilizado para el análisis de riesgos, creado por el Centro de informática y la Agencia Nacional de Telecomunicaciones (CCTA) de Gran Bretaña. Consiste en un procedimiento estructurado que busca asegurar la confidencialidad, integridad y disponibilidad de la información tratada en un sistema. Se puede aplicar a todo tipo de procedimientos, sistemas u organizaciones.

CRAMM es más sencillo y menos costoso que MAGERIT, pero esto supone unos análisis menos precisos y argumentados.

Con este procedimiento, se calculan los riesgos en una escala del 1 al 7, en la que el nivel 1 indica un bajo nivel de riesgo y el 7 un nivel de riesgo muy alto. [17]

Esta metodología consta de tres fases:

Fase 1: Registro y evaluación de los bienes

Se busca definir los objetivos en materia de seguridad, es decir, que es lo que hay que defender.

Se define el alcance, se registran y se valoran el hardware, el software, la información que va a almacenar el sistema y el resto de los activos.

Y, por último, se analizan los posibles impactos que puede provocar un posible daño en los bienes, de manera que los activos físicos se valoran por el precio que

costaría reemplazarlos o arreglarlos, y la posible información se valora según el impacto que puede sufrir la organización al ser atacada.

Fase 2: Identificación de amenazas y vulnerabilidades y cálculo de los riesgos.

En esta fase se trata de valorar la probabilidad de que se materialicen las amenazas sobre nuestro sistema, tanto las accidentales como las realizadas deliberadamente.

Fase 3: Evaluación y elección de salvaguardas

En esta última fase se escogen las medidas de seguridad que necesita el sistema y se evalúan los riesgos residuales (riesgo que queda permanente aunque se le trate con salvaguardas)

Esta metodología cuenta con un libro que explica detalladamente más de 3000 medidas a tomar dependiendo el riesgo. Además, el software de CRAMM analiza conjuntamente los riesgos con sus salvaguardas para calcular si cada riesgo es lo suficientemente importante como para implantar su salvaguarda. [18]

La metodología aplicada por CRAMM se puede resumir así:

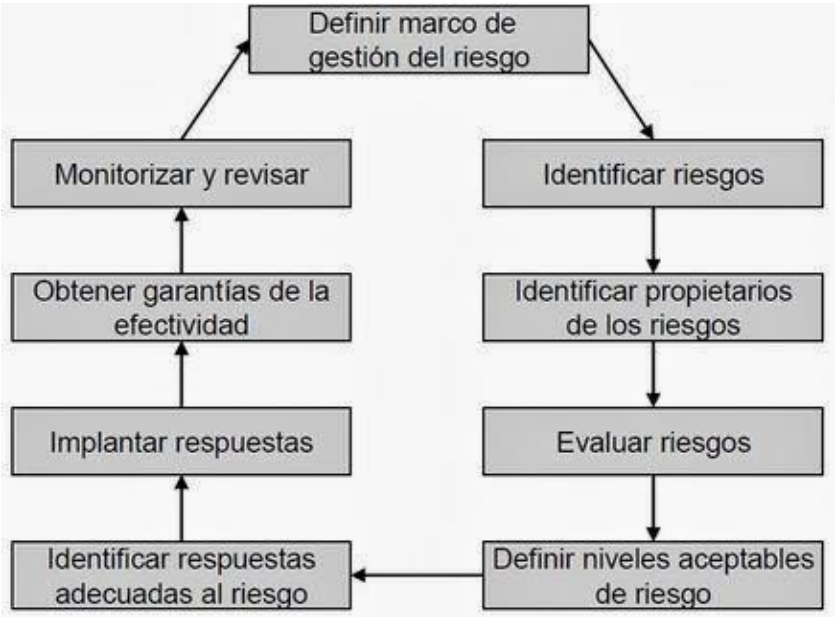

Figura 9. *Metodología CRAMM.* Fuente: http://evaluries.blogspot.com/

4.5.2. OCTAVE:

Esta metodología de análisis de los riesgos de las tecnologías de la información fue creada por la Universidad Carnegie Mellon en 2001. Proviene de “Operationally

Critical Threat, Asset and Vulnerability Evaluation", traducido al español, "Procedimiento de Evaluación de Amenazas, Activos y Vulnerabilidades Críticas". Busca preservar la confidencialidad, integridad y disponibilidad de la información y es usada por varios gobiernos alrededor del mundo, el de EEUU entre ellos. [19]

Consta de 3 metodologías diferentes dependiendo el sistema que se quiera tratar:

- La versión original(OCTAVE)
- Una versión para empresas pequeñas (OCTAVE-S)
- Una versión simplificada (OCTAVE-ALLEGRO)

Nos vamos a centrar en la versión original ya que es la más completa. Esta versión cuenta con una guía que incluye instrucciones detalladas para realizar todo el proceso, materiales de apoyo y ejemplos para facilitar su implementación. [20]

La metodología OCTAVE consta de 3 fases, y cada fase se compone de varios procesos: [21]

La fase 1 se encarga de organizar el plan que se va a ejecutar en el análisis de riesgos, la fase 2 de encontrar las vulnerabilidades que puede tener el sistema, y la fase 3 de encontrar una estrategia adecuada para la gestión de los riesgos.

Figura 10. Diagrama de fases OCTAVE. Fuente: [21]

Fase 1: Relación activos-amenazas

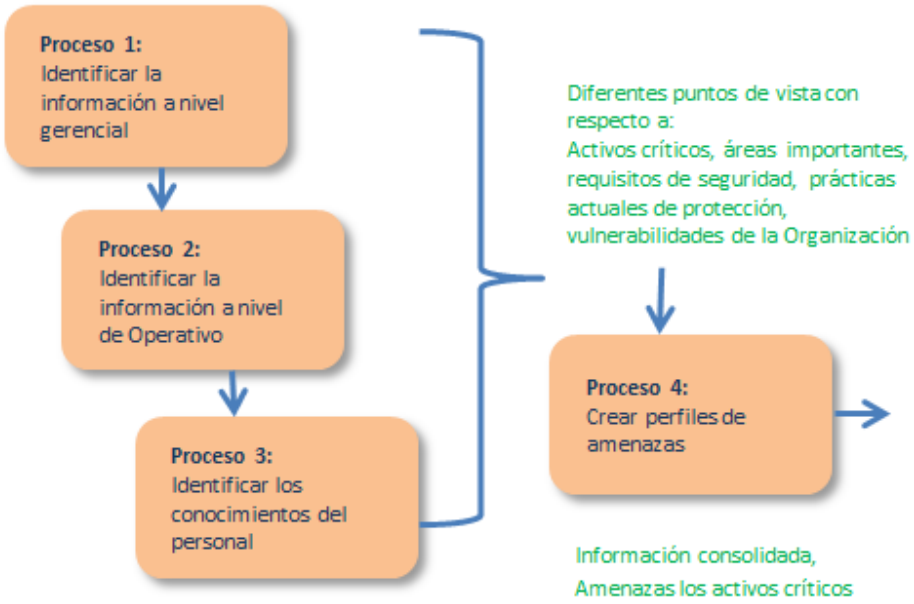

Figura 11. *Fase 1 OCTAVE*. Fuente: [21]

Los tres primeros procesos se centran en conocer los distintos puntos de vista de la Alta Dirección, los responsables de los distintos departamentos y los empleados de la organización respecto a qué activos son más importantes para la organización, priorizarlos respecto a otros, detallar aquellas situaciones en las que estos bienes pueden verse amenazados, explicar los requisitos de seguridad necesarios para esos activos y controlar las salvaguardas actuales sobre esos activos.

El cuarto proceso recoge toda la información que han aportado los 3 puntos de vista, y, a partir de ella, selecciona los activos más críticos para la organización, se detallan las posibles amenazas sobre estos activos críticos y se hace una valoración de los distintos requisitos de seguridad.

Fase 2: Localizar las vulnerabilidades

En esta segunda fase se realiza un examen a toda la infraestructura que abarque el alcance del análisis y se estudian sus posibles vulnerabilidades que puedan provocar daños contra los activos críticos

Figura 12. *Fase 2 OCTAVE*. Fuente: [21]

.

En el proceso 5 se seleccionan los elementos clave para cada activo crítico que tienen que ser analizados en busca de posibles vulnerabilidades.

En el proceso 6 se evalúan aquellos elementos cuyo daño puede tener repercusión para el activo crítico, con el fin de identificar sus vulnerabilidades

Fase 3: Análisis de riesgos y estrategia de protección

Esta última fase se centra en analizar los riesgos que pueden tener los activos críticos y plantear una estrategia para tratar esos riesgos.

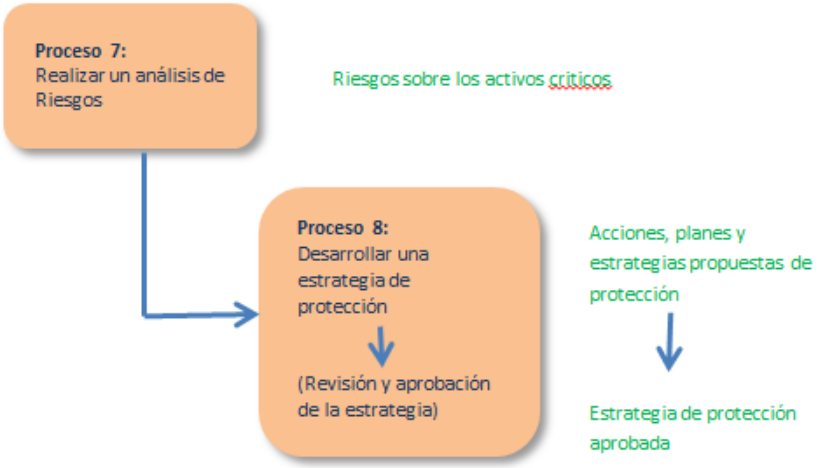

Figura 13. *Fase 1 OCTAVE*. Fuente: [21]

Durante el proceso 7, se reconocen los riesgos y su posible impacto (tanto por pérdidas económicas, como posible daño a la imagen de la organización, posibles daños a personas, etc.) con una escala simple (alto, medio, bajo)

Por último, en el proceso 8, se revisan todos los pasos anteriores y se crea un plan de protección y prevención a largo plazo, y una lista de operaciones a realizar a corto plazo debido a que requieran mayor celeridad. [21]

4.5.3. MEHARI

Esta metodología ha sido diseñada para analizar de manera precisa distintas situaciones de riesgo. Aporta una gran cantidad de soluciones y herramientas destinadas a la seguridad a corto, medio y largo plazo. Es flexible en cuanto a tamaño y madurez de la organización y adaptable a muchas situaciones de riesgo.

Esta metodología depende de una base de datos de información y técnicas computarizadas para la evaluación de cada riesgo. Además, este método ayuda a determinar los tratamientos que se les debe dar a esos riesgos. [19]

Para la evaluación de los riesgos se proponen dos alternativas:

- Hacer uso de la base de datos de la información (más simple)
- Utilizar una aplicación software (RISICARE2) (más óptima) con posibilidad de realizar simulaciones.

CAPITULO 5: APLICACIÓN DE MAGERIT CON PILAR

Vamos a realizar un análisis para una pyme utilizando para ello la herramienta PILAR Basic.

Hemos realizado el análisis con la metodología MAGERIT y su herramienta PILAR a un gimnasio de Valladolid.

El gimnasio consta de una recepción para la atención al cliente, situada al lado de la entrada al recinto del gimnasio, con 3 puestos de trabajo donde se recogen los datos de los clientes:

- Datos de carácter identificativo (nombre y apellidos, NIF/DNI, dirección postal, e-mail, teléfono de contacto y código postal)
- Características personales (fecha y lugar de nacimiento, sexo y nacionalidad)
- Datos bancarios

Para acceder al interior del recinto del gimnasio, hay que colocar una pulsera magnética o una tarjeta (a elección del cliente) en un lector magnético. Una vez leídos los datos, se permite el acceso mediante una barrera giratoria y llega la información del cliente a un monitor situado en la recepción para la comprobación de los trabajadores de la recepción, asegurando así que el usuario que ha entrado en el gimnasio es cliente de éste.

El gimnasio cuenta con una página web donde tienes que registrarte aportando el número de socio obtenido al darse de alta y donde se solicita e-mail y contraseña para poder acceder a la cuenta personal. Además cuenta con una aplicación (tanto para Mac como para Android) donde detallan los horarios de las distintas actividades y también se puede acceder a la cuenta personal utilizando e-mail y contraseña.

5.1. Identificación de activos:

Primera fase y la más importante del análisis, ya que una buena identificación de los activos permitirá valorar los activos con precisión, analizar las dependencias entre los distintos activos, conocer de manera precisa las posibles amenazas y riesgos para la organización y ayudará a elegir las salvaguardas que se tienen que implantar.

Se pueden seguir todos los pasos a realizar en el manual del usuario. [22]

Hemos creado dos dominios de seguridad. Uno relativo a la red corporativa por la que interactúan todos los trabajadores del gimnasio y otra relativa a la conexión a internet de la empresa.

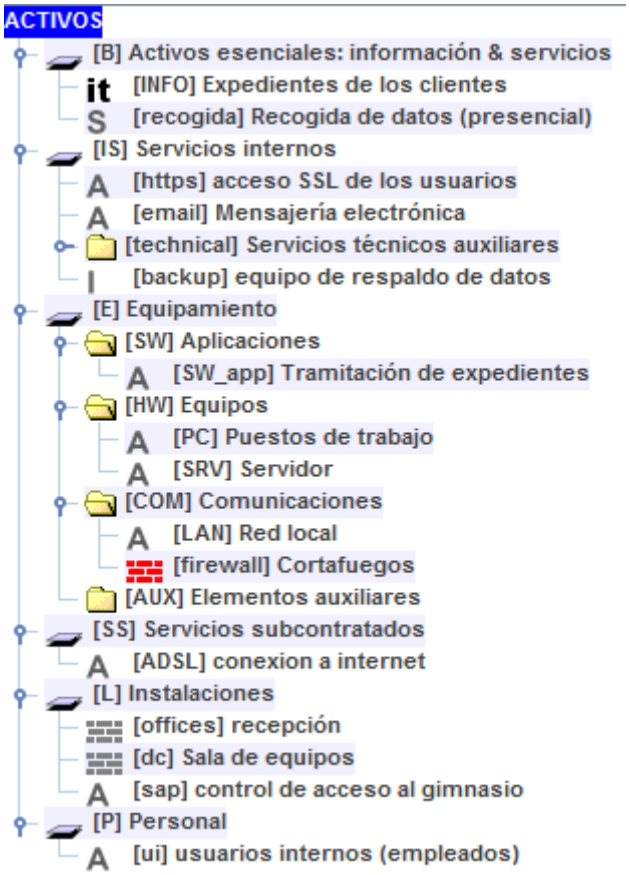

Figura 14. *Identificación de activos.* Fuente: PILAR

Hemos considerado activos esenciales para la seguridad de la información los datos recogidos en el registro de los clientes (información), donde se requiere principalmente confidencialidad e integridad y la recogida de estos datos por los trabajadores de la recepción (servicio), donde se requiere principalmente disponibilidad.

El gimnasio tiene una aplicación utilizada para la recogida y el almacenamiento de los datos de los clientes de manera segura (SW_app), que cuenta con una copia de seguridad.

La web del gimnasio cuenta con el certificado SSL, por lo que se asegura que cualquier información confidencial que se aporte en ella, estará cifrada.

Se cuenta con varias cuentas de correo electrónico para la atención al cliente, para la comunicación con proveedores y para la comunicación entre empleados.

En los puestos de trabajo, se cuenta con tres ordenadores. Para acceder a ellos los empleados tienen que introducir usuario y contraseña.

Cuentan con un servidor red que permite el acceso a recursos compartidos en las distintas estaciones de trabajo, una red de área local con sus equipos conectados inalámbricamente al servidor red.

El gimnasio contrató una línea de ADSL que incluye el teléfono fijo de atención al cliente y la conexión a internet del gimnasio.

Como dispositivo de seguridad para controlar el acceso a los elementos de la red, se ha instalado un firewall.

5.2. Valoración de los dominios

Sirve para conocer la importancia para la organización de los distintos activos.

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[GIM] Gimnasio							
[essential] Activos esenciales	[8]	[8]	[8]	[6]	[7]		[1]
[INFO] Expedientes de los clientes		[4]	[7]	[4]	[4]		[1]
[recogida] Recogida de datos (presencial)	[8]			[6]	[7]		
[backup] equipo de respaldo de datos	[7]	[8]	[8]	[4]			
Dominios de seguridad							
[base] red corporativa	[8]	[8]	[8]	[6]	[7]		[1]
[INFO] Expedientes de los clientes		[4]	[7]	[4]	[4]		[1]
[recogida] Recogida de datos (presencial)	[8]			[6]	[7]		
[backup] equipo de respaldo de datos	[7]	[8]	[8]	[4]			
[bps] conexión a Internet							

Figura 15. *Valoración de los dominios.* Fuente: PILAR

En este paso se determina la importancia de los activos para la empresa. Se valoran, según su disponibilidad (D), integridad (I) y confidencialidad de los datos (C), autenticidad de los usuarios y de la información(A), trazabilidad del servicio y de los datos (T), valor (V) y datos personales (DP).

Los expedientes de los clientes requieren principalmente confidencialidad e integridad; la recogida de los datos, disponibilidad, autenticidad y trazabilidad; y el backup, requiere de integridad, confidencialidad y disponibilidad.

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto(-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo(+)
1	Bajo
0	Depreciable

Figura 16. *Criterios de valoración.* Fuente: Manual Básico Herramienta PILAR

5.3. Factores agravantes/atenuantes:

En esta pantalla se permite calificar a los dominios para establecer las posibles amenazas a las que puede estar expuesto el sistema.

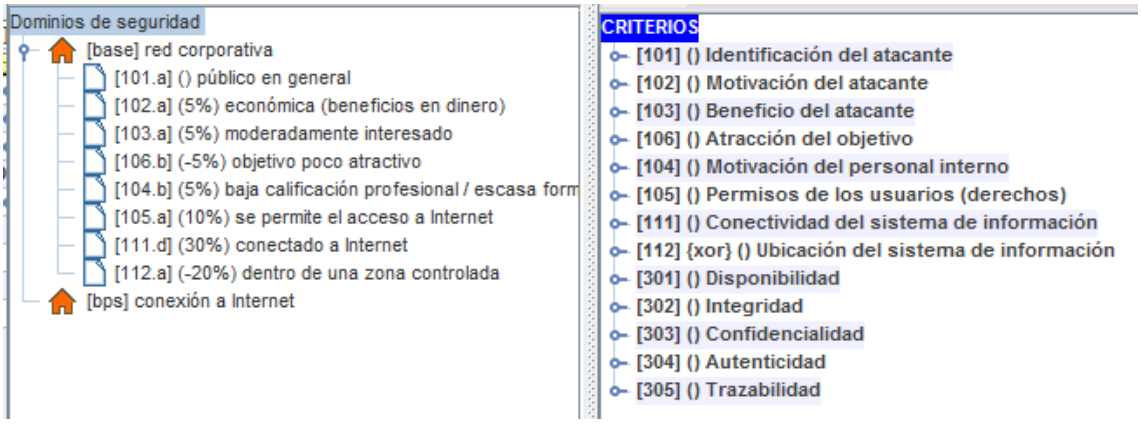

Figura 17. *Factores agravantes/atenuantes.* Fuente: PILAR

En este caso, detallaremos paso a paso la situación de la empresa respecto a posibles ataques.

5.4. Amenazas

Una vez introducidos todos los datos en los pasos anteriores, el programa proporciona automáticamente las posibles amenazas para cada activo.

Hay 5 tipos de amenazas:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques deliberados
- [PR] Riesgos de privacidad

"El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, que puede pasar, que consecuencias se derivan y como de probable es que pase. Podemos resumirlo en la expresión "Conoce a tu enemigo"." [11]

Figura 18. *Amenazas.* Fuente: PILAR

5.5. Eficacia de las salvaguardas:

La herramienta PILAR analiza los parámetros introducidos y nos informa de cuáles son las salvaguardas. Una salvaguarda perfecta tendría una eficacia del 100% (L5). Se necesita la eficacia de las salvaguardas para calcular el impacto y el riesgo residual sobre los activos.

nivel	significado	eficacia
L0	inexistente	0%
L1	inicial / ad hoc	10%
L2	reproducible pero intuitivo	50%
L3	proceso definido	90%
L4	gestionado y medible	95%
L5	optimizado	100%

Figura 19. *Eficacia de las salvaguardas.* Fuente: PILAR

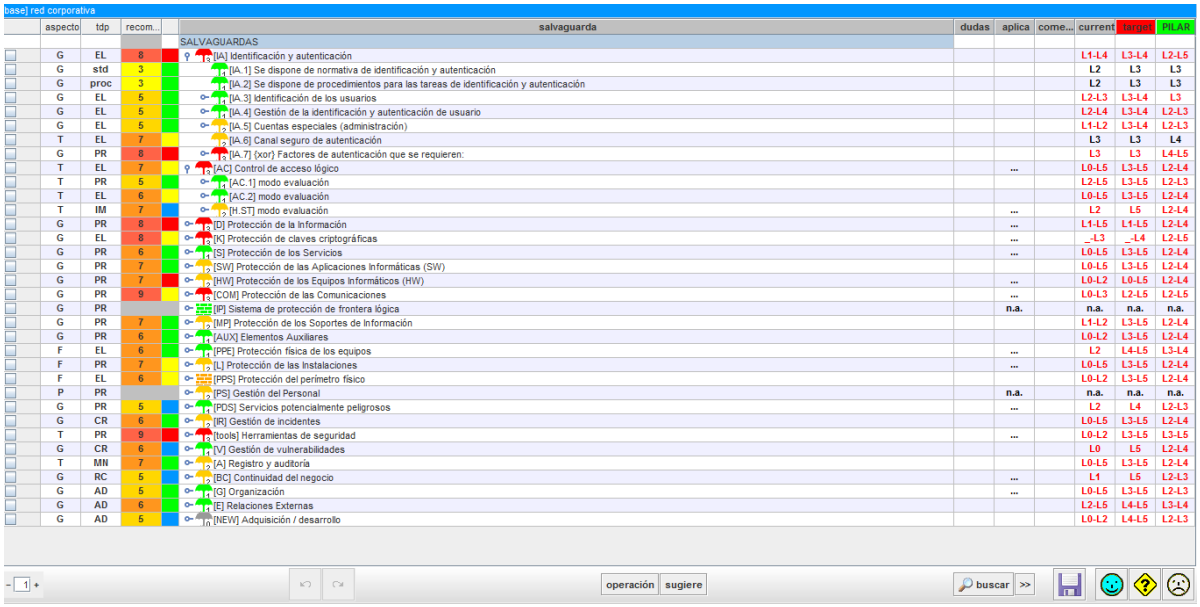

Figura 20. *Eficacia de las salvaguardas 1.* Fuente: PILAR

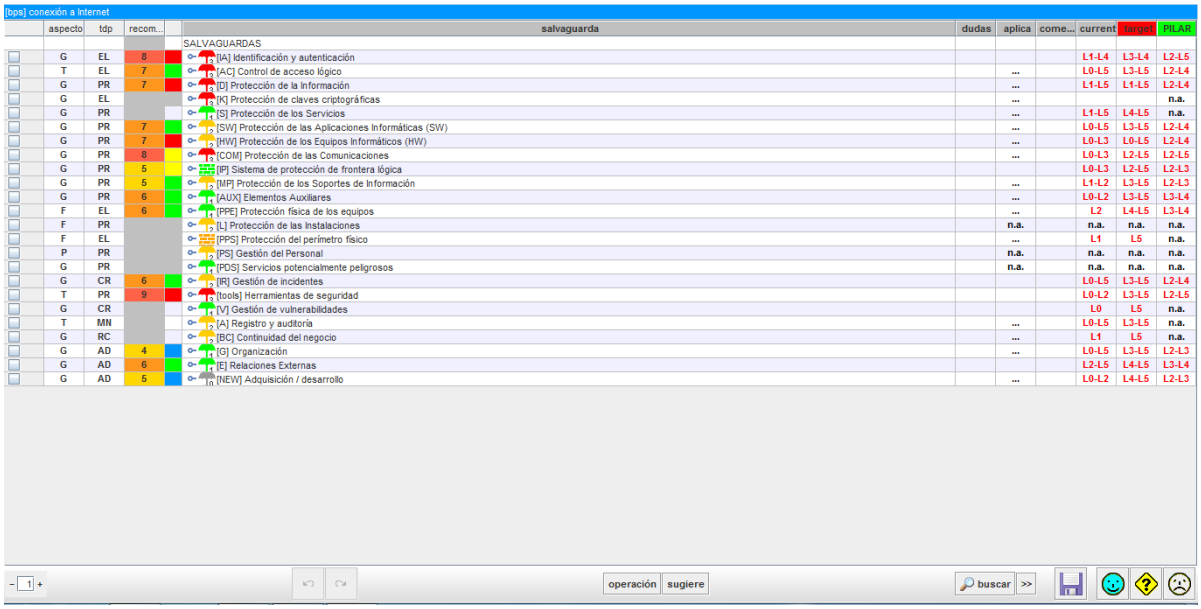

Figura 21. *Eficacia de las salvaguardas 2.* Fuente: PILAR

PILAR recomienda para cada salvaguarda que nivel de importancia tiene para nuestro sistema. En este caso las más importantes son las salvaguardas de identificación y autenticación, control de acceso lógico, protección de la información, protección de las claves criptográficas, protección de las comunicaciones y las herramientas de seguridad contra códigos dañinos.

3	máximo peso	crítica
2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

Figura 22. *Importancia de las salvaguardas.* Fuente: Manual PILAR Basic

Para cada salvaguarda, el programa te explica el aspecto de las salvaguardas, es decir, pueden ser de gestión “G”, de aspectos técnicos “T”, de seguridad física “F” o relacionado con el personal “P”. Además te explica el tipo de protección de cada una de ellas en la columna “tdp”. Pueden ser: de prevención “PR”, de disuasión “DR”, de eliminación “EL”, de minimización de impacto “IM”, de corrección “CR”, de

recuperación “RC”, administrativa “AD”, de concienciación “AW”, de detección “DC”, de monitorización “MN”, normas “std”, de procedimiento “proc” o de certificación o acreditación “cert”.

Introduciendo el nivel de madurez en cada fase, el programa nos dará automáticamente las salvaguardas más eficaces.

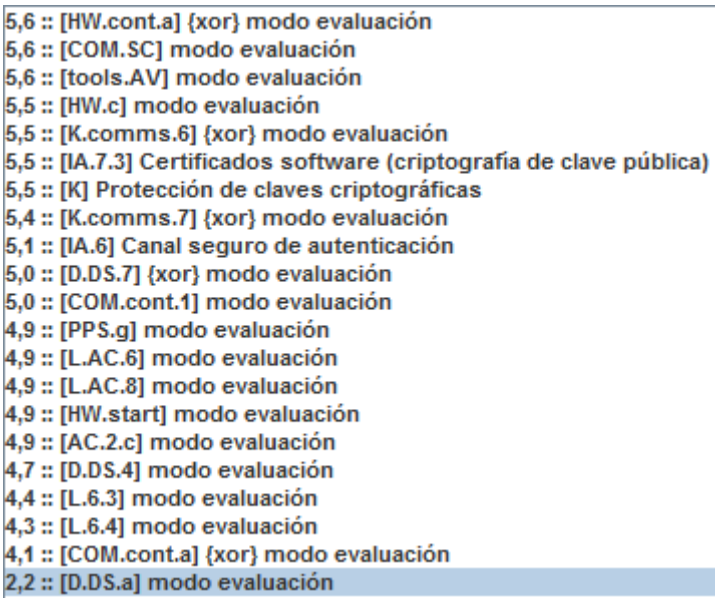

Figura 23. *Eficacia de las salvaguardas 3.* Fuente: PILAR

Haciendo uso del libro 2 aportado por MAGERIT (el catálogo de elementos) [23], podemos obtener información más detallada sobre estas salvaguardas.

5.6. Valoración de las salvaguardas

En esta pantalla de la herramienta, se puede hacer una valoración de la situación actual (current) y del objetivo (target) con ayuda de los objetivos razonables de seguridad de las salvaguardas recomendados por la herramienta teniendo en cuenta el tipo de activos (el rango es 0-10).


[base] red corporativa

	recome...		control	dudas	aplica	comen...	current	target	PILAR
			[27002:2013] Código de prácticas para los controles de seguridad de la información				L0-L5 (_-L5)	L3-L5 (_-L5)	L2-L5
	2		[5] Políticas de seguridad de la información				L0	L5	L2
	7		[6] Organización de la seguridad de la información		...		L0-L5 (L0-L2)	L4-L5	L2-L4
			[7] Seguridad relativa a los recursos humanos		n.a.				
	7		[8] Gestión de activos		...		L1-L2 (L0-L5)	L4-L5 (L3-L5)	L2-L4
	7		[9] Control de acceso				L0-L4 (L0-L5)	L3-L5	L2-L4
	8		[10] Criptografía				L2-L3 (_-L3)	L4 (_-L4)	L3-L5 (L2-L5)
	7		[11] Seguridad física y del entorno				L0-L2 (L0-L5)	L3-L5	L3-L4 (L2-L4)
	9		[12] Seguridad de las operaciones				L0-L5	L3-L5	L2-L5
	9		[13] Seguridad de las comunicaciones		...		L0-L5	L4-L5 (L3-L5)	L3-L5 (L2-L5)
	6		[14] Adquisición, desarrollo y mantenimiento de los sistemas de información				L0-L3	L4-L5 (L1-L5)	L2-L4
	6		[15] Relación con proveedores				L2-L5	L4-L5	L2-L4
	5		[16] Gestión de incidentes de seguridad de la información				L0-L5	L3-L5	L3 (L2-L3)
	6		[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio				L0-L1 (L0-L2)	L3-L5 (L0-L5)	L3-L4 (L2-L4)
	5		[18] Cumplimiento		...		L0-L5	L3-L5	L2-L3

Figura 24. *Valoración de las salvaguardas 1.* Fuente: PILAR

En la tercera columna se indica si la madurez de la salvaguarda es suficiente. Se indica con distintos colores.

- Azul: si la madurez objetivo está por encima de la recomendación
- Verde: si la madurez objetivo está a la altura de la recomendación
- Amarillo: si la madurez objetivo está por debajo de la recomendación
- Rojo: si la madurez objetivo está muy por debajo de la recomendación
- Gris: si la salvaguarda no es aplicable.

En la presentación gráfica:

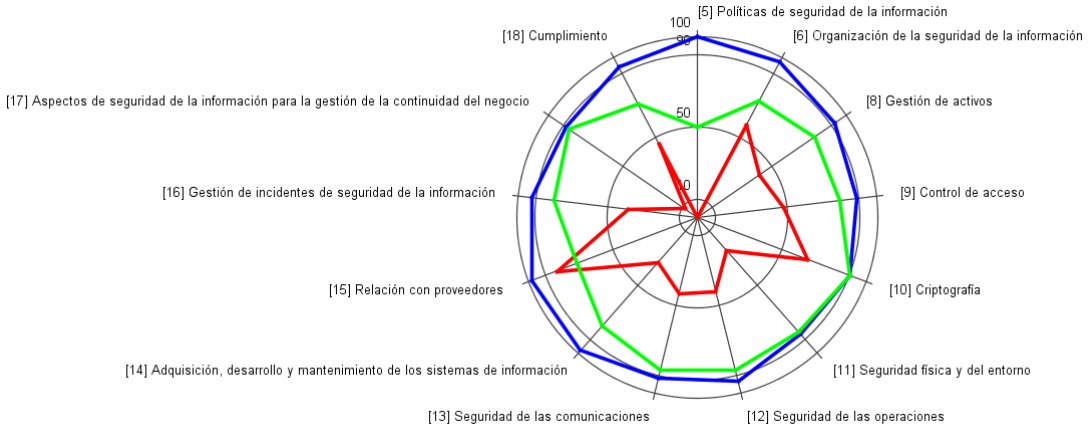

Figura 25. Gráfica de v*aloración de las salvaguardas 1.* Fuente: PILAR

Se pueden obtener los resultados de la valoración en forma gráfica, donde la línea verde es la recomendación de PILAR, la roja es la situación actual y la azul el objetivo marcado por nosotros.

En esta gráfica, se puede observar que, con la situación actual aportada, hay que mejorar en todos los aspectos de seguridad, excepto en la relación con proveedores para mejorar la protección de la información. El objetivo del estudio es mejorar la seguridad en esos aspectos.

Más detalladamente:

[base] red corporativa

	recome...		control	dudas	aplica	comen...	current	target	PILAR
			[27002:2013] Código de prácticas para los controles de seguridad de la información				L0-L5 (_-L5)	L3-L5 (_-L5)	L2-L5
	2		[5] Políticas de seguridad de la información				L0	L5	L2
☑	2		[5.1] Directrices de gestión de la seguridad de la información				L0	L5	L2
	7		[6] Organización de la seguridad de la información		...		L0-L5 (L0-L2)	L4-L5	L2-L4
☑	7		[6.1] Organización interna				L0-L5 (L0-L2)	L4-L5	L2-L4
☑			[6.2] Los dispositivos móviles y el teletrabajo		n.a.				
			[7] Seguridad relativa a los recursos humanos		n.a.				
☑			[7.1] Antes del empleo		n.a.				
☑			[7.2] Durante el empleo		n.a.				
☑			[7.3] Finalización del empleo o cambio en el puesto de trabajo		n.a.				
	7		[8] Gestión de activos		...		L1-L2 (L0-L5)	L4-L5 (L3-L5)	L2-L4
☑	6		[8.1] Responsabilidad sobre los activos		...		L2 (L0-L5)	L4-L5 (L3-L5)	L2-L3
☑	6		[8.2] Clasificación de la información				L1-L2	L4-L5	L3-L4 (L2-L4)
☑	7		[8.3] Manipulación de los soportes				L2 (L1-L2)	L4 (L3-L4)	L3-L4 (L2-L4)
	7		[9] Control de acceso				L0-L4 (L0-L5)	L3-L5	L2-L4
☑	4		[9.1] Requisitos de negocio para el control de acceso				L1 (L1-L2)	L4-L5	L2-L3
☑	7		[9.2] Gestión de acceso de usuario				L0-L4 (L0-L5)	L3-L5	L2-L4
☑	7		[9.3] Responsabilidades del usuario				L3	L3	L4
☑	7		[9.4] Control de acceso a sistemas y aplicaciones				L0-L3	L3-L5	L3-L4 (L2-L4)
	8		[10] Criptografía				L2-L3 (_-L3)	L4 (_-L4)	L3-L5 (L2-L5)
☑	8		[10.1] Controles criptográficos				L2-L3 (_-L3)	L4 (_-L4)	L3-L5 (L2-L5)
	7		[11] Seguridad física y del entorno				L0-L2 (L0-L5)	L3-L5	L3-L4 (L2-L4)
☑	7		[11.1] Áreas seguras				L1-L2 (L1-L5)	L3 (L3-L5)	L3-L4 (L2-L4)
☑	6		[11.2] Seguridad de los equipos				L0-L2	L3-L5	L3-L4 (L2-L4)
	9		[12] Seguridad de las operaciones				L0-L5	L3-L5	L2-L5
☑	5		[12.1] Procedimientos y responsabilidades operacionales				L0-L2 (L0-L3)	L3-L5	L2-L3
☑	9		[12.2] Protección contra el software malicioso (malware)				L3 (L0-L2)	L3 (L3-L5)	L5 (L2-L5)
☑	8		[12.3] Copias de seguridad				L3 (L2-L5)	L5	L5 (L2-L5)
☑	7		[12.4] Registros y supervisión				L2-L5	L5 (L4-L5)	L2-L4

Figura 26. *Valoración de las salvaguardas 2.* Fuente: PILAR

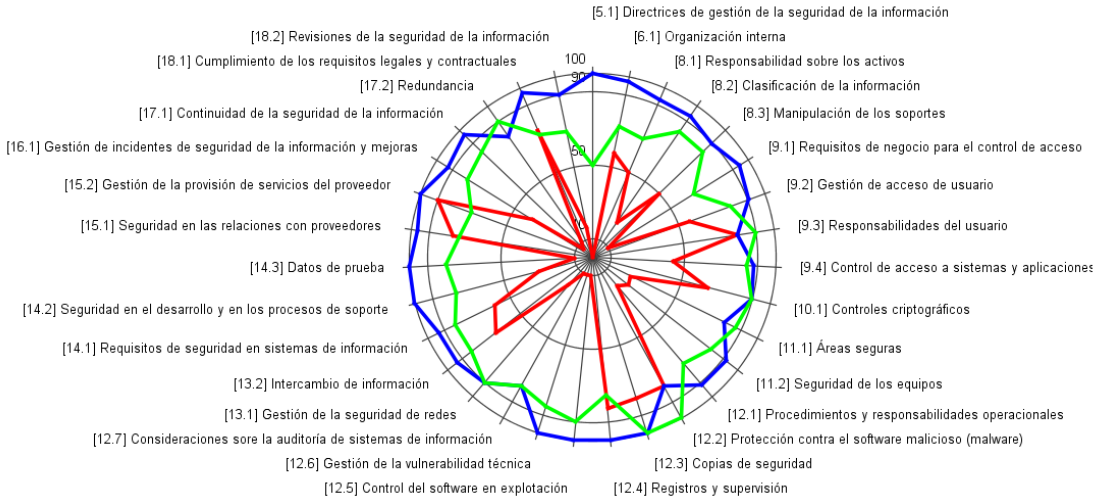

Figura 27. Gráfica de v*aloración de las salvaguardas 2.* Fuente: PILAR

Con estos datos introducidos, el programa nos valora los puntos más necesarios en los que hay que implantar salvaguardas, y nos sugiere unas salvaguardas automáticamente.

5,6 :: [13.1.2] Seguridad de los servicios de red
5,6 :: [12.2] Protección contra el software malicioso (malware)
5,5 :: [10.1.2] Gestión de claves
5,2 :: [9.3] Responsabilidades del usuario
5,1 :: [11.1.4] Protección contra las amenazas externas y ambientales
5,1 :: [9.4.3] Sistema de gestión de contraseñas
5,0 :: [17.2] Redundancia
4,9 :: [11.1.2] Controles físicos de entrada
4,9 :: [11.1.3] Seguridad de oficinas, despachos y recursos
4,9 :: [11.1.5] El trabajo en áreas seguras
4,9 :: [9.4.2] Procedimientos seguros de inicio de sesión

Figura 28. S*alvaguardas 1.* Fuente: PILAR

Para obtener más información sobre estas salvaguardas, se puede buscar en la ISO27002 [24]:

[13.1.2] *"Mecanismos de seguridad asociados a servicios en red: Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados."* [24]

[12.2] *"Controles contra el código malicioso: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios."* [24]

[10.1.2] *"Gestión de claves: Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida."* [24]

[9.3] *"Uso de información confidencial para la autenticación: Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación."* [24]

[11.1.4] *"Protección contra las amenazas externas y ambientales: Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes."* [24]

[9.4.3] *"Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad."* [24]

[17.2] *"Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad."* [24]

[11.1.2] *"Controles físicos de entrada: Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso."* [24]

[11.1.3] *"Seguridad de oficinas, despachos y recursos: Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización."* [24]

[11.1.5] *"El trabajo en áreas seguras: Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras."* [24]

[9.4.2] *"Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on."* [24]

Por tanto, estas son las salvaguardas más importantes que sería necesario aplicar en nuestro gimnasio para mantenerlo seguro de posibles ataques a la información.

5.7. Informes

Riesgo acumulado

En la siguiente figura están representados los riesgos acumulados actuales, potenciales, los recomendados por la herramienta y los objetivos marcados por nosotros sobre cada uno de los activos.

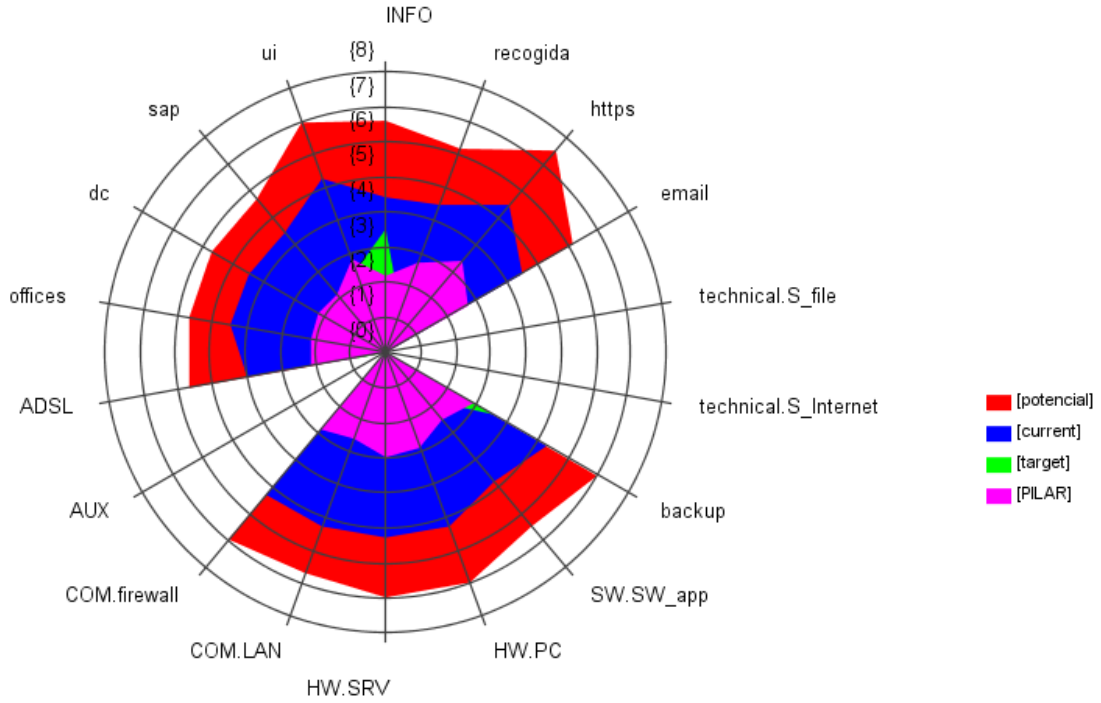

Figura 29. *Gráfica de riesgo acumulado.* Fuente: PILAR

Con la implantación de las salvaguardas se buscará reducir lo máximo posible los riesgos acumulados.

Los informes de análisis de riesgos, declaración de aplicabilidad y de cumplimiento de la normativa ISO/IEC 27000 se adjuntarán en los anejos.

CAPÍTULO 6: PROPUESTAS DE MEJORA

Nos hemos centrado en la versión PILAR Basic con un análisis cualitativo para la aplicación de la metodología MAGERIT y hemos observado que la herramienta puede ser muy práctica y útil para pequeñas y medianas empresas que quieran asegurar su información de posibles ataques. Además, se puede obtener un análisis relativamente rápido de los riesgos que pueden amenazar a una empresa. Esto ayuda a que los responsables de la seguridad de la información de la empresa conozcan los posibles riesgos y amenazas a los que se exponen.

Es una buena metodología para ayudar a planificar medidas de seguridad adecuadas para minimizar o eliminar riesgos y mantener a la empresa preparada para posibles auditorías.

La herramienta PILAR es muy completa con un elevado nivel de detalle, que aporta una gran cantidad de relaciones activos-amenazas y puede ayudar a los responsables de la seguridad de la empresa a ahorrar tiempo en este proceso.

Para pequeñas empresas sin una necesidad de seguridad muy alta, es muy útil porque esta metodología se basa en los riesgos que pueden ser más importantes y perjudiciales para la empresa y ayuda a minimizarlos. Además, al estar relacionado con la normativa ISO, si la empresa implanta las salvaguardas, la empresa cumplirá con la normativa.

Sin embargo, hemos observado algunas fases de la metodología y su herramienta que no están del todo optimizadas.

1. ESTATICISMO DE LA METODOLOGÍA: Con esta metodología solo se consigue un escenario estático, donde no se tienen en cuenta posibles cambios en el sistema, como pueden ser nuevos ataques o amenazas hacia la empresa, activos nuevos o actualizados, nuevas salvaguardas disponibles, etc.

Esto es debido a que la metodología no tiene adoptado una fase que vaya actualizando los datos de las nuevas amenazas que puedan existir, nuevos antivirus disponibles más eficaces, nuevas medidas de protección física, etc.

Por tanto, después de los 5 pasos propuestos por MAGERIT, se debe añadir uno al final que controle y avise de las nuevas actualizaciones, es decir:

1. Determinar aquellos elementos del sistema de información que pueden ser víctima de una amenaza y el coste que supondría que ese activo sufriera algún perjuicio.

2. Definir las amenazas que pueden causar algún perjuicio a los activos.

3. Definir las medidas de protección posibles y cómo de eficaces serían para minimizar el daño de las amenazas.

4. Evaluar el impacto, es decir, el perjuicio que provocaría al activo que una amenaza se materializara.

5. Evaluar el riesgo, es decir, el daño que provocaría a la organización que la amenaza se materializara.

6. Seguimiento de las nuevas actualizaciones que puedan interesar a la organización.

El objetivo de esta fase es el seguimiento y control de las novedades que pueden tener importancia para cada empresa respecto a la seguridad de la información.

Se podría hacer mediante una aplicación en la que se guarden los datos del usuario y sus diferentes estudios, y para cada uno de ellos se pudieran recibir las notificaciones.

En caso de existir una nueva amenaza: La aplicación puede distinguir por el tipo de negocio, el tipo de información que tramita la empresa, y el nivel de seguridad que ofrece contra esta posible nueva amenaza para considerar si debe ser notificada o no. Además debería explicar que pasos se deben seguir para actualizar los datos oportunos en la herramienta PILAR, e informar de las nuevas medidas que se deberían tener en cuenta.

En caso de existir nuevos activos más seguros: La aplicación distinguirá los usuarios a los que ese activo les puede ser útil según precio, eficacia y eficiencia, y los enviará una notificación informándolos sobre ellos. En caso de adquirir el nuevo activo, la aplicación explicará la manera de actualizar los datos en la herramienta PILAR para llevar a cabo la actualización.

En caso de existir nuevas salvaguardas disponibles: La aplicación informará a los usuarios a los que les pueda ser útil la nueva salvaguarda según la cantidad de riesgo que pueden minimizar, según la necesidad de minimizar un riesgo y según el precio del riesgo (a una empresa pequeña no se le pueden asignar salvaguardas de precio muy elevado, mientras que a una empresa grande pueden serle útiles). Se informará al usuario si debe deshacerse de alguna otra salvaguarda que ya no fuera necesaria aplicando la nueva.

En caso de pérdida de valor de un activo: La aplicación informará al usuario en el caso de que uno de sus activos haya perdido valor y como consecuencia, sea posible eliminar o cambiar alguna salvaguarda que ya no sea necesaria. El objetivo de esta medida sería meramente económico.

2. REALIZACIÓN DE ENCUESTAS PARA LA PRIORIZACION DE LOS ACTIVOS

En la primera fase de la metodología MAGERIT, se habla sobre la priorización cualitativa de los activos. Se propone la realización de encuestas en los 3 niveles humanos básicos de la organización (gerencial, operativo y empleados), para reunir toda la información aportada desde los distintos puntos de vista, y poder hacer una valoración más precisa como se utiliza en la metodología OCTAVE. [21]

3. POSIBILITAR UN ANÁLISIS CUANTITATIVO EN LA VERSIÓN PARA PYMES PILAR BASIC.

En esta versión PILAR, solo es posible realizar un análisis cualitativo, por lo que se pierde mucha información y no es posible precisar el escenario que se quiere evaluar.

Sería de utilidad que la herramienta fuera capaz de tener en cuenta el valor de los activos para poder obtener un resultado más preciso.

4. MODERNIZACIÓN DE LA INTERFAZ DE LA HERRAMIENTA PILAR:

El diseño de la herramienta PILAR es la carta de presentación para los usuarios. Es difícil que la herramienta tenga la credibilidad suficiente para ganarse la confianza de los usuarios con un diseño tan anticuado. Se debe contratar a un experto en diseño de aplicaciones informáticas para modernizar la herramienta.

5. EXPLICACIÓN MÁS DETALLADA DE LAS SALVAGUARDAS:

Sería relativamente sencillo incluir una función en el programa donde se explique la salvaguarda seleccionada, tal y como viene en la serie ISO 27002, de manera que,

para obtener más información sobre la salvaguarda, no haya que buscar en la normativa. De esta forma ser podría reducir el tiempo invertido en el análisis. Además, sería de utilidad, que con cada salvaguarda, se aportara una pequeña explicación de los puntos sobre los que va a actuar la salvaguarda para conseguir transmitir mayor confianza en usuarios no especializados en la materia.

6. REDUCCIÓN DE COMPLEJIDAD PILAR BASIC

Se debe intentar reducir la complejidad aún más teniendo en cuenta que los empleados de las pymes normalmente no van a estar muy cualificados en la materia. El punto más complejo es el de la identificación de los activos. Con la finalidad de que esta fase sea más sencilla de lo que es actualmente, se podrían aportar muchos más ejemplos que se pudieran asemejar a diferentes empresas pequeñas con distintos procesos. Esto permitiría a sus usuarios coger algunas partes de los distintos procesos, para disminuir el tiempo empleado en esta parte y, además, no olvidarse algunos datos importantes de sus activos.

7. ANÁLISIS A PARTIR DE UN DISEÑO VIRTUAL

Con el fin de facilitar la relación entre activos, sería muy útil poder hacer un análisis a partir de un diseño virtual de la empresa, que ayudara a identificar los activos y a relacionarlos entre sí para poder ser más precisos y poder tener una visión virtual de las conexiones de los activos. Con este diseño virtual, sería más sencillo no olvidarse de activos, y, en caso de tener que añadir algún activo nuevo, facilitar la conexión con los activos antiguos.

8. CONTROL DE ACCESO PILAR BASIC

En esta versión de la herramienta, no se proporcionan medios para proteger el proyecto de modificaciones no autorizadas (Sí lo hace en la versión completa). Esta función es muy simple (solicitar usuario y contraseña), y, a la vez muy importante para la seguridad de la empresa.

9. AÑADIR UN MODO SIMULACIÓN

Con esta función dentro de la herramienta PILAR, el usuario podría investigar qué sucedería en caso de incluir o modificar activos, o modificar los objetivos de seguridad, salvaguardas o valoraciones sin necesidad de cambiarlo y luego tener que borrarlo. Ahorraría muchos problemas y ayudaría a la hora de tomar decisiones.

CONCLUSIONES

MAGERIT "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" es una metodología utilizada por las empresas para conocer en qué medidas de protección hay que invertir para proteger la información que tramitan.

Muchas empresas invierten mucho dinero en medidas de protección innecesarias y dejan sin proteger los puntos más importantes.

Gracias a incibe [25] y a los documentos explicativos de la metodología y su herramienta [11] [23], hemos podido estudiar y analizar todo lo relativo a la seguridad de la información.

Tras estudiar MAGERIT y compararla con otras metodologías similares, hemos sacado la conclusión de que es una buena metodología para el análisis y gestión de los riesgos de la información. Sin embargo, no está del todo optimizada y debería estudiarse alguna manera de conseguir que el análisis pueda actualizarse automáticamente para poder conseguir sistemas mucho mejor protegidos. Además se deberían realizar encuestas para conocer las preocupaciones de los distintos puntos de vista de la organización, ya que es posible que la alta dirección no conozca algunos problemas que puedan tener los empleados en relación a la seguridad de la información.

En cuanto a la herramienta PILAR, se debería estudiar principalmente la manera de reducir su complejidad para facilitar su uso a empresas pequeñas sin un alto conocimiento en la materia.

BIBLIOGRAFÍA

[1] «¿Por qué es tan importante la Seguridad informática?,» 19 julio 2017. [En línea]. Available: https://www.tuyu.es/importancia-seguridad-informatica/. [Último acceso: 01 07 2019].

[2] «Ciberataques,» [En línea]. Available: https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/. [Último acceso: 01 07 2019].

[3] A. Gómez, Enciclopedia de la seguridad informática (2ª edición actualizada), RA-MA, 2014.

[4] J. L. R. A. &. S. R. Morant, SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN, EDITORIAL UNIVERSITARIA RAMON ARECES. , 1994.

[5] «¿Qué es un virus informático? Definición y tipos,» 21 diciembre 2017. [En línea]. Available: http://www.valortop.com/blog/virus-informatico-definicion-tipos. [Último acceso: 01 07 2019].

[6] J. MIGUEL, Protección de datos y seguridad de la información, RA-MA, 2015.

[7] «Análisis de riesgos en 6 pasos,» 16 enero 2017. [En línea]. Available: https://www.incibe.es/en/node/2789. [Último acceso: 01 07 2019].

[8] «Principio de defensa en profundidad,» [En línea]. Available: https://smr2rubenblanco.wordpress.com/2017/11/10/principio-de-defensa-en-profundidad/. [Último acceso: 01 07 2019].

[9] ISO, «Sistema de Gestión de la Seguridad de la Información.,» [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdfhttp://www.iso27000.es/download/doc_iso27000_all.pdf. [Último acceso: 01 07 2019].

[10] R. Marcos Carvajal, «Estudio de las normas españolas y estadounidenses de seguridad de la información,» EII- Universidad de Valladolid, 2015.

[11] «Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información libro 1,» [En línea]. Available:

https://www.administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XPU1ixYzYdU. [Último acceso: 01 07 2019].

[12] «ISO 27001,» 2013. [En línea]. Available: https://www.pmg-ssi.com/norma-27001/.

[13] 1&1 IONOS España S. L. U., «El RGPD: normativa europea de protección de datos.,» 29 mayo 2019. [En línea]. Available: https://www.ionos.es/digitalguide/paginas-web/derecho-digital/el-rgpd-normativa-europea-de-proteccion-de-datos/. [Último acceso: 01 07 2019].

[14] Iberley, «Publicada la nueva Ley de Protección de Datos Personales (LOPDGDD),» 7 diciembre 2018. [En línea]. Available: https://www.iberley.es/noticias/publicada-nueva-ley-proteccion-datos-personales-lopdgdd-29303. [Último acceso: 01 07 2019].

[15] «Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico - ¿Cómo se aplica la LSSI?,» [En línea]. Available: http://www.lssi.gob.es/LA-LEY/ASPECTOS-BASICOS/Paginas/ambito-aplicacion-lssi.aspx. [Último acceso: 01 07 2019].

[16] «Base legal de la Firma Electrónica,» [En línea]. Available: https://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html. [Último acceso: 01 07 2019].

[17] A. Huerta, «Introducción al análisis de riesgos - Metodologías (I),» 30 marzo 2012. [En línea]. Available: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/. [Último acceso: 01 07 2019].

[18] «Herramienta de Evaluación de Riesgo-CRAMM.,» [En línea]. Available: http://evaluries.blogspot.com/. [Último acceso: 01 07 2019].

[19] A. Huerta, «Introducción al análisis de riesgos – Metodologías (II),» 2 abril 2012. [En línea]. Available: https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/. [Último acceso: 01 07 2019].

[20] «OCTAVE, metodología para el análisis de riesgos de TI.,» [En línea]. Available: https://www.uv.mx/universo/535/infgral/infgral_08.html. [Último acceso: 01 07 2019].

[21] «Temas Seguridad Informática.,» [En línea]. Available: http://apuntesseguridadit.blogspot.com/2014/03/octave-o-perationally-c-

ritical-t-hreat.html. [Último acceso: 01 07 2019].

[22] «PILAR basic - Manual de usuario,» [En línea]. Available: https://www.pilar-tools.com/doc/v62/manual_basic_es_2016-08-21.pdf. [Último acceso: 01 07 2019].

[23] Ministerio de Hacienda y Administraciones Públicas, «MAGERIT – versión 3.0 Metodología de Análisis y Gestión Libro II - Catálogo de Elementos,» 2012. [En línea]. Available: https://www.administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XPU1ixYzYdU.. [Último acceso: 01 07 2019].

[24] «ISO 27002,» 2013. [En línea]. Available: http://www.iso27000.es/iso27002.html. [Último acceso: 01 07 2019].

[25] «Instituto Nacional de Ciberseguridad,» [En línea]. Available: https://www.incibe.es/. [Último acceso: 01 07 2019].