Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Análisis y aplicación de protocolos de seguridad basados en la ISO 27001/2 en una empresa de servicios de consultoría informática

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Alfredo Valle Signes

Tutor: Ignacio Gil Pechuán

Curso 2019/2020

Resumen

El proyecto que se va a presentar expone las herramientas y conocimientos necesarios para comprender la norma ISO 27001 y poder aplicarla en una organización que se dedica a la consultoría informática, con el objetivo de lograr obtener una certificación de dicha norma. Se explican una serie de marcos de referencia útiles para lograr comprender el proceso, así como la legislación aplicable. Por otro lado, se especifica en que consiste una empresa de consultoría informática y que beneficios aporta la obtención de una certificación en la norma ISO 27001, además de exponer los riesgos a los que se enfrenta. Como resultado final se presenta un proyecto de guía de implementación y se expone un ejemplo de ejecución de análisis de riesgos haciendo uso de la metodología MAGERIT.

Palabras clave: ISO 27001, Certificación, SGSI, LOPD, RGPD, MAGERIT, Análisis de riesgos.

Abstract

The project to be presented presents the tools and knowledge necessary to understand the ISO 27001 standard and to be able to apply it in an organization that is dedicated to computer consulting, with the aim of obtaining a certification of said standard. A series of useful reference frameworks are explained to help you understand the process as well as the applicable legislation. On the other hand, it is specified what a computer consulting company consists of and what benefits obtaining a certification in the ISO 27001 standard provides, in addition to exposing the risks it faces. As a final result, a draft implementation guide is presented and an example of risk analysis execution using the MAGERIT methodology is presented.

Keywords: ISO 27001, Certification, SGSI, LOPD, RGPD, MAGERIT, Risk analysis.

ABREVIATURAS Y ACRÓNIMOS

ADM. Architecture Development Method - Método de desarrollo de arquitectura.

AENOR. Asociación Española de Normalización y Certificación.

AEPD. Agencia Española de Protección de Datos.

COBIT. Control Objectives for Information Systems and related Technology - Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.

IEC. International Electrotechnical Commission - Comisión Electrotécnica Internacional.

ISACA (Information Systems Audit and Control Association). Asociación de Auditoría y Control de Sistemas de Información.

ISO. International Organization for Standardization - Organización Internacional de Estandarización.

ITIL. Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de la Información.

JTC. Join Technical Committee - Comité Técnico Conjunto.

LOPD. Ley 15/1999 de Protección de Datos de Carácter Personal.

LSSI. Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

PDCA – PHVA. Siglas del Ciclo de Deming (Planificar, Hacer, Verificar, Actuar – en inglés, Plan, Do, Check, Act).

PYME. Pequeña y Mediana Empresa.

RDLOPD. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

RGPD. Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

SFIA. Skills Framework For the Information Age - Marco de Referencia de Competencias para la Era de la Información.

SGSI. Sistema de Gestión de la Seguridad de la Información.

SOA. Statement of Applicability - Declaración de Aplicabilidad

TI. Tecnología de la Información.

TIC. Tecnología de la Información y la Comunicación.

TOGAF. The Open Group Architecture Framework - Esquema de Arquitectura del Open Group.

VPN. Virtual Private Network - Red Privada Virtual.

Índice

Índice de Figuras y Tablas

1. Introducción

La información es un activo vital para la continuidad y desarrollo de cualquier organización. Su adecuada protección se ha vuelto esencial para mantener la confianza de los clientes, para proteger la reputación de una organización, y para protegerse ante posibles reclamaciones por responsabilidad legal. De este modo, la información ha resultado ser un elemento imprescindible en nuestra forma de trabajar y cuesta imaginarse el desempeño de un profesional o el correcto funcionamiento de una organización sin ella.

Al hablar de información como activo es necesario tener presente la seguridad de la información como concepto y norma que impera no solo en las organizaciones TIC, sino en cualquier tipo de organización, siendo especialmente útil en aquellos sectores donde la información manejada sea crítica y se manejen grandes volúmenes de información.

Sólo hay una forma de gestionar de forma adecuada la seguridad: Identificar, Analizar, Evaluar, y Gestionar los riesgos de seguridad de la información a los que se enfrenta la organización, y tomar las medidas técnicas, organizativas y legales necesarias. Una de las herramientas más utilizadas para ello es la norma ISO/IEC 27001 que corresponde a los sistemas de gestión de seguridad de la información (SGSI).

En este trabajo se analizan y exponen las pautas necesarias para implementar dicha norma y obtener la correspondiente certificación desde el punto de vista de una pequeña o mediana empresa (PYME) de consultoría informática con amplia experiencia en el sector.

En la primera parte del presente documento, correspondiente al marco teórico, se analizan cinco marcos de referencia (frameworks) sobre buenas prácticas y modelos de implementación de la ISO 27001. El primero de ellos, el Ciclo de Deming, es el modelo base sobre el que se estructura el proceso de mejora. Este modelo en concreto adquiere gran relevancia a la hora de aplicar la ISO 27001.

En el siguiente apartado se analiza la ISO 27001 y el marco legal de referencia en materia de protección de datos y gestión de la seguridad de la información. Se contempla legislación nacional e internacional haciendo especial referencia al Reglamento Europeo de Protección de Datos (RGPD).

A continuación, se expone la relación de la certificación en materia de gestión de seguridad de la información y la empresa de consultoría informática, teniendo en cuenta los riesgos a los que está expuesta cualquier tipo de organización. Por otra parte, se analizan los beneficios de obtener una certificación en seguridad de la información

Los puntos sexto y séptimo se centran en analizar el modelo de política de gestión de seguridad y el modelo de aplicación de la ISO en la empresa de consultoría informática, respectivamente. Se abordan de manera más específica aspectos importantes como la documentación necesaria la preparación de la ISO 27001. Asimismo, se exponen una serie de buenas prácticas para minimizar vulnerabilidades referentes a la seguridad de la información.

Por último, se presentan sucintas conclusiones de la información analizada y expuesta además de indicarse unas breves recomendaciones para maximizar la eficacia y el beneficio de la implementación de los SGSI en empresas de consultoría informática.

2. Objetivos

El objetivo principal de este Trabajo Final de Grado es la adquisición de los conocimientos necesarios para poder aplicarlos y afrontar el proceso de certificación de la norma ISO 27001 en una empresa de consultoría informática. Las normas ISO 2700x, específicamente la 27001 es aplicable a todo tipo de organizaciones y sectores de actividad y permite su integración con otros sistemas de gestión como la ISO 9001, la de Continuidad de Negocio (ISO 22301 y BS 25999) y otras específicas como ITIL, COBIT, etc.

Teniendo en cuenta que la finalidad de aplicación de esta norma es abordar con mejores garantías la problemática de la seguridad de la información, surge la necesidad de alcanzar una serie de objetivos secundarios:

- Conocer y entender algunos marcos de referencia relacionados con el proceso.
- Estudiar la legislación nacional e internacional relacionada con la seguridad de la información.
- Comprender en que consiste la empresa de consultoría informática y analizar los riesgos a los que se enfrenta.

3. Marco teórico

Existen una gran cantidad de marcos, normas y referencias en la actualidad a tener en cuenta y sobre los que poder apoyarse para realizar una mejor explicación de la ISO 27001/2 así que para comenzar con la explicación del proyecto voy a exponer previamente dichos modelos y marcos de referencia que se utilizan actualmente para la gestión de departamentos de SI/TI y servicios TIC y me basaré en ellos para crear un SGSI.

3.1. Ciclo de Deming

Para acometer un proyecto de aplicación de la ISO 27001 recurrimos a las fases propuestas en el Ciclo Deming al objeto de tener en cuenta una mejora continua y considerar que dispone de múltiples indicadores. El ciclo consiste en un proceso de 4 fases que puede ser implementado en cualquier ámbito. Este método también es conocido como PDCA (en inglés) o PHVA:

- Primera fase: Plan/Planificar

El primer paso que debe llevarse a cabo es establecer los objetivos que se pretenden alcanzar y los procesos que se requieren para alcanzar los resultados deseados según las necesidades y las políticas de seguridad de cada organización.

- Segunda fase: Do/Hacer

Tras establecer los objetivos y señalar los procesos necesarios se procede a implantar dichos procesos con el propósito de avanzar hacia el resultado esperado.

- Tercera fase: Check/Verificar

Una parte importante de esta metodología consiste en verificar los resultados. Para ello se debe someter a revisión y evaluación continua cada uno de los servicios y procesos desarrollados en base a las políticas y objetivos establecidos previamente. Esta fase permite comprobar que se cumplen los requisitos establecidos.

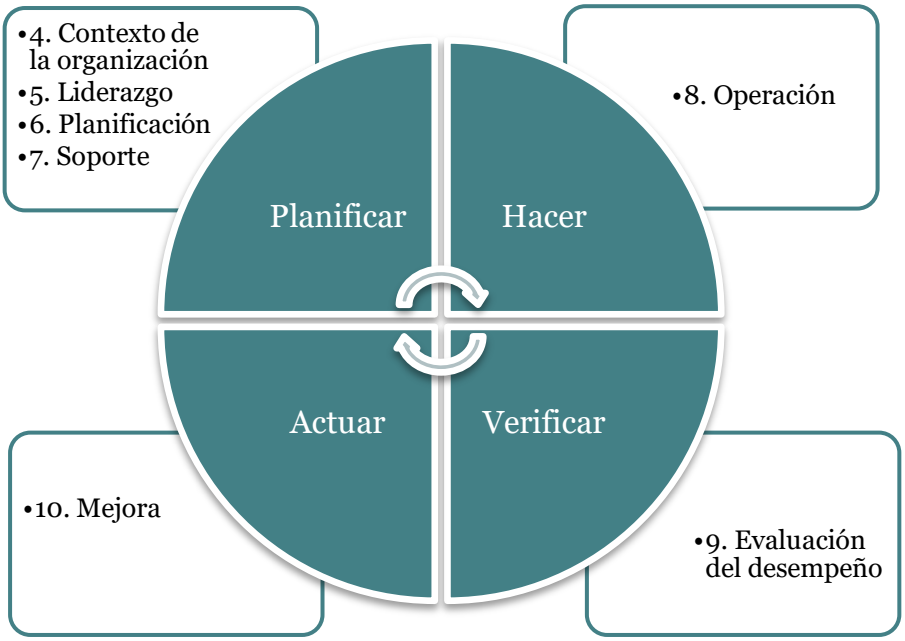
- Cuarta fase: Act/Actuar

Se toman decisiones y se actúa en consecuencia con el fin de mantener una mejora constante del rendimiento del SGSI.

El SGSI basado en la ISO 27001 y aplicando la metodología del Ciclo Deming es altamente eficiente porque cuenta con diversos indicadores que aportan datos actualizados sobre la realidad de la organización en materia de seguridad de los sistemas de información. El análisis actualizado y la gran cantidad de datos que se recogen constituyen un mecanismo de alarma para realizar las modificaciones pertinentes en aras de la mejora continua[1].

En la figura que aparece a continuación se muestra la relación entre cada una de las fases del ciclo Deming o PHVA con diferentes apartados de la ISO 27001.

Figura 2. Relación del Ciclo PHVA con la ISO 27001



Fuente: elaboración propia a partir de [2]

Para llevar a cabo cada una de las actividades necesarias y utilizar el Ciclo de Deming, se necesitan profesionales que reúnan las aptitudes requeridas para las competencias que se pretende desarrollar. Una herramienta con reconocimiento internacional para identificar dichos profesionales es SFIA.

A la hora de trabajar haciendo uso del Ciclo de Deming es fundamental el uso de marcos de referencia para las buenas prácticas, ya que se pueden conseguir resultados de manera más eficiente. Algunos de los marcos de referencia de buenas prácticas más reconocidos son COBIT e ITIL.

Para lograr una buena gestión de los recursos cuando se pretende trabajar con el Ciclo de Deming es necesario contar con una arquitectura empresarial de información. TOGAF es un marco de referencia en este ámbito.

A continuación, se incluye una tabla de relación de los marcos de referencia que se van a exponer en los puntos siguientes:

Tabla 2. Comparación de marcos de referencia

	SFIA	COBIT	ITIL	TOGAF
Función	Describir y gestionar las competencias TIC de los profesionales	Ayudar a empresas a conseguir sus objetivos para el gobierno y gestión de las TIC	Recoge el conjunto de mejores prácticas de gestión de servicios de TI	Asistir en la aceptación, creación, uso y mantenimiento de una arquitectura empresarial
Fases	Seleccionar Aplicar Evaluar Analizar Desarrollar Recompensar	Iniciar el programa Definir prioridades y oportunidades Definir hoja de ruta Planificar el programa Ejecutar el plan Obtener beneficios Revisar la efectividad	Estrategia del Servicio Diseño del Servicio Transición de Servicios Operación del Servicio Mejora continua del Servicio	Fase preliminar Visión de la arquitectura Arquitectura de negocio Arquitectura de sistemas de información Arquitectura tecnológica Oportunidades y soluciones Planificación de la migración Gobernanza de la implementación Gestión del cambio de arquitectura.
Categorías	Estrategia y arquitectura Cambio en el negocio Desarrollo de soluciones y aplicación Administración de servicio Soporte de administración y aprovisionamiento Interfaz con el cliente	Principios, políticas y marcos de trabajo Procesos Estructuras organizativas Cultura, ética y comportamiento, de los individuos y de la empresa Información Servicios, infraestructura y aplicaciones Personas, habilidades y competencias	Gestión de incidencias Gestión de la configuración Gestión de cambios Gestión de problemas	Arquitectura de negocio Arquitectura de aplicaciones Arquitectura de datos Arquitectura tecnológica

Fuente: Elaboración propia a partir de [3]

Como se puede observar en la tabla anterior, cada uno de los marcos de referencia que a continuación se desarrollan tienen funciones diferentes. Sin embargo, todos siguen un proceso lógico muy similar. Las fases de planificación, acción, revisión y corrección están presentes en cada uno de ellos. Conjuntamente son útiles, complementándose unas a otras en diferentes aspectos, para el correcto gobierno de ciertos sistemas de gestión de las TIC aplicables a la mayoría de las organizaciones.

3.2. SFIA

El marco de las competencias en la era de la información (SFIA) es una herramienta para las organizaciones para la definición y gestión de los profesionales TIC que las componen, además de una herramienta para dichos profesionales TIC para el propio desarrollo de su carrera profesional. SFIA es una colaboración hoy en día y se actualiza periódicamente a través de un proceso global de consulta abierto. Es un marco basado en la experiencia, no está alineado a ninguna calificación o certificación si no a la demostración de una serie de habilidades por parte del individuo y va dirigido desde el mismo individuo hasta el líder de alguna organización o profesionales de recursos humanos. SFIA se rige por siete niveles de responsabilidad siendo el nivel uno el más bajo y el siete el más alto, estos niveles describen los comportamientos, valores, conocimientos y características que un individuo debe tener para ser identificado como competente en ese nivel, cada nivel está marcado con una palabra o frase guía para resumir el grado de responsabilidad como se puede observar en la siguiente imagen:

Tabla 3. Niveles de responsabilidad de SFIA con su guía asociada

Nivel 1	•Seguir
Nivel 2	•Asistir
Nivel 3	•Aplicar
Nivel 4	•Permitir
Nivel 5	•Asegurar, aconsejar
Nivel 6	•Iniciar, influir
Nivel 7	•Establecer una estrategia, inspirar, movilizar

Fuente: Elaboración propia a partir de Fundación SFIA [4]

Además de los niveles de responsabilidad SFIA divide cada uno de los niveles en cinco atributos genéricos para poder explicar mejor cada nivel, en la siguiente imagen se puede observar a modo de ejemplo el nivel uno de responsabilidad de SFIA y sus cinco atributos explicados a modo de ejemplo:

Tabla 4. Ejemplo del nivel uno de responsabilidad y atributos explicados

Nivel 1	Seguir
Autonomía	Trabaja bajo supervisión. Usa poca discreción. Se espera que busque orientación en situaciones inesperadas.
Influencia	Influencia mínima. Podría trabajar solo o interactuar con sus compañeros inmediatos.
Complexity	Realiza actividades rutinarias en un ambiente estructurado. Requiere ayuda para solucionar problemas inesperados.
Complejidad	Tiene un conocimiento genérico básico apropiado para el área de trabajo. Aplica el conocimiento recién adquirido para desarrollar nuevas habilidades.
Habilidades empresariales	Tiene suficiente capacidad de comunicación para el diálogo efectivo con otros. Demuestra un enfoque organizado para el trabajo. Utiliza sistemas y herramientas, aplicaciones y procesos básicos. Contribuye a la identificación de oportunidades de desarrollo propio. Sigue el código de conducta, la ética y los estándares de la organización. Conoce los problemas de salud y seguridad. Entiende y aplica prácticas básicas.

Fuente: Elaboración propia a partir de Fundación SFIA [4]

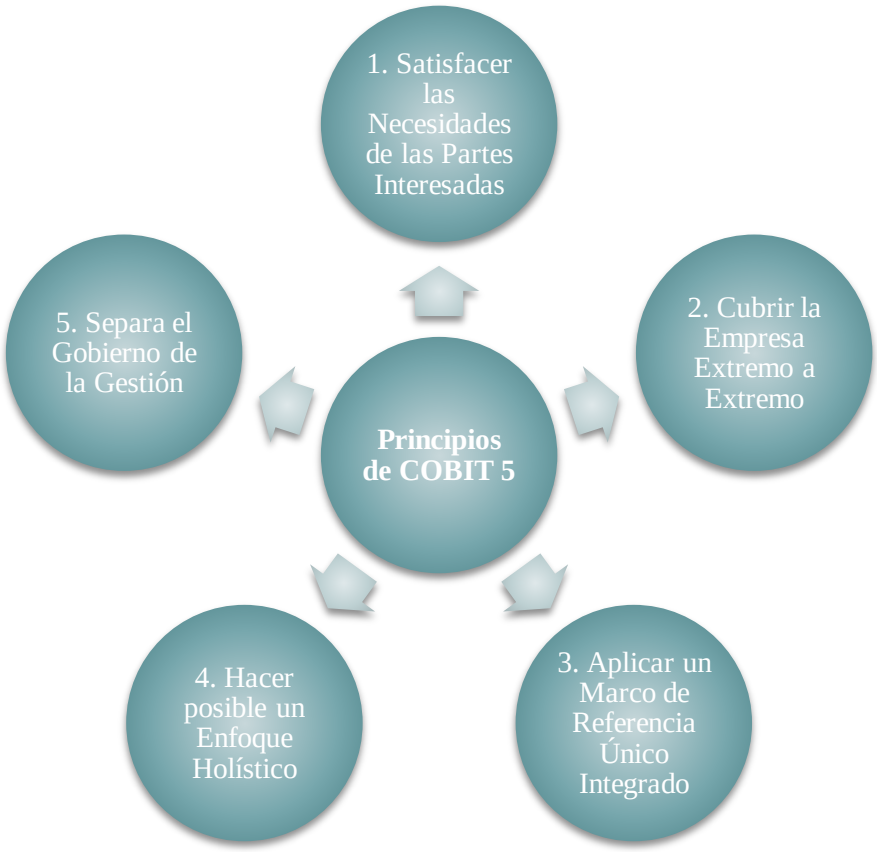
3.3. COBIT

Los objetivos de control para la información y tecnologías relacionadas (COBIT) es una guía para saber cuáles son las mejores prácticas. Ofrece a las empresas un marco integral para lograr sus objetivos mediante su gobierno de las TIC, principalmente guía a dichas empresas a la estandarización de los procesos de TI y la infraestructura, tratando de alinear las TI con los objetivos comerciales generales, ayudando a otros ejecutivos y gerente a comprender mejor los objetivos de las TI. La versión actual del COBIT, se basa en cinco principios clave:

- Satisfacer las necesidades de las partes interesadas.
- Cubrir la organización de principio a fin integrando el gobierno corporativo con el gobierno de las TI orientándolo al negocio.
- Aplicación de un modelo de referencia integrado único
- Habilitación de un enfoque holístico para conseguir una gestión y un gobierno de las TI con eficiencia y eficacia.
- Separación del gobierno de las TI de la gestión de las TI

En la siguiente figura se puede ver un gráfico representativo de los cinco principios de COBIT 5:

Figura 3. Principios de COBIT 5



Fuente: Elaboración propia a partir de [5]

Además de estos cinco principios clave, COBIT 5 define siete catalizadores (*enablers*) que introducen flexibilidad en la implementación al incorporar una estructura común que puede ser adaptada a las necesidades de cada organización, dichos catalizadores son los siguientes:

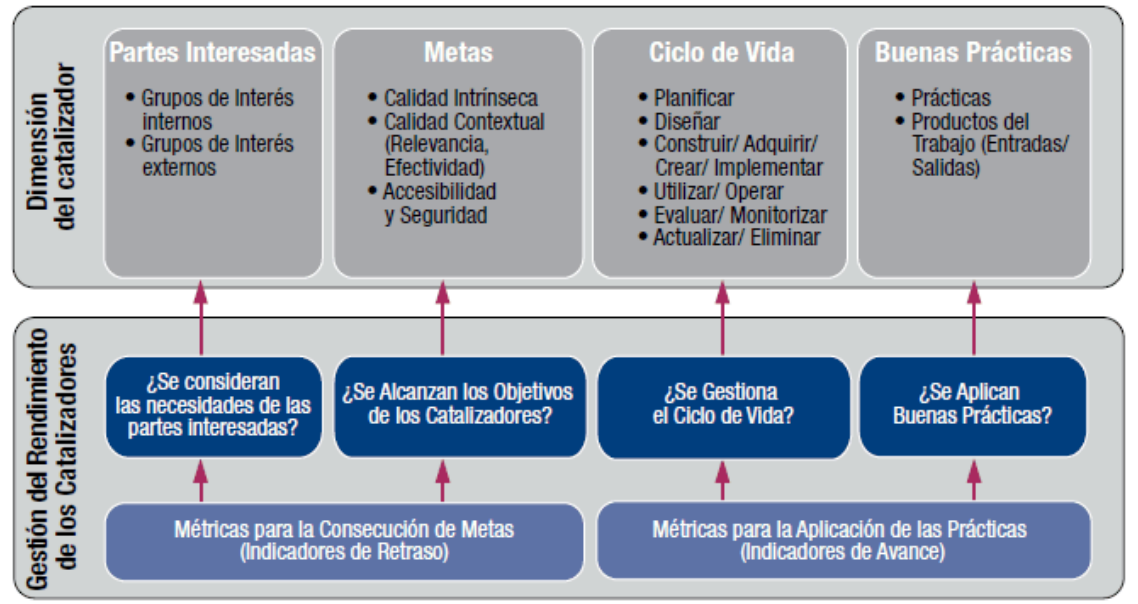
- Principios, políticas y marcos de referencia.
- Procesos.
- Estructuras organizativas.
- Cultura, ética y comportamiento.
- Información.
- Servicios, infraestructuras y aplicaciones.
- Personas, habilidades y competencias.

Estos catalizadores comparten la misma estructura que comprende las dimensiones y la gestión del rendimiento para así facilitar su comprensión y entendimiento[6], [7]. Estas dimensiones deben:

- Proporcionar una manera común, simple y estructurada de tratar con los catalizadores.
- Permitir a una entidad manejar sus complejas interacciones.
- Facilitar resultados exitosos de los catalizadores.
- Además, los catalizadores trabajan sobre 4 dimensiones concretas:
- Grupos de interés: Cada catalizador tiene grupos de interés.
- Metas: Cada catalizador tiene varias metas y estos catalizadores proporcionan valor por la consecución de dichas metas. Estas metas pueden ser definidas en términos de resultados esperados del catalizador o aplicación u operación del catalizador.
- Ciclo de vida: Cada catalizador tiene un ciclo de vida, las fases son las siguientes:
    - Planificar (Incluyendo selección y desarrollo de conceptos).
    - Diseñar.
    - Construir/Adquirir/Crear/Implementar.
    - Utilizar/Operar.
    - Evaluar/Monetizar.
    - Actualizar/Eliminar.
- Buenas prácticas: Para cada uno de los catalizadores se pueden definir buenas prácticas, estas soportan la consecución de los objetivos de dicho catalizador. Estas proporcionan ejemplos y sugerencias sobre como implementar de la mejor manera el catalizador y qué entradas y salidas son necesarias.

En la siguiente imagen puede observarse un esquema para la gestión de dichos catalizadores:

Figura 4. Esquema de gestión de los catalizadores de COBIT 5



Fuente: [5], [6]

3.4. ITIL

La biblioteca de infraestructura de tecnologías de la información (ITIL) hace referencia a una metodología de gestión que propone una serie de prácticas estandarizadas que nos ayudan a mejorar la presentación de un servicio, reorganizando la manera que tiene el departamento TI de una empresa a trabajar[8]. ITIL se organiza en 5 etapas[9], [10]:

- La primera corresponde con la estrategia del servicio en la que se pretende alinear la estrategia de las TI con los objetivos y expectativas generales del negocio asegurando que las decisiones resulten en valores mesurables para la organización.
- La segunda etapa es la del diseño del servicio donde se busca transformar los objetivos estratégicos en servicios activos.
- La tercera etapa hace referencia a la transición del servicio, para ello se recogen todos los servicios de TI nuevos, modificados y retirados y se estudia que cumplen las

necesidades del negocio y cómo afrontar la evolución de dichos servicios, siempre gestionados y controlados para que estos otorguen mayor valor.

- La cuarta etapa gestiona las operaciones del servicio para que estas se realicen de manera adecuada para dar apoyo a las necesidades del negocio.
- La quinta y última etapa se centra en la mejora continua del servicio estudiando cómo mejorar la calidad y eficiencia de los servicios TI y en la reducción de sus costos.

3.5. TOGAF

El marco de arquitecturas del Open Group (TOGAF) es una arquitectura empresarial que ofrece un marco de alto nivel para el desarrollo de software empresarial. Ayuda a organizar el proceso de desarrollo a través de un enfoque sistemático para reducir los errores, mantener los plazos, mantenerse dentro del presupuesto y alinear las TI con las unidades de negocios para producir resultados de calidad.

La versión 9.2 del estándar TOGAF está dividida en 6 secciones[11]:

- Parte I: La introducción a un alto nivel de los conceptos clave de la arquitectura empresarial y en particular un acercamiento a TOGAF, contiene definiciones y términos utilizados a través del estándar.
- Parte II: El método de desarrollo de arquitectura (ADM), el núcleo del marco TOGAF, describe el método de desarrollo de arquitectura con un paso a paso sobre como desarrollar una arquitectura empresarial.
- Parte III: Las técnicas y guías para el ADM, son una colección de guías y técnicas disponibles para el acercamiento a TOGAF al igual que para el método de desarrollo de arquitectura de TOGAF. Guías y técnicas adicionales están recopiladas en la librería de TOGAF.
- Parte IV: El marco de contenido de arquitectura, incluye un metamodelo para los artefactos de la arquitectura, el uso de bloques de construcción de la arquitectura reutilizables y una visión de conjunto de los entregables de arquitectura típicos.

- Parte V: El continuum empresarial y herramientas, muestra taxonomías y herramientas para clasificar y almacenar las salidas de la actividad de la arquitectura dentro de la empresa.
- Parte VI: El marco de la capacidad de la arquitectura, hace referencia a la organización, procesos, habilidades, roles y responsabilidades requeridos para establecer y operar una función de la arquitectura dentro de una empresa.

4. La ISO 27001/2 en el contexto de Normas y Estándares de Gestión de la seguridad

La Organización Internacional de Normalización o ISO (International Organization for Standarization, en inglés) es una organización independiente y no gubernamental cuya historia comenzó en 1946 en el Institute of Civil Engineers en Londres, dónde delegados de 25 países decidieron crear una organización para "facilitar la coordinación y unificación internacional de los estándares industriales". El 23 de febrero 1947 esta nueva organización comenzó sus operaciones.

Hasta la fecha llevan publicados más de 23000 estándares internacionales cubriendo prácticamente todos los aspectos de la tecnología y la fabricación. Tienen miembros de 164 países y 781 comités y subcomités técnicos para controlar el desarrollo de estándares.

La tabla que se muestra a continuación presenta de manera resumida la serie ISO 27000. La serie proporciona un marco de gestión de la seguridad de la información a partir de un conjunto de estándares desarrollados por ISO e IEC (International Electrotechnical Commission), que puede ser utilizado por cualquier organización.

Tabla 5. Serie ISO 27000

Norma	***Contenido***
27000	Visión general de la serie.
27001	Norma principal de la serie. Requisitos del SGSI. Certificable.
27002	Guía de buenas prácticas: (11) dominios, (39) objetivos de control y (133) controles.
27003	Aspectos críticos para el diseño e implementación de un SGSI.
27004	Guía para el desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles.
27005	Directrices para la gestión del riesgo.
27006	Requisitos para la acreditación de entidades de auditoría y certificación.
27007	Guía de auditoría de un SGSI.

27008	Guía de auditoría de los controles seleccionados.
27013	Guía de implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
27014	Guía de gobierno corporativo de la seguridad de la información.
27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
27032	Guía relativa a la ciberseguridad.
27033	Guía de seguridad en redes (7 partes).
27034	Guía de seguridad en aplicaciones informáticas.
27035	Guía de gestión de incidentes de seguridad de la información.
27036	Guía de seguridad de externalización de servicios.
27037	Guía de identificación, recopilación y preservación de evidencias digitales.

Fuente: Elaboración propia a partir de [12]

En el año 2005 como consecuencia del evidente aumento de la cantidad de información digital que albergan la gran mayoría de empresas, la ISO y el joint technical committee JTC1 de la Comisión Electrotécnica Internacional o IEC (International Electrotechnical Comission, en inglés) lanzaron la ISO/IEC 27001, para poder asegurar dicha información y minimizar los riesgos del almacenamiento de esta.

Uno de los puntos fuertes de esta norma es su capacidad de adaptación, ya que es capaz de ser implementada en cualquier organización sea del tipo que sea, tanto en una gran multinacional como en una pequeña PYME que acaba de arrancar, empresas con o sin ánimo de lucro incluso privadas o públicas.

Otra clave de las ISO son las certificaciones, ya que una entidad de certificación independiente acredita, en este caso concreto, que se ha implantado un SGSI con éxito y además de cumplir con los requisitos expuestos en la norma, se han adecuado correctamente con el proceder diario de la empresa certificada sin que esto repercuta en su producción.

4.1. ISO 27001

Según la introducción de esta norma internacional está preparada para proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI. El hecho de adoptar un SGSI es una estrategia determinante para una organización.

La implementación y el establecimiento de un SGSI por parte de una organización está condicionado por sus requisitos de seguridad, al mismo tiempo que sus necesidades y objetivos, por otra parte, los procesos organizativos utilizados, su tamaño y estructura también son clave a la hora de tomar una decisión. Todos estos factores que condicionan el SGSI cambiarán con el tiempo previsiblemente.

Mediante la aplicación de un proceso de gestión de riesgos, el SGSI preserva la confidencialidad, integridad y disponibilidad de la información además de otorgar confianza sobre la correcta gestión de los riesgos a las partes interesadas.

Es importante que el SGSI esté integrado y forme parte de los procesos de la organización y de la estructura de global de gestión, también es fundamental que, a medida que se diseñan los procesos, se tenga en consideración la seguridad de la información, de los mismos sistemas de información y de los controles.

Cabe esperar que, el SGSI esté implementado de manera que se ajuste a la organización además de sus necesidades y requisitos. Así pues, la evaluación del cumplimiento por parte de la organización de los propios requisitos de seguridad puede ser realizada de manera externa o interna.

4.2. Marco legal

Dado el incremento progresivo en la complejidad de las organizaciones y los sistemas de información que utilizan, el marco legal por el que se rigen dichas organizaciones es extenso y muchas veces da lugar a confusión. Las organizaciones necesitan cumplir ciertos requisitos para ser visibles en ciertos mercados concretos, ya que por un lado pueden exigirlo las leyes vigentes o bien, está muy bien valorado por proveedores o clientes. Las organizaciones suelen establecer planes sobre la innovación y la mejora continua para poder destacar en su sector a la

vez que resultar atractivas y la evaluación de cómo están gestionando las TI, la seguridad y sus riesgos es primordial para ello.

En el marco legal aparecen requisitos de dos clases, aquellos que exige el propio mercado dónde se desarrolla la actividad y los requisitos legales impuestos por las autoridades del ámbito geográfico en el que se encuentra el mercado. Estos requisitos se pueden cumplir en forma de certificación o de estándar de calidad. A su vez, también cabe la auditoria de los mismos, tanto externa como internamente, para evaluar la progresión y poder ejecutar acciones de mejora.

A continuación, se recogen algunos de los requisitos mencionados que pueden ser objetivo de auditoria.

Tabla 6. Normativa aplicable

Requisito	Categoría	Descripción
LOPD [13]	Ley	Ley 15/1999 de Protección de Datos de Carácter Personal. Tiene como objeto garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas en lo que concierne al tratamiento de sus datos personales.
LSSI [14]	Ley	Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico. Ley que regula las actividades de los proveedores de servicios a través de Internet
Ley de Administración Electrónica [15]	Ley	Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Esta ley confiere unos derechos concretos a los ciudadanos en lo referente a su forma de comunicarse con la Administración Pública.
RDLOPD [16]	Real Decreto	Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
RGPD[17]	Reglamento	Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
ISO 9001	Norma	Norma que determina los requisitos para un sistema de gestión de la calidad.
ISO 20000	Norma	Norma para gestión de servicios de TI
ISO 27001	Norma	Norma que especifica los requisitos para la implantación de un sistema de gestión de la seguridad de la información.

ISO 19011	Norma	Proporciona una orientación para la realización de auditorías de sistemas de gestión.
COBIT	Framework	Framework desarrollado por ISACA dirigido al control y gestión de los sistemas de información en las empresas.
ITIL	Framework	Modelo de buenas prácticas ampliamente aceptado a nivel mundial para la gestión de servicios de TI.
SFIA	Framework	Marco de las competencias en la era de la información.
TOGAF	Framework	El marco de arquitecturas del Open Group es una arquitectura empresarial que ofrece un marco de alto nivel para el desarrollo de software empresarial

Fuente: Elaboración propia a partir de Millet [18]

En el ámbito especifico de este proyecto y de la empresa que se ha tomado como referencia, es de gran importancia la legislación estatal y europea sobre protección de datos. En este caso, el mercado de las empresas dedicadas a la consultoría informática valora la certificación e implementación de las ISO 27000. A su vez, tanto Europa como España exigen la aplicación de las normas sobre protección de datos. Ambas pueden certificarse y auditarse.

No obstante, no debe confundirse la certificación ISO 27001 con la adaptación al RGPD. Estas normas pueden considerarse complementarias entre sí al compartir el objetivo de incrementar la protección de los datos personales y de la información que contienen los sistemas de gestión. La ISO es de aplicación mundial mientras que el RGPD es una norma española que cumple con el requisito de la adaptación de la normativa europea a nuestro ordenamiento interno.

Al ser normas complementarias tienen un gran número de elementos comunes que permiten la implementación en el ámbito de la empresa privada, como es nuestro caso, de una manera sencilla. Este es el principal motivo de confusión entre ambas, ya que las empresas con sede en Europa que inician una certificación en ISO 27001 aprovechan el proceso para adaptarse a la normativa europea.

El RGPD surge como respuesta a la multitud de riesgos que soportan los datos desde el inicio de su tratamiento. La exposición a riesgos con impacto en la protección de datos evoluciona según las variaciones del contexto y los elementos que intervienen en las mismas. De esta forma, se introduce el concepto de “protección de datos desde el diseño y por defecto” (artículo 25 y en los considerandos 78 y 108 RGPD).

Este concepto se refiere a la adopción de medidas técnicas y organizativas, por parte de los responsables del tratamiento, para garantizar el cumplimiento de los requisitos del Reglamento.

El RGPD indica algunas medidas que se deben llevar a cabo, tales como:

1. Al desarrollar, diseñar, seleccionar y utilizar aplicaciones, servicios y productos basados en el procesamiento de datos personales, se debe alentar a los productores para tener en cuenta el derecho a la protección de datos en el desarrollo y diseño de estos productos, servicios y aplicaciones, y asegurar que los responsables y encargados del tratamiento cumplan con sus obligaciones en materia de protección de datos (considerando 78).
2. Garantizar que solo se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento (minimización de datos – artículo 5, apartado 1, letra c).
3. Dar transparencia a las funciones y el tratamiento de los datos (artículo 12).
4. Proceder a la seudonimización de los datos personales lo antes posible (artículo 25.1)[1].
5. Garantizar que los datos personales no sean accesibles sin la intervención de la persona a un número indeterminado de personas físicas. Es decir, permitir a los interesados la supervisión del tratamiento (artículo 25, apartados 2 y siguientes).

Adquiere especial relevancia en relación al trabajo que aquí se presenta la regulación que se recoge en los artículos 32 a 34 del RGPD por hacer referencia a la auditoria de seguridad. Así como, los artículos 35 y siguientes en materia de cumplimiento de la normativa en cuestión.

El artículo 32 RGPD se centra en la Seguridad del tratamiento. En este punto la auditoria debería centrarse en las medidas que deben aplicarse a partir de la realidad de cada organización como, por ejemplo, el cifrado de datos personales.

Respecto de las Violaciones de seguridad, artículos 33 y 34, se deben analizar los protocolos de notificación y los mecanismos de detección y comunicación.

[1] Este término se encuentra en el glosario de términos (Anexo I) y se define en el artículo 4 RGPD como: "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*"

Los artículos 35 y 36 detallan el procedimiento de evaluación y consulta previas al tratamiento cuando se vayan a utilizar nuevas tecnologías que entrañen un riesgo para los datos personales objeto de dicho tratamiento.

Como ya se ha expuesto anteriormente, la ISO 27001 persigue la protección de la información de carácter personal que se maneja en las empresas. Ampara tanto los datos de clientes como los activos digitales e impresos de la organización. Este es el principal motivo y punto de conexión para dar cumplimiento al RGPD a partir de la certificación en ISO 27001.

Al estar centralizado, el SGSI basado en los resultados de la evaluación de riesgos, impide las posibles brechas de seguridad y permite un control más eficiente sobre el proceso a la hora de realizar controles de seguridad.

5. La Empresa de consultoría

La empresa de consultoría informática que hemos tomado como referencia pretende obtener la certificación ISO 270001, es una empresa con mucha experiencia en el sector, fundada en 1995 al comienzo de la gran expansión del sector de la informática como herramienta de trabajo.

Esta empresa desarrolló una herramienta para implementar de una manera más sencilla circuitos de gestión ya que están presentes en todo tipo de empresa tanto privada como pública.

Como toda empresa, manejan información de todo tipo, desde facturas y contratos hasta información más sensible como claves de bases de datos y de accesos a VPNs restringidas. Dada la importancia de esta información es necesario, tanto por protección para la información como para la misma empresa, asegurarla lo máximo posible y una forma adecuada de hacerlo es generando un SGSI que concuerde con su política de empresa.

La consultoría es un servicio profesional dirigido a empresas, instituciones u otro tipo de organizaciones, y que tiene como finalidad someter a examen sus procesos e identificar problemas, irregularidades o incumplimientos de algún marco normativo o legal, o aspectos técnicos que se pueden mejorar[19].

Según PWC[2] (PricewaterhouseCoopers)[20] las empresas de consultoría ofrecen un servicio de asesoría especializado y ajeno a las empresas usuarias para poner solución a posibles problemas o necesidades. Este tipo de empresas se encuentran en constante proceso de innovación para desarrollar a sus profesionales y los métodos y herramientas que emplean en su trabajo.

Las consultoras tienen como objetivo proporcionar a sus clientes un enfoque innovador respecto de la propuesta planteada, ya sea un problema, una necesidad o un proyecto futuro. Estas empresas asesoran a múltiples organizaciones en diferentes sectores y los conocimientos que se adquieren a partir de la formación y el trabajo en proyectos de diversa índole, las convierten en un elemento clave para el desarrollo de los negocios.

[2] PwC es una de las cuatro firmas de consultoría reconocidas como las Big Four, junto con Deloitte, EY y KPMG. Todas ellas tienen reconocido prestigio a nivel mundial en el ámbito de las empresas de consultoría y auditoría empresarial en diferentes ámbitos.

Los elementos esenciales que definen este tipo de empresas son la independencia y la especialización en una materia. Son independientes porque no toman decisiones y especialistas porque poseen un conocimiento amplio y técnico sobre una materia, aunque existen consultoras que trabajan varios ámbitos, sus departamentos están especializados según áreas empresariales concretas[21].

La empresa de consultoría informática evalúa procesos relacionados con las TIC para optimizarlos. El principal trabajo de estas empresas consiste en asesorar a sus clientes en la implantación de las nuevas tecnologías en sus respectivas organizaciones. Es decir, comprender como funciona la organización cliente, comprobar que uso hace de las TIC y tratar de entender el funcionamiento de la empresa cliente. Posteriormente, orientarle hacia nuevas formas de trabajo que les permitan obtener un mejor rendimiento y productividad[22], [23].

5.1. Riesgos

La ISO 27000 define el riesgo como el *efecto de la incertidumbre sobre los objetivos*. Se entiende por efecto una *desviación de lo esperado: positivo o negativo;* y por incertidumbre el *estado de deficiencia de información relacionada con un evento, sus consecuencias o probabilidad*[24]. Tal y como se especifica en la propia norma, el riesgo se caracteriza por referencia a potenciales eventos y sus consecuencias, o una combinación de ambos. Con frecuencia, los riesgos aparecen como una combinación entre las consecuencias del evento y la probabilidad de su ocurrencia[25].

En el contexto que aquí nos atañe, los SGSI, los riesgos que afectan a la seguridad de la información son el resultado de la incertidumbre sobre los propios objetivos de seguridad de la información. Es decir, *el riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización* (ISO 27000: 2018, 3.61).

Otras definiciones que también tienen cabida son la que arroja la UNE 71504: 2008,

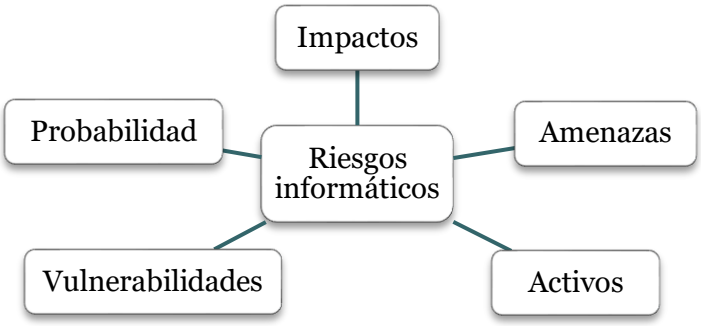
Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización;

Y la facilitada por ITIL: 2007:

Un posible Evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar Objetivos. Un Riesgo es medido por la probabilidad de una Amenaza, la Vulnerabilidad del Activo a esa Amenaza, y por el Impacto que tendría en caso de que ocurriera.

Para poder analizar los riesgos a los que una organización se enfrenta es necesario entender una serie de conceptos, en especial los conceptos de vulnerabilidad y amenaza, ya que se encuentran íntimamente ligados al concepto de riesgo.

Figura 5. Elementos de los Riesgos Informáticos



Fuente: Elaboración propia a partir de [26]

Según S. Quiroz y D. Macías[27], el riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Es la probabilidad de un impacto[3] sobre los activos[4] aprovechando una vulnerabilidad.

En el ámbito de la seguridad de información las vulnerabilidades pueden ser entendidas como los puntos débiles del propio sistema informático. En cambio, las amenazas consisten en los posibles ataques al sistema a partir de una vulnerabilidad. En este sentido, el riesgo viene representado por las posibles formas que puedan adoptar las amenazas y la posibilidad real de su perpetración en una organización concreta.

[3] Es el efecto nocivo que se produce contra un activo determinado de la organización cuando se materializa una amenaza.
[4] Son los elementos objeto de los planes de seguridad, aquellos que la organización quiere proteger.

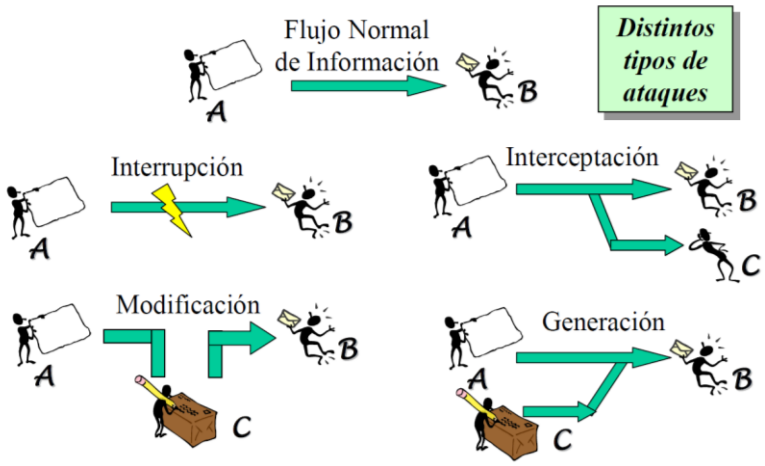
De este modo, podemos afirmar que los riesgos surgen de las amenazas, por lo que, desde una perspectiva de privacidad, es importante comprender qué es una amenaza y cómo identificar los escenarios de riesgo.

5.1.1. Amenazas

Las amenazas informáticas se relacionan con la probabilidad de un daño material o inmaterial provocado por un evento sobre los activos de los sistemas informáticos y de información. Las personas pueden atacar los sistemas ocasionando daños a la infraestructura tecnológica, a los sistemas de gestión de la información y a la propia información de las organizaciones.

Las fuentes que originan estos ataques son muy diversas. Pueden ser constitutivas de ilícitos penales o sucesos naturales, así como de errores humanos por negligencia o incapacidad. En cada interacción con el sistema hay una amenaza latente, por ejemplo, a través de dispositivos externos sin protocolos de seguridad, acceso a una URL (Localizador de recursos uniforme, en inglés, Uniform Resource Locator) no segura, uso mal intencionado o negligente de los propios empleados, etc. Por lo tanto, las amenazas pueden clasificarse en diversos tipos: generación, intercepción, interrupción o modificación. A su vez, estos ataques se pueden subclasificar en activos y pasivos. Los primeros producen cambios en la información que se transmite o en los recursos del sistema. Los segundos acceden a la información o registran el uso que se hace de los recursos.

Figura 6. Tipos de ataques informáticos



Fuente: [28].

5.1.2. Tipos de riesgos

Al igual que las amenazas, los riesgos también pueden clasificarse. En este caso, encontramos cinco grupos diferentes:

I. Riesgos de Integridad

Este grupo de riesgos abarca todos aquellos asociados a la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas por una organización.

II. Riesgos de Relación

Hacen referencia al uso pertinente de la información creada por una concreta aplicación.

III. Riesgos de Acceso

Los riesgos de acceso están enfocados al acceso inadecuado a sistemas, datos e información. Dentro de esta tipología se pueden encontrar:

- Riesgos de segregación de trabajo.
- Riesgos asociados a la integridad de la información.
- Riesgos asociados a la confidencialidad de la información.

IV. Riesgos de Utilidad

Esta clase de riesgos está dividida en tres niveles:

- Técnicas de recuperación y/o restauración.
- Copias de seguridad (Backups).
- Planes de contingencia.

V. Riesgos de Infraestructura

Hacen referencia a la carencia de infraestructuras tecnológicas efectivas en las organizaciones: hardware, software, personal y protocolos.

5.1.3. Brechas de seguridad

Las brechas de seguridad son sucesos que afectan a los datos personales. Estos sucesos pueden ser accidentales o intencionados y acaecer sobre datos tratados de manera digital o analógica. El resultado de estos sucesos es la pérdida, destrucción, acceso fraudulento o alteración a los datos[29].

El RGPD amplió la obligación que la Ley General de Telecomunicaciones (TGL) imponía a las operadoras de servicios de comunicaciones de notificar las brechas de seguridad que afectan a datos personales a todos los responsables de protección de datos de las organizaciones, con independencia del sector en el que operen.

Al informar sobre una brecha de seguridad se notifica también que tipos de medidas se han tomado para mitigar los daños. Las organizaciones informan a sus clientes y usuarios cuando se produce una brecha de seguridad que afecta a su información personal. En estas comunicaciones, además de notificar (o no) las medidas que la organización ha llevado a cabo, se realizan una serie de recomendaciones a los usuarios para paliar posibles repercusiones.

El principal problema a nivel de usuario asociado a estos sucesos es la cadena de ataques o intrusiones a la que puedan verse sometidos por la información sustraída o consultada sin su autorización. La información comprometida se convierte en una "puerta abierta" a otras informaciones personales. Un caso común es el uso del mismo identificador (por ejemplo, el correo electrónico) y de la misma contraseña para acceder a todas las plataformas y servicios web. Si se produce un ataque al servidor de una de las plataformas, ese usuario vería comprometida la información que recogen todas las demás plataformas de las que también es usuario[30].

5.1.4. Riesgos en la corporación

Gestionar la seguridad de la información implica analizar las características de la organización en la que se trabaje.

El nuevo RGPD no se especifica qué medidas deben emplearse según el tipo de información. En la LOPD en cambio, sí se recoge un catálogo de manera clara. La decisión sobre qué medida implementar corresponde a cada organización. El tipo de información que se pretende proteger dicta, generalmente, el criterio utilizado para adecuar las medidas técnicas y organizativas al riesgo contra el que se quiere hacer frente[31].

El tipo de información que se maneja varía según el sector en el que se desarrolle la actividad. Sin embargo, podemos afirmar que existen tres tipos genéricos de información[32] que se manejan en cualquier entidad:

I. Información crítica:

Sobre este tipo de información se aplican los protocolos de seguridad de la información. La información crítica es imprescindible para el funcionamiento de la propia organización. Sin ella la empresa no podría ejecutar ninguna operación.

II. Información valiosa:

La información valiosa, como su nombre indica, es aquella que constituye un componente esencial para los servicios de seguridad informática de la organización.

III. Información sensible:

Este tipo de información adquiere una relevancia notoria desde el punto de vista de la seguridad de la información porque tiene relación directa con la protección de datos de los clientes o usuarios de las organizaciones.

5.2. Beneficios de la certificación

Como ya hemos explicado, la implementación de la ISO 27001 tiene como objetivo mejorar la seguridad de la Organización. Aprovechar el camino recorrido y certificar la calidad del SGSI conlleva, además, una serie de beneficios específicos de cara al mercado, como por ejemplo aumentar la confianza de los clientes, e internamente en la propia Organización.

Beneficios respecto del mercado:

I. Reputación

Las certificaciones, nacionales e internacionales, promueven una imagen más profesional. En algunos casos estas certificaciones son requisito indispensable para el comercio con clientes extranjeros.

II. Transparencia

La transparencia ha adquirido un carácter fundamental a la hora de relacionarse con consumidores y Administraciones, así como con el resto de elementos que configuran el mercado. Las empresas opacas tienden a suscitar desconfianza y mal estar, perdiendo clientes día a día.

La certificación de la implementación de la ISO 27001 permite demostrar que el tratamiento que la Organización da a la información y datos de los clientes es conforme a la legislación.

III. Confianza

Las noticias sobre filtraciones y ventas de datos que grandes empresas han realizado en la última década ha hecho reaccionar a los consumidores. Las personas están más alerta y no confían la información personal tan libremente. La certificación permite a los usuarios confiar en las Organizaciones a la hora de trabajar e interactuar con ellas, ya que se garantiza que se cumplen los requisitos de seguridad y garantías de protección.

IV. Beneficios y clientes

Correlativas a las anteriores, una imagen profesional en el mercado permite destacar por encima de la competencia. Del mismo modo el ejercicio de una actividad transparente y trabajar por ganar la confianza de los clientes permite una mejor posición respecto de clientes potenciales.

El aumento de clientes conlleva el aumento de beneficios económicos y de mayor peso en el mercado.

V. Brechas de seguridad

Evitar brechas de seguridad no solo redunda en beneficios económicos. La reputación de la empresa puede verse afectada de manera negativa si se llegan a producir, pero el principal problema son las sanciones del RGPD.

Cualquier persona con conocimientos informáticos puede atacar una Organización y esto supone un riesgo tanto para las Organizaciones como para los datos personales y sus propietarios. La certificación impone una serie de protocolos que se complementan con el nuevo Reglamento garantizando una mayor seguridad frente a este tipo de ataques.

Beneficios para la Organización:

I. Liderazgo:

Este elemento es imprescindible en la alta dirección. La implementación y certificación de la ISO 27001 permite reformar esta cualidad al involucrar a la alta dirección en las medidas organizativas, técnicas y legales que deben aplicarse para lograr los estándares de protección requeridos.

II. Servicios.

Los protocolos de seguridad pueden conllevar la instalación de mecanismos de control de acceso, criptográficos y controles de red, así como la necesidad de nuevos softwares y licencias. Estas medidas conllevan la interrelación con proveedores de servicios y favorecen la interrelación con otros sectores, ampliando la cartera de clientes potenciales o la posibilidad de acuerdos de colaboración.

III. Estructura.

La implementación de protocolos de seguridad sea cual sea el ámbito de estos, hace necesaria la definición de los puestos de control específicos. Se crea paso a paso un organigrama claro que permite la gestión de las posibles incidencias de una manera rápida y eficaz.

Desde el punto de vista de los SGSI la comunicación interna y el compromiso, así como la toma de conciencia de la importancia de la gestión de las incidencias, de todas las personas implicadas es indispensable para el éxito del sistema.

IV. Formación

Para poder garantizar la competencia de las personas encargadas de la seguridad de la información es necesario mantener los planes de formación actualizados. La formación pasa a ser la inversión en desarrollo del capital humano y como toda inversión, supone un beneficio, en este aspecto a medio y largo plazo.

V. Flexibilidad

Las organizaciones con un SGSI basado en la ISO 27001 son capaces de documentar toda la información que está a su disposición de manera rápida y eficaz, lo cual repercute directamente en beneficio de los clientes y de la propia gestión de la organización.

Esta flexibilidad ayuda a conocer de una manera apropiada la información crítica y facilita la gestión de riesgos que afectan a la confidencialidad e integridad de los activos de la empresa.

VI. Eficiencia

El SGSI basado en ISO 27001 permite la sistematización y aplicación de mejora continua al realizar evaluaciones sobre el tratamiento y aplica los mecanismos de control necesarios para minimizar los riesgos asociados. Los mecanismos y controles garantizan la preservación de la información y logran la eficiencia en los procesos de gestión y tratamiento.

Estos mecanismos que permiten la gestión de la información crítica y sensible de una manera segura mejoran la percepción interna de la organización y ayudan a dar cumplimiento a los preceptos legales y los reglamentos de desarrollo. Sin embargo, según Intedya[5][33], el principal beneficio que se obtiene es la reducción de fallos o errores a la hora de integrar los riesgos en la propia gestión que se realiza de manera preventiva y con fines de mejora

En conclusión, la implementación y certificación de la ISO 27001 permite una adecuada gestión de la información de los clientes y proveedores, consolidando la cartera de clientes y ampliando las fronteras hacia clientes potenciales atraídos por la fiabilidad y profesionalidad de la Organización. Los SGSI basados este estándar de calidad garantizan la confidencialidad, integridad y disponibilidad de la información, mostrando el compromiso con la seguridad de la información y la protección de sus activos.

[5] Intedya es la mayor firma internacional especializada en consultoría, formación y auditoría en materia de gestión de riesgos y cumplimiento normativo.

6. Políticas de gestión de seguridad de la información

La privacidad puede verse comprometida en cualquier momento por algún incidente relacionado con la confidencialidad, la integridad y la disponibilidad, por tanto, deben utilizarse combinaciones de medidas de seguridad para confrontarlos.

En el artículo 33 del RGPD se establece la obligación de que, en caso de que se produzca cualquier brecha de seguridad de datos personales debe notificarse a la autoridad de control competente (AEPD) en un plazo máximo de 72 horas, siempre y cuando dicha brecha suponga un riesgo para los derechos y libertades de las personas físicas.

Según la AEPD a fecha de 6 de abril de 2020, una vez entró en vigor la normativa de brechas de seguridad que repercuten en datos personales, haciendo uso de su sede electrónica, se registraron más de 2400 brechas de seguridad y más de 400 en el primer trimestre del año 2020, indicando un incremento del 48% respecto al mismo trimestre del año anterior. En las estadísticas que son publicadas de manera periódica se observan los tipos de brechas de seguridad más comunes y sus víctimas[34].

En gran medida, las brechas de seguridad no están relacionados con ciberataques complejos, además, en la mayoría de los casos, podrían haberse evitado o al menos disminuido las consecuencias aplicando un análisis de riesgos lógico y utilizando medidas básicas de seguridad que pueden ser aplicadas en organizaciones de diferente índole y tamaño. Algunas medidas básicas de seguridad que propone la AEPD[34] son las siguientes:

I. Uso de contraseñas seguras y segundo factor de autenticación

Debe ser establecida una política de claves de acceso para los sistemas, empezando por no almacenar dichas claves en los sistemas sin ningún tipo de cifrado, obligando a su actualización periódicamente y no siendo reutilizadas para diferentes servicios.

Dadas las incidencias relacionadas con sustracciones masivas de claves, aparece la necesidad imperativa de la utilización de un segundo factor de autenticación para sistemas críticos, pudiendo ser aplicable también para todos los sistemas. Este segundo factor de autenticación consiste en proporcionar, además del usuario y la clave, un elemento adicional

para poder identificar a dicho usuario, como por ejemplo elementos biométricos, códigos pseudoaleatorios, o envíos de claves desechables al ser utilizadas.

II. Copias de seguridad

En la actualidad, el ramsomware o secuestro de información se ha extendido además de ser más peligroso y perjudicial, imposibilitando el acceso a información o servicios de manera temporal o en algunos casos permanentemente.

Las herramientas de copias de seguridad son imprescindibles para la pronta recuperación tras una brecha de seguridad de este tipo, por otro lado, es necesaria la implantación de una política respecto a la realización de copias de seguridad en cualquier organización.

III. Sistemas actualizados

Dado que los desarrolladores aplican mejoras y parches de seguridad de manera continua a medida que encuentran problemas en sus productos, tener los sistemas actualizados es una forma eficaz de evitar brechas de seguridad. Estas actualizaciones no hacen referencia exclusivamente a los sistemas operativos con los que se trabaje, sino a todo el entorno de trabajo, incluyendo aplicaciones y programas que se utilicen en todos los dispositivos, debe ser la versión más reciente publicada por el mismo fabricante, siempre que sea posible. Actualizar de manera periódica documentando y registrando las actualizaciones debe establecerse como rutina.

Como ejemplo, cabe destacar el reciente y famoso ataque WannaCry, el cual afectó a una gran cantidad de equipos por todo el planeta, y que podría haberse evitado en algunos equipos con sistemas operativos recientes, con una actualización que Microsoft había publicado varios meses antes de que el ataque fuera ejecutado.

IV. Exposición de servicios en internet

Algunas de las configuraciones que son aplicadas en ciertas ocasiones para realizar pruebas, tareas de mantenimiento o permitir puntualmente un acceso, se consideran peligrosas en cierta medida, ya que la seguridad puede llegar a verse comprometida. Estas configuraciones temporales, en algunos casos, no están sujetas a vigilancia y acaban por convertirse en permanentes, generando de esta manera una posible brecha de seguridad. Por ejemplo, configuraciones permitiendo el libre acceso a una base de datos desde internet.

Es fundamental el establecimiento de políticas de exposición de servicios en internet, también es imprescindible el uso de conexiones VPN o recursos similares.

V. Cifrado de dispositivos

El cifrado de dispositivos portátiles o aquellos que se pueden perder con facilidad o ser sustraídos de manera ilegitima, es una medida básica para garantizar que la información que contienen es confidencial. El cifrado no es aplicable excepcionalmente a los ordenadores portátiles, las memorias USB, los teléfonos inteligentes (smartphones), teléfonos móviles, tabletas (tablets), discos duros externos e incluso copias de seguridad almacenadas en un lugar diferente al mismo equipo, también están sujetos a dicha medida. En caso de robo perdida, una contraseña no garantiza la confidencialidad de la información, de modo que el cifrado es necesario para asegurar dicha confidencialidad.

Además del cifrado de dispositivos, una buena práctica para evitar brechas de seguridad sería utilizar la cantidad necesaria de información personal el tiempo justo para realizar las acciones pertinentes, ya que almacenar información en dispositivos durante mucho tiempo no es recomendable, principalmente por su exposición a posibles incidentes de seguridad.

7. Aplicación de la norma ISO 27001/2 en la empresa de consultoría.

Siguiendo a M.A. Ramos, Presidente de IEE (Informáticos Europeos Expertos) [35], en materia de protección de datos, el objetivo de toda empresa, entidad, Administración y organización de cualquier otra clase es alcanzar el mayor nivel de seguridad posible. Por ello, la implementación y certificación de la ISO 27001 junto con la adaptación de los sistemas al RGPD son el binomio perfecto para conseguir un sistema firme y seguro.

Como ya se ha explicado a lo largo del presente trabajo, el objetivo principal de la ISO 27001 es proteger la información de una organización, en concreto, la integridad, disponibilidad y confidencialidad de esta. Para ello, se requiere de un análisis de riesgos, vulnerabilidades y amenazas, que puedan afectar a la información.

7.1. Documentación anexa

Para implementar correctamente la norma ISO 27001 es recomendable preparar una serie de documentación, previa o paralelamente a las diferentes fases de la implementación. Los documentos a los que se hace referencia son los siguientes:

I. Política de gestión de seguridad de la información

Este documento constituye el material básico para la implementación de cualquier SGSI. En él se describe de manera detallada la política que la organización quiere implantar.

II. Procedimiento de auditorías internas

Recoger en un documento el procedimiento de auditoria para el SGSI tiene como objetivo principal asegurar que la organización opere de acuerdo con las políticas previamente definidas, en base a una serie de procedimientos y cumpliendo con los requisitos especificados para asegurar el cumplimiento de los objetivos del SGSI.

III. Indicadores

Se trata de las métricas o valores que van a servir de referencia para medir la eficiencia de los controles que se implementen.

IV. Procedimiento de revisión

El Equipo Directivo tiene una función relevante en la implementación del SGSI desde el punto de vista de la revisión. La alta dirección de la organización es la encargada de evaluar según el calendario establecido que se mantienen los niveles de adecuación y eficacia de las medidas.

V. Responsables

Para el correcto funcionamiento de los protocolos de seguridad es necesario que se determine que personas deben ser responsables y cuáles son sus responsabilidades. El equipo directivo debe, por tanto, asignar los roles de responsables o autoridades internas a cada una de las personas que consideren según su cualificación profesional y este reparto debe quedar reflejado de manera documental para poder ser consultado en cualquier momento y por cualquier persona que lo requiera.

VI. Declaración de Aplicabilidad - SOA (por sus siglas en inglés, Statement of Applicability)

La Declaración de Aplicabilidad se desarrolla entre la fase de evaluación y la de tratamiento de riesgos. Este documento tiene como objetivo recoger las medidas de seguridad o controles que se aplicarán en la implementación de la ISO 27001. Se incluye información sobre los objetivos que persigue cada control, una breve descripción y los argumentos para su elección.

La implementación de cada uno de estos controles se desarrollará en un documento separado que deberá ser referenciado en el SOA.

VII. Método de análisis de riesgos

Para poder certificarse de la ISO 27001 la organización debe realizar un análisis de riesgos de su sistema y concretar que activos se encuentran o pueden encontrarse en riesgo. Para ello, el equipo directivo tiene la responsabilidad de evaluar los riesgos aceptados. En este documento se recogen y definen las fases en las que se va a dividir el análisis de riesgos.

7.2. Análisis y gestión de riesgos en la empresa

El RGPD impone a los responsables y encargados del tratamiento de datos personales un análisis de riesgos para establecer qué medidas y controles deben aplicarse en aras de alcanzar los *principios de protección desde el diseño y por defecto* para poder garantizar los derechos y libertades de las personas titulares de los datos[36].

El modelo de gestión más eficiente en la época actual de constante proceso tecnológico es aquel que trabaja desde la monitorización continua del riesgo. Este modelo define los controles y medidas de seguridad a partir de los requisitos de privacidad y evalúa periódicamente la efectividad de las medidas implantadas.

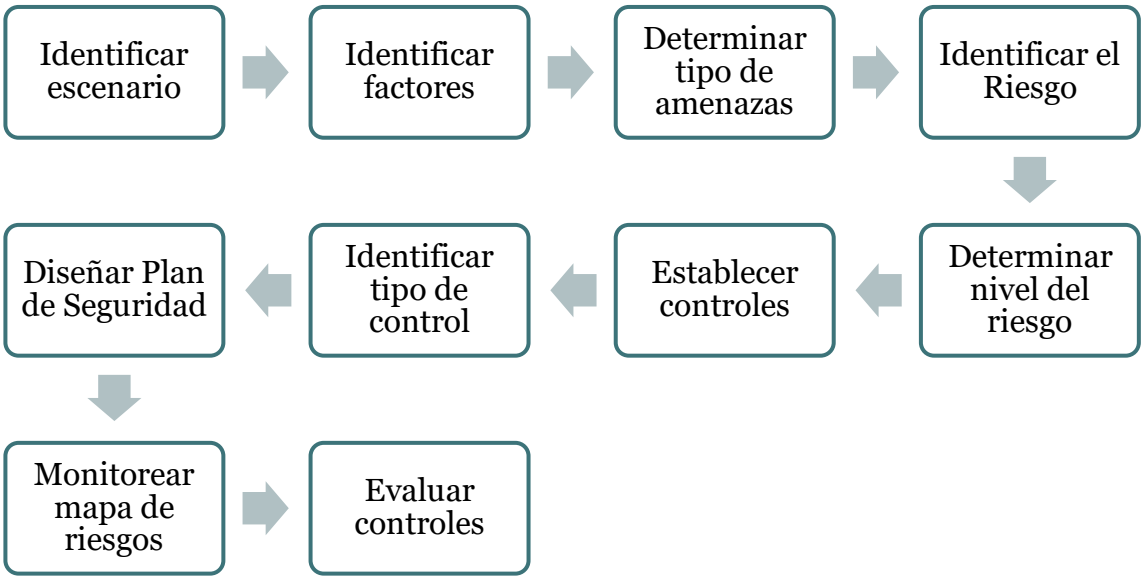
Figura 7. Ciclo de gestión de riesgos

Fuente: [36]

El análisis de riesgos consiste en un análisis sistemático para cuantificar el nivel de riesgo en una organización. Para poder desarrollar este análisis debe seguirse una metodología orientada a determinar los niveles de riesgo aceptables objetivamente. La propia organización

puede definir esta metodología, sin embargo, encontramos instrumentos como la ISO o MAGERIT[6] (de la AEPD) prediseñadas[37].

Figura 8. Fases del análisis de riesgos



Fuente: [26]

1) Identificación de activos:

Los activos son los elementos objeto de la protección. Cada activo entraña un riesgo y requiere un nivel de protección diferente, por ellos deben valorarse e identificarse en primer lugar.

2) Determinar las amenazas

Las amenazas pueden ser de índole muy diversa, natural o humana, intencionada o accidental. Deberán valorarse todas las amenazas posibles respecto de los activos que se quieran proteger.

[6] MAGERIT es la metodología de análisis y gestión de riesgos *elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión*[40].

3) Evaluación de impacto:

La Evaluación de Impacto relativa a la Protección de Datos (EIPD) es un concepto introducido por el RGPD (artículo 35). Es un proceso ligado a los *principios de protección de datos desde el diseño y protección de datos por defecto*[38].

La Agencia Española de Protección de Datos (AEPD) ha elaborado una Guía de Evaluación de Impacto en la Protección de Datos para simplificar la identificación de actividades que implican un riesgo alto y establecer los controles para disminuir el riesgo con anterioridad al inicio del tratamiento de los datos, por parte de las organizaciones[39].

4) Controles:

Una vez determinados los riesgos a los que la Organización está expuesta deben aplicarse las medidas oportunas. Los procesos de gestión de riesgos se encargan de controlar, minimizar y eliminar los riesgos que afectan a los activos. En la ISO 270012 se puede encontrar un catálogo exhaustivo de controles aplicables.

5) Mapa de riesgos:

El Mapa de riesgos de una organización viene constituido por el conjunto de los riesgos potenciales que le afectan. Como los propios riesgos, el Mapa no es estático y va asociado a la evolución del mercado, la tecnología y la sociedad en general sobre la que se desarrolle la organización. A cada riesgo debe asociarse una medida de seguridad, conformando estas el Mapa de medidas de seguridad que se introducirá en el ciclo de mejora continua que lleve a cabo la organización[37].

Como ejemplo se han confeccionado las siguientes tablas siguiendo la metodología MAGERIT:

Tabla 7. Leyenda: Frecuencia-Criticidad-Impacto

	Abreviatura	Valor	Descripción
Criticidad	E	10	Extremo – Daño extremadamente grave
	MA	9	Muy Alto – Daño muy grave
	A	6-8	Alto – Daño grave
	M	3-5	Medio – Daño importante
	B	1-2	Bajo – Daño menor
	D	0	Despreciable – Irrelevante a efectos prácticos
Frecuencia	MF	1	Muy frecuente – Una vez al día
	F	1/21 → 0,048	Frecuente – Una vez cada 3 semanas
	N	1/90 → 0,011	Normal – Una vez cada 3 meses
	PF	1/180 → 0,005	Poco frecuente – Una vez cada 6 meses
	MPF	1/365 → 0,003	Muy poco frecuente – Una vez al año
Impacto	MA	valor > 80%	Muy alto
	A	60% > valor > 80%	Alto
	M	40% > valor > 60%	Medio
	B	20% > valor > 40%	Bajo
	MB	valor < 20%	Muy Bajo

Fuente: Elaboración propia a partir de [40]

Se van a utilizar los valores mencionados en la tabla anterior para calcular la matriz de riesgo.

Tabla 8. Matriz de estimación de riesgo

Riesgo		Impacto				
		100,00%	80,00%	60,00%	40,00%	20,00%
Frecuencia	1	100,00%	80,00%	60,00%	40,00%	20,00%
	0,048	4,80%	3,84%	2,88%	1,92%	0,96%
	0,011	1,10%	0,88%	0,66%	0,44%	0,22%
	0,005	0,50%	0,40%	0,30%	0,20%	0,10%
	0,003	0,30%	0,24%	0,18%	0,12%	0,06%

Fuente: Elaboración propia

A la vista de los porcentajes de riesgo obtenido se requiere una clasificación de niveles de aceptación como se expone en la siguiente tabla:

Tabla 9. Nivel de riesgo

Valor	Abreviatura	Descripción
Valor > 4%	MA	Muy alto
4% > valor > 0,9%	A	Alto
0,9% > valor > 0,35%	M	Medio
0,35% > valor > 0,15%	B	Bajo
valor < 0,15%	MB	Muy bajo

Fuente: Elaboración propia

Estas tablas servirán de referencia para el análisis de riesgos que se muestra ejemplificándolo en el siguiente apartado.

7.3. Propuesta de aplicación

La finalidad de este proyecto consiste en la recopilación de información sobre diferentes marcos de referencia y sobre la norma ISO 27001, además de la posterior aplicación de dichos conocimientos sobre una PYME de servicios de consultoría informática para la preparación de esta en aras de obtener una certificación de dicha norma. Para ello se plantea una propuesta de guía de implementación de la norma ISO 27001 en una PYME de servicios de consultoría informática.

Para implementar la ISO 27001 es recomendable seguir un proceso que podría sintetizarse en el siguiente decálogo agrupado según las fases del Ciclo de Deming:

Planificar:

1) Obtener la participación y el apoyo del Equipo Directivo de la Organización.
2) Definir el alcance del SGSI.

Hacer:

3) Redactar la Política de gestión de seguridad de la información.
4) Seleccionar una metodología para evaluar los riesgos y realizar el tratamiento de estos.

5) Redactar la Declaración de aplicabilidad y el Plan de tratamiento de los riesgos.
6) Concretar los parámetros para medir la efectividad del SGSI.
7) Implementar los controles y procedimientos, así como los programas de formación y capacitación necesarios.

Verificar:

8) Realizar mediciones aleatorias de la eficacia del SGSI y las auditorías internas.
9) Llevar a cabo las revisiones programadas por parte del Equipo Directivo.

Actuar:

10) Aplicar las medidas de corrección que se estimen necesarias.

En la fase de *Planificar* se incluye el requisito del apoyo de la directiva de la organización que resulta ser fundamental y en ocasiones, uno de los más complicados de conseguir. La implicación de la directiva en el proceso de implantación de un SGSI es determinante para su éxito. La definición del alcance y comprensión de la organización y sus circunstancias para determinar cuáles son los límites del SGSI es importante para orientar la implantación.

Tras la obtención del apoyo de la directiva y la definición del alcance, comienza la fase de *Hacer*, en la que se confeccionará el documento de Política de gestión de la seguridad de la información enfocado a la organización desarrollado en el punto 6 del documento. A continuación, se escogerá la metodología de evaluación de riegos que más se adecúe a la organización, en este sentido el apartado 7.2 puede servir de orientación.

Como ejemplo, se va a utilizar MAGERIT para realizar un análisis de riesgos sobre los activos de una empresa de consultoría informática. A continuación, se expone una tabla con el resultado[7].

[7] La tabla mostrada en esta página es una imagen. La tabla original y los datos necesarios para elaborarla se encuentran en el Anexo III.

Tabla 10. Análisis de riesgos

Código	Tipos de Activos Afectados	Amenazas	Frecuencia	Criticidad					Impacto					Riesgo				
				D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
N.2	[HW][Media][AUX][L]	Daños por agua	MPF	10					100%					0,30%				
I.1	[HW][Media][AUX][L]	Fuego	MPF	10					100%					0,30%				
I.6	[HW][Media][AUX]	Corte del suministro eléctrico	PF	6					60%					0,30%				
I.8	[COM]	Fallos de servicios de comunicaciones	N	5					50%					0,55%				
E.1	[D][K][S][SW][Media]	Errores de los usuarios	PF	5	8	10			50%	80%	100%			0,25%	0,40%	0,50%		
E.18	[D][K][S][SW][COM][Media][L]	Destrucción de información	PF	2					20%					0,10%				
E.28	[P]	Indisponibilidad del personal	MPF	5					50%					0,15%				
A.11	[D][K][S][SW][COM][Media][AUX][L]	Acceso no autorizado	MPF		10	10				100%	100%				0,30%	0,30%		

Fuente: Elaboración propia.

En esta etapa se redactarán los documentos de Declaración de Aplicabilidad y de Plan de tratamiento de riesgos, paralelamente se definirán los parámetros de medición de la efectividad del SGSI. Por último, se implementarán los controles recogidos en la norma ISO 27002 y procedimientos necesarios para la gestión de riesgos. Con relación a estos controles se requieren ciertas aptitudes por parte de las personas de la organización, por tanto, cobra especial relevancia la formación continua en buenas prácticas y seguridad de la información. Los marcos de referencia desarrollados en el punto 3 son herramientas útiles a tener en cuenta.

La primera parte de la fase de *Verificar* consiste en medir la eficacia del SGSI a partir de los indicadores establecidos en la fase anterior. Se llevarán a cabo de manera paralela las auditorias internas pertinentes para comprobar el correcto desarrollo del proceso de implementación. El Equipo Directivo revisará periódicamente el correcto funcionamiento del SGSI para garantizar el cumplimiento de la evaluación en función de los criterios establecidos.

La fase de *Actuar* está estrechamente ligada a la anterior, en función de los resultados obtenidos en esta se contemplará la opción de aplicar medidas de corrección ante los posibles errores detectados. Dichos errores repercutirán en la posterior evaluación del Ciclo.

8. Conclusiones

Al comienzo de este Trabajo Final de Grado se exponen ciertos objetivos relacionados con la obtención de conocimientos. Los marcos de referencia expuestos se han explicado para poder aplicar el Ciclo de Deming correctamente, en conjunto con dichos marcos de referencia, a la hora de confeccionar la guía de implantación de la norma ISO 27001. La alusión a la norma ISO 27001 y a la legislación, resulta imprescindible para implantar un SGSI de manera adecuada. Comprender en que consiste una empresa de consultoría informática, además de los riesgos y brechas de seguridad a los que se expone es fundamental para poder detectar y prevenir vulnerabilidades en una organización.

Tras la lectura de esta información, se puede concluir que se han alcanzado estos objetivos. El análisis realizado tanto de los marcos de referencia como de la legislación aplicable nos dan las herramientas para afrontar el proceso de evaluación de riesgos previo a la implantación de un SGSI según la norma ISO 27001.

Dada la inmensa cantidad de información relacionada con protocolos de seguridad referentes a la protección de la información y la legislación vigente sobre protección de datos, es comprensible que exista, en algunos casos, cierta confusión respecto a la correcta gestión de un SGSI en una organización. Tras la revisión de modelos y normas expuestos en esta memoria, podrían resultar relevantes para algunas PYMEs las siguientes recomendaciones:

- Ante la situación actual frente el COVID-19, las organizaciones que pueden desempeñar sus funciones con el teletrabajo se han acogido a él, lo que conlleva ciertas medidas de seguridad a tener en cuenta por parte del personal de dicha organización. Centrarse en la seguridad de la conexión a internet de la que se disponga en el domicilio de cada usuario, como por ejemplo haciendo uso de una VPN para conectarse a la red de la organización, es algo básico para evitar posibles brechas de seguridad.

- Aunque no se pudo continuar con la aplicación práctica de la guía por diversas circunstancias, tras realizar la primera fase de *Planificar* en una PYME de consultoría informática, se recomienda encarecidamente, a la hora de realizar la reunión en la que se deben fijar el alcance y los límites del SGSI, la asistencia de un auditor experto en la materia, ya que pueden llegar a surgir una serie de dudas y casuísticas que podrían ser

resueltas de una manera eficaz. Un auditor, desde su propia experiencia, puede aconsejar y mejorar el proceso.

- La elección de las métricas orientadas a determinar si el SGSI se ha implantado de forma correcta son la clave para lograr comprender en qué puntos se debe mejorar, o incluso si se ha fijado un alcance que se debe redireccionar en otro sentido.

9. Bibliografía

[1] PMG SSI, "ISO 27001: la mejora continua en los SG de Seguridad de la Información," *ISO Tools Excellence*, Jul. 22, 2017. https://www.pmg-ssi.com/2017/07/iso-27001-mejora-continua/ (accessed Aug. 28, 2020).

[2] J. E. Delgado Mena, "ISO/IEC 27001:2013 - Ciclo de mejora continua o Deming," *Seguridasd info Perú*, May 02, 2017. http://seguridadinfoperu.blogspot.com/2017/05/isoiec-270012013-ciclo-de-mejora.html (accessed Aug. 28, 2020).

[3] D. López and F. Martí, "Estándares y marcos de referencia," 2012.

[4] "Cómo funciona SFIA — Español." https://sfia-online.org/es/about-sfia/how-sfia-works (accessed Jul. 21, 2020).

[5] Netmind, "COBIT 5, el nuevo marco para la Gobernanza de las TIC," *Netmind*, 2014. https://www.netmind.es/knowledge-center/cobit-5-el-nuevo-marco-para-la-gobernanza-de-las-tic-2/ (accessed Jul. 22, 2020).

[6] Business Solutios, "Catalizadores COBIT 5," *Business Solutios*. https://bhuertateran.wixsite.com/catalizadores2 (accessed Aug. 30, 2020).

[7] "COBIT 2019," *ISACA*. https://www.isaca.org/resources/cobit (accessed Sep. 03, 2020).

[8] H. Acevedo Juárez, "ITIL: ¿qué es y para qué sirve? (parte 1)," *Magazcitum*, 2010. https://www.magazcitum.com.mx/?p=50 (accessed Jul. 16, 2020).

[9] A. J. Segovia, "¿Qué es ITIL?," *20000 Academy*. https://advisera.com/20000academy/es/que-es-itil/ (accessed Jul. 16, 2020).

[10] M. Molero, "¿Qué es ITIL? | ITIL: Definición y conceptos," *ServiceTonic*. https://www.servicetonic.com/es/itil/3-itil-conceptos-y-principios/ (accessed Jul. 16, 2020).

[11] S. K. White, "¿Qué es TOGAF? Una metodología de arquitectura empresarial para negocios," *Cio Spain*, 2018. https://www.ciospain.es/finanzas/que-es-togaf-una-metodologia-de-arquitectura-empresarial-para-negocios (accessed Jul. 14, 2020).

[12] Grupo de Trabajo de Nuevas Actividades Profesionales, "Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001," 2012. Accessed: Aug. 26, 2020. [Online].

[13] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

[14] *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*.

[15] *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*.

[16] *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*.

[17] *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*.

[18] E. Millet Colomar, "Estudio de una metodología de trabajo para la realización de auditorías integradas de sistemas de información," Valencia, 2015.

[19] "¿Qué Es Una Consultoría Informática? ," *Sale Systems*. https://salesystems.es/que-es-una-consultoria-informatica/ (accessed Sep. 02, 2020).

[20] "¿Qué es Consultoría?," *PwC*. https://www.pwc.com/ia/es/carreras/consultoria.html (accessed Sep. 02, 2020).

[21] "¿Qué es una consultoría?," *Debitoor*. https://debitoor.es/glosario/consultoria (accessed Sep. 02, 2020).

[22] "Consultoría tecnológica," *Neosystems*. http://www.neosystems.es/es/soluciones-y-servicios-neosystems/consultoria-tecnologica (accessed Sep. 02, 2020).

[23] "¿Qué es la consultoría informática? ," *Tecnozero*. https://www.tecnozero.com/mantenimiento-informatico/la-consultoria-informatica/ (accessed Sep. 02, 2020).

[24] J. A. Mañas, "GUÍA DE SEGURIDAD (CCN-STIC-401)," Madrid, 2016. Accessed: Aug. 27, 2020. [Online]. Available: http://www.dit.upm.es/~pepe/401/index.html#!6437.

[25] ISO, "ISO/Guide 73:2009(en), Risk management ," 2009. Accessed: Aug. 28, 2020. [Online]. Available: https://www.iso.org/obp/ui/es/#iso:std:iso:guide:73:ed-1:v1:en.

[26] A. L. Molina Ochoa, "Administración de Riesgos en Informáticos," *SlideShare*, 2013. https://pt.slideshare.net/angelicalorenamolinaochoa/riesgos-informticos-41678365/7 (accessed Aug. 27, 2020).

[27] S. M. Quiroz-Zambrano and D. G. Macías-Valencia, "Seguridad en informática: consideraciones Computer security: considerations," *Dominio de las Ciencias*, vol. 3, no. Extra 3, pp. 676–688, 2017, doi: 10.23857/dom.cien.pocaip.2017.3.5.agos.676-688.

[28] Á. Gómez Vieites, "Tipos de ataques e intrusos en las redes informáticas," 2014, Accessed: Aug. 27, 2020. [Online]. Available: https://scholar.googleusercontent.com/scholar?q=cache:sWTgHghnna4J:scholar.google.com/+VIEITES,+%C3%81lvaro+G%C3%B3mez.+Tipos+de+ataques+e+intrusos+en+las+redes+inform%C3%A1ticas.+&hl=es&as_sdt=0,5.

[29] Agencia Española de Protección de Datos, "Brechas de seguridad," Aug. 06, 2020. https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-seguridad (accessed Aug. 27, 2020).

[30] Agencia Española de Protección de Datos, "Qué son las brechas de seguridad, cómo te pueden afectar y cómo protegerte," Dec. 28, 2018. https://www.aepd.es/es/prensa-y-comunicacion/blog/que-son-las-brechas-de-seguridad-como-te-pueden-afectar-y-como (accessed Aug. 27, 2020).

[31] M. Ibáñez, "La ISO 27001 como herramienta para cumplir con el GDPR," *La Innovación Necesaria*, Dec. 28, 2018. https://www.lainnovacionnecesaria.com/la-iso-27001-como-herramienta-para-cumplir-con-el-gdpr/ (accessed Aug. 28, 2020).

[32] Ingertec, "¿Qué es la seguridad de la información? Aspectos clave," *Ingertec*. https://ingertec.com/que-es-la-seguridad-de-la-informacion/ (accessed Aug. 28, 2020).

[33] International Dynamic Advisors, "ISO 27001, Gestión de la Seguridad de la Información," *Intedya*. https://www.intedya.com/internacional/54/consultoria-isoiec-27001-sistemas-de-gestion-de-seguridad-de-la-informacion.html (accessed Aug. 26, 2020).

[34] AEPD, "Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta," *Agencia Española de Protección de Datos*, Apr. 06, 2020. https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-el-top-5-de-las-medidas-tecnicas-que-debes-tener-en (accessed Aug. 30, 2020).

[35] M. Á. Ramos González, "La auditoría y el Reglamento Europeo de Protección de Datos (RGPD)," *Protección de Datos de Carácter Personal (y RGPD - Reglamento General de Protección de Datos)*, Sep. 2016.

[36] AEPD, "Análisis de riesgos y adopción de medidas de seguridad," *Agencia Española de Protección de Datos*, Oct. 28, 2019. https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/analisis-de-riesgos (accessed Aug. 30, 2020).

[37] AEPD, “El enfoque de riesgos en el Reglamento,” *Agencia Española de Protección de Datos*, Dec. 15, 2018. https://www.aepd.es/es/prensa-y-comunicacion/blog/el-enfoque-de-riesgos-en-el-reglamento (accessed Aug. 30, 2020).

[38] AEPD, “Evaluaciones de impacto de protección de datos,” *Agencia Española de Protección de Datos*, Mar. 09, 2020. https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluaciones-de-impacto (accessed Aug. 30, 2020).

[39] AEPD, “Análisis de Riesgos Evaluación de Impacto La AEPD presenta las Guías de Análisis de Riesgo y Evaluación de Impacto en la Protección de Datos Personales,” *Agencia Española de Protección de Datos*, Feb. 28, 2018. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/analisis-de-riesgos-evaluacion-de-impacto-la-aepd-presenta (accessed Aug. 30, 2020).

[40] M. A. Amutio Gómez, J. Candau, and J. A. Mañas, *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid, 2012.

[41] ISO27000.es, “Serie 27k,” *ISO27000.es*. https://www.iso27000.es/iso27000.html (accessed Aug. 26, 2020).

10. Anexos

Anexo I: Glosario

ISO 19011

3.1. Auditoría: *proceso sistemático, independiente y documentado para obtener evidencias objetivas (3.8) y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (3.7).*

Nota 1 a la entrada: Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por, o en nombre de la propia organización.

Nota 2 a la entrada: Las auditorías externas incluyen lo que se denomina generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tales como los clientes o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes, tales como las que otorgan la certificación/registro de conformidad o agencias gubernamentales.

[ORIGEN: ISO 9000:2015, 3.13.1, modificada — las Notas a la entrada han sido modificadas]

3.2 Auditoría combinada: *auditoría (3.1) llevada a cabo conjuntamente a un único auditado (3.13) en dos o más sistemas de gestión (3.18).*

Nota 1 a la entrada: Se conoce como sistema de gestión integrado cuando dos o más sistemas de gestión específicos de una disciplina se integran en un único sistema de gestión.

[ORIGEN: ISO 9000:2015, 3.13.2, modificada]

3.3 Auditoría conjunta: *auditoría (3.1) llevada a cabo a un único auditado (3.13) por dos o más organizaciones auditoras.*

[ORIGEN: ISO 9000:2015, 3.13.3]

3.4 Programa de auditoría: *acuerdos para un conjunto de una o más auditorías (3.1) planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.*

[ORIGEN: ISO 9000:2015, 3.13.4, modificada — se ha añadido texto a la definición]

3.5 Alcance de la auditoría: *extensión y límites de una auditoría (3.1).*

Nota 1 a la entrada: El alcance de la auditoría incluye generalmente una descripción de las ubicaciones físicas y virtuales, las funciones, las unidades de la organización, las actividades y los procesos, así como el periodo de tiempo cubierto.

Nota 2 a la entrada: Una ubicación virtual es un lugar donde la organización desempeña trabajo o presta un servicio usando un entorno en línea que permite a las personas ejecutar procesos con independencia de su ubicación física.

[ORIGEN: ISO 9000:2015, 3.13.5, modificada — se ha modificado la Nota 1 a la entrada, se ha añadido la Nota 2 a la entrada]

3.6 Plan de auditoría: *descripción de las actividades y de los detalles acordados de una auditoría (3.1).*

[ORIGEN: ISO 9000:2015, 3.13.6]

3.7 Criterios de auditoría: *conjunto de requisitos (3.23) usados como referencia frente a la cual se compara la evidencia objetiva (3.8).*

Nota 1 a la entrada: Si los criterios de auditoría son requisitos legales (incluyendo los reglamentarios), las palabras “cumplimiento” o “no cumplimiento” se utilizan a menudo en los hallazgos de la auditoría (3.10).

Nota 2 a la entrada: Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, etc.

[ORIGEN: ISO 9000:2015, 3.13.7, modificada — se ha cambiado la definición y se han añadido las Notas 1 y 2 a la entrada]

3.8 Evidencia objetiva: *datos que respaldan la existencia o veracidad de algo.*

Nota 1 a la entrada: La evidencia objetiva puede obtenerse por medio de la observación, medición, ensayo o por otros medios.

Nota 2 a la entrada: La evidencia objetiva con fines de auditoría (3.1) generalmente se compone de registros, declaraciones de hechos u otra información que son pertinentes para los criterios de auditoría (3.7) y verificables.

[ORIGEN: ISO 9000:2015, 3.8.3]

3.9 Evidencia de la auditoría: *registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría (3.7) y que es verificable.*

[ORIGEN: ISO 9000:2015, 3.13.8]

3.10 Hallazgos de la auditoría: *resultados de la evaluación de la evidencia de la auditoría (3.9) recopilada frente a los criterios de auditoría (3.7).*

Nota 1 a la entrada: Los hallazgos de la auditoría indican conformidad (3.20) o no conformidad (3.21).

Nota 2 a la entrada: Los hallazgos de la auditoría pueden conducir a la identificación de riesgos, oportunidades para la mejora o el registro de buenas prácticas.

Nota 3 a la entrada: En inglés, si los criterios de auditoría se seleccionan de entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o no cumplimiento.

[ORIGEN: ISO 9000:2015, 3.13.9, modificada — se han modificado las Notas 2 y 3 a la entrada]

3.11 Conclusiones de la auditoría: *resultado de una auditoría (3.1), tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría (3.10).*

[ORIGEN: ISO 9000:2015, 3.13.10]

3.12 Cliente de la auditoría: *organización o persona que solicita una auditoría (3.1).*

Nota 1 a la entrada: En el caso de una auditoría interna, el cliente de la auditoría también puede ser el auditado (3.13) o las personas que gestionan el programa de auditoría. Las solicitudes de una auditoría externa pueden provenir de fuentes como autoridades reglamentarias, partes contratantes o clientes existentes o potenciales.

[ORIGEN: ISO 9000:2015, 3.13.11, modificada — se ha añadido la Nota 1 a la entrada]

3.13 Auditado: *organización que es auditada en su totalidad o partes.*

[ORIGEN: ISO 9000:2015, 3.13.12, modificada]

3.14 Equipo auditor: *una o más personas que llevan a cabo una auditoría (3.1) con el apoyo, si es necesario, de expertos técnicos (3.16).*

Nota 1 a la entrada: A un auditor (3.15) del equipo auditor (3.14) se le designa como auditor líder del mismo.

Nota 2 a la entrada: El equipo auditor puede incluir auditores en formación.

[ORIGEN: ISO 9000:2015, 3.13.14]

3.15 Auditor: *persona que lleva a cabo una auditoría (3.1).*

[ORIGEN: ISO 9000:2015, 3.13.15]

3.16 Experto técnico: *persona que aporta conocimientos o experiencia específicos al equipo auditor (3.14).*

Nota 1 a la entrada: El conocimiento o pericia específicos se relacionan con la organización, la actividad, el proceso, el producto, el servicio, la disciplina a auditar, o el idioma o la cultura.

Nota 2 a la entrada: Un experto técnico del equipo auditor (3.14) no actúa como un auditor (3.15).

[ORIGEN: ISO 9000:2015, 3.13.16, modificada — se han modificado las Notas 1 y 2 a la entrada]

3.17 Observador: *persona que acompaña al equipo auditor (3.14) pero no actúa como un auditor (3.15).*

[ORIGEN: ISO 9000:2015, 3.13.17, modificada]

3.18 Sistema de gestión: *conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos (3.24) para lograr estos objetivos.*

Nota 1 a la entrada: Un sistema de gestión puede tratar una sola disciplina o varias disciplinas, por ejemplo, gestión de la calidad, gestión financiera o gestión ambiental.

Nota 2 a la entrada: Los elementos del sistema de gestión establecen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, las políticas, las prácticas, las reglas, las creencias, los objetivos y los procesos para lograr esos objetivos.

Nota 3 a la entrada: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

[ORIGEN: ISO 9000:2015, 3.5.3, modificada — se ha eliminado la Nota 4 a la entrada]

3.19 Riesgo: *efecto de la incertidumbre.*

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad.

Nota 3 a la entrada: Con frecuencia el riesgo se caracteriza por referencia a eventos potenciales (según se define en la Guía ISO 73:2009, 3.5.1.3) y consecuencias (según se define en la Guía ISO 73:2009, 3.6.1.3), o a una combinación de éstos.

Nota 4 a la entrada: Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la probabilidad (según se define en la Guía ISO 73:2009, 3.6.1.1) asociada de que ocurra.

[ORIGEN: ISO 9000:2015, 3.7.9, modificada — se han eliminado las Notas 5 y 6 a la entrada]

3.20 Conformidad: *cumplimiento de un requisito (3.23).*

[ORIGEN: ISO 9000:2015, 3.6.11, modificada — se ha eliminado la Nota 1 a la entrada]

3.21 No conformidad: *incumplimiento de un requisito (3.23).*

[ORIGEN: ISO 9000:2015, 3.6.9, modificada — se ha eliminado la Nota 1 a la entrada]

3.22 Competencia: *capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.*

[ORIGEN: ISO 9000:2015, 3.10.4, modificada — se han eliminado las Notas a la entrada]

3.23 Requisito: *necesidad o expectativa establecida, generalmente implícita u obligatoria.*

Nota 1 a la entrada: "Generalmente implícita" significa que es habitual o práctica común para la organización y las partes interesadas el que la necesidad o expectativa bajo consideración está implícita.

Nota 2 a la entrada: Un requisito especificado es aquel que está establecido, por ejemplo, en información documentada.

[ORIGEN: ISO 9000:2015, 3.6.4, modificada — se han eliminado las Notas 3, 4, 5 y 6 a la entrada]

3.24 Proceso: *conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto.*

[ORIGEN: ISO 9000:2015, 3.4.1, modificada — se han eliminado las Notas a la entrada]

3.25 Desempeño: *resultado medible.*

Nota 1 a la entrada: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño se puede relacionar con la gestión de actividades, procesos (3.24), productos, servicios, sistemas u organizaciones.

[ORIGEN: ISO 9000:2015, 3.7.8, modificada — se ha eliminado la Nota 3 a la entrada]

3.26 Eficacia: *grado en el que se realizan las actividades planificadas y se logran los resultados planificados.*

[ORIGEN: ISO 9000:2015, 3.7.11, modificada — se ha eliminado la Nota 1 a la entrada]

REGLAMENTO EUROPEO RELATIVO A PROTECCIÓN EN EL TRATAMIENTO DE DATOS PERSONALES

Artículo 4. Definiciones

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona

física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (19);

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Anexo II: Serie 27000

Las normas que componen la serie ISO 27000 son muchas y se van a exponer a continuación [41]:

- ISO 27000:

Para comprender y poder aplicar la norma es necesario conocer y entender una serie de términos y definiciones que se van a utilizar durante toda la serie para evitar así alguna posible confusión o mala interpretación de conceptos técnicos o de gestión, esta norma engloba y recoge dichos conceptos. A diferencia de las otras normas que componen la serie, esta es gratuita.

- ISO 27001:

Especificación de los requisitos necesarios para la implantación y gestión de un SGSI en una organización. Esta norma es certificable.

- ISO 27002:

Esta norma es un manual de buenas prácticas en la que se describen evaluaciones y controles recomendables. La norma reúne en 11 dominios distintos 133 controles y 39 objetivos de control. Uno de los anexos de la norma ISO 27001 agrupa todos los controles que se pueden encontrar en la ISO 27002.

- ISO 27003:

Manual para la implementación de un SGSI, además de instrucciones e información para el uso del ciclo Deming (Planificar, Hacer, Verificar, Actuar, PHVA; en inglés, Plan, Do, Check, Act, PDCA) además de los requisitos de las distintas fases.

- ISO 27004:

Compendio dónde aparecen las especificaciones de las métricas y formas de medir aplicables a determinar el rendimiento de un SGSI y los controles con los que está relacionado.

- ISO 27005:

Establecimiento de directrices relacionadas con la gestión de riesgos en el ámbito de la seguridad de la información. Apoya algunos conceptos detallados en la ISO 27001, además está diseñada para reforzar la aplicación de un SGSI partiendo desde un principio relacionado con la

gestión de riesgos. Es aplicable a cualquier tipo de organización que pretenda poder gestionar cualquier riesgo posible en dicha organización y que esté relacionado con la seguridad de la información.

- ISO 27006:

Establecimiento de las especificaciones acerca de los requisitos necesarios para que aquellas organizaciones que lo deseen puedan auditar y certificar un SGSI basado en la ISO 27001.

- ISO 27007:

Manual de realización de una auditoría tanto interna como externa de un SGSI con el fin de constatar una implementación de este basado en la ISO 27001.

- ISO 27008:

Definiciones sobre la evaluación de controles de un SGSI basado en la ISO 27001 y la revisión de la aplicación técnica de estos, con el fin de saber si son válidos para la detección y prevención de riesgos.

- ISO 27009:

Complementos para la ISO 27001 que incluye nuevos controles y requerimientos para sectores específicos.

- ISO 27010:

Especificaciones sobre el tratamiento y compartición de la información entre diversas organizaciones, además de posibles riesgos y la ejecución de controles para poder prevenirlos, haciendo hincapié en riesgos que pueden comprometer un SGSI en una infraestructura de nivel crítico.

- ISO 27011:

Establecimiento de los principios de implantación, gestión y mantenimiento de un SGSI en una organización relacionada con las comunicaciones telemáticas, indicando además como realizar la implantación de controles de la manera más eficiente posible.

- ISO 27012:

Aunque esta norma fue cancelada, trataba de un conjunto de requerimientos de gestión de la seguridad de la información para organizaciones relacionadas con servicios de administración electrónica.

- ISO 27013:

Establecimiento de una guía para posibilitar la integración tanto de un SGSI con la ISO 27001 como un Sistema de Gestión de Servicios (SGS) con la ISO 20000 en aquellas organizaciones que tengan las dos implementadas.

- ISO 27014:

Establecimiento de los principios para la gestión de la seguridad de la información, para que las organizaciones tengan control sobre la evaluación, monitorización y comunicación de las actividades.

- ISO 27015:

Principios relacionados con la implantación de un SGSI de organizaciones relacionadas con servicios financieros como la banca electrónica.

- ISO 27016:

Guía de apoyo a la dirección de las organizaciones para la toma de decisiones económicas relacionadas con un SGSI.

- ISO 27017:

Guía con 37 controles específicos basados en la ISO 27002 para los servicios en la nube o cloud.

- ISO 27018:

Implantación de procedimientos y controles para la protección de datos personales en servicios cloud proporcionados por organizaciones para terceros, como complemento de las ISO 27001 e ISO 27002.

- ISO 27019:

Guía de implantación de un SGSI basada en la norma ISO 27002 para la aplicación en organizaciones relacionadas con la energía.

- ISO 27021:

Especificación de requerimientos para profesionales que dirigen el establecimiento, implementación, mantenimiento y mejora continua de algún proceso del SGSI cumpliendo la norma ISO 27001.

- ISO 27022:

En proceso de creación, abarcará una descripción de procedimientos relacionados con un SGSI.

- ISO 27023:

Guía de equivalencias entre las versiones del 2005 y 2013 de la ISO 27001 e ISO 27002 para apoyar la transición.

- ISO 27030:

En proceso de creación, abarcará la privacidad y seguridad, controles, riesgos y principios, aplicables al Internet de las Cosas (IoT, Internet of Things).

- ISO 27031:

Guía para la adaptación de las tecnologías de la información y la comunicación en una organización para su futuro.

- ISO 27032:

Guía para mejorar el estado de la ciberseguridad, recogiendo especificaciones de dicha actividad y de sus dependencias en otros ámbitos de seguridad como la seguridad de las redes, información de seguridad, información de protección de infraestructuras críticas (CIIP, Critical Information Infrastructure Protection) y seguridad en internet. Aborda prácticas de seguridad básicas para gente interesada en la ciberseguridad.

- ISO 27033:

Norma centrada en la seguridad de redes, consta de seis partes:

I. ISO 27033-1: Conceptos sobre seguridad de redes.
II. ISO 27033-2: Guía para el diseño e implementación de seguridad de redes.
III. ISO 27033-3: Escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control.
IV. ISO 27033-4: Asegurar las comunicaciones entre redes mediante pasarelas de seguridad.
V. ISO 27033-5: Asegurar las comunicaciones a través de Redes Privadas Virtuales (Virtual Private Network, VPN).
VI. ISO 27033-6: Asegurar el acceso a la red de protocolo de internet (Internet Protocol, IP) inalámbrica.

- ISO 27034:

En desarrollo, especificaciones sobre seguridad de aplicaciones informáticas, consta de siete partes:

I. ISO 27034-1: Conceptos generales.
II. ISO 27034-2: Marco normativo de la organización.
III. ISO 27034-3: Proceso de gestión de seguridad en aplicaciones.
IV. ISO 27034-4: Validación de seguridad en aplicaciones.
V. ISO 27034-5: Estructura de datos y protocolos y controles de seguridad en aplicaciones.
VI. ISO 27034-6: Guía para la seguridad en aplicaciones de uso específico.
VII. ISO 27034-7: Marco predictivo de seguridad.

- ISO 27035:

Guía referente a la gestión de incidentes de seguridad de la información, consta de dos partes:

I. ISO 27035-1: Principios de la gestión de incidencias.
II. ISO 27035-2: Guía de planificación y preparación para la respuesta a incidencias.

- ISO 27036:

Guía referente a la seguridad en relaciones con proveedores, consta de cuatro partes:

I. ISO 27036-1: Conceptos generales.
II. ISO 27036-2: Requerimientos.

III. ISO 27036-3: Directrices para la seguridad de la cadena de suministro de tecnología de la información y las comunicaciones.
IV. ISO 27036-4: Directrices para la seguridad de los servicios en la nube.

- ISO 27037:

Guía que pone a nuestra disposición directrices para actividades relacionadas con la identificación, recopilación, adquisición y preservación de evidencias digitales que pueden tener valor probatorio. Proporciona orientación respecto a situaciones comunes que se encuentran a lo largo del proceso de tratamiento de evidencias digitales, por otro lado, ayuda a las organizaciones en sus procedimientos disciplinarios además de facilitar el intercambio de evidencias digitales potenciales entre jurisdicciones.

- ISO 27038:

Guía con especificaciones sobre la redacción digital.

- ISO 27039:

Guía para ayudar a las organizaciones para implementar sistemas de detección y prevención de intrusiones (en inglés, Intrusion Detection and Prevention Systems, IDPS).

- ISO 27040:

Guía técnica detallada sobre cómo las organizaciones pueden definir un nivel apropiado de mitigación de riesgos mediante el empleo de un enfoque consistente y probado para la planificación, el diseño, la documentación y la implementación de la seguridad del almacenamiento de datos.

- ISO 27041:

Proporciona orientación sobre mecanismos para garantizar que los métodos y procesos utilizados en la investigación de incidentes de seguridad de la información sean "adecuados para su propósito".

- ISO 27042:

Proporciona orientación sobre el análisis y la interpretación de la evidencia digital de una manera que aborda cuestiones de continuidad, validez, reproducibilidad y repetibilidad.

- ISO 27043:

proporciona pautas basadas en modelos idealizados para procesos de investigación de incidentes comunes en varios escenarios de investigación de incidentes que involucran evidencia digital.

- ISO 27045:

En desarrollo, incluirá procesos de seguridad y privacidad en el campo del big data.

- ISO 27050:

Proporciona requisitos y recomendaciones sobre actividades en el descubrimiento electrónico, que incluyen, entre otros, identificación, preservación, recopilación, procesamiento, revisión, análisis y producción de información almacenada electrónicamente (Electronically Stored Information, ESI).

- ISO 27070:

En desarrollo, proporciona técnicas de seguridad y requisitos para establecer “raíces de confianza virtualizadas” que se refiere a la provisión de entornos informáticos confiables en la nube, donde las máquinas virtuales se crean de forma dinámica para brindar servicios en la nube.

- ISO 27071:

En desarrollo, proporciona recomendaciones para establecer conexión de confianza entre dispositivo y servicio.

- ISO 27099:

En desarrollo, proporciona prácticas y marco de políticas sobre la infraestructura de clave pública (Public Key Infraestructure, PKI) que se refiere al sistema de creación compuesto por hardware, software, políticas, procesos y procedimientos requeridos para crear, gestionar, distribuir, utilizar, almacenar y revocar certificados digitales o claves públicas.

- ISO 27100:

En desarrollo, resumen y conceptos sobre la ciberseguridad.

- ISO 27101:

En desarrollo, guía sobre el desarrollo del marco relacionado con la ciberseguridad.

- ISO 27102:

Proporciona pautas a la hora de comprar un seguro cibernético como una opción de tratamiento de riesgos para gestionar el impacto de un incidente cibernético dentro del marco de gestión de riesgos de seguridad de la información de la organización.

- ISO 27103:

proporciona orientación sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad.

- ISO 27550:

Proporciona pautas sobre ingeniería de la privacidad destinadas a ayudar a las organizaciones a integrar los avances más recientes en ingeniería de la privacidad en los procesos del ciclo de vida del sistema.

- ISO 27551:

En desarrollo, proporciona requerimientos para la autenticación de entidades no vinculables basada en atributos.

- ISO 27553:

En desarrollo, proporciona requisitos de seguridad para la autenticación en dispositivos móviles mediante biometría.

- ISO 27554:

En desarrollo, proporciona una relación sobre cómo aplicar la ISO 31000 para la evaluación de riesgos relacionados con la gestión de identidad.

- ISO 27555:

En desarrollo, proporciona directrices sobre la eliminación de información de identificación personal.

- ISO 27556:

En desarrollo, proporciona un marco para la gestión de información de identificación personal (Personally Identifiable Information, PII) basado en preferencias de privacidad.

- ISO 27570:

En desarrollo, proporciona una guía sobre la privacidad para las Smart Cities[8].

- ISO 27701:

Especifica los requisitos y proporciona una guía para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Información de Privacidad (Privacy Information Management System, PIMS) en forma de extensión de la ISO 27001 e ISO 27002 para la gestión de la privacidad dentro del contexto de la organización.

- ISO 27799:

Directrices para los estándares de seguridad de la información de las organizaciones y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de estas.

[8] Ciudades Inteligentes.

Anexo III: Análisis de riesgos

- Seleccionar los activos que serán objeto del análisis.

Tabla 11. Tipos de activos

Código	Activo
D	Datos / Información
K	Claves Criptográficas
S	Servicios
SW	Software
HW	Hardware
COM	Redes de comunicaciones
Media	Soportes de información
AUX	Equipamiento auxiliar
L	Instalaciones
P	Personal

Fuente: Elaboración propia a partir de [40]

Según MAGERIT los activos se clasifican en los grupos que hemos presentado en la tabla anterior. Dentro de cada clase se determinan qué activos concretos se van a incluir (por ejemplo, equipos de trabajo, ficheros, copias de seguridad, servidor de ficheros, etc.)

- Determinar las amenazas que pueden afectar a los activos.

Tabla 12. Tipos de amenazas

Código	Amenaza
N	**Desastres Naturales**
N.2	Daños por agua
I	**De origen industrial**
I.1	Fuego
I.6	Corte del suministro eléctrico
I.8	Fallos de servicios de comunicaciones
E	**Errores y fallos no intencionados**
E.1	Errores de los usuarios
E.18	Destrucción de información

E.28	Indisponibilidad del personal
A	**Ataques intencionados**
A.11	Acceso no autorizado

Fuente: Elaboración propia a partir de [40]

Hemos seleccionado algunas amenazas estrechamente relacionadas con una empresa de consultoría informática. En el Libro II de MAGERIT se puede encontrar el catálogo completo de dichas amenazas.

- Estimar el riesgo

Código	Tipos de Activos Afectados	Amenazas	Frecuencia	Criticidad					Impacto					Riesgo				
				D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
N.2	[HW][Media][AUX][L]	Daños por agua	MPF	10					100%					0,30%				
I.1	[HW][Media][AUX][L]	Fuego	MPF	10					100%					0,30%				
I.6	[HW][Media][AUX]	Corte del suministro eléctrico	PF	6					60%					0,30%				
I.8	[COM]	Fallos de servicios de comunicaciones	N	5					50%					0,55%				
E.1	[D][K][S][SW][Media]	Errores de los usuarios	PF	5	8	10			50%	80%	100%			0,25%	0,40%	0,50%		
E.18	[D][K][S][SW][COM][Media][L]	Destrucción de información	PF	2					20%					0,10%				
E.28	[P]	Indisponibilidad del personal	MPF	5					50%					0,15%				
A.11	[D][K][S][SW][COM][Media][AUX][L]	Acceso no autorizado	MPF		10	10				100%	100%				0,30%	0,30%		