Universidad San Jorge

Escuela de Arquitectura y Tecnología

Grado en Ingeniería Informática

Proyecto Final

Implementación y aplicación de la ISO 27001:2013 en una consultora de TI de tamaño mediano

Autor del proyecto: José Baltasar Couce López

Director del proyecto: Germán Latorre Antín

Zaragoza, 17 de junio de 2021

universidad SANJORGE
GRUPO SANVALERO

Este trabajo constituye parte de mi candidatura para la obtención del título de Graduado en Ingeniería Informática por la Universidad San Jorge y no ha sido entregado previamente (o simultáneamente) para la obtención de cualquier otro título.

Este documento es el resultado de mi propio trabajo, excepto donde de otra manera esté indicado y referido.

Doy mi consentimiento para que se archive este trabajo en la biblioteca universitaria de Universidad San Jorge, donde se puede facilitar su consulta.

Firma Fecha 17 de Junio del 2021

Dedicatoria y Agradecimiento

A mis padres, Carme y Jose (D.E.P.), por apoyarme siempre en todos los proyectos, y muy especialmente en los de formación, para crecer como profesional y como persona.

A mi pareja e hijos por permitirme quitarles tiempo de estar en su compañía y proporcionarme el apoyo necesario para continuar hasta el final con este proyecto.

A mis compañeros de trabajo por su comprensión y disposición durante el desarrollo de este proyecto.

Y finalmente y no menos importante a mi tutor German, por la gestión, revisión y correcciones realizadas en el proyecto.

Tabla de contenido

Tabla de Ilustraciones

Tabla de Tablas.

Resumen

La idea de este proyecto surge por la necesidad actual de que las pymes necesitan concienciarse de la toma de medidas de seguridad y de las ventajas que ofrece disponer de un Sistema de Gestión de Seguridad de la Información (SGSI), tanto a nivel interno como externo.

Se desarrolla un análisis y comparativa entre diferentes normas certificables para la implantación de un SGSI y se estudia la que consideramos que mejor encaja a nivel global en una pyme, siempre teniendo en mente el contexto empresarial y los objetivos de la organización.

Se presenta una secuencia de pasos necesarios y viables para poder implementar y superar la certificación de la norma, junto con los requisitos documentales imprescindibles.

El caso de uso presentado, se utiliza como referencia para crear las plantillas de la documentación imprescindible para la superación de la implementación y certificación de la normativa de seguridad seleccionada.

Abstract

The idea of this project comes from the current need for SME's to be more aware of the security measures which should be taken, both at an internal and external level, and the advantages of having an Information Security Management System (ISMS).

Firstly, we develop an analysis and comparison between different certifiable standards for the implementation of an ISMS. Then, we study the option we consider fits best globally for the SME, always keeping in mind the business context and the objectives of the organization.

A sequence of necessary and feasible steps is then presented to implement and pass the certification of the standard, together with the essential documentation requirements.

The presented use case is employed as a template for the documentation of the selected security standard, a necessary requirement to receive a passing grade in the aforementioned implementation and associated certification

1. Introducción

1.1. Introducción

A lo largo de los años la información en las empresas siempre ha sido un recurso importante, pero actualmente se está convirtiendo en uno de los activos más críticos.

Hoy en día nos encontramos en la era de la información digital. La mayoría de las empresas dependen de las tecnologías de la información para el progreso y crecimiento de dichas empresas: Tratamiento de información financiera de la empresa y de los competidores, estudios e investigaciones del negocio y los mercados, redes sociales, información de los clientes, etc.

Otras muchas empresas que están surgiendo en la actualidad, están basando su núcleo de negocio en el almacenamiento de los datos y tratamiento de los datos.

Al mismo tiempo que la información ha crecido como centro de negocio, también ha crecido en mayor medida los ataques e intentos de robo de dicha información digital, tal como se puede ver en los medios de comunicación e informes de diferentes agencias nacionales.

Según el informe de la Agencia Española de Protección de Datos, correspondiente al mes de marzo del 2021 se indica que durante el año 2018 recibieron un total de 547 notificaciones, durante el año 2019 un total de 1460 notificaciones, durante el año 2020 un total de 1370 y el total acumulado de los últimos 12 meses a marzo del 2020 se llevaban registradas 1437 notificaciones [1].

Como consecuencia de esto, es muy importante mantener todos estos datos e información segura y protegida contra eventuales pérdidas o ataques.

Por lo que a lo largo de este proyecto se realizará un análisis y comparativa de las diferentes normativas para certificar la seguridad de la información en el ámbito empresarial, así como las tareas y documentación necesarias para superar la norma ISO/IEC 27001. Para completar se presentará un caso práctico sobre el que se aplicarán parte de las fases y se creará parte de la documentación.

1.2. Justificación

Como la información es uno de los elementos más valiosos en la actualidad para cualquier organización, siendo utilizada para lograr ventajas competitivas. Por lo que es muy importante implantar procedimientos o normas que nos permitan asegurar la información.

Hasta hace pocos años y salvo casos muy contados, los comités de dirección empresariales no tenían en su foco de atención la protección de la información o la inversión en seguridad, pues se consideraba más como un gasto que como una inversión.

En los últimos años y debido al incremento de los ataques y pérdidas de información, con su consecuente pérdida de capital o reputación, dichos comités comienzan a valorar la importancia

de disponer de un Sistema de Gestión de Seguridad de la Información (SGSI), a partir de ahora se referenciará por sus iniciales.

Actualmente a nivel nacional destacan dos normativas para certificar los sistemas de Gestión de Seguridad de la información: La ISO/IEC 27001:2013 y el Esquema Nacional de Seguridad (ENS), regulado en el Real Decreto España 3/2010.

Cualquiera de las dos normativas es una buena opción para que las empresas dispongan de una correcta gestión de la ciberseguridad, focalizando en la mejora continua del control de riesgos y amenazas.

La implantación de un SGSI basado en cualquiera de los estándares permite una implantación sencilla de métodos, políticas, procedimiento y controles que permiten disminuir los riesgos de la información aportando:

- Reducción de riesgos sobre los activos empresariales, pues se establece un control y seguimiento.
- La seguridad de la información pasa a formar parte integral de la gestión empresarial, pues se transforma en un ciclo de vida controlado en el que participa toda la organización implicada en la implantación.
- La empresa asegura el cumplimiento de la legislación vigente en el ámbito de la seguridad de la información.
- Poseer el certificado puede ayudar a mejorar la imagen y confianza de colaboradores, proveedores y clientes.

1.3. Estructura del documento

El presente documento consta de tres partes diferenciadas:

La primera parte, tratada en el punto4, nos presenta de forma los más sintetizada posible el contexto de las normativas actuales que más auge tienen actualmente para la certificación de un SGSI a nivel nacional y europeo y las seleccionadas para implementar el SGSI y el caso de uso.

La segunda parte, tratada en el punto 6, presenta una secuencia de pasos o fases necesarias para implementar la ISO/IEC 27001:2013 en el ámbito de las Pymes. Se destaca y detalla el contenido de la documentación y registros imprescindibles que debe de presentar una Pyme para superar dicha normativa.

La tercera y última parte, tratada en el punto 7, presenta un caso de uso de una pyme a partir de la cual se crearán y presentará unas plantillas de parte de la documentación imprescindible para superar la ISO/IEC 27001:2013. Parte de dichas plantillas y por su extensión se presentarán como parte del Anexo.

2. Objetivos

Los objetivos principales definidos para del PFG fueron:

Este es el objetivo principal definido para del PFG en la propuesta inicial:

> "Analizar los pasos y tareas que debe de realizar y cumplir una consultora de TI para lograr obtener la certificación ISO/IEC 27001:2013."

Después de analizar y profundizar en la definición inicial del objetivo principal, se ha reformulado de forma que el proyecto tenga un alcance más amplio:

> "Presentar una perspectiva global del proceso de implantación de la normativa ISO/IEC 27001:2013 en una Pyme, considerando la definición de pyme como la empresa que cumple al menos dos de los siguientes criterios:
>
> - Constar de menos de 250 empleados.
> - Tener unas ventas anuales inferiores a 40 millones de euros.
> - Tener un valor total de activos de la empresa inferior a 27 millones de euros."

Una vez definido el objetivo principal, se han definido los siguientes objetivos para el proyecto:

1. Analizar las diferentes normativas que certifican la implantación de un SGSI.
2. Presentar la secuencia de pasos, tareas que debe de realizar y cumplir una pyme para lograr obtener la certificación ISO/IEC 27001:2013.
3. Identificar la documentación requerida e imprescindible que se tiene que presentar para superar la certificación ISO/IEC 27001:2013
4. Presentar un caso práctico basado en una consultora TI de tamaño mediano.
5. Presentar las plantillas de la mayoría de la documentación imprescindible para superar la certificación ISO/IEC 27001:2013, tomando como base el caso práctico.

3. Metodología

La metodología empleada en el desarrollo de este PFG, ha consistido en la investigación de diferentes normativas y el proceso de aplicación de un SGSI en el ámbito empresarial de una Pyme.

En la primera etapa se investiga y profundiza en las dos normativas más destacadas en el ámbito de la certificación de SGSI a nivel nacional europeo, ENS y la ISO/IEC 27001:2013 para poder seleccionar la que más se adecua al proyecto.

En una segunda etapa se investiga las formaciones y recursos disponibles de los que dispone una Pyme en internet y diferentes proveedores para poder llevar a cabo la implementación de un SGSI. Seleccionando objetivamente los cursos y certificación con el contenido más destacable al menor coste económico.

En una tercera etapa se realiza la formación de los cursos seleccionados y la certificación correspondiente que se considera útil y suficiente para obtener los conocimientos necesarios para la implementación de un SGSI en una Pyme.

En una cuarta etapa, por ser el núcleo principal de la implementación de cualquier SGSI, se analizan, comparan diferentes metodologías de Gestión de Riesgos, la ISO 31000, ISO/IEC 27005 y Magerit v.3, implementando la que más se adecua a nuestro caso de uso.

En una quinta etapa se presenta y documenta la secuencia de pasos, tareas y requisitos documentales considerados necesarios e imprescindibles para que una Pyme pueda certificarse en la normativa de SGSI seleccionada.

En la sexta y última etapa se presenta un caso de uso en el que se llevan a la práctica la implementación de la normativa aplicada en base a todas las decisiones tomadas en las etapas anteriores. Generando la mayoría de las plantillas y documentos necesarios para implementar y certificar un SGSI implantado en una Pyme.

4. Contexto

Es de vital importancia conocer y definir las diferentes normas y conceptos que se tratarán a lo largo del proyecto.

4.1. Normativas para la implantación de un SGSI (Sistema de Gestión de Seguridad de la Información)

A continuación presentamos varias de las normas más destacadas para la implementación de un SGSI. Definiendo un SGSI como una herramienta que proporciona soporte a las organizaciones para implementar políticas de seguridad, controles y procedimientos alineados con los objetivos del negocio.

Se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad. De este modo estos tres términos son la base de la seguridad de la información.

- Confidencialidad. La información no está disponible para personal o procesos no autorizados.
- Integridad. Mantener la exactitud y completitud de la información.
- Disponibilidad. Proporcionar el acceso a la información al personal o procesos autorizados cuando estos lo requieran.

4.1.1. Esquema Nacional de Seguridad (ENS)

La ENS, regulada por el Real Decreto 3/2010 de 8 enero, es el resultado del trabajo coordinado de varios ministerios y su principal aplicación es en la administración pública española y las organizaciones privadas que proveen de servicios a la administración. Su objetivo es la creación de las condiciones necesarias para garantizar la seguridad en el uso de los medios electrónicos para asegurar las comunicaciones y el intercambio de los datos entre la administración y los ciudadanos.

Los objetivos principales de la ENS son [2]:

- Crear las condiciones necesarias para la confianza en los medios electrónicos
- Introducir metodologías y un lenguaje común
- Servir de modelo de buenas prácticas
- Promover la continuidad en la gestión de la seguridad y su tratamiento homogéneo

A continuación se detalla gráficamente la evolución a lo largo de los años del ENS y normativas relacionadas directamente.

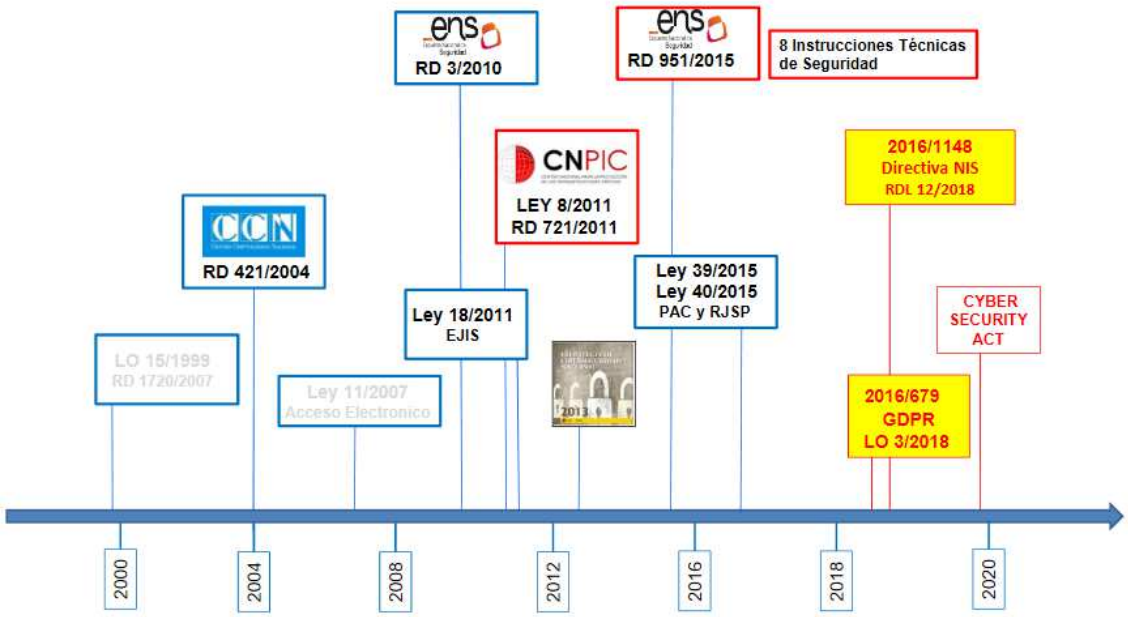


Ilustración 1. Evolución ENS. Fuente: sindicon.gva.es

4.1.2. ISO/IEC 27000

Proporciona una lista de términos y definiciones, en relación con la seguridad de la información, que puede utilizarse como referencia para el resto de estándares ISO 27K.

4.1.3. ISO/IEC 27001:2013

La ISO/IEC 27001 es un estándar internacional que en el año 2020 cumplió 15 años desde su publicación como norma ISO. Su objetivo principal es la implantación de la seguridad en los procesos y objetivos del negocio considerando el análisis de riesgos. Esta norma tiene como origen la BS 7799-1 de 1995 en la que se definían las mejores prácticas para ayudar a las empresas británicas a administrar la seguridad de la información (documento generado por la entidad normalizadora británica BSI).

En el año 2000 la Organización Internacional de Estándares (ISO) creó la primera versión de la ISO 17799 tomando como referencia la norma BS 7799-1. En el año 2002 se actualizo la versión de la BS 7799 por la que las empresas podían certificar su Sistema de Gestión. En el año 2005 aparece la primera versión de la ISO 27001 y en el 2013 el aparece el estándar ISO/IEC 27001:2013 sobre la que se continúan emitiendo los certificados, aunque haya aparecido una revisión menor en el año 2017 [3].

Ilustración 2 Evolución ISO 27001:2013. Fuente pmg-ssi.com

La ISO/IEC 27001:2013 ayuda a detectar, minimizar y solventar diferentes problemas en diferentes ámbitos industriales [4].

Industria	Problemas a Resolver	Soporte de la ISO/IEC 27001:2013
Todas	Cumplir con requerimientos legales y regulatorios.	Ofrece un marco de trabajo para identificar la legislación de seguridad y requerimientos.
Todas	Defenderse ante el incremento de incidencias de seguridad.	Ofrece una metodología para tratar las diferentes amenazas de seguridad al integrar diferentes actividades de seguridad.
Todas	Priorizar inversiones en seguridad	Mediante el análisis de riesgos se muestra una visión clara de la seguridad para poder priorizar la implementación
Todas	Disminuir los costos de los incidentes.	Mediante la prevención de riesgos, el costo de la implementación es menor que los del incidente.
Todas	Herramienta para la alta dirección en relación a la seguridad	Se genera mucha documentación para la alta dirección que es necesario revisar, evaluar y tratar, mostrando el estado de la seguridad.
Todas	Licitaciones y proyectos.	Muchos clientes reclaman a sus proveedores la implementación de normas de SGSI.
Todas	Definición de roles	Es un requerimiento de la norma que permite la identificación de los responsables de seguridad.
Proveedores de TI	Los clientes tienen su información segura.	Los proveedores ofrecen evidencias de la protección de la información de los clientes.
Salud	Proteger registros.	Ofrece metodología para la protección de todo tipo de información, especialmente la sensible.
Alta Tecnología	Proteger propiedad intelectual	Ofrece metodología para la protección de todo tipo de información, especialmente la sensible.
Consultoras	Metodologías para solventar problemas de seguridad.	Ofrece un esquema para que las consultoras puedan implementar medidas de seguridad en las organizaciones de sus clientes.

Tabla 1. Soporte de la ISO/IEC 27001:2013 a diferentes industrias.

4.1.4. ISO/IEC 27002:2018

Es una guía de buenas prácticas que describe los objetivos y controles en relación a la seguridad de la información y no es certificable a diferencia de la anterior ISO/IEC 27001:2013.

Se propone como una guía para implantar los controles y medidas de seguridad, utilizándola a modo de lista de comprobación. Surge en el año 2007 a partir del renombramiento de la ISO 17799:2005 que pasa a llamarse ISO/IEC 27002:2005 y en el año 2013 aparece el estándar ISO/IEC 27002:2013 [5]

4.1.5. ISO/IEC 27017

Proporciona una guía de buenas prácticas para controlar la seguridad en el cloud. Provee de controles adicionales a los ofrecidos por la ISO 27002 para la protección de la información procesada y almacenada en el cloud.

Es una normativa focalizada en las organizaciones que ofrecen servicios en el cloud y que necesitan proteger todos los frentes de seguridad de la computación en ese entorno [6].

Dominio de control ISO/IEC 27001:2013 / ISO 27002	Nivel de cambio en ISO 27017
5. Políticas de seguridad de la información	Moderados
6. Organización de seguridad de la información	Moderado
7. Seguridad relativa a los recursos humanos	Moderado/Bajo
8. Gestión de activos	Moderado/Bajo
9. Control de accesos	Alto
10. Criptografía	Moderado
11. Seguridad física y del entorno	Moderado/Bajo
12. Seguridad de operaciones	Moderado/Alto
13. Seguridad de comunicaciones	Moderado/Alto
14. Adquisición, desarrollo y mantenimiento de sistemas informáticos	Moderado
15. Relaciones con proveedores	Moderado/Alto
16. Gestión de incidentes de seguridad de la información	Moderado
17. Aspectos de seguridad de la información para la gestión de continuidad del negocio	Bajo
18. Cumplimiento	Moderado/alto

Tabla 2. Ampliación ISO 27017

4.1.6. ISO/IEC 27018

Proporciona un guía de buenas prácticas para controlar la seguridad en el cloud. Provee de controles adicionales a los ofrecidos por la ISO 27002 para proteger la información personal identificable.

Esta normativa estás más centrada en organizaciones que gestionan datos de carácter personal y necesitan asegurar la manera más adecuada de proteger esta información.

Dominio de control ISO/IEC 27001:2013 / ISO 27002	Nivel de cambio en ISO 27018
5. Políticas de seguridad de la información	Moderados

6. Organización de seguridad de la información	Bajo
7. Seguridad relativa a los recursos humanos	Bajo
8. Gestión de activos	Bajo
9. Control de accesos	Bajo
10. Criptografía	Bajo
11. Seguridad física y del entorno	Bajo
12. Seguridad de operaciones	Alto
13. Seguridad de comunicaciones	Bajo
14. Adquisición, desarrollo y mantenimiento de sistemas informáticos	Bajo
15. Relaciones con proveedores	Bajo
16. Gestión de incidentes de seguridad de la información	Moderado
17. Aspectos de seguridad de la información para la gestión de continuidad del negocio	Bajo
18. Cumplimiento	Moderado

Tabla 3. Ampliación ISO 27018

4.1.7. ISO/IEC 27032

No es un estándar que permita certificar a la organización. Proporciona recomendaciones específicas en relación a la ciberseguridad. Explica la relación de la ciberseguridad con la seguridad de la información, como enfrentarse a los problemas más habituales de la ciberseguridad.

4.2. Normativas sistema de Gestión de Riesgos

El punto clave de todo SGSI (Sistema de Gestión de Seguridad de la Información) es la implementación de un análisis de riesgos sobre los activos de la información.

A continuación presentamos varias de las normas más destacadas para la gestión del riesgo.

4.2.1. ISO 31000:2018

Es un estándar internacional, que establece un enfoque para la implementación de la gestión de riesgos en cualquier tipo de empresa sea pública o privada. Proporciona unos principios y directrices para la gestión de riesgos. Solo formula recomendaciones, por lo que no permite la implementación de un sistema de gestión certificable.

4.2.2. MAGERIT v.3

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que actualmente está en la versión 3.0 es un referente a nivel nacional cuando se trata de la

gestión de riesgos. Elaborada por el Consejo Superior de Administración Electrónica (CSAE) y publicada por Ministerio de Administración Publica de España (MAP)

Es una metodología para facilitar el análisis y aplicación del sistema general de riesgos, proporcionando los principios básicos y requisitos mínimos para la protección de la información.

MAGERIT persigue los siguientes Objetivos Directos [7]:

- Concienciar a los responsables de las organizaciones de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos.
- Ayudar a encontrar y planificar el tratamiento adecuado para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría o certificación.

Esta metodología está reconocida junto con otras metodologías internacionales y europeas.

4.2.3. ISO/IEC 27005:2018

Este estándar sustituyo la norma ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000 desde su publicación en el año 2008. Presenta un conjunto de directrices para la correcta implementación de un análisis de riesgos de la seguridad de la información [8].

No proporciona una metodología concreta de Gestión de Riesgos, mediante sus cláusulas describe le proceso de análisis incluyendo las fases que lo componen:

- Establecimiento del contexto: Objetivos y alcance.
- Valoración del riesgo:
    - Identificar los riesgos que pueden provocar pérdidas en el sistema de información.
    - Estimar los riesgos, utilizando un método cuantitativo o cualitativo, teniendo en cuenta las amenazas y salvaguardas.
    - Evaluar el riesgo comparando los riesgos estimados con los criterios de aceptación definidos.
- Tratamiento del riesgo: Definir la estrategia para cada riesgo mediante la reducción, aceptación o transferencia.
- Aceptación del riesgo: Identificar los riesgos que se aceptan y se justifican.
- Consulta y comunicación: Intercambiar información relacionada con los riesgos entre los grupos de interés definidos.
- Revisión y monitorización del riesgo: Actualizar el análisis del riesgo.

Incluye seis anexos que tratan la identificación de activos, vulnerabilidades, amenazas y más.

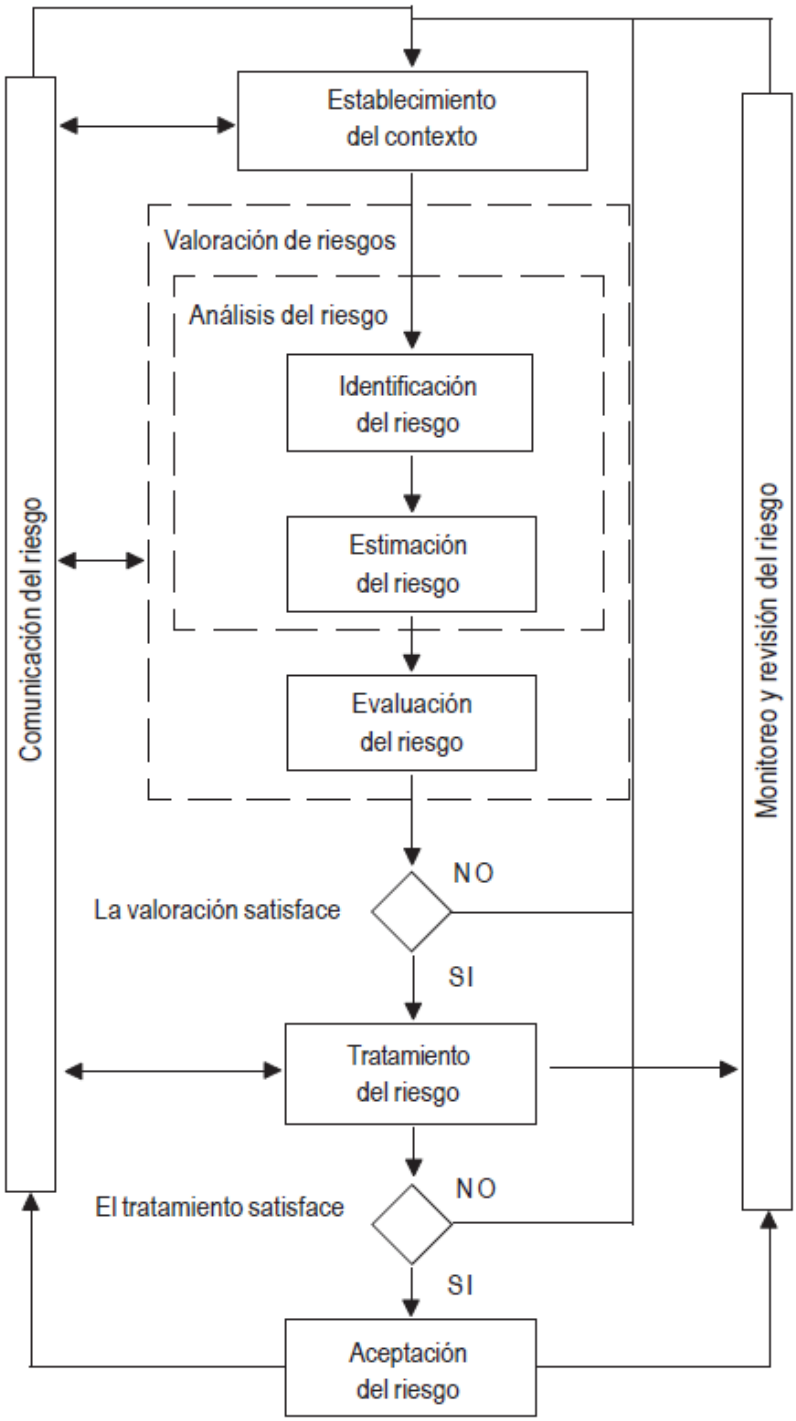


Ilustración 3. Proceso para gestión de riesgos basado en la ISO 27005

4.3. Normativas seleccionadas

En este punto realizaremos una breve comparativa entre las diferentes normativas revisadas para la implantación de un SGSI y las normativas revisadas para la implantación de la gestión de riesgos.

4.3.1. Selección de la norma de implementación del SGSI

Las dos principales opciones para la elección de la norma de implementación del SGSI son la norma ISO/IEC 27001:2013 y el Esquema Nacional de Seguridad (ENS) [9].

A continuación, se detallan las principales diferencias y características de ambas opciones:

METODOLOGIA	ISO/IEC 27001	ENS
Diferencias	• Normativa internacional de seguridad • Carácter voluntario • Aplica a toda la información que queremos proteger • Se aplica al nivel de seguridad que necesita la organización • 114 controles	• Regulación de carácter Nacional • Obligación legal derivada ley 40/2015 • Aplica a toda aquella información necesaria para prestar servicio • Se establecen unos mínimos de seguridad para el sistema: Básico, Medio o Alto • 75 medidas de seguridad
Objetivo	• Su objetivo es la gestión de la seguridad de la información • Deja libertad para elegir el alcance del SGSI • El análisis de riesgo siempre es obligatorio	• Regula los principios básicos y establece requisitos mínimos • Se refiere a los medios electrónicos en relación con la administración publica • El análisis de riesgo solo es real para sistemas de categoría media y alta

Tabla 4. Diferencias ISO/IEC 27001:2013 vs ENS. Referencia: CCN-STIC 825

Tanto la ENS como la ISO/IEC 27001:2013 son dos estándares muy validos que tienen como objetivo principal establecer unas políticas de seguridad en la utilización de los recursos, a través de principios básicos y requisitos mínimos, que permitan una protección adecuada de la información.

Analizando y comparando las normativas para la implantación de un SGSI, por su recorrido, por su internacionalización y por abarcar un ámbito más amplio durante su implantación la norma seleccionada para llevar a cabo el proceso de implantación es la **ISO/IEC 27001:2013**

4.3.2. Selección de la norma de gestión de riesgos

Las dos principales opciones para la elección de la norma o metodología de gestión de riesgos durante la implantación y certificación del SGSI son las normas ISO/IEC 27005 y Magerit v3 [10] [11].

A continuación, se detallan las principales características, ventajas y desventajas de ambas opciones:

METODOLOGIA	ISO/IEC 27005	MAGERIT
Características	• Conjunto de directrices para la correcta realización de un análisis de riesgos. • Ha nacido para apoyar las tareas de análisis y la gestión de riesgos en el marco de un SGSI • Apoya los conceptos generales especificados en la ISO/IEC 27001	• Ofrece un método sistemático para analizar los riesgos derivados del uso de las TIC • Ayuda a descubrir y planificar el tratamiento necesario para mantener los riesgos bajo control
Fases del Análisis de Riesgo	• Alcance • Normativas de referencia • Términos y referencias • Estructura • Antecedentes • Visión del progreso de la gestión de riesgos • Establecimiento del contexto • Evaluación del riesgo • Tratamiento del riesgo • Aceptación del riesgo • Comunicación del riesgo • Monitorización y revisión del riesgo	• Identificar activos relevantes • Identificar amenazas • Determinar los controles disponibles • Estimar impacto sobre los activos derivado de la materialización de la amenaza • Estimar el riesgo. Impacto ponderado con la tasa de ocurrencia de la amenaza.
Ámbito	• Aplicable en cualquier organización	• Aplicable en cualquier organización • Más orientada a organismos públicos, que disponen de una aplicación, PILAR, para el análisis y gestión de riesgos.
Ventajas	• Estándar internacional permitiendo una mayor aceptación • Clausula completa orientada a la	• Es metódica facilitando la comprensión • Es una metodología líder con

	monitorización y revisión del riesgo • Alcance enfocado en ser muy completo en el análisis y gestión del riesgo • Permite un análisis cuantitativo completo	buenos referentes en su aplicación • Dispone de un alcance completo en el análisis y gestión del riesgo
Desventajas	• No recomienda una metodología concreta • No detalla una forma de valorar las amenazas • No es certificable • No posee alguna herramienta técnica de ayuda a la implementación	• No involucra los procesos, recursos o vulnerabilidades en el método de gestión de riesgos • La necesidad de cambiar las valoraciones en valores económicos hace que la aplicación del método sea costos

Tabla 5. Diferencias ISO/IEC 27005 vs MAGERIT

En base a que la normativa de la ISO/IEC 27001:2013 no especifica una metodología de gestión de riesgos concreta y tanto Magerit v3 como la ISO/IEC 27005 son dos estándares muy válidos para la gestión de riesgos que garantizan a cualquier organización tener identificados los riesgos y controles que le permitirán actuar ante una amenaza o simplemente evitar que se materialice.

Como la **ISO/IEC 27005** ha surgido para apoyar las tareas de análisis y la gestión de riesgos en el marco de un SGSI, tal como su nombre indica "Information technology – Security techniques – Information security risk management", será la normativa seguida en lo concerniente a la Gestión de Riesgos.

4.3.3. Ciclo Deming.

Las normativas seleccionadas se fundamentan en el Ciclo de Deming, conocido como PHVA (PDCA). Planificar (Plan) – Hacer (Do) – Verificar (Check) – Actuar (Act), que es un proceso iterativo de calidad en cuatro fases:

- Planificar: Se establecen los objetivos, procesos y procedimientos para los procesos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance tanto del SGSI como de la gestión de riesgos tecnológicos.

- Hacer: Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la operación en un SGSI y la valoración y tratamiento de los riesgos.
- Verificar: Evaluar y medir el desempeño de los procesos contra las políticas y los objetivos de seguridad e informar sobre los resultados.
- Actuar: Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios necesarios en el SGSI para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye la monitorización y mejora continua, donde se verifican los cambios y el cumplimiento de los indicadores que fueron establecidos durante la planificación.

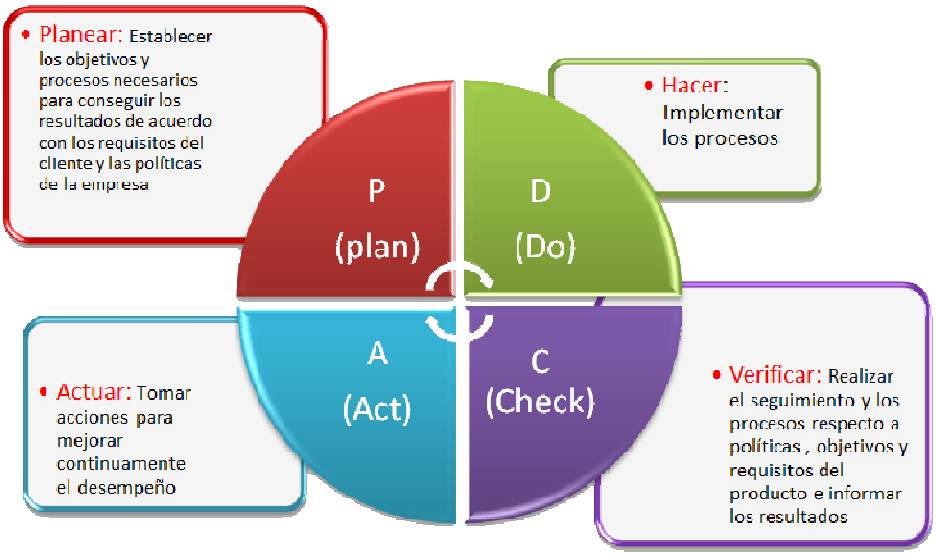


Ilustración 4. Ciclo Deming. Fuente: https://www.trevenque.es

5. Búsqueda, estudio y ejecución del proceso de formación

Uno de los puntos clave que resalta la normativa ISO/IEC 27001:2013 es la formación en el ámbito de la seguridad, tanto del personal implicado directamente en su implantación como el personal de la organización.

Teniendo en cuenta esto se procedió a realizar una búsqueda y revisión de algunas de las entidades que ofrecen formación en relación a la ISO/IEC 27001:2013.

5.1. AENOR

Siendo una de las organizaciones con una de las trayectorias más largas en el ámbito de las normativas y certificaciones, a nivel nacional, se ha tomado con referencia tanto a nivel de contenido como de precios y por su capacidad de formación online [12].

Cursos de formación	Horas - Precios
Auditor Líder ISO 27001 (S-0A)	40 horas – 440€ + IVA
Especialista Implantador ISO 27001 (S-0B)	40 horas – 1.050€ + IVA
Implantación de un SGSI según ISO 27001 (S-02)	10 horas – 410€ + IVA
Auditor Interno ISO 27001 (S-5)	40 horas – 1.050€ + IVA

Tabla 6. Formaciones AENOR.

5.2. Bureau Veritas Formación

Es una división de la compañía internacional Bureau Veritas. Esta división está especializada en formaciones centradas en aspectos relacionados con calidad, seguridad, salud, medio ambiente y Responsabilidad Social [13].

Cursos de formación	Horas - Precios
Auditor interno de Sistemas de Gestión de Seguridad de la información ISO 27001	45 horas – 380€
Auditor Jefe Certificación de SGSI ISO 27001	45 horas – 975€

Tabla 7. Formaciones Bureau Veritas.

5.3. 27001 Academy

Es la división de formación de la empresa Advisera Expert Solutions Ltd, que ofrece soporte en línea para la implementación de múltiples normativas tales como RGDP, ISO 27001, ISO 9001, etc [14], [15].

Cursos de formación	Horas - Precios	Certificación
ISO 27001 Foundation Course	8 horas – 0€	205€
ISO 27001 Internal Auditor Course	15 horas – 0€	370€
ISO 27001 Lead Implementer Course	15 horas – 0€	1400€

ISO 27001 Lead Auditor Course	15 horas – 0€	1400€

Tabla 8. Formaciones 27001 Academy.

La característica que destaca de esta formación es que los cursos son todos online y de coste 0€.

Lo que tienen un coste asociado es la realización del examen de certificación y la documentación adicional incluida.

5.4. CertiProf

Es una entidad certificadora fundada en Estados Unidos en el año 2015, que actualmente está en auge en los procesos de certificación de conocimientos tanto a nivel nacional como internacional [16].

Cursos de formación	Horas	Certificación
ISO/IEC 27001 Foundation	--	125€
ISO/IEC 27001 Internal auditor	--	125€
ISO/IEC Certified Lead Implementer	--	125€

Tabla 9. Formaciones CertiProf.

Al contratar los exámenes de certificación, desde la entidad certificadora proporcionan la documentación necesaria para preparar las pruebas y se dispone de 6 meses para presentarse al examen.

Periódicamente este centro de formación ofrece descuentos del 30% sobre el precio estándar.

5.5. Formación seleccionada

Después de estudiar todas las opciones y para tener una perspectiva real de la formación en el ámbito de la norma 27001 optó por realizar una mezcla de opciones:

Primeramente se realizaron los cursos de formación gratuitos de Academy 27001, para tener un buen conocimiento de la normativa ISO/IEC 27001:2013 y el proceso de auditoría.

Y finalmente se contrataron y prepararon los dos primeros cursos de certificación de CertiProf, para poder validar los conocimientos adquiridos de forma autodidactica.

6. Proceso implantación ISO/IEC 27001:2013

La ISO/IEC 27001:2013 no describe en detalle todo lo que se debe hacer ni el tipo de tecnología que se debe utilizar para proteger la información. La ISO/IEC 27001:2013 proporciona un marco para tomar decisiones en relación a la protección más adecuada para la organización.

Indica que se deben implementar los controles que son necesarios en base a los riesgos y requisitos, y no los que le parezca al personal técnico o responsable del SGSI. No puede excluir un control, simplemente porque no encaje en el proyecto o implementación tecnologías.

Hay que tener en consideración que no toda la información crítica está en formato digital, por lo que será necesario aplicar controles adicionales que no son únicamente controles técnicos. Por lo tanto, la norma explica como implantar la seguridad de la información como un proyecto empresarial implicando diferentes áreas de negocio y no solo al departamento de TI.

A continuación se procede a detallar la norma ISO/IEC 27001:2013 y a desglosar lo más detalladamente posible la secuencia de pasos necesarios para crear los procedimientos, documentos y requerimientos necesarios para implantar un SGSI en base a dicha norma.

6.1. Estructura y cláusulas de la ISO/IEC 27001:2013

La estructura de la norma ISO/IEC 27001:2013 está basada en diferentes puntos y sobre esta norma se aplica el círculo PDCA basado en la mejora continua de la calidad.

6.1.1. Descripción de las secciones:

Se divide en 11 secciones. Las secciones de la 0 a la 3 son una introducción y no es obligatorio su implementación. Las secciones de la 4 a la 10 son obligatorias, por lo que para cumplir el estándar es necesaria su implementación [17].

En la siguiente imagen se puede observar la estructura de la norma a implementar:

Ilustración 5 Estructura ISO/IEC 27001:2013. Fuente: Internet.

0. Introducción. Explica el propósito de la ISO/IEC 27001:2013 y compatibilidad con otros estándares.
1. Alcance. Explica que la ISO/IEC 27001:2013 se puede aplicar en cualquier organización.
2. Normativas de referencia. Señala al estándar ISO/IEC 27000, como el estándar de términos y referencias.
3. Términos y definiciones. Vuelve a referenciar al estándar ISO/IEC 27000.
4. **Contexto de la organización**. Define las necesidades y expectativas de las partes interesadas. Entender las cuestiones internas y externas de la organización. Determina el alcance del SGSI.
5. **Liderazgo**. Define el compromiso de la alta dirección, políticas de seguridad y roles de la organización y sus responsabilidades.
6. **Planificación**. Define las acciones para abordar la evaluación y tratamiento de los riesgos, la declaración de aplicabilidad y los objetivos y planes para lograrlo.
7. **Soporte**. Define los recursos, competencias, sensibilización, comunicación y control de la documentación y registros.
8. **Operación**. Define la implementación de la evaluación y tratamiento de los riesgos junto con los controles y procesos necesarios para lograr la seguridad de la información.
9. **Evaluación de Desempeño**. Define el proceso de auditoría interna, monitoreo, medición y revisión por la alta dirección.

10. **Mejora**. Define las acciones correctivas y no conformidades junto con la mejora continua.

Además, la ISO/IEC 27001:2013 incorpora un anexo A de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Los controles del Anexo A deben implementarse en el caso de que se declaren aplicables en el documento de Declaración de Aplicabilidad. Este anexo está compuesto por 114 controles distribuidos en 14 dominios de seguridad siendo los siguientes:

Ilustración 6. Dominios ISO/IEC 27001:2013. Fuente: isaca.org

6.2. Planteamiento auditoría: Interna vs Externa vs Mixta.

Para comenzar la implementación de un estándar, como la ISO/IEC 27001:2013, es aconsejable disponer de una visión global de los conocimientos y capacidades de la organización para afrontar el proyecto y en base a esto seleccionar uno de los tres planteamientos siguientes [18].

6.2.1. Interna.

Implementar la ISO/IEC 27001:2013 apoyándose únicamente en el personal propio de la empresa. Tomando la decisión de confiar en la formación y conocimientos internos y no utilizar ayuda externa de un tercero. Con lo que el personal de la empresa realiza todas las tareas de auditoría, análisis y documentación necesaria.

Esta opción tiene sus pros y sus contras:

- PROS: A primera vista es la opción más barata, pues se eliminan los costos de un proveedor. No se externaliza ninguna documentación, procesos o información significativa a un tercero. Y uno de los puntos más fuertes es la implicación del personal interno en la implantación.
- CONTRAS: Es la opción más lenta debido a que todo el proceso se realiza con recursos internos y si los recursos asignados no disponen de la capacitación adecuada, al final puede ser una de las opciones con mayor inversión en tiempo y dinero.

6.2.2. Externa.

Implementar la ISO/IEC 27001:2013 apoyándose totalmente en un consultor externo experto en la implantación de dicho estándar. Este consultor realizará todas las tareas de auditoría, análisis y documentación necesaria para implantar la norma.

Esta opción tiene sus Pros y Contras:

- PROS: Todas las tereas de implantación recaen un consultor externo.
- CONTRAS: Es una de las opciones más costosas en base del proveedor que se contrate. Es necesario trasmitir toda la información interna de procedimientos e infraestructura empresarial al proveedor. Dos de los puntos más débiles son a) que el personal interno no se ve integrado en la implantación y puede ver la implantación del estándar como una imposición de nuevas políticas y procedimientos, y b) que tras la finalización del proveedor, la falta de conocimientos interna no permita mantener la documentación y procesos de evolución necesarios.

6.2.3. Mixta.

Implementar la ISO/IEC 27001:2013 con implicación del personal propio de la empresa y recibiendo soporte y herramientas de un consultor externo. En este caso el personal interno realiza la implantación, pero recibe formación, plantillas y apoyo para solventar dudas de un consultor externo.

Esta opción tiene sus Pros y Contras:

- PROS: No se disparan los precios al no realizar todo el trabajo el consultor externo y al mismo tiempo tampoco se externaliza la información crítica de la organización. Fomenta la implicación de los empleados al crear parte de la documentación.
- CONTRAS: Será necesario que personal de la organización se forme en la norma para poder llevar a cabo esta nueva tarea.

6.2.4. Conclusión y planteamiento recomendado

La recomendación sería optar por un planteamiento mixto, que nos provee de un soporte cuando surjan dudas, lo que ayuda reducir los tiempos de implementación, la información confidencial y critica de la organización no se externaliza y no se disparan los costes de la implantación.

6.3. Estimación de tiempos

La duración de implementación de la ISO/IEC 27001:2013 dependerá del tamaño de la organización, del alcance definido, de la situación inicial de la que parte en el cumplimiento de los requisitos, de los conocimientos de auditoria e implantación disponibles, la finalidad de obtención de la normativa, etc.

Para realizar una implantación que produzca resultados (menos incidencias, ahorro de costos, control de riesgos de la información, etc.), la mayor dedicación se centrará en las fases de Plan y Do, es decir, en la evaluación de riesgos y la implementación de los controles.

Una buena estimación temporal si las asignaciones en el proyecto están correctamente ponderadas es:

Dimensiones estimadas de la organización	Tiempo estimado de implantación
Organizaciones con 50 empleados	8 meses
Organizaciones con 300 empleados	De 8 a 12 meses
Organizaciones con 500 empleados o más	De 12 a 15 meses

Tabla 10. Estimación temporal implantación

6.4. Obtener apoyo de la dirección.

Uno de los pasos más importante es obtener el apoyo de la alta dirección para poder llevar a buen fin la implantación correcta de un SGSI basado en la ISO/IEC 27001:2013, pues necesitará una fuerte inversión.

Para esto tendrá que indicar los beneficios, satisfacción de los clientes, ampliación de cuotas del mercado, nuevas estrategias de negocio y disminución de los riesgos empresariales gracias a la implementación del SGSI basado en la ISO/IEC 27001:2013.

6.5. Fases de la Implantación de la ISO/IEC 27001:2013 basándose en las clausulas.

La norma ISO/IEC 27001:2013 está escrita de una forma secuencial, que permite utilizarse como referencia para la implementación y poder seguir el orden en el que está escrita la norma.

En este apartado se describen las fases de la implantación que se consideran necesarias tras interpretar las cláusulas que definen la norma. Para cada fase se listan los documentos que es necesario generar, indicando la obligatoriedad (o no) de los mismos [19] [20] [21].

6.5.1. Entender el contexto de la organización.

A continuación se detallan las algunas de las cuestiones a tener en cuenta para construir un SGSI que atienda las necesidades de la organización:

- El contexto interno. Es la estructura organizacional, funciones y responsabilidades. La estrategia y objetivos de negocio, recursos, procesos y sistemas de información.
- Asegurar que los objetivos de SI están alineados con la estrategia de negocio.
- Realizar la evaluación de riesgos identificando sistemas y relaciones contractuales.
- Determinar los recursos.
- Definir roles de seguridad de la información y sus responsabilidades.
- Definir las capacidades.
- Documentar los objetivos de SI, los resultados de evaluación de riesgos y mantener un registro de competencias de los empleados.
- Debido al control A 18.1.1 es obligatorio tener una lista de requisitos legales, reglamentarios y contractuales

Documentación	Obligatorio
Objetivos del Sistema de Información	SI
Resultado de la evaluación de riesgos	SI
Registro de competencia de empleados	SI
Lista de disposiciones legales	SI

Tabla 11. Doc. Contexto Organización.

6.5.2. Listar las partes interesadas y sus requerimientos.

El contexto externo es el procedimiento encargado de identificar todas las partes interesadas, requisitos legales, reglamentos e intereses. Donde las partes interesadas son: trabajadores, accionistas, clientes, socios, proveedores... Es necesario identificar lo que quieren de la organización las partes interesadas antes indicadas, especificando leyes, reglamentos y cláusulas de contratos

Documentación	Obligatorio
Objetivos y parte interesadas (Contexto)	SI

Tabla 12. Doc. Partes Interesadas

6.5.3. Definición del alcance del SGSI.

Es necesario definir claramente qué información se desea proteger, sin importar el medio o el lugar donde esté almacenada.

Cuando la organización tiene una sola oficina, entonces el alcance debería ser toda la organización. Si tiene varias o en distintas ubicaciones, lo mejor es comenzar una a una.

Se puede utilizar un gráfico de procesos. En el caso de disponer ya de la ISO 9001 puede utilizar este gráfico como base. Es muy importante definir los límites del alcance del SGSI.

El documento incluye la ubicación física (planos), organigrama funcional, productos y servicios.

Documentación	Obligatorio
Alcance del SGSI	SI

Tabla 13. Doc. Alcance

6.5.4. Requerimientos de la alta dirección.

De la alta dirección se requiere que lleve a cabo las siguientes acciones:

- Publicar las políticas de seguridad de la información en las que se define la principal intención.
- Determinar los objetivos, para saber la orientación del SGSI.
- Determinar los responsables del SGSI y asegurarse de que han realizado el trabajo.
- Explicar la importancia de la implantación del SGSI a toda la organización.
- Revisar la evolución y cumplimiento de los objetivos.

Documentación	Obligatorio
Políticas y Objetivos de seguridad de la información	SI
Resultado de la revisión por parte de la dirección	SI

Tabla 14. Doc Alta Dirección

6.5.5. Escribir la política de seguridad de la información.

La política de seguridad de la información debe:

- Definir cómo se proponen los objetivos, como se aprueban y como se revisan.
- Demostrar el compromiso de la alta dirección para la mejora del SGSI.
- Indicar quien es el encargado de comunicar las políticas.

Se puede incluir en el alcance del SGSI, los responsables de los diferentes niveles (operaciones, evaluación de riesgos, ejecutivo, incidencias, etc.).

Documentación	Obligatorio
Políticas y Objetivos de seguridad de la información	SI

Tabla 15. Doc Políticas

6.5.6. Definir los objetivos del SGSI de alto nivel.

Se tienen que fijar objetivos fáciles de medir: específicos, medibles, alcanzables, relevantes y basados en tiempo.

Documentación	Obligatorio
Políticas y Objetivos de seguridad de la información	SI

Tabla 16. Doc Políticas y Objetivos

6.5.7. Definir roles y responsabilidades, así como documentarlas.

Es necesario un documento que defina detalladamente todos los roles y responsabilidades relacionados con la seguridad.

También se pueden documentar los roles y responsabilidades de seguridad en el documento de los diferentes puestos de la organización.

Documentación	Obligatorio
Definición de Roles y responsabilidades	SI

Tabla 17. Doc Roles

6.5.8. La gestión de los documentos y los registros.

Se trata de establecer reglas para el formato de los documentos, quien los aprueba, donde se publican, sistemas de control de versionado, seguimiento de los cambios, etc.

Si se ha implantado la ISO 9001, se puede utilizar dicha referencia.

Hay que tener en cuenta si se trabaja con un software documental, software de gestión de proyectos o si existen plantillas.

Es recomendable definir el formato de la documentación e identificar el propietario del cada documento, que será el responsable de actualizarlo y revisarlo.

Documentación	Obligatorio
Procedimiento para control de documentos y registros	NO

Tabla 18. Doc Control documentación

6.5.9. Proporcionar recursos para el SGSI.

Se trata de identificar los recursos necesarios, tanto personal como financieros.

Puede documentarse a través del presupuesto, plan de recursos humanos, plan de gestión de riesgos o el de capacitación.

Documentación	Obligatorio
Plan de recursos y presupuestos	NO

Tabla 19. Doc Recursos

6.5.10. Proporcionar formación en seguridad.

Documento que define los conocimientos necesarios para el personal que tenga algún rol en el SGSI.

Si no se dispone de dichos conocimientos, se debe de realizar dicha capacitación para lograr los niveles de conocimientos imprescindibles a demás es deseable disponer de una evaluación final de los conocimientos adquiridos.

Documentación	Obligatorio
Registro de formación, experiencia y habilidades	SI

Tabla 20. Doc Formación

6.5.11. Concienciar al personal de la organización por qué es importante la seguridad de la información.

Todo el personal de la organización debe ser consciente de las políticas de seguridad, de su rol y el impacto que tiene en el SGSI, así como el impacto que puede tener no cumplir las reglas del SGSI.

Medios para comunicar:

- Foros internos.
- Contratar o crear cursos online.
- Videos distribuidos a través de email.
- Reuniones y charlas personales.

En el documento se puede incluir cuales de los métodos anteriores se utilizan y su periodicidad.

Documentación	Obligatorio
Plan de concienciación de la seguridad	NO

Tabla 21. Doc Concienciación

6.5.12. Cómo comunicar y a quien es necesario comunicar.

Se puede crear un documento que defina:

- Que debería de comunicar como vulnerabilidades, amenazas, eventos, etc.
- Quien debería de realizar esta comunicación
- A quien se debe de comunicar: interna o externa.
- Medio de comunicación

Documentación	Obligatorio
Política de comunicación	NO

Tabla 22. Doc Comunicación

6.5.13. Acometer los riesgos y oportunidades.

Los riesgos se refieren a eventos no deseados que pueden tener impacto negativo en la SI, y por lo tanto en la organización [22].

Las oportunidades se refieren a las acciones que podría emprender la organización para mejorar el estado de la SI

Los cinco pasos básicos para la gestión de riesgos serían:

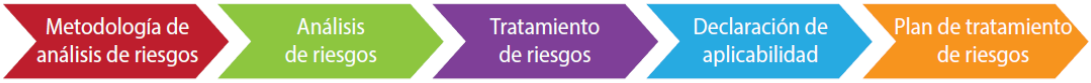


Ilustración 7. Secuencia Gestión riesgos. Fuente: internet

1. Seleccionar la metodología o adaptar una existente a las necesidades de la organización.
2. Implementar el análisis, mostrando los activos, las amenazas y las vulnerabilidades asociadas a los activos. La evaluación del impacto y la probabilidad para cada combinación de activos/amenazas/vulnerabilidades y finalmente calcular el riesgo.
3. Implementar el tratamiento de los riesgos inaceptables mediante la: aplicación de controles, transferencia del riesgo, evitar el riesgo o aceptación del riesgo
4. El documento de Declaración de aplicabilidad, muestra el estado de seguridad de la organización, basándose en los resultados del tratamiento. Es necesario disponer de una lista de controles que han implementado, como y porque se han aplicado.
5. El Plan de tratamiento, define quien implementará cada control, en que tiempo, prepuestos, etc. Se conoce como Plan de implementación o de acción.

6.5.14. Documentar la metodología de análisis de riesgos.

Se debe desarrollar o adaptar una metodología a las circunstancias y necesidades de la organización.

La ISO requiere en su punto 6.1.2:

- Definir cómo identificar los riesgos que podrían casar perdida de confidencialidad, integridad, disponibilidad en la información de la organización
    - Identificar activos-amenazas-vulnerabilidades, aunque la actual versión no lo requiera. Puede basarse en los procesos y departamentos, utilizando solo amenazas y vulnerabilidades.
- Definir cómo identificar a los propietarios de los riesgos
    - Persona responsable de la resolución de un riesgo que este capacitada para poder afrontar la tarea.
- Definir los criterios para evaluar las consecuencias y las probabilidades del riesgo.
    - Evaluar por separado las consecuencias y probabilidades para cada riesgo. Se puede utilizar cualquier escala como Bajo-Medio-Alto.
- Definir como se calcula el riesgo

  - Se realiza mediante la suma o multiplicación de las consecuencias y la probabilidad.

- Definir los criterios para la aceptación del riesgo.
  - Si su sistema de cálculo produce un valor, debe definir un nivel aceptable de riesgo (6 o 7).
  - El nivel de riesgo aceptable debe estar en concordancia con la estrategia de negocio de la organización.

El documento de Metodología de gestión de riesgos el cual debe de incluir, todo lo anteriormente detallado. El tratamiento de los riesgos, incluyendo responsabilidades y documentación. La periodicidad de las revisiones, que es como mínimo una vez al año. Roles en el proceso completo (realización del análisis y tratamiento de riesgos). La documentación que deber generarse (realización del análisis y tratamiento de riesgos). Quien debe comunicar, que debe de comunicar y a quien. Como proteger la confidencialidad de la información generada durante el análisis.

Documentación	Obligatorio
Metodología de análisis y tratamiento de riesgos	SI

Tabla 23. Doc Metodología I

6.5.15. Análisis de riesgos I: Identificar los riesgos.

Es necesario realizar un proceso minucioso para identificar todo lo que puede poner en peligro los tres pilares de la seguridad: Confidencialidad, Integridad y Disponibilidad, comúnmente referenciados como CIA por su nombre en inglés.

- **Confidencialidad**, la información es accesible únicamente al personal autorizado para tratar dicha información.
- **Integridad**, la información debe mantenerse inalterable, salvo por el personal autorizado a realizar dichas modificaciones.
- **Disponibilidad**, la información debe de estar disponible a los usuarios autorizados cuando estos necesiten acceder.

Identificar el nivel de riesgo, responsable, consecuencias y asignar una probabilidad que tengan sentido dentro de la organización.

Identificar activos por Departamento: HW, SW, servicios, información digital, información papel, infraestructura, personas, etc. Los activos similares a nivel de SI pueden agruparse.

Para las amenazas y vulnerabilidades es una buena recomendación utilizar catálogos. Las amenazas pueden agruparse según el tipo: Software malicioso, naturales, mal funcionamiento y errores humanos.

Las vulnerabilidades pueden organizarse según el tipo de activo con el que se relacionan: HW, SW, servicios, información digital, información en papel, infraestructura y recursos humanos.

Es muy importante la vinculación de activos-amenazas-vulnerabilidades. Se puede recopilar en una hoja de Excel si no se dispone de una aplicación adecuada a dicho cometido.

Activo	Amenaza	Vulnerabilidad	Propietario del riesgo
Servidor	Corte de electricidad	No existe UPS	Jefe de TI
	Fuego	No existe extintor de incendios	Coordinador de seguridad & salud
Portátil (laptop)	Acceso de personas no autorizadas	Contraseña inadecuada	Usuario del portátil
	Pérdida de datos	No se realizan copias de seguridad regularmente	Usuario del portátil
Administrador de sistemas	Deja la compañía	No existe reemplazo	Jefe de Recursos humanos

Ilustración 8. Vinculación Activos, amenazas. Fuente: Secure & Simple.

Documentación	Obligatorio
Evaluación de riesgos	SI
Inventario de activos	SI

Tabla 24. Doc Riesgos I

6.5.16. Análisis de riesgos II: Analizar y evaluar los riesgos.

El análisis de riesgo consiste en identificar cual es la importancia de los riesgos descubiertos. Y la evaluación de riesgos es la conclusión de si son aceptables o no.

Se deben utilizar las escalas de evaluación de las consecuencias y la probabilidad definida en la metodología.

- En la evaluación de las consecuencias se debe de pensar en la afectación sobre la CIA de la información.
- La evaluación de la probabilidad debe de basarse en ocurrencias anteriores y teniendo en cuenta los controles de seguridad actuales.

Por ejemplo, en esta tabla donde la escala es 1=Muy baja, 2=Bajo, 3=Medio, 4=Alto y 5=Muy alto y el riesgo se calcula a través de la suma siendo el umbral 7.

Activo	Amenaza	Vulnera-bilidad	Propie-tario del riesgo	Conse-cuencia	Proba-bilidad	Ries-go
Servidor	Corte de electricidad	No existe UPS	Jefe de TI	4	2	6
	Fuego	No existe extintor de incendios	Coordi-nador de seguridad & salud	5	3	8
Portátil (laptop)	Acceso de personas no autorizadas	Contrase-ña inade-cuada	Usuario del por-tátil	4	4	8
	Pérdida de datos	No se realizan copias de seguridad regular-mente	Usuario del por-tátil	4	3	7
Adminis-trador de sistemas	Deja la compañía	No existe reemplazo	Jefe de Recursos humanos	5	3	8

Ilustración 9. Escala Riesgo. Fuente: Secure & Simple

Documentación	Obligatorio
Análisis y tratamiento de riesgos	SI
Informe del análisis y tratamiento de riesgos	SI

Tabla 25. Doc Riesgos II

6.5.17. Realizar el tratamiento o mitigación de los riesgos.

Se trata de controlar los riesgos detectados durante el análisis de riesgos. Disminuir el riesgo reduciendo la probabilidad de un incidente y reducir el impacto sobre los activos.

Es aconsejable centrarse en los riesgos que no son aceptables, para poder priorizar.

- Reducir el riesgo, implementando controles del Anexo A o cualquiera que decida la organización.
- Evitar el riesgo, paralizando ciertas tareas como el uso de portátiles.
- Transferir el riesgo, lo normal es utilizar la contratación de una póliza junto con una de las dos anteriores.
- Asumir el riesgo, es lo menos deseable y solo si el coste de la mitigación es muy superior al daño producido.

Activo	Amenaza	Vulnera-bilidad	Opción de trata-miento	Justificación de implementa-ción
Servidor	Fuego	No existe extintor de incendios	1) Reducir riesgo + 2) Compartir riesgo	Comprar extintor de incendios + contratar póliza de seguro contra incendios
Portátil (laptop)	Acceso de personas no autorizadas	Contraseña inadecuada	1) Reducir riesgo	Escribir política de contraseñas
Administra-dor de sistemas	Deja la compañía	No existe reemplazo	1) Reducir riesgo	Contratar un segundo administrador de sistemas que lo aprenda todo del primero

Ilustración 10. Tratamiento Riesgo. Fuente: Secure & Simple

Se puede calcular el Riesgo Residual que queda después de implantar el control.

Documentación	Obligatorio
Metodología de análisis y tratamiento de riesgos	SI
Resultados del tratamiento de riesgos	NO

Tabla 26. Doc Riesgos III

6.5.18. Desarrollar la Declaración de aplicabilidad (SoA):

En ocasiones se conoce como SoA (Statement of Applicability) y es el documento donde se define como implementar los principales elementos de seguridad, siendo el documento central de la implantación del SGSI.

El propósito es definir cuáles de los controles del Anexo A serán aplicados y como se aplicarán, estado, etc.

En este documento se pueden incluir los objetivos de seguridad por cada control y también se pueden incluir la forma en la que se implementarán los controles.

ID	Nombre del control	Aplicabilidad	Justificación	Objetivos de control	Método de implementación	Estado
A.6.2.1	Política de dispositivos móviles	Sí	Riesgos #34, 45 y 66	Reducir el número de incidentes de seguridad relacionados con los dispositivos móviles en un 25% durante el siguiente año	Política Traer Su Propio Dispositivo (BYOD del inglés Bring Your Own Device)	Completamente implementado
A.6.2.2	Teletrabajo	No	Los empleados sólo trabajan desde las oficinas	-	-	-

Ilustración 11. SOA. Fuente: Secure & Simple

Para cada control hay que detallar:

- ID del Control.
- Nombre del control.
- Indicar si aplico a no.
- Si aplica, justificar la inclusión.
- Si no aplicar, justificar la exclusión.
- Objetivo del control, que es opcional.
- Método de implementación, que es opcional, referenciando el procedimiento, política o describiendo el proceso que se utiliza.
- Estado: Planificado, No implementado, Parcialmente Implementado, Implementado.

Documentación	Obligatorio
Declaración de aplicabilidad (SoA)	SI

Tabla 27. Doc SoA I

6.5.19. Desarrollar el Plan de tratamiento de riesgos.

Es el plan en el que se especifican los controles de seguridad a implementar, responsables, plazos y recursos si se considera necesario.

Es el documento de transición de la fase de Planificar a Hacer. Necesita de la escritura de políticas y procedimientos e implementar soluciones técnicas, etc.

El plan debe de listar todos los controles que no están aplicados en base al documento anterior y el detalle de cómo se implementarán.

Controles que serán implemen-tados	Referencia a riesgos	Persona responsa-ble	Plazo	Recursos	Resul-tados
Documen-tar una política de copias de seguridad	Riesgo 16 – Indispo-nibilidad de información electrónica debido a la pérdida ac-cidental de información	Respon-sable de Seguridad (CISO)	Mar-zo 2016	1 hombre/día	Imple-menta-do
Implemen-tar la políti-ca de copias de seguri-dad	Riesgo 16 – Indispo-nibilidad de información electrónica debido a la pérdida ac-cidental de información	Adminis-trador de sistemas	Junio 2016	3 hombres/ días; presu-puesto para los controles técnicos	En pro-ceso de imple-menta-ción

Ilustración 12. Plan Tratamiento. Fuente: Secure & Simple

Debe detallar:

- Controles que implementar.
- Referenciar el riesgo que generó la implementación de este control.
- Responsable de la implementación.
- Plazo de implementación.
- Recursos necesarios para la implementación.
- Resultado de la implementación: No implementado, Parcialmente Implementado, Implementado.

Documentación	Obligatorio
Plan de tratamiento de riesgos	SI

Tabla 28. Doc Plan Tratamiento

6.5.20. Establecer los objetivos para controles de seguridad y procesos.

El propósito de estos objetivos es medir si los controles y procesos implantados están justificados. Se deberían de aplicar antes de comenzar a utilizar los controles y procesos. Para establecerlos se tiene en cuenta:

- Objetivos de seguridad por grupos de controles.
- Objetivos de seguridad por procesos.

- Objetivos de seguridad por departamentos, los más habituales en pymes. Objetos del firewall u objetivos de la pérdida de datos.

Documentación	Obligatorio
Declaración de Aplicabilidad (SoA)	SI

Tabla 29. Doc SoA II

6.5.21. Comenzar con la documentación. Políticas y procedimientos

Para comenzar con las diferentes políticas, procedimientos, guías se pueden utilizar los siguientes criterios:

- Áreas donde se terminará rápidamente con la documentación.
- Áreas con mayor riesgo, para comenzar por lo más crítico, en casos de fallos graves.
- Áreas que ya tienen otros proyectos en activo y que se pueden integrar. Procedimientos de incidencias.

La ISO/IEC 27001:2013 no especifica que documentación es necesaria, a parte de la estrictamente obligatoria, indicada más adelante. Por lo que queda a cargo de la organización decidir que registros o documentos se crean para el SGSI.

A continuación se muestras varios criterios a utilizar:

- Si existe un riesgo, no implica que tenga que escribir un documento, pero será necesario tenerlo en cuenta.
- Requerimientos con clientes, como acuerdos de confidencialidad.
- Cuanto más importante es el proceso, más probable es que se tenga que documentar.
- Cuantas más personas involucradas en el proceso, más probable es que se tenga que documentar.
- Cuanto más complejo el proceso, más probable es que se tenga que documentar.
- Procesos que se ejecutan a intervalos no especificados y que puede olvidarse la operativa.

Documentación	Obligatorio
Procedimientos de operaciones para la gestión de TI	SI

Tabla 30. Doc Operaciones para la gestión

6.5.22. Gestionar los cambios en el SGSI.

La gestión de los cambios es un punto importante en la seguridad de la información. Es bueno tener un procedimiento de gestión de cambios, pero no es obligatorio.

Puede controlar quién y cómo puede iniciar el cambio, análisis que debe realizarse de afectación del cambio, quién implementa los cambios, quién los aprueba, proceso de rollback, etc.

Documentación	Obligatorio
Control de cambios	NO

Tabla 31. Doc Control de cambios

6.5.23. Mantener la documentación.

Se debe supervisar que los documentos no se han quedado obsoletos, por lo que se aconseja definir un periodo de revisión. En caso de cambio, confirmar que se actualiza la documentación asociada.

Se puede asignar un propietario de documento, en cada una de las políticas, procedimientos o planes creados, para que sea el responsable de mantenerlo actualizado.

Documentación	Obligatorio
Procedimiento para control de documentos y registros	NO

Tabla 32. Doc Control de documentos

6.5.24. Gestionar los servicios externalizados.

La ISO/IEC 27001:2013 requiere que todas las operaciones externalizadas sean identificadas y controladas adecuadamente en materia de seguridad de la información.

Se puede mantener una lista de acuerdos firmados con proveedores o socios y como se controlan los servicios externalizados a dichos proveedores.

Documentación	Obligatorio
Política de seguridad de proveedores	SI

Tabla 33. Doc Proveedores

6.5.25. Revisión periódica del análisis y tratamiento de riesgos.

La ISO/IEC 27001:2013 especifica claramente que el análisis de riesgos debe realizarse periódicamente y los resultados deben ser analizados por la alta dirección en cada revisión.

Se deben de utilizar los mismos registros de análisis de riesgos para documentar las actualizaciones, indicando de forma muy clara las actualizaciones y los cambios.

El calendario para la revisión regular debe de estar registrado en la Metodología de análisis de riesgos.

Documentación	Obligatorio
Metodología de análisis y tratamiento de riesgos	SI

Tabla 34. Doc Metodología II

6.5.26. Monitorizar, medir, analizar y evaluar el SGSI.

La monitorización se refiere a observar y examinar, la medición se refiere a determinar la cantidad mediante la utilización de valores concretos.

Se puede tener un sistema de medición para los objetivos estratégicos (generales del SGSI) y otro diferente para los objetivos tácticos (controles, proceso).

En la documentación se indican los resultados de las mediciones y el proceso de monitorización.

El método de medición está asociado el objetivo a valorar. Quien comunicar los resultados, que lo tendrá que valorar y a quien se enviarán.

Documentación	Obligatorio
Resultados de monitoreo y medición	SI

Tabla 35. Doc Monitoreo

6.5.27. Auditoría interna acción I: Preparación.

Lo más habitual es que la auditoría la realice personal interno una vez al año en el caso de pymes [23].

Se debe de disponer de los siguientes documentos en relación a la auditoria interna:

- Procedimiento de auditoría interna: reglas básicas para realizar la auditoría, como se planifican las auditorías, actividades para realizar la auditoría y seguimiento y el método de información.
- Indicar la periodicidad y el alcance de la auditoría interna.
- Disponer de una lista de verificación para no olvidar nada durante el proceso
- Informe en el que se reportarán las no conformidades y otros hallazgos

Documentación	Obligatorio
Programa de auditoría interna	SI
Resultados de la auditoría interna	SI

Tabla 36. Doc Auditoría

6.5.28. Auditoría interna acción II: Pasos en la auditoría y preparación de la lista de verificación

Los pasos para realizar la auditoría interna serían:

- Revisión de los documentos y buscar si existen no conformidades en relación a lo exigido en la ISO/IEC 27001:2013.
- Crear la lista de verificación de auditoria.
- Planificar la auditoría principal.
- Realizar la auditoría principal, desplazándose y revisando la infraestructura.
- Crear el informe con las no conformidades y el documento de auditoría interna.

- Seguimiento de las acciones correctivas indicadas por la auditoría interna.

Documentación	Obligatorio
Lista de verificación	NO

Tabla 37. Doc Lista verificación

6.5.29. Revisión por parte de la alta dirección.

La revisión por parte de la alta dirección, debe de ser como mínimo una vez al año. No es aconsejable que se mezcle con la revisión de otras normas.

La ISO/IEC 27001:2013 requiere que la alta dirección revise los siguientes puntos:

- Estado de las acciones desde las anteriores revisiones realizadas por la dirección.
- Información sobre el análisis de las acciones correctivas, monitorización, mediciones y los resultados de la auditoría interna.
- Revisar comentarios, relacionados con la seguridad de la información, provenientes de terceros
- Resultado del análisis de riesgos y el estado de plan de tratamiento
- Oportunidades para la mejora continua del SGSI.

Documentación	Obligatorio
Resultados de la revisión por parte de la alta dirección	SI

Tabla 38. Revisión dirección

6.5.30. Uso práctico de las no conformidades y acciones correctivas.

Las no conformidades no solo provienen de la gestión de activos, igual que las acciones correctivas, que puede ser creada por cualquiera que intervenga en el SGSI.

Se debe de disponer de la siguiente documentación:

- Procedimientos de acciones correctivas, que definan las reglas básicas para la resolución de no conformidades. Donde se documenta, quien toma las decisiones, control de la ejecución, etc. Se puede incluir en una herramienta de HelpDesk que registra incidencias de seguridad, gestión de tareas y solo será necesario añadir una categoría adicional.
- Acciones correctivas, son las no conformidades y actividades que hay que resolver. Siendo obligatorio por parte de la ISO/IEC 27001:2013 tenerlas documentadas.

Las ISO/IEC 27001:2013 necesita que la organización tome las siguientes acciones cuando se detecta una no conformidad:

- Controlar y corregir dicha conformidad.

- Decidir si se eliminan el origen de la no conformidad para prevenir que vuelva a aparecer.
- Indicar quien implementará las acciones correctivas.
- Revisar la eficacia de las acciones correctivas implementadas

Documentación	Obligatorio
Resultados de acciones correctivas	SI
Naturaleza de las no conformidades y acciones tomadas	SI

Tabla 39. Doc Correcciones

6.5.31. Mejora constante del SGSI.

Crear un documento o política, no obligatorio, que defina:

- Responsable de planificar, gestionar y coordinar actividades de mejora.
- Comunicar que todos los empleados pueden contribuir para la mejora continua del SGSI.
- Definir métodos para registrar la información relacionada con la mejora.
- Implementar las mejoras como cambios y de esta forma quedarán documentadas las razones, resultados y la eficacia del cambio.

6.5.32. Comprobaciones a realizar antes de enfrentarse a la certificación.

Lo que se aconseja hacer antes de la certificación oficinal es:

- Confirmar que ha implementado todos los controles de acuerdo con el Plan de tratamiento de riesgos.
- Confirmar que se ha realizado la auditoría interna, revisión por parte de la alta dirección y las acciones correctivas.
- Comprobar que tienen todos los documentos obligatorios indicados en uno de los puntos siguientes.
- Comprobar que la documentación cumple los requerimientos de la ISO/IEC 27001:2013.
- Desplazarse por la organización y comprobar y confirmar que se realiza todos lo que está documentado

6.5.33. Pasos en la certificación de la organización por parte del Auditor.

Básicamente consta de tres pasos:

- Auditoría Fase 1 o revisión documental, donde se comprueba si existe toda la documentación obligatoria requerida por la ISO/IEC 27001:2013.

- Auditoría Fase 2 o auditoría principal, es una comprobación práctica de que se cumple lo que está documentado y recopilación de evidencias. Durante esta fase se pueden levantar:
    - No conformidades mayores (no permiten obtener el certificado), se incumple un requisito de la norma o de su propia documentación. Y se tienen un plazo aproximado de 90 días para resolverlas después de ser documentadas por el auditor.
    - No conformidades menores (permiten obtener el certificado, pero deben resolverse antes del año de revisión).
- Auditoría de seguimiento.

6.6. Documentación obligatoria y recomendada.

En base a lo analizado en el apartado 6.5, en este apartado se resume la documentación obligatoria y la recomendada para presentar al auditor. Para cada documento o registro que aparece, se describe su propósito y su contenido [24].

6.6.1. Documentación obligatoria ISO/IEC 27001:2013.

A continuación se presentan los documentos y registros de presentación obligatoria para superar la ISO/IEC 27001:2013.

Documento	Número de clausula ISO/IEC 27001:2013
Alcance del SGSI	4.3
Políticas y Objetivos de seguridad de la información	5.2 y 6.2
Definición de roles y responsabilidades	A7.1.2 y A.13.2.4
Inventario de activos	A.8.1.1
Política de uso aceptable de activos	A.8.1.3
Políticas de control de acceso	A.9.1.1
Procedimientos de operaciones para la gestión de TI	A.12.1.1
Principios de ingeniería de sistemas seguros	A.14.2.5
Política de seguridad de proveedores	A.15.1.1
Procedimientos de gestión de incidencias	A.16.1.5
Procedimientos de continuidad de negocio	A.17.1.2
Identificación de la legislación aplicable y los requisitos contractuales	A.18.1.1
Metodología de análisis y tratamiento de riesgos	6.1.2
Declaración de Aplicabilidad (SoA)	6.1.3
Plan de tratamiento de Riesgos	6.1.3 y 6.2

Informe de Análisis y Tratamiento de riesgos	8.2 y 8.3

Tabla 40. Documentación obligatoria

6.6.2. Contenido de los documentos:

- Alcance del SGSI. Se escribe al comienzo de la implantación de la ISO/IEC 27001:2013. Puede estar combinado con el documento de políticas de seguridad de la información y objetivos. El propósito de este documento es describir que información se intenta proteger, sin importar la ubicación de dicha información y donde, como y quien puede acceder a dicha información.
- Políticas y Objetivos de seguridad de la información. Describe el propósito general del SGSI. Los Objetivos de SGSI pueden estar en un documento independiente, pero también pueden estar combinados con las políticas. El propósito principal es que la dirección defina que necesita lograr con el SGSI. Define el marco para establecer los Objetivos de seguridad de la información, como se proponen los objetivos, cómo se aprueban y cómo se revisan. Debe mostrar el compromiso de la dirección de cumplir con los requisitos y la mejora continua del SGSI. Esta política debe revisarse periódicamente, por lo que se debe de definir un propietario.
- Definición de roles y responsabilidades. Elaborar la lista de partes interesadas en la seguridad de la información y describir las acciones o responsabilidades de cada uno. Un método recomendable es describir dichos roles y sus responsabilidades en las políticas y procedimientos.
- Inventario de activos. El concepto de registro de activos para la ISO/IEC 27001:2013 es bastante diferente a un registro de contabilidad. "Se considera como cualquier cosa que tenga valor para la organización". La ISO/IEC 27001:2013 trata la confidencialidad, integridad y disponibilidad de la información por lo que los activos abarcan: Hardware, Software, Información en cualquier formato, Infraestructura, personas, servicios subcontratados, etc.
- Política de uso aceptable de activos. El estándar no define correctamente este documento y puede abarcar una gran variedad de temas. Por lo que la recomendación es dejarlo para el final e incluir todos los controles que no se han tratado en otro documento y que afectan a todos los empleados.
- Políticas de control de acceso. Se describe la parte relacionada con la aprobación de accesos a la información y a los sistemas. Se pueden definir reglas para el acceso lógico y/o acceso a áreas seguras. En los accesos lógicos, definir roles identificando cual es el acceso de que disponen a cada servicios y recursos de red. Otra opción, es definir un propietario de los activos, el cual aprobará el acceso a los recursos de red o servicios a quien lo necesite.

- Procedimientos de operaciones para la gestión de TI. Se puede escribir como un solo documento o como varios. Aplicado a una Pyme puede cubrir todas las áreas de los Anexos A.12 y A.13 (backup, código malicioso, monitoreo, etc.). Este documento se cumplimenta después de haber terminado el proceso de análisis y tratamiento de riesgos.
- Principios de ingeniería de sistemas seguros. Es un nuevo control de la ISO 27001:2013. El documento define como incorporar técnicas de seguridad en todos los proyectos y toda la infraestructura como puede ser negocio, datos, aplicaciones y tecnología.
- Políticas de seguridad de proveedores. Es un nuevo control de la ISO/IEC 27001:2013. Describe como se realiza la selección de proveedores, como se analizan los riesgos de tratar con los proveedores y las cláusulas que se insertan en los contratos… etc.
- Procedimientos de gestión de incidencias. Define como notificar, clasificar, tratar y cerrar una incidencia de seguridad. También se define como generar una base de conocimiento de dichas incidencias.
- Procedimientos de continuidad de negocio. Son planes de continuidad de negocio y recuperación de las infraestructuras TI ante un desastre. Se puede estructurar en base a la ISO/IEC 22301.
- Identificación de la legislación aplicable y los requisitos contractuales. En el caso que nos aplica de España.

  Otros documentos sin estatus de ley:

  - Magerit – v3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
  - Guías CCN-STIC para la seguridad de los sistemas de la Administración Pública.
- Metodología de análisis y tratamiento de riegos. Se escribe antes de comenzar con el análisis y tratamiento de riegos. Uno de los errores principales es comenzar la evaluación de riesgos sin haber descrito la metodología que se implementará. Debemos basarnos en lo que necesita la cláusula 6.1.2 de la ISO/IEC 27001:2013.
- Declaración de aplicabilidad. También conocida como (SoA - Statement of Applicability) se escribe basándose en los resultados del análisis de riesgos. Este documento es uno de los más importantes de la ISO/IEC 27001:2013 porque se indican si los controles aplicables del Anexo A ya están implementados o no. Se describe cómo se implementa cada control explicando el procedimiento o referenciando un documento. Por lo general es un documento en formato Excel, que contiene todos los controles de estándar (Anexo A) y en el que se indica para cada control, si se aplica o no dentro del SGSI.

- Plan de tratamiento de riesgos. Se debe de describir el plan de acción para implantar los diferentes controles definidos en el documento de declaración de aplicabilidad (SoA). Su propósito principal es controlar los riesgos identificados durante la evaluación de riesgos. Debe centrase en los riesgos que no son aceptables para definir correctamente las prioridades y financiar la mitigación de los riesgos identificados.

ID	Nivel Riesgo	Opción	Controles	Acciones	Recursos	Plazos
A01	Muy Alto	Reducir	A.12.3.1	Desarrollar política de backups	Responsable Sistemas	Diciembre 2020

Ilustración 13. Plan de Riesgos.

6.6.3. Registros obligatorios ISO/IEC 27001:2013.

Registros	Número de clausula ISO/IEC 27001:2013
Registro de formación, experiencia y habilidades	7.2
Resultados de monitoreo y medición	9.1
Programa de auditoría interna	9.2
Resultados de la auditoria interna	9.2
Resultados de la revisión por parte de Dirección	9.3
Resultado de acciones correctivas	10.1
Resultados de la revisión de la gestión	10.1
Naturaleza de las no conformidades y acciones tomadas	10.1
Registro de las actividades de usuario, excepciones y eventos de seguridad	A.12.4.1 y A.12.4.3

Tabla 41. Registros obligatorios

Los controles del Anexo A, se pueden excluir cuando se concluya que no hay riesgo para la información.

6.6.4. Contenido de los registros:

- Registro de formación, experiencia y habilidades. Son registros que mantiene el departamento de Recursos Humanos de registros de los empleados.
- Resultados de monitoreo y medición. Define los tipos de KPI que se tiene que medir para cada control o grupo de controles.
- Programa de auditoría interna. Describe el plan de un año para la realización de la auditoría. Define quien la realizará, los métodos, criterios, etc.
- Resultados auditoría interna. Informe elaborado por el auditor interno incluyendo los hallazgos durante la auditoría.

- Resultados de la revisión por parte de Dirección. Acta que involucra a la dirección y que registra todo el material y decisiones.
- Resultado de las acciones correctivas. Listas de tareas indicando los responsables y los plazos.
- Registro de las actividades de usuario, excepciones y eventos de seguridad. Registros de logs de diferentes sistemas de TI o mediante registros realizados manualmente.

6.6.5. Documentación recomendados ISO/IEC 27001:2013.

A continuación se detallan otros documentos que son utilizados para mejorar el nivel de la seguridad de la información.

Documento	Número de clausula ISO/IEC 27001:2013
Procedimientos para control de la documentación	7.5
Controles de la información documentada	7.5.3
Procedimientos para la auditoría interna	9.2
Procedimientos para acciones correctivas	10.1
Política BYOD	A.6.2.1
Política de dispositivos móviles y teletrabajo	A.6.2.1
Políticas de clasificación de la información	A.8.2 con todos sus apartados
Políticas de eliminación y destrucción	A.8.3.2 y A.11.2.7
Políticas de gestión y control de acceso a sistemas y aplicaciones	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3
Procedimientos para trabajos en áreas seguras	A.11.1.5
Políticas de pantalla y escritorio limpios	A.11.2.9
Políticas de gestión del cambio	A.12.1.2 y A.14.2.4
Políticas de copia de seguridad	A.12.3.1
Políticas de seguridad de las comunicaciones	A.13.2.1, A.13.2.2 y A.13.2.3
Análisis y planes de continuidad en el negocio	A.17.1.1 y A17.1.3
Estrategia de redundancia y disponibilidad de los recursos	A.17.2.1

Tabla 42. Documentos aconsejables

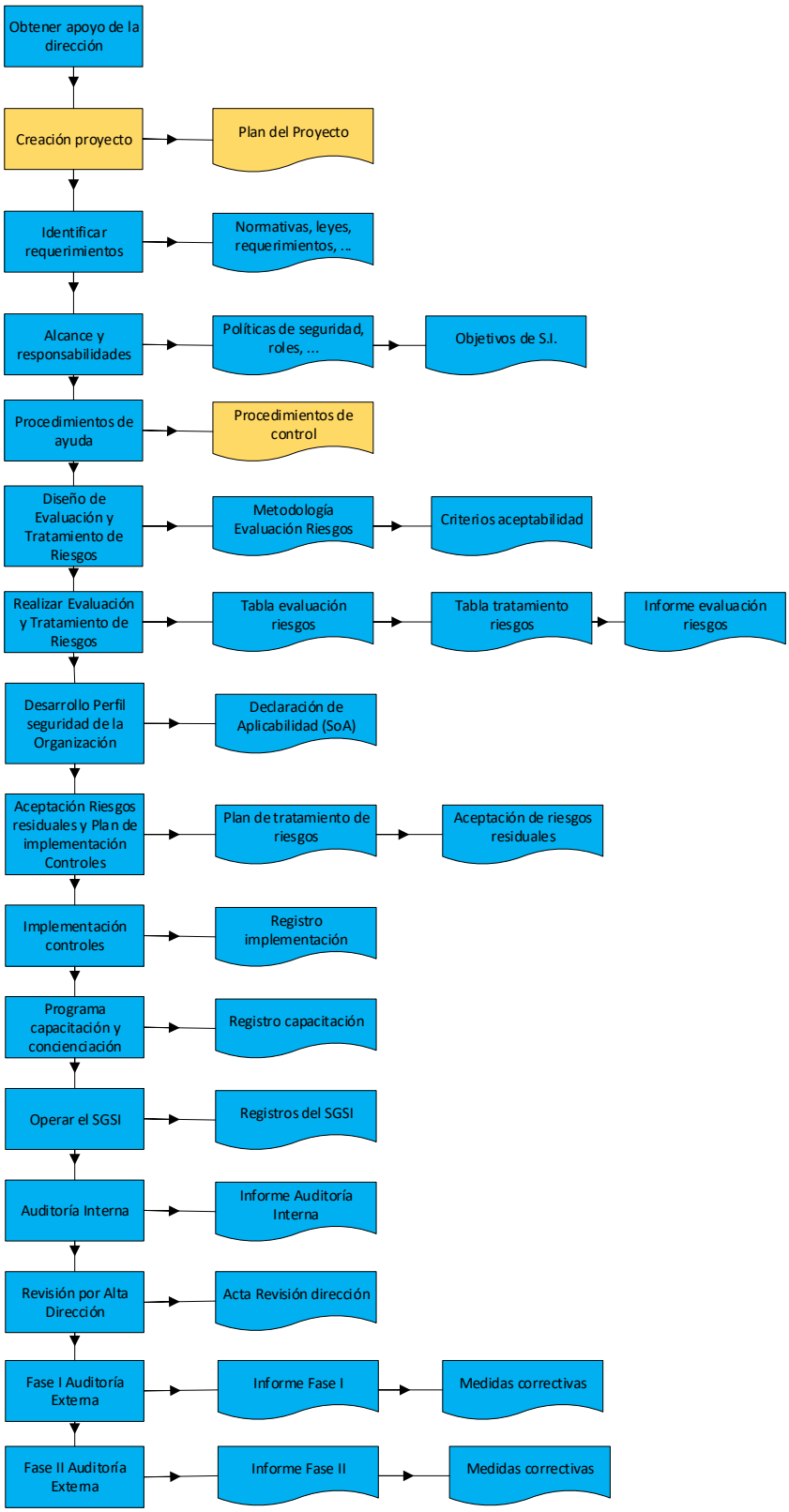
6.6.6. Contenido de alguno de los documentos:

- Procedimiento para el control de la documentación. Es un documento, que en el caso de disponer de otra ISO como la ISO 9001, ISO 14001 se puede utilizar un documento único.

- Procedimiento auditoría interna. Es un documento genérico para cualquier sistema de gestión. Indicar el procedimiento aplicable, listas de comprobaciones, periodicidad de la auditoría interna, etc.
- Lista de verificación de la implementación de la ISO/IEC 27001:2013. Es muy aconsejable disponer de dicho documento, pues facilita el seguimiento del estado de los procesos de implementación de la normativa y los documentos generados.

6.7. Esquema del proceso de implementación de la ISO/IEC 27001:2013

Finalmente, y para cerrar este punto, se crea un esquema para facilitar la visualización del proceso de implantación de la norma ISO/IEC 27001:2013 [25].



7. Caso Práctico

7.1. Presentación Empresa Consultora TI.

A continuación se describe la infraestructura de la consultora TI que se utilizará para presentar los puntos más destacados en la implantación de un SGSI.

7.1.1. Contextualización.

El foco de negocio principal es el Desarrollo de aplicaciones y consultoría.

Cuenta con un total de 145 empleados que se encuentran repartidos en distintas áreas de trabajo: Dirección, administración y contabilidad, recursos humanos, oficina de proyectos y diferentes equipos técnicos que están ejerciendo su trabajo de la oficina empresarial o desde ubicaciones remotas, en sus domicilios o en las propias oficinas de los clientes.

La empresa dispone de una oficina en el parque industrial de la Grela, ocupando la planta 3 del portal 1º. Es un espacio diáfano, salvo varias salas reservadas para:

- **Sala de CPD**. Sala con acceso mediante huella o mediante tarjeta. En dicha sala se encuentra, dos armarios de comunicaciones, uno de los cuales también aloja el servidor de virtualización. Dicha sala dispone de un sistema climatizado independiente del resto de la oficina. En dicha sala también se almacena material para reemplazo dispositivos que fallen en el día a día de los técnicos (portátiles, teclados, pantallas, ratones,….).
- **Sala de Almacén**. Sala con acceso mediante huella o mediante tarjeta. En dicha sala se guarda todo el material en depósito de los clientes necesario para poder realizar las pruebas y desarrollos para los clientes.
- **Sala de Reuniones**. Dispone de dos salas de reuniones, tanto para clientes externos como para reuniones internas.
- **Despacho de Dirección**. Despacho con acceso restringido mediante llave.
- **Despacho de RRHH**. Despacho con acceso restringido mediante llave. Compartido por el equipo de RRHH formado por tres personas.
- **Despachos individuales**, o cubículos de trabajo para un máximo 7 técnicos.
- **Entorno de la oficina**. El resto del área está disponible para acceso por todo el personal, tratándose de mesas alargadas con separaciones por paneles donde ejercen su trabajo la gran mayoría de técnicos cuando está en la oficina.
- **Espacio de aseos**.
- **Cuadro eléctrico general**.
- **Cámaras de seguridad**. Ubicada en la entrada de la oficina y zona general.

7.1.2. Organigrama Empresarial.

Al ser una pyme mediana dispone de una organización simple. Las principales áreas empresariales están estructuradas de la siguiente manera:

- Equipo de Dirección, 4 persona. Son los coordinadores del resto de áreas de la empresa las cuales a su vez cuentan con un responsable y personal específico por departamento.
- Departamento financiero, 2 personas. Un responsable y un administrativo para las tareas de contabilidad.
- Departamento de Recursos Humanos, 3 personas. Un responsable y dos técnicos encargados de parte de contratación, formación, concienciación, etc.
- Departamento de Proyectos, 1 persona. Un responsable que lleva toda la oficina de PMO.
- Sistema Integrado de Gestión, 2 personas.
- Personal de Sistemas, 27 personas. Dos responsables y 25 técnicos asignados a proyectos de operaciones.
- Personal técnico, 110 personas repartidas en diferentes grupos/proyectos. Que a su vez se diferencian claramente en:
    - Oficina de Proyectos.
    - Proyectos en clientes. (outsourcing)

En cada grupo o proyecto hay un responsable de proyecto que responde al PMO y un equipo técnico en función de la envergadura del proyecto.

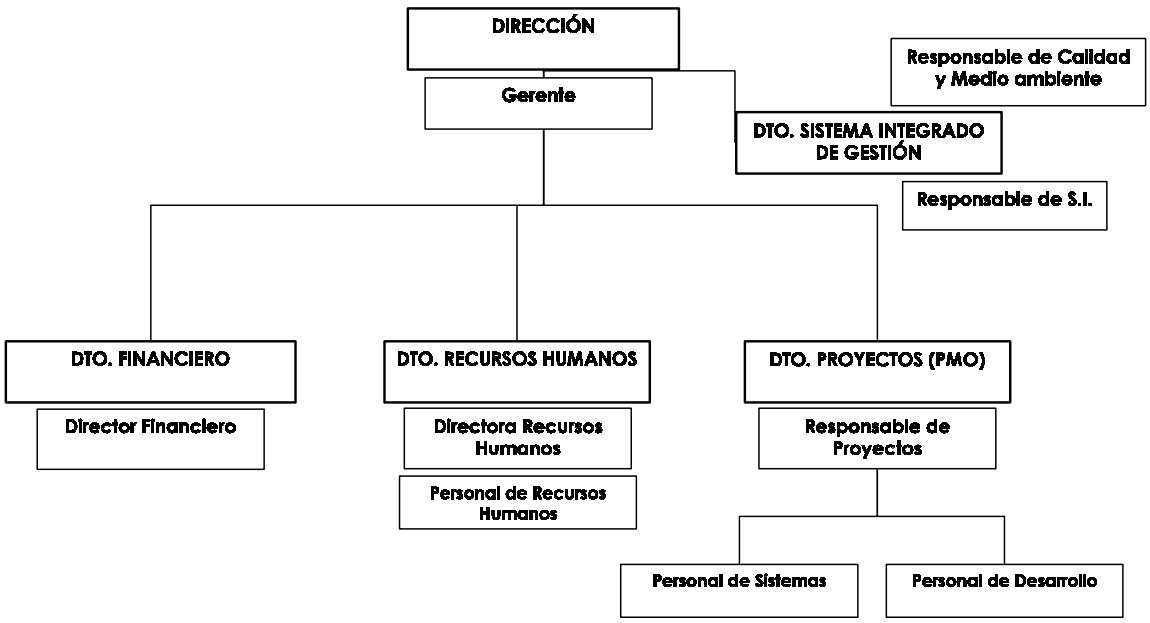


Ilustración 14. Organigrama

7.1.3. Diagrama de Red

Toda la infraestructura física incluida en el alcance del SGSI se encuentra situada en un único edificio y única planta, salvo por la excepción del personal que:

- Trabaja en las oficinas de los clientes.
- Trabajan desde sus domicilios por situaciones excepcionales o contrato de teletrabajo.

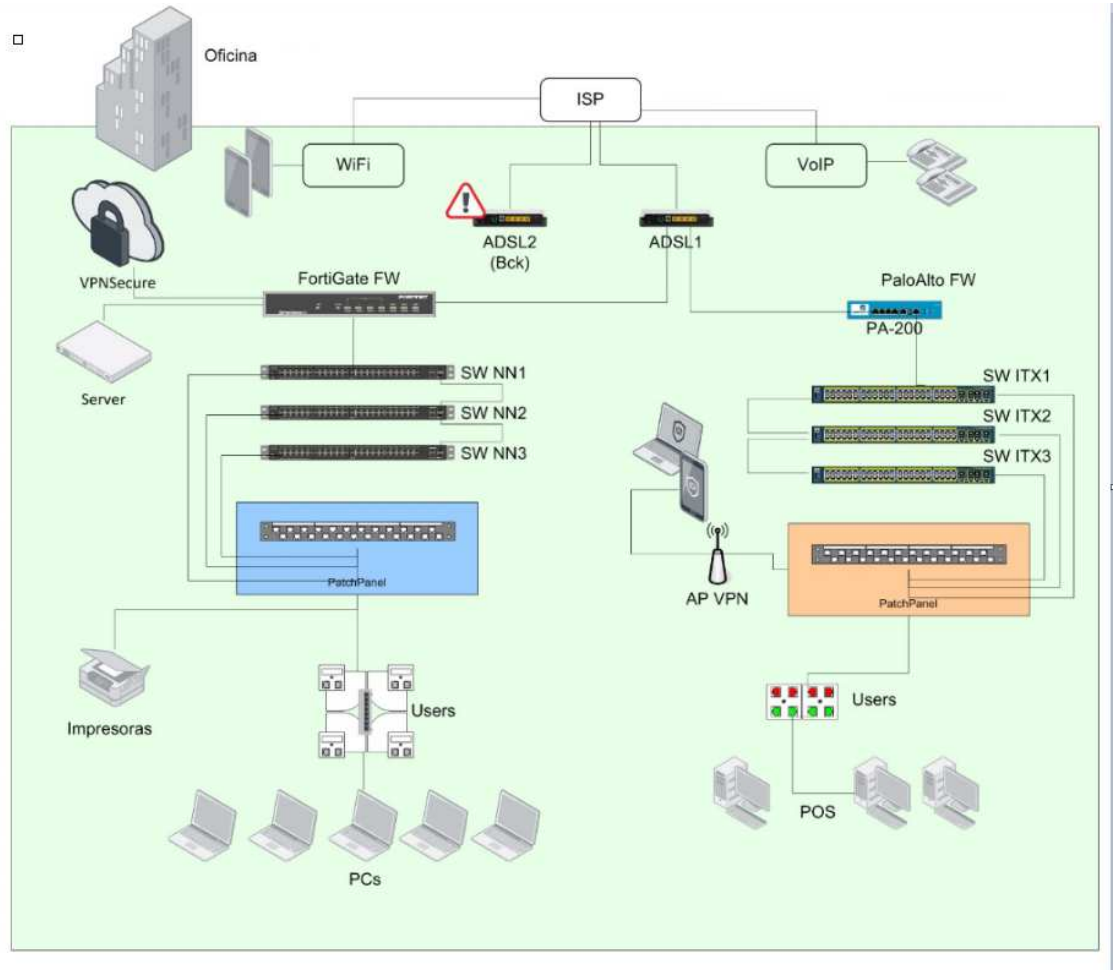


Ilustración 15. Esquema de red

Tal como se indicó anteriormente el armario de comunicaciones, que aloja los switchs, routers ADSL (primario y secundario), dispositivos wifi, el firewall, también aloja el servidor físico que es un virtualizador para soportar la infraestructura lógica de servicios de Active Directory que se describirá a continuación.

El servidor de virtualización es un único servidor físico DELL PowerEdge R340, con discos redundados en RAID I y con la capacidad de intercambio en caliente.

La alimentación de los dispositivos no está redundada y depende de una única línea de tensión.

7.1.4. Diagrama lógico a nivel de Active Directory y Cloud.

La infraestructura de autenticación de los dispositivos, la mayoría portátiles, se basa en una máquina virtual que mantiene el Controlador de Dominio de Active Directory para todos los equipos clientes con Windows.

Actualmente están dados de alta en el Active Directory como mucho unos 20 dispositivos clientes, correspondientes al personal que está trabajando en la oficina. El resto de equipos después de una año sin contactar con el domino ha perdido la relación con el dominio local y las políticas que aplicaban.

Actualmente los servicios de mensajería y herramientas colaborativas están alojadas en la nube de Microsoft, soportado por el licenciamiento de Ms Office 365 Bussines Premium.

Dispone una plataforma de antivirus, también alojada en la nube, para poder mantener un control de todos los equipos, se encuentren en la oficina o desplazados en los clientes u otras ubicaciones.

Las aplicaciones empresariales están alojadas en un hosting de un tercero, por lo que no están integradas con la autenticación de A.D. Consta de varias aplicaciones,

- Aplicación que utiliza el departamento de RRHH y dirección.
- Aplicación que es un portal para los empleados.

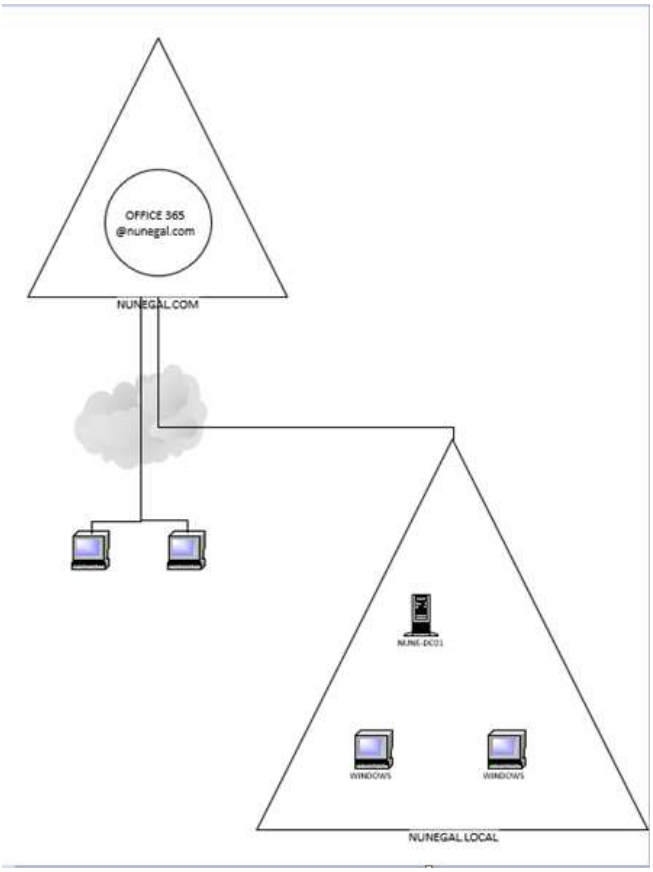


Ilustración 16.Esquema lógico

7.2. Exposición de la documentación y Plantillas

A continuación se detallan y presentan las plantillas de una parte de la documentación imprescindible para poder superar el proceso de certificación de la norma ISO/IEC 27001:2013.

Basaremos su creación y parte del contenido de dichas plantillas en el caso práctico presentado en el punto anterior.

La creación de las plantillas, aunque se basan en el caso práctico de la consultora TI presentada anteriormente, se intentará realizar de la forma más extensa y genérica posible, de modo que puedan servir de referencia para cualquier pyme. Se han utilizado múltiples fuentes de referencia para la creación de dichas plantillas. [26] [27] [28] [29] [30]

Debido a su naturaleza, formato y extensión, todas las plantillas descritas en este apartado se adjuntan a este proyecto como anexos. Se han creado utilizando formatos de Microsoft Office, que permiten que las plantillas sean modificables y adaptables a las necesidades de cada empresa, y cuyo uso está suficientemente extendido en el entorno empresarial y doméstico.

7.2.1. Contexto Interno/Externo y partes interesadas.

Dentro de la contextualización de la empresa uno de los puntos a resaltar para disponer de una perspectiva global de la organización es la creación del análisis DAFO.

	DEBILIDADES	**FORTALEZAS**
FACTORES INTERNOS	Escasez de personal que cumpla con las necesidades de la organización para la incorporación de nuevos proyectos	Capacidad de diversificación de servicios ofrecidos a nuestros clientes
	Pandemia COVID-19, dificulta la captación de profesionales TIC.	Capacidad de la organización mostrada, en el rápido crecimiento
	Escasez de herramientas para la automatización de la gestión de incidentes	Amplio conocimiento sector TIC en recursos humanos y gestión de clientes
	Control de la documentación	Fidelidad de clientes
	Falta de documentación de procesos de operación	Asignación de roles diferenciados para la gestión de la SI
	No existe un análisis de impacto financiero de la prevención y materialización de los riesgos de seguridad	Herramientas de control de amenazas y software maliciosos
		Apoyo de la alta dirección a la implementación del SGSI
FACTORES EXTERNOS	Descentralización de las copias de seguridad de la información	Proyecto de futuro con clientes

	Entorno legal en constante actualización sobre aspectos de seguridad	Demanda de empresas tecnológicas, preparadas para la prestación de servicios en modalidad de teletrabajo.

Tabla 43. DAFO

También es necesario disponer dentro del contexto de la organización la identificación de las partes interesadas.

	NECESIDADES	EXPECTATIVAS	APLICACIÓN DEL SISTEMA DE GESTIÓN
Junta directiva	• Rentabilidad suficiente de la organización. • Mejora continua y garantizar cumplimiento técnico, organizativo y legal	• Mejorar ambiente de trabajo • Orientación hacia la innovación.	• Gestión Comercial • Prestación del Servicio. • Incidencias de SGSI • Indicadores • Objetivos • Control operacional
Gerencia	• Capacidad para organizar medios y crear entorno favorable, cara el desarrollo de las actividades de la organización.	• Consecución del crecimiento empresarial de la organización.	• Liderazgo. • Objetivos de control y controles de referencia. • Revisión por Dirección • Gestión de RR.HH. • Infraestructuras • Inversiones realizadas • Cumplimiento del ordenamiento jurídico
Empleados	• Condiciones laborables satisfactorias. • Empleo seguro	• Mejora de las condiciones laborales actuales	• Ambiente de trabajo • Prestación del Servicio y Diseño • Requisitos Legales aplicables • Definición de funciones y responsabilidades. Roles. Comunicación interna. • Formación. • Gestión de activos y soportes
Clientes	• Cumplimiento de los requisitos establecidos en el servicio de desarrollo de software. • Cumplimiento a aspectos relativos a la preservación de la información manejada, como fugas de	• Mejoras en las condiciones del servicio de desarrollo de software. Mejoras en los aspectos relativos a la preservación de la información	• Incidencias de seguridad de la información. • Protección de datos, gestión y manipulación de soportes información, control de accesos. • Cumplimiento del ordenamiento jurídico

	información, robo o pérdida de datos personales	manejada, como fugas de información, robo o pérdida de datos personales.	aplicable • Prestación del Servicio • Cumplimiento de contratos • Satisfacción del cliente • Indicadores
Proveedores	• Demanda de sus productos/servicios por parte de nuestra organización. • Cumplimiento de requisitos de pagos.	• Aumento de la demanda de sus productos/servicios por parte de nuestra organización.	• Gestión de proveedores, preservación de la información intercambiada, acuerdo de intercambio. • Comunicaciones a proveedores: criterios de homologación • Evaluación de proveedores • Compras • Comercial • SLA.

Tabla 44. Partes interesadas

7.2.2. Alcance del SGSI

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "01 Alcance de SGSI v1.0.doc"**

7.2.3. Políticas y seguridad de la información.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "02 Políticas de seguridad de la información v1.0.doc"**

7.2.4. Roles y responsabilidades.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "03 Definición de roles y responsabilidades v1.0.doc"**

7.2.5. Lista de disposiciones legales.

Este documento, por ser una de las novedades en la documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "04 Identificación legislación aplicable v1.0.doc"**

7.2.6. Gestionar los servicios externalizados.

Este documento, por ser una de las novedades en la documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación**

ISO/IEC 27001:2013 – "05 Políticas de seguridad de proveedores v1.0.doc" y "Anexo – EVALUACIÓN DE PROVEEDORES.XLSX"

7.2.7. Gestión de incidencias.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "06 Procedimiento Gestión de Incidencias v1.0.doc"**

7.2.8. Control de acceso.

Este documento, por ser una de las novedades en la documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "07 Políticas de control de acceso v1.0.doc"**

7.2.9. Continuidad del negocio.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "08 Procedimientos de continuidad del negocio v1.0.doc"**

7.2.10. Principios de ingeniería de sistemas seguros.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "09 Principios de ingeniería de sistemas seguros v1.0.doc"**

7.2.11. Análisis diferencial (GAP).

Basándonos y adaptando la hoja de Excel publicada y disponible para su uso proporcionada por el equipo de ISO27001security.com se realiza un primer análisis diferencial con respecto a los requisitos de la norma ISO/IEC 27001:2013y con respecto a los controles del Anexo A de dicha norma [31] [32] [33].

Este documento se encuentra disponible en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "GAP - Análisis referencial controles ISO 27001.xlsx"**

Para la evaluación, tanto de la ISO/IEC 27001:2013 como del Anexo A, se utiliza un escalado propio indicado a continuación.

Porcentaje	Significado		Descripción
0%	No existente	**L0**	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	Inicial	**L1**	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	Repetible	**L2**	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	Definido	**L3**	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	Gestionado y medible	**L4**	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	Optimizado	**L5**	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Ilustración 17. Escala GAP

El resultado obtenido para el estado de cumplimento de los requisitos de la norma se muestra en la siguiente ilustración.

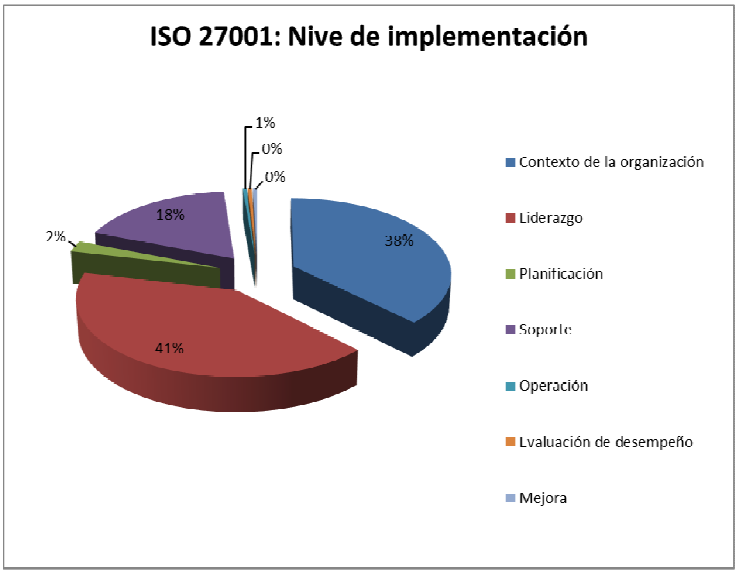


Ilustración 18. Estado de la implantación ISO/IEC 27001:2013

Como se puede observar algunas secciones de la norma están implementadas en unos porcentajes próximos al 50%. Destaca que el grueso de los requisitos no implementados forma parte de la gestión de riesgos y auditoría interna, siendo estos unos de los primeros requisitos que se deben de enfrentar.

También es importante destacar secciones de vital importancia como Liderazgo, Contexto de la organización están en un porcentaje de implementación muy importante.

A continuación se presenta el estado actual de las secciones de la norma en relación con el estado de implementación ideal.

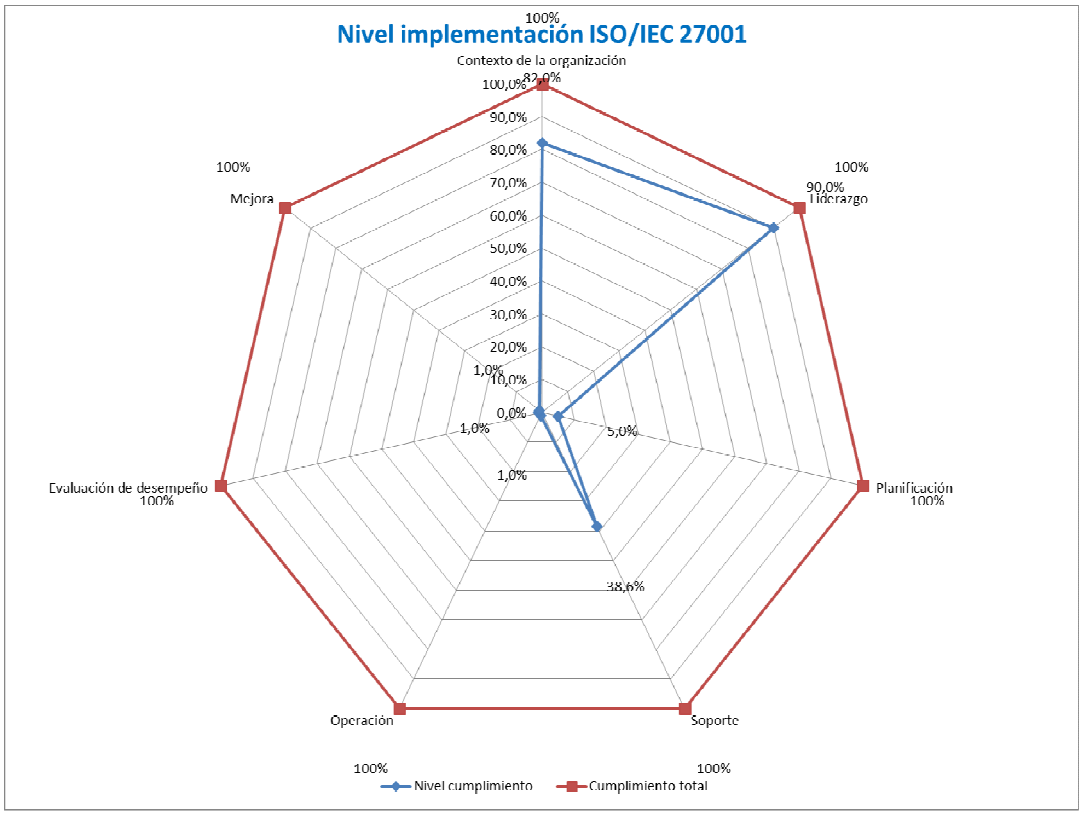


Ilustración 19. Nivel implementación Secciones.

En lo que respecta al estado de madurez de los 114 controles del Anexo A de la norma ISO/IEC 27001:2013, a continuación se muestra en la siguiente gráfica.

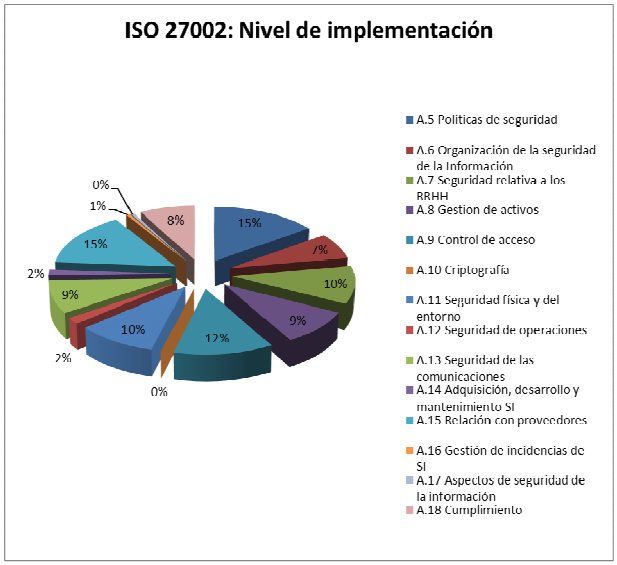


Ilustración 20. Estado de los Controles Anexo A

El estado de implantación y madurez de los controles del Anexo A muestra una visión general de la orientación que tiene actualmente la empresa en relación a la protección de la información.

Este análisis diferencial puede ser actualizado periódicamente, para ayudar a realizar un seguimiento en la evolución de la protección de la información y los controles aplicados para este fin.

A continuación se presenta el estado actual de los controles en relación con el estado de implementación ideal.

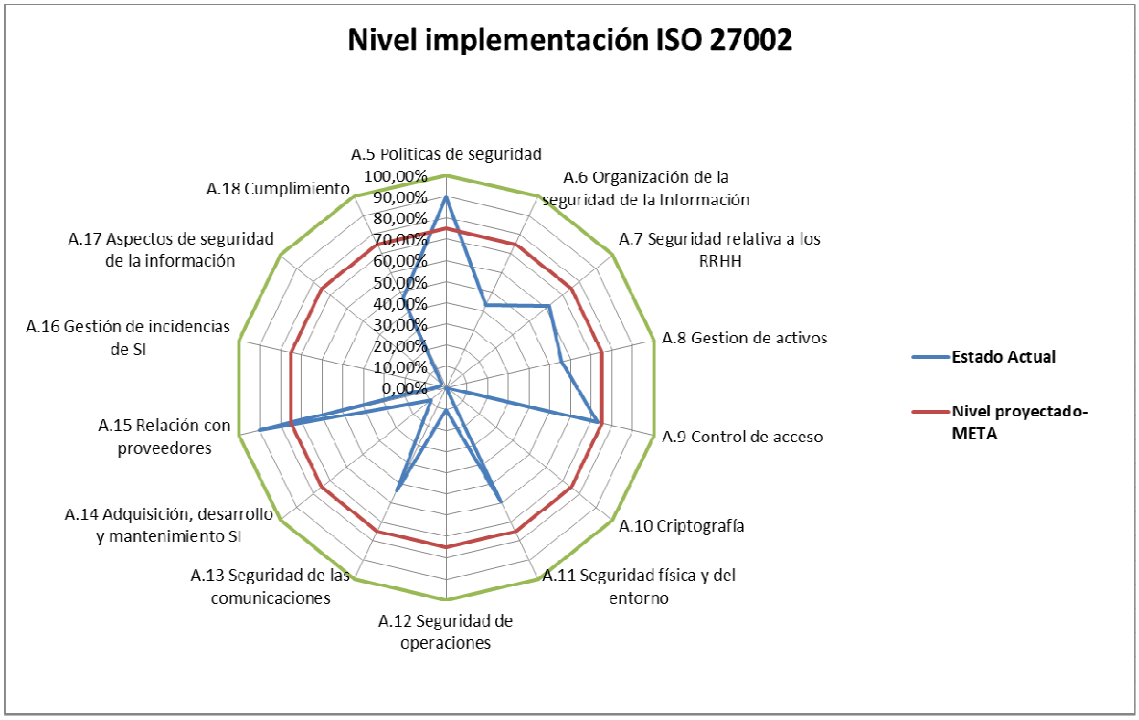


Ilustración 21. Nivel implementación Controles.

7.2.12. Metodología de la gestión de riesgos.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO /IEC 27001:2013 – "10 Metodología de la gestión de riesgos v1.0.doc**"

Esta metodología se ha creado basándose en la ISO/IEC 27005 pero no se aplica estrictamente, pues la norma solo recomienda utilizar o crear una metodología para la organización basándose en una de las existentes en el mercado para facilitar su revisión.

7.2.13. Identificación y análisis del riesgo

En la hoja de Excel que se encuentra en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "Análisis Riesgos.xls"** se puede seguir el proceso de análisis de riesgos desglosado en las diferentes hojas del documento de Excel:

- En la hoja "**Inventario de activos**", están clasificado y detallados los activos más importantes de la organización que nos sirve de caso de uso.

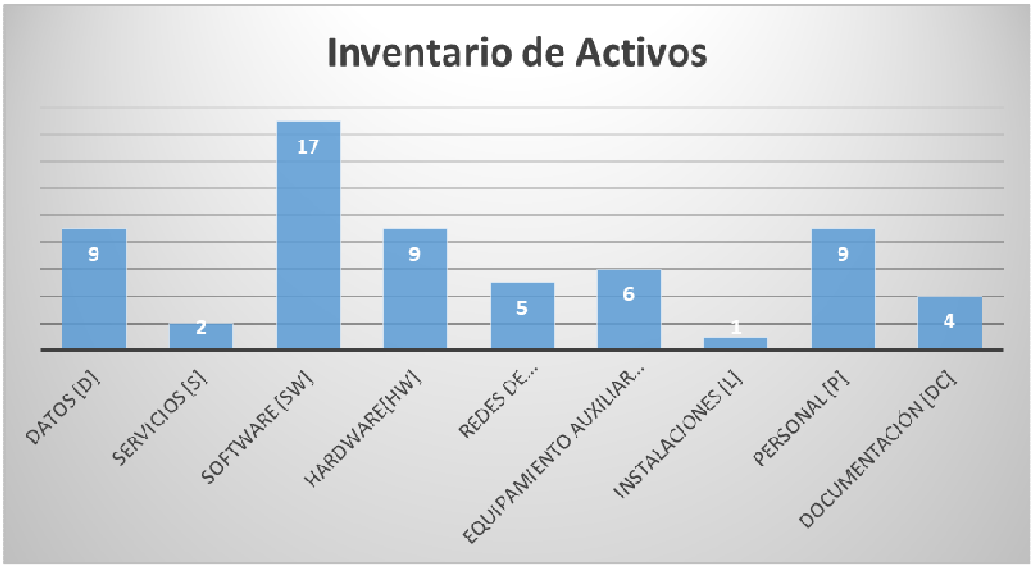


Ilustración 22. Inventario de activos.

- En la hoja "**Valoración de activos**", se ha realizado el clasificado de cada uno de los activos anteriormente identificados, basándose en la criticidad de dicho activo para la organización.

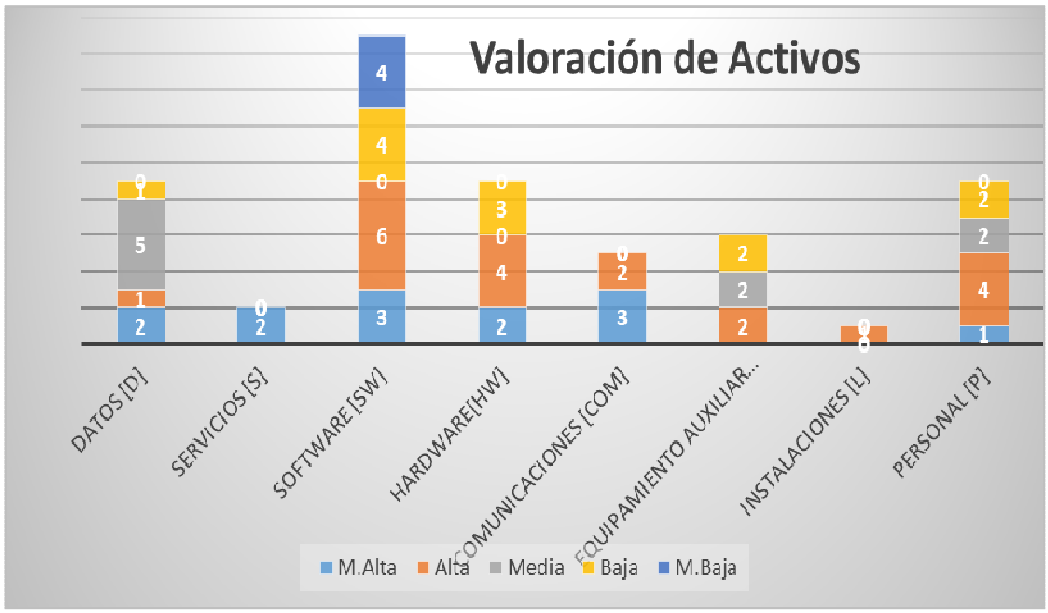


Ilustración 23. Valoración activos

- En la hoja **"Catálogo Amenazas"** Se han identificado y clasificado un considerable número de amenazas que pueden afectar a los activos de la organización. Estas amenazas se han obtenido de diferentes fuentes, siendo una de ellas uno de los Anexos de la ISO/IEC 27005.

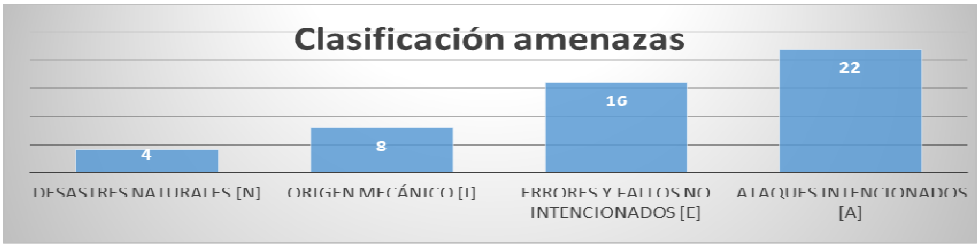


Ilustración 24. Clasificación amenazas

- En la hoja "**Valoración Amenaza**", se ha realizado el clasificado de cada uno de las amenazas anteriormente identificadas, basándose en la frecuencia de ocurrencia de dichas amenazas en la organización.

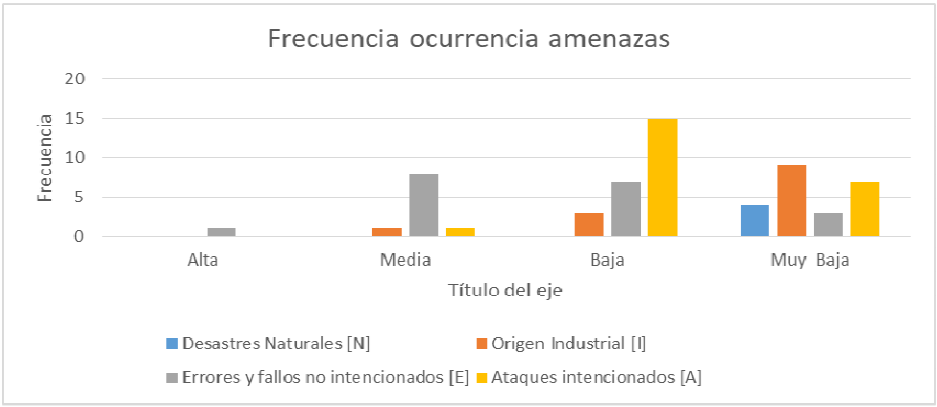


Ilustración 25. Frecuencia ocurrencia amenazas

- En la hoja "**Escenario de riesgos**", se ha creado una matriz de la afectación de las diferentes amenazas sobre los activos identificados y se ha agrupado para poder obtener una un numeral que nos permita aproximar las ocurrencias de las amenazas sobre los diferentes activos.

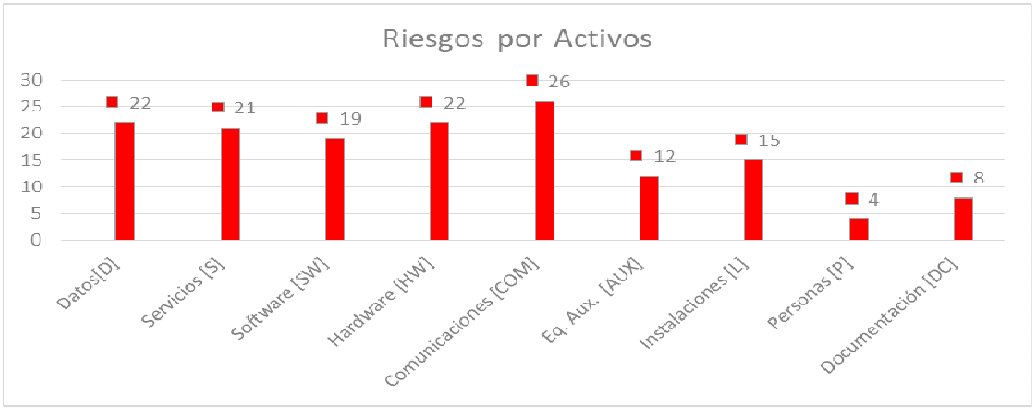


Ilustración 26. Número de riesgos detectados por activos

- En la hoja "**Evaluación Riesgo Max.**", se calcula el riesgo asociado a cada activo, afectado por una amenaza, utilizando la formula indicada en la Metodología de gestión de riesgos.

  Riesgo = Valor Activo X Frecuencia aparición Amenaza.

Estos resultados nos permiten detectar cuales son los activos de la organización que están en mayor riesgo y también nos permite priorizar el tratamiento de dichos riesgos.

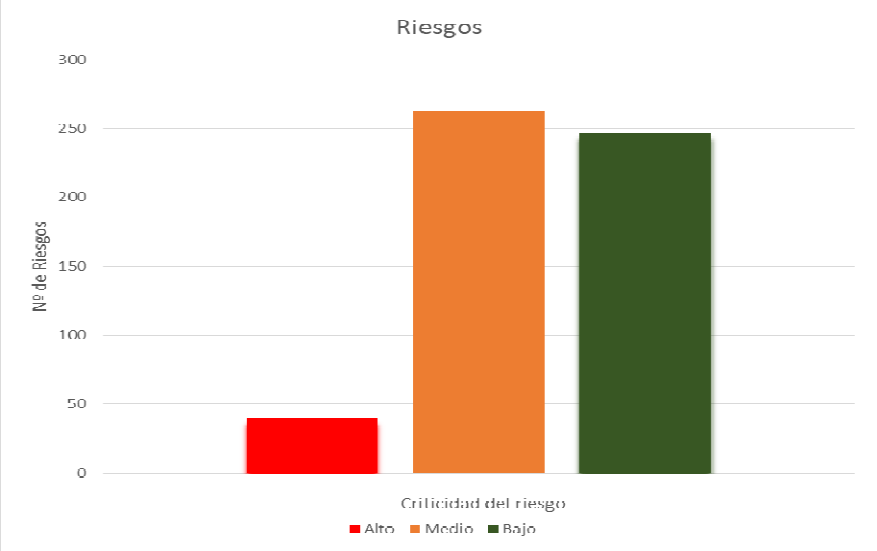


Ilustración 27. Valor del riesgo de los activos

7.2.14. Plan de Tratamiento del riesgo

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "11 Plan de tratamiento de Riesgos v1.0.doc"** junto con su archivo complementario **"11a Identificación de Controles para tratamiento de Riesgos v.0.1.docx**

Primeramente se identifican los controles que aplican a cada riesgo crítico.

Posteriormente a la identificación de los controles que aplican se genera el plan de acciones para mitigar o eliminar en lo posible los riesgos críticos cumplir las necesidades para implementar el SGSI.

7.2.15. Declaración de Aplicabilidad (SoA)

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "12 Declaración de aplicabilidad v1.0.docx"** junto con su archivo complementario **"12a Declaración de aplicabilidad v.0.1.xlsx"**

7.2.16. Auditoría interna.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "13 Auditoría Interna v1.0.doc"** junto con su archivo complementario **"13a Auditoría interna - Informe de Auditoría v.0.1.docx**

7.2.17. Revisión alta dirección.

Este documento por formar parte de documentación obligatoria en la norma ISO/IEC 27001:2013, se encuentra detallado en el **Anexo III: Plantillas documentación ISO/IEC 27001:2013 – "14 Acta de revisión por la dirección v1.0.doc"**

8. Estudio Económico

Esta valoración depende de muchos factores, estado actual de la implementación del SGSI, conocimientos de la normativa ISO, etc. Por lo que esto es una estimación basándose en:

- Personal interno sin alta formación en la normativa o auditoría interna.
- Contratación de una consultora externa para ayudar en la implementación.

8.1. Formación

Dentro de las muchas opciones de formación se ha optado por el más económico y con alto nivel de formación autodidactica.

- Cursos de formación gratuitos impartidos por *27001Academy*, pues no se optará a los certificados ofertados por este centro de formación online.
- No se contabilizan las horas de estudio y autoformación, pues esto es muy subjetivo.
- Realización de los dos primeros exámenes de certificación oficial de *CertiProf*, con un coste total de 300€

8.2. Auditoría Interna e implantación

Para la preparación de la organización para adaptar sus procedimientos, infraestructuras, documentación para implementar un SGSI y poder superar la certificación, se ha optado por la opción de contratar a una consultora externa que nos ayudará a preparar toda la documentación y realizar una auditoría interna imparcial, lo que supondrá un coste de implantación de 3000€ por la ISO y un coste de seguimiento de 200 € mensuales en el caso de superar los 6 meses previstos.

La dedicación de una persona interna de la empresa durante unos 6 meses:

960 h x 15,64€/h = 15.000€

8.3. Auditoría Externa

Precio de la consultora homologada y emisión del certificado para el primer año: 4.000 €

8.4. Coste total de la implementación.

El coste final para la empresa, sin proyectos de infraestructura asociados, sería de:

Recursos	Precios
Formación de una persona interna a la organización	300€
Consultora externa para ayuda a implementar el SGSI	3.000€
Ingeniero interno dedicado completamente durante 6 meses	15.000€
Certificación oficial en las instalaciones durante 5 días aproximadamente	4.000€
Coste total	**22.300€**

Tabla 45. Costes Auditoría SGSI

9. Conclusiones

Concluimos que se ha cumplido con los objetivos presentados y previstos para este proyecto.

Inicialmente los objetivos de este proyecto eran:

- Analizar diferentes normativas que certifican la implantación de un SGSI.
- Presentar la secuencia de pasos, tareas que debe de realizar y cumplir una pyme para lograr obtener la certificación ISO/IEC 27001:2013.
- Identificar la documentación requerida e imprescindible que se tiene que presentar para superar la certificación ISO/IEC 27001:2013
- Presentar un caso práctico basado en una consultora TI de tamaño mediano.
- Presentar las plantillas de la mayoría de la documentación imprescindible para superar la certificación ISO/IEC 27001:2013, tomando como base el caso práctico.

A lo largo del proyecto se han analizado las dos normas más destacadas en el ámbito nacional para la implementación y certificación de un SGSI en una Pyme, siendo la seleccionada la norma ISO/IEC 27001:2013

Se ha realizado el análisis y comparativa de las dos normativas de gestión de riesgos más destacadas del ámbito nacional y seleccionamos como base la ISO/IEC 27005 para la gestión de riesgos de la ISO/IE C27001:2013

Aun cuando la mayor parte de la documentación existente trata de simplificar/reducir los pasos para implementar la ISO/IEC 27001:2013, en nuestro caso se ha optado por desglosar la secuencia de pasos lo más detalladamente posible y asociando la documentación necesaria para la implementación de un SGSI.

Basándonos en la norma IOS/IEC 2001:2013 y los múltiples manuales de implantación de un SGSI se han identificado los documentos y registros que se deben de presentar obligatoriamente para superar la certificación.

Adicionalmente se ha crea un supuesto práctico de una empresa "ficticia". A partir de este supuesto práctico se han creado 14 plantillas de los 16 documentos reflejados en la "*Tabla 39. Documentación obligatoria"*, como necesarios para superar la certificación de la normativa ISO/IEC 27001:2013.

No se ha creado la plantilla "*Procedimiento de operaciones para la gestión de TI*", pues esta plantilla depende mucho de los recursos y herramientas de las que disponga la organización para operar los sistemas.

Estas plantillas se han presentado como producto del presente proyecto.

Con este proyecto se ha aprendido que el grado de complejidad de la implementación de un SGSI y certificación de la normativa seleccionada para certificar dicho sistema de seguridad de la información viene determinado por muchos factores internos y externos a la organización:

- Dimensión de la organización.
- Servicios y ámbito sobre el que se quiere aplicar el SGSI.
- Preparación del personal de la organización a nivel de conocimientos de las normativas que se desean implantar y conocimientos del proceso de auditoría.
- Implicación del personal, abarcando desde la dirección hasta el último departamento que se encuentre en el alcance de la implantación del SGSI.
- Presupuestos disponibles, etc.

En conclusión, se considera que aunque el proceso de implantación de un SGSI es una tarea ardua, laboriosa y que en función del tamaño de la empresa y los objetivos para los que se necesita la certificación, se tiene que dedicar un mínimo de 5 a 6 meses, consideramos que lo más importante y más complejo no es superar la primera certificación de la normativa, sino que es, el mantenimiento diario de todos los procesos y tareas desarrollados, la constante evolución de la infraestructura, procesos, documentación, etc. para poder mejorar la seguridad de la información y cumplir los criterios de recertificación y mantener los datos de la organización, y clientes lo más seguro posibles.

10. Bibliografía

[1] Agencia española protección de datos. *Marzo 2021 Notificaciones de Brechas de Datos Personales*. España: AEPD, 2021. [En línea]. Disponible: https://www.aepd.es/es/documento/informe-brechas-2021-03.pdf [Accedido Abril 2021].

[2] Esquema Nacional de Seguridad – *ENS*. [En línea]. Disponible: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html?idioma=es#.YMpsa0ztaUk [Accedido Marzo 2021].

[3] ISOTools. *La NCh ISO 27001. Origen y evolución*. [En línea]. Disponible: https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/. [Accedido Marzo 2021].

[4] Aplicabilidad de ISO 27001 dividida por industrias. Croatia: 2017 [En línea]. Disponible: https://advisera.com/27001academy/es/descargas-gratuitas/ [Accedido Marzo 2021].

[5] AENOR. *UNE-EN ISO/IEC 27002 Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información*. Madrid: AENOR, 2017. [En línea]. Disponible: https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx. [Accedido Febrero 2020].

[6] Kosutic Dejan. *Seguro & Simple, Una guía para la pequeña empresa para la implementación de la ISO 27001 con medio propios*. 2016. Croatia: EPPS Services Ltd, 2016. 221-240 p. ISBN: 978-953-57452-7-3.

[7] Ministerio de Hacienda y Administración Pública. *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: MINHAP, 2012. [En línea]. Disponible: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YMp1FEztaUk [Accedido Abril 2021].

[8] Díaz Manuel. *Análisis de Riesgos: ISO 27005 vs Magerit y otras metodologías*. Madrid: [s.n.] 2009 [En línea]. Disponible: https://www.audea.com/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias/ [Accedido Mayo 2021].

[9] Centro Cristológico Nacional. *Guía de Seguridad TIC CCN-STIC 825 Esquema nacional de seguridad certificaciones 27001*. España: CCN-STIC, 2013. [En línea]. Disponible: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html. [Accedido Mayo 2021].

[10] Sulay Velásquez. *Comparativa entre las metodologías de análisis y gestión del riesgo NTC – ISO/IEC27001 y MAGERIT*. Universidad Piloto de Colombia, [s.a.]. 13p. [En línea] Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8666/Comparativa%20entre%20las%20metodologias%20de%20analisi%20y%20gestion%20del%20riesgo.pdf?sequence=1&isAllowed=y. [Accedido Mayo 2021].

[11] Ramirez Abby. *Metodologías de análisis de riesgos*. (Diapositivas). [s.l.]. [s.n.]. 2015. [En línea]. Disponible: https://es.slideshare.net/abbyramirez89/anlisis-comparativo-50183515 [Accedido Mayo 2021].

[12] AENOR. *Catálogo de cursos 2021*. Madrid: AENOR, 2021. [En línea]. Disponible: https://catalogo.aenor.com/#page=65 [Accedido Febrero 2021].

[13]. Bureau Veritas Formación. *Cursos seguridad de la información*. Barcelona: Bureau Veritas Formación, 2021. [En línea]. Disponible: https://www.bureauveritasformacion.com/seguridad-de-la-informacion.aspx [Accedido Marzo 2021].

[14] Kosutic Dejan. *ISO 27001 Foundations Course* [En línea]. Disponible: https://training.advisera.com/course/iso-27001-foundations-course/. [Accedido Marzo 2021].

[15] Kosutic Dejan. *ISO 27001 Internal Auditor Course* [En línea]. Disponible: https://training.advisera.com/course/iso-27001-internal-auditor-course/. [Accedido Marzo 2021].

[16] CertiProf. Certified ISO/IEC 27001 Foundation (I27001F) [En línea]. Disponible: https://certiprof.com/pages/certified-iso-iec-27001-foundation. [Accedido Marzo 2021].

[17] AENOR. *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información*. Madrid: AENOR, 2017. [En línea]. Disponible: https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx. [Accedido Febrero 2010].

[18] Kosutic Dejan. *Seguro & Simple, Una guía para la pequeña empresa para la implementación de la ISO 27001 con medio propios*. 2016. Croatia: EPPS Services Ltd, 2016. 221-240 p. ISBN: 978-953-57452-7-3.

[19] [En línea]. Disponible: https://normaiso27001.es/. [Accedido Abril 2021].

[20] Kosutic Dejan. *Seguro & Simple, Una guía para la pequeña empresa para la implementación de la ISO 27001 con medio propios*. 2016. Croatia: EPPS Services Ltd, 2016. 73-142 p. ISBN: 978-953-57452-7-3.

[21] Kenyon Bridget and Humphreys Edward (Ted). *Guide to the implementation and Auditing of ISMS Controls Based on ISO/IEC 27001*. Fourth edition, 2014. London: BSI Standards Limited, 2014. 141p. ISBN: 978-0-580-82910-9.

[22] Brewer David. ISO/IEC 27001 *Mastering Risk Assessment and the Statement of Applicability*. First Editon, 2021. USA: Independently published, 2021. 130p. ASIN: B08TQ4TQ6.

[23] Merino Bada Cristina y Cañizares Sales Ricardo. *Auditoría de sistemas de gestión de seguridad de la información (SGSI)*. 1ª ed., 2014. España: Fund. Confemetal, 2014. 264p. ISBN: 978-8415683971.

[24] Ramiro Rubén. *Documentos y registros requeridos en la ISO 27001:2013*. [En línea]. Disponible: https://ciberseguridad.blog/documentos-y-registros-iso-27001-2013/ [Accedido Abril 2021].

[25] Diagrama del proceso de implementación de la norma ISO 27001:2013. Croatia: 2017 [En línea]. Disponible: https://advisera.com/27001academy/es/descargas-gratuitas/ [Accedido Mayo 2021].

[26] Instituto Nacional de Ciberseguridad. *Kit de concienciación*. [s.l.]. [s.n.], [s.a.]. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/kit-concienciacion. [Accedido Abril 2021].

[27] Instituto Nacional de Ciberseguridad. *Políticas de seguridad para la pyme*. [s.l.]. [s.n.], [s.a.]. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/herramientas/politicas. [Accedido Abril 2021].

[28] Instituto Nacional de Ciberseguridad. *Guías*. [s.l.]. [s.n.], [s.a.]. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/guias. [Accedido Mayo 2021].

[29] Instituto Nacional de Ciberseguridad. *Plan Director de Seguridad*. [s.l.]. [s.n.], [s.a.]. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad. [Accedido Abril 2021].

[30] Instituto Nacional de Ciberseguridad. *Formación*. [s.l.]. [s.n.], [s.a.]. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/formacion. [Accedido Abril 2021].

[31] [En línea]. Disponible: https://www.iso27001security.com/html/toolkit.html. [Accedido Mayo 2021].

[32] Herramientas para ISO 27001 e ISO 22301. [En línea] Disponible: https://advisera.com/27001academy/es/herramientas/ [Accedido Mayo 2021].

[33] Enlaces y herramientas. [En línea]. Disponible: https://www.iso27000.es/Enlaces.html. [Accedido Mayo 2021].

11. Anexos.

11.1. Anexo I: Propuesta Proyecto Fin de Grado

Nombre alumno: José Baltasar Couce López

Titulación: Grado en Ingeniería Informática (itinerario).

Curso académico: 2020/2021

1. TÍTULO DEL PROYECTO

Implementación y aplicación de la ISO 27001:2013 en una consultora de TI de tamaño mediano.

2. DESCRIPCIÓN Y JUSTIFICACIÓN DEL TEMA A TRATAR

Dado el incremento en el número de ataques de seguridad a infraestructuras empresariales y gubernamentales hoy en día es aconsejable poder certificar que se cumplen unos criterios mínimos de seguridad en la gestión de la información. Bajo esta premisa se plantea la idea de:

Desarrollar los requisitos necesarios para una consultora de TI para cumplir y certificarse en la ISO 27001.

Que requisitos debe de cumplir para certificarse en la ISO y como cumplir dichos requisitos.

Que documentación se deberá de entregar, etc.

3. OBJETIVOS DEL PROYECTO

Analizar los pasos, tareas que debe de realizar y cumplir una consultara de TI para lograr obtener la certificación ISO 27001.

4. METODOLOGÍA

La metodología se fijará en las primeras reuniones con el tutor

5. PLANIFICACIÓN DE TAREAS

Estudios de los requisitos necesarios para cumplir la ISO 27001

Presentar el conjunto de servicios de una empresa consultora de TI, que deben de evaluar para la norma ISO 27001

Estudio y análisis de la documentación necesaria para cumplir la norma ISO27001

Creación de las plantillas, documentación necesaria que se debe de entregar para superar la ISO27001

6. OBSERVACIONES ADICIONALES

Presentar los procesos necesarios y documentos requeridos para superar los criterios exigidos por la ISO 27001 a una empresa consultora de TI en la presentación de sus servicios.

Revisado por Tutor: German Latorre Antin.

7. ENTREGABLES

- Documentación del desarrollo del proyecto, que es la documentación estándar de un proyecto.
- Entrega de las plantillas creadas a partir de los requerimientos de la ISO 27001, para la documentación que es necesaria presentar por la consultora TI para superar los requisitos indicados por la ISO 27001.

11.2. Anexo II: Actas de reunión del Proyecto Fin de Grado

11.2.1. Primera reunión.

REUNIÓN: Acta reunión del seguimiento del PFG

Fecha:	02/04/21		
Hora comienzo:	16:00h	**Hora finalización:**	17:30h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Revisión del cronograma de ejecución del proyecto, tareas realizadas desde la última reunión.	
2	Actualización del cronograma a la situación actual.	
3	Dudas en relación a los entregables (proyecto, plantillas y Anexos).	
4	Dudas en relación al estudio económico del proyecto.	
5	Presentación del desglose de tareas con Project o Kanban.	
6	Planificación de las próximas reuniones de seguimiento.	
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Actualización cronograma	05/04/21	Baltasar
002	Comenzar la documentación de los primeros puntos del proyecto.	15/04/21	Baltasar
003	Consultar el contenido del campo "Metodología"	15/04/21	German
004	Ver la posibilidad de obtener algún documento de PFG, para seguir como guía y ver los desgloses	15/04/21	German
005	Consultar el material y el medio (digital o analógico) para los entregables y presentación del PFG	15/04/21	German
006			

11.2.2. Segunda reunión.

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	23/04/21		
Hora comienzo:	10:00h	**Hora finalización:**	12:00h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Actualización del cronograma de ejecución del proyecto, tareas realizadas desde la última reunión.	
2	Actualizar la relación de los entregables (proyecto, plantillas y Anexos).	
3	Aclarar las dudas que habían surgido en la reunión anterior.	
4	Presentación del índice del entregable del documento del PFG	
5	Planificación de las próximas reuniones de seguimiento.	
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Actualización cronograma	07/05/21	Baltasar
002	Presentar el contenido de los primeros puntos del índice acordado.	07/05/21	Baltasar
003	Presentar los activos que se están bajo el análisis de riesgos del caso de uso planteado.	07/05/21	Baltasar
004	Consultar la parte de la entrega de documentación física	07/05/21	German
005			
006			

11.2.3. Tercera reunión

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	07/05/21		
Hora comienzo:	11:30h	**Hora finalización:**	13:00h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Presentación de la evolución del contenido del PFG	
2	Actualizar la relación de los entregables (proyecto, plantillas y Anexos).	
3	Tratar el punto de Gestión de Riesgos, por ser uno de los más importantes	
4	Aclarar las dudas que habían surgido en la reunión anterior.	
5	Planificación de las próximas reuniones de seguimiento.	
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Enviar el documento de PFG para ver la evolución	10/05/21	Baltasar
002	Presentar los activos que se están bajo el análisis de riesgos del caso de uso planteado.	10/05/21	Baltasar
003	Consultar la parte de la entrega de documentación física en la situación de COVID	14/05/21	German
004	Consultar la forma de presentar el PFG en la situación de COVID	14/05/21	German
005			
006			

11.2.4. Cuarta reunión

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	14/05/21		
Hora comienzo:	12:30h	**Hora finalización:**	13:30h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Revisar la evolución del contenido del PFG	
2	Actualizar la relación de los entregables (proyecto, plantillas y Anexos).	
3	Tratar el punto de Gestión de Riesgos, metodologías y procedimientos	
4	Planificación de las próximas reuniones de seguimiento. (Pendiente los temas aclarados con Paqui)	
5		
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Enviar el documento de PFG con las modificaciones sugeridas	19/05/21	Baltasar
002	Ampliar puntos del documento PFG.	19/05/21	Baltasar
003	Hablar más en detalle de los temas aclarados por Paqui	21/05/21	German
004	Revisar un par de puntos del PFG para ver su correcta presentación	21/05/21	German

11.2.5. Quinta reunión

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	27/05/21		
Hora comienzo:	18:00h	**Hora finalización:**	19:30h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Revisar la evolución del contenido del PFG	
2	Presentar las modificaciones indicadas para ver como encajan	
3	Presentar las tres primeras plantillas del entregable	
4		
5		
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Enviar el documento de PFG con los últimos cambios recomendados: Tablas, formación, …etc.	03/06/21	Baltasar
002	Presentar los activos que se están bajo el análisis de riesgos del caso de uso planteado.	03/06/21	Baltasar
003	Confirmar de las peticiones a Paqui	04/06/21	German
004			

11.2.6. Sexta reunión

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	03/06/21		
Hora comienzo:	16:30h	**Hora finalización:**	18:30h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Revisar la evolución del contenido del PFG	
2	Presentar las modificaciones indicadas para ver como encajan	
3	Tratar los diferentes recursos externos que se pueden utilizar para las plantillas	
4	Presentar las 7 primeras plantillas del entregable	
5		
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Enviar el documento de PFG con los últimos cambios recomendados: Tablas, formación, …etc.	10/06/21	Baltasar
002	Presentar los activos que se están bajo el análisis de riesgos del caso de uso planteado.	12/06/21	Baltasar
003	Confirmar el contenido del punto conclusiones	12/06/21	German
004			

11.2.7. Séptima reunión

REUNIÓN:	**Acta reunión del seguimiento del PFG**

Fecha:	12/06/21		
Hora comienzo:	17:30h	**Hora finalización:**	19:00h
Lugar:	Online - Microsoft Teams		
Elabora acta:			
Convocados:	German Latorre, Baltasar Couce		

Orden del día / Acta

No.	**Asunto**	**Acuerdo**
1	Revisar la evolución del contenido del PFG	
2	Presentar las modificaciones indicadas para ver como encajan	
3	Presentar la metodología de riesgos que se aplicará	
4	Definir que documentos deberán presentarse como mínimo	
5		
6		
7		
8		
9		
10		

Resumen de acuerdos

Número	**Acuerdo**	**Plazo**	**Responsable**
001	Enviar el documento de PFG con los cambios finales	15/06/21	Baltasar
002	Presentar todo el proceso de análisis de riesgos.	15/06/21	Baltasar
003	Terminar todas las plantillas que están pendientes.	15/06/21	Baltasar

11.3. Anexo III: Plantillas documentación ISO/IEC 27001:2013

Se adjunta las siguientes plantillas, creadas para poder utilizar como referencia, para poder implementar parte de la documentación obligatoria necesaria para superar la normativa ISO/IEC 27001:2013 en una pyme:

01 Alcance de un SGSI v1.0.docx
02 Política de seguridad de la información v1.0.docx
03 Definición de roles y responsabilidades v1.0.docx
04 Identificación legislación aplicable v1.0.docx
05 Política de seguridad de proveedores v1.0.docx
05a Evaluación de proveedores.xlsx
06 Procedimientos Gestión de Incidencias v1.0.docx
07 Políticas de control de acceso v1.0.docx
08 Procedimientos de continuidad del negocio v1.0.docx
09 Principios de ingeniería de sistemas seguros v1.0.docx
GAP – Análisis referencial controles iso27001.xlsx
10 Metodología de la Gestión de Riesgos v1.0.docx
10a Análisis de Riesgos.xlsx
11 Plan de tratamiento de Riesgos v1.0.docx
11a Identificación de Controles para tratamiento de Riesgos.xlsx
12 Declaración de aplicabilidad v1.0.docx
12 Declaración de aplicabilidad v1.0.xlsx
13 Auditoría Interna v1.0.docx
13a Auditoría interna – Informe de Auditoría v1.0.docx
14 Acta de revisión por la dirección v1.0.docx