Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001

Manuel Muñoz Martín

Junio, 2015

Ficha

Título del trabajo:	Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001
Tipo de trabajo:	Trabajo de final de carrera
Autor:	Manuel Muñoz Martín
Centro:	Universitat Oberta de Catalunya
Tutor:	Ana Cristina Domingo Troncho
Fecha:	Junio de 2015
Área del trabajo:	Gestión de proyectos
Titulación:	Ingeniería Técnica Informática de Sistemas

Licencia

Copyright © 2015 Manuel Muñoz Martín.

Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

Índice general

Agradecimientos **7**

Presentación **8**

I Plan de trabajo **9**

1. Introducción **10**
1.1. La norma UNE-ISO/IEC 27001 10
1.2. Ciclo de mejora continua 10
1.2.1. Planificar 11
1.2.2. Hacer 11
1.2.3. Comprobar 11
1.2.4. Mejorar 11

2. Descripción de la empresa **12**

3. Objetivos **13**
3.1. Generales 13
3.2. Específicos 13

4. Planificación **15**
4.1. Plan de implantación 15
4.2. Fechas de entrega 16
4.3. Documentos generados 16

II Análisis **17**

5. Plan de seguridad **18**
5.1. Descripción 18
5.2. Objetivos de negocio 18
5.3. Situación actual 19
5.3.1. Organización de la empresa 19
5.3.2. Infraestructura tecnológica 20

5.4. Alcance del SGSI 20

6. Análisis diferencial **22**

7. Definición de la política de seguridad **40**
7.1. Política de seguridad 40
7.2. Objetivos 40
7.3. Alcance 41
7.4. Políticas de seguridad 41
7.4.1. Referente al SGSI 41
7.4.2. Organización 41
7.4.3. Gestión de activos 41
7.4.4. Recursos humanos 42
7.4.5. Seguridad física y del entorno 42
7.4.6. Comunicaciones y operaciones 42
7.4.7. Control de accesos 42
7.4.8. Adquisición, desarrollo y mantenimiento 43
7.4.9. Gestión de incidentes 43
7.4.10. Continuidad de negocio 43
7.4.11. Conformidad 43

8. Definición del enfoque del análisis de riesgo **44**

9. Análisis de riesgos **45**
9.1. Inventario de activos 45
9.2. Valoración de activos 46
9.3. Identificación de amenazas 47
9.4. Valoración de riesgos por activo 48
9.5. Aceptación de dirección 50
9.6. Declaración de aplicabilidad 50

III Implantación **68**

10.Plan de tratamiento de riesgos **69**
10.1. Plan de políticas de seguridad de la Información 69
10.2. Plan de la organización de la seguridad de la información 70
10.3. Plan de gestión de activos 71
10.4. Plan de seguridad de los recursos humanos 72
10.5. Plan de seguridad física y del entorno 73
10.6. Plan de gestión de comunicaciones y operaciones 74
10.7. Plan de control de accesos 76
10.8. Plan de adquisición, desarrollo y mantenimiento 77

10.9. Plan de gestión de incidentes 78
10.10Plan de gestión de continuidad 79
10.11Plan de conformidad 80

11.Implementación del plan **81**

IV Conclusiones **84**

12.Resumen **85**

Bibliografía **87**

Índice de tablas

4.1. Plan de implantación del TFC. 15
4.2. Fechas de entrega. 16
4.3. Documentos generados 16

6.1. Análisis diferencial. 22

9.1. Inventario de activos. 45
9.3. Valoración de activos. 47
9.4. Tratamiento de riesgos. 49
9.6. Declaración de aplicabilidad. 50

10.1. Presupuesto de políticas de seguridad de la Información. 70
10.2. Presupuesto de la organización de la seguridad de la información. 71
10.3. Presupuesto de gestión de activos. 72
10.4. Presupuesto de seguridad de los recursos humanos. 73
10.5. Presupuesto de seguridad física y del entorno. 74
10.6. Proveedores cloud. 75
10.7. Presupuesto de gestión de comunicaciones y operaciones. 76
10.8. Presupuesto de control de accesos. 77
10.9. Presupuesto de adquisición, desarrollo y mantenimiento. 77
10.10Presupuesto de gestión de incidentes. 78
10.11Presupuesto de gestión de continuidad. 79
10.12Presupuesto de conformidad. 80

11.1. Plan de trabajo de implementación. 81
11.3. Coste total del proyecto. 83

Agradecimientos

Agradecer a toda la gente de la UOC, compañeros, profesores, tutores y consultores el tiempo compartido junto a ellos durante estos años. Dar las gracias también a mi consultor de área de Gestión de Proyectos Ana Cristina Domingo Troncho por su ayuda, consejos y guía en la elaboración de este documento.

Presentación

Este trabajo de fin de carrera forma parte del área de Gestión de Proyectos y más concretamente de la gestión de implantación de la norma ISO 27001, esta norma es un estándar internacional para la seguridad de la información y un referente por los beneficios que aporta a las organizaciones en materia de seguridad.

La implantación de un SGSI es una de las partes más complejas y la que más tiempo lleva dentro de todo proyecto y que depende mucho del grado de madurez de las organizaciones en cuanto a seguridad de la información se refiere.

Uno de los objetivos de este proyecto es poder trabajar con normas, estándares y marcos sobre seguridad de la información y su aplicación dentro de las organizaciones, además de sentar las bases para poder de manera independiente y externa certificar la eficacia y conformidad de la ISO 27001.

A través de este trabajo diseñaremos los planes de trabajo necesarios para la realización del proyecto, analizaremos los requisitos previos necesarios para aplicar los controles de la norma y detallaremos los contenidos de éstos, finalmente aplicaremos estos controles y comprobaremos su conformidad.

La implantación de esta norma proporcionará una serie de ventajas y beneficios que no sólo afectará a la propia organización sino a todos los que trabajen con ella y mejorará el funcionamiento e imagen de la propia empresa.

Parte I

Plan de trabajo

Capítulo 1

Introducción

1.1. La norma UNE-ISO/IEC 27001

Uno de los aspectos más importantes de cualquier organización es la información, garantizar su seguridad debería ser una prioridad en toda empresa aunque en la mayoría de veces no se le da la importancia que merece. En muchas empresas no se sigue ningún procedimiento o marco de trabajo que garantice dicha seguridad y esto supone un riesgo elevado el no contar con un SGSI que permita a dicha organización aunar esfuerzos y procesos para garantizar la seguridad de la información.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

ISO/IEC 27001 es un estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming".

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

1.2. Ciclo de mejora continua

Esta norma nos presenta un sistema de gestión basado en el ciclo de Deming: Plan, Do, Check, Act, conocido como PDCA y que traducido al castellano sería Planificar, Hacer, Comprobar y Mejorar. El ciclo PDCA supone la implantación de un sistema de mejora continua que requiere una constante evolución para adaptarse a los cambios producidos en su ámbito y para tratar de conseguir la máxima eficacia operativa mediante las cuatro

fases que lo componen. Cada una de estas fases marca los objetivos que describe la norma ISO 27001.

1.2.1. Planificar

En esta fase se analizará el entorno de actividad de la compañía. La información tratada por la misma, las directivas corporativas establecidas y los requisitos legales aplicables a cada compañía. Durante esta etapa la empresa deberá diseñar un procedimiento formal para la continua identificación y evaluación de los riesgos y la selección de los objetivos de control, así como los controles que le permitan gestionar estos riesgos.

1.2.2. Hacer

En esta fase habrá que centrarse en el desarrollo e implementación de un plan efectivo a medio y largo plazo que evite o atenúe los posibles riesgos para la seguridad de la información. En esta fase, se iniciará también la formación e información del personal de la empresa, de forma que se garantice la correcta implementación del SGSI.

1.2.3. Comprobar

La implantación del SGSI exige el seguimiento y revisión de los controles y medidas implantadas. Por ello es imprescindible, la realización de auditorías tanto internas como externas que revisen la eficacia y eficiencia del SGSI, y que identifiquen las posibles amenazas, vulnerabilidades y riesgos del sistema.

1.2.4. Mejorar

La implantación de un SGSI exige actuar, mantener y mejorar constantemente el SGSI. Cuando en la revisión del SGSI se detecten amenazas, vulnerabilidades y riesgos, es necesario llevar a cabo medidas correctoras y preventivas adecuadas, que garanticen en todo momento la seguridad y protección de la información de la empresa.

Capítulo 2

Descripción de la empresa

Este proyecto pretende ser una guía de referencia para la implantación de un SGSI basado en la ISO 27001 en una empresa informática con orientación a servicios TI, todos los procesos y documentos estarán orientados a la esta norma pero sólo como referencia para su adopción o implantación y no como herramienta para la obtención de la certificación de dicha norma. Nuestra empresa presta servicios TI a pymes, consta de una única sede y de unos 20 trabajadores.

Dentro de la organización se siguen buenas prácticas de algunos marcos de referencia conocidos como ITIL pero no se ha implantado ningún SGSI, es por eso que utilizar ISO 27001 como guía en materia de seguridad de la información ayudará tanto a la organización como a las empresas que presta servicios.

En un futuro puede servir para la obtención de la certificación en dicha norma.

Capítulo 3

Objetivos

3.1. Generales

Los objetivos que persigue la implantación de dicha norma se pueden describir como:

- Proporcionar una mejora en la imagen y las relaciones con clientes y proveedores con la adopción de la norma en cuanto a forma de trabajo en materia de seguridad de la información.
- Aumento en el control de las personas que participan en los proyectos así como de los procesos.
- Control y registro de incidentes y debilidades de los sistemas de información.
- Mejora en la gestión de continuidad de negocio debido a incidentes relacionados con la seguridad de la información.

3.2. Específicos

Para la implantación de un SGSI los objetivos se definen a partir de fases y actividades que componen el ciclo de Deming:

- **Definición del alcance, los objetivos y la política de seguridad.** Cubrir todos los aspectos relacionados con la seguridad: seguridad física, seguridad lógica y seguridad del personal.
- **Desarrollar el inventario de activos.** Hay que tener en cuenta cuales son los activos más valiosos y cuales más vulnerables.
- **Realizar el análisis de riesgos.** Hay que mirar las amenazas que afectan a cada activo, este análisis nos proporcionará los puntos débiles del negocio.
- **Seleccionar las medidas de seguridad a implementar.** Hay que seleccionar e implementar las medidas necesarias para reducir y controlar los riesgos identificados.

- **Evaluar los riesgos residuales.** Consiste en saber cómo se reducen los riesgos al aplicar las medidas.
- **Documentar los procedimientos necesarios para implementar las medidas seleccionadas.** Se debe documentar los pasos de la implementación para evitar cometer errores en la ejecución de tareas.
- **Implementación de controles y procedimientos.** Planificación de la ejecución de los controles y procedimientos.
- **Formación del personal.** Desarrollar un plan formativo para asegurar el éxito de la implantación del SGSI.

Capítulo 4

Planificación

Para la implantación de un SGSI se va a utilizar la norma ISO 27001 que describe, como se ha indicado anteriormente, parte del ciclo PDCA de gestión del sistema de seguridad de la información. Las partes implicadas en la implantación de dicha norma corresponden a las dos primeras fases del ciclo de vida de Deming.

4.1. Plan de implantación

Debido a que un plan de implantación basado en la norma ISO 27001 puede tener una duración de 6 a 12 meses tomaré como referencia los tiempos dados para las entregas de las pac y memoria final.

Tabla 4.1: Plan de implantación del TFC.

Fase	**Inicio**	**Fin**
1. Creación de plan de trabajo	25-02-2015	18-03-2015
2. Definición del alcance del SGSI	19-03-2015	22-03-2015
3. Definición de la política de seguridad	23-03-2015	26-03-2015
4. Identificación de los activos de información	27-03-2015	29-03-2015
5. Definición del enfoque del análisis de riesgo	30-03-2015	02-04-2015
6. Metodología de análisis de riesgo	03-04-2015	05-04-2015
7. Tratamiento de los riesgos	06-04-2015	09-04-2015
8. Selección de controles	10-04-2015	12-04-2015
9. Gestión de riesgos	13-04-2015	16-04-2015
10. Declaración de aplicabilidad	17-04-2015	22-04-2015
11. Aprobación y gestión de recursos	22-04-2015	25-04-2015
12. Plan de tratamiento de riesgo	26-04-2015	29-04-2015
13. Definir conjunto de objetivos y métricas	30-04-2015	03-05-2015
14. Asignación y delimitación de responsabilidades	04-05-2015	06-05-2015
15. Implementación y puesta en marcha	07-05-2015	13-05-2015
16. Formación y capacitación	14-05-2015	21-05-2015

4.2. Fechas de entrega

Tabla 4.2: Fechas de entrega.

Entregas	**Fases**	**Fecha**
PAC1		18-03-2015
	1. Creación de plan de trabajo	
PAC2		22-04-2015
	2. Definición del alcance del SGSI	
	3. Definición de la política de seguridad	
	4. Identificación de los activos de información	
	5. Definición del enfoque del análisis de riesgo	
	6. Metodología de análisis de riesgo	
	7. Tratamiento de los riesgos	
	8. Selección de controles	
	9. Gestión de riesgos	
	10. Declaración de aplicabilidad	
PAC3		21-05-2015
	11. Aprobación y gestión de recursos	
	12. Plan de tratamiento de riesgo	
	13. Definir conjunto de objetivos y métricas	
	14. Asignación y delimitación de responsabilidades	
	15. Implementación y puesta en marcha	
	16. Formación y capacitación	
Entrega final		18-06-2015
	Documentación del proyecto	
	Elaboración de memoria final	

4.3. Documentos generados

Tabla 4.3: Documentos generados

Fase	**Documento de soporte**
1. Creación de plan de trabajo	Documento del plan de trabajo
3. Definición de la política de seguridad	Política de seguridad
4. Identificación de los activos de información	Inventario de activos
6. Metodología de análisis de riesgo	Análisis de riesgos
7. Tratamiento de los riesgos	Gestión de riesgos
10. Declaración de aplicabilidad	Documento de aplicabilidad
12. Plan de tratamiento de riesgo	Plan de tratamiento de riesgo
16. Formación y capacitación	Planes de formación
	Registros de formación

Parte II

Análisis

Capítulo 5

Plan de seguridad

5.1. Descripción

La empresa sobre la que implantaremos el SGSI, nos referiremos a ella como Treval a partir de ahora, es una empresa privada. Su principal actividad es la de prestar servicios TI a otras empresas privadas y a organismos públicos de forma eventual. Estos servicios son en su mayoría proyectos de desarrollo de software a medida, adaptación de software y soporte técnico de infraestructuras TI Cloud. La mayoría de estos servicios se realizan a través de tecnología virtual haciendo hincapié en la seguridad de las comunicaciones ya que es el principal motivo de preocupación del director, al utilizar los servicios Cloud como plataforma de comunicación con los clientes y proveedores los procesos y tecnologías son susceptibles a tener problemas de seguridad.

Treval hasta la fecha ha seguido algunas prácticas como ITIL en la que algunos de sus responsables de negocio o departamento han intentado implantar pero sin demasiado éxito, por lo tampoco tienen experiencia en adoptar marcos de referencia y certificaciones de como ISO 20000 o similares. Sin embargo reconocen que un SGSI podría aportarles no sólo un marco de seguridad como modelo de referencia sino una base también para la adopción de certificaciones futuras.

5.2. Objetivos de negocio

Los principales motivos de seguridad por los que han decidido implantar ISO 27001 podrían describirse como:

- Utilización telemática de los servicios por parte de clientes y proveedores.
- Implantar medidas como LOPD y similares.
- Tener políticas y sistemas de respaldo y salvaguarda de la información.
- Pruebas de desarrollo de software en entornos seguros.
- Asegurar la integridad y privacidad de la gestión documental.

- Sistemas de comunicación seguros entre miembros de empresa y externos.
- Medidas para el control y detección de accesos no autorizados.
- Utilización de soportes telemáticos seguros para el transporte de información.
- Tener un sistema de respuesta ante incidentes de seguridad.
- Ofrecer un servicio de disponibilidad tolerante a fallos.

5.3. Situación actual

5.3.1. Organización de la empresa

Treval dispone de unas oficinas centrales en donde se encuentran todos sus departamentos y trabajan sus 20 empleados ubicados en cinco áreas:

1. **Dirección.** El gerente compone este departamento y a su vez es responsable de los demás departamentos.
2. **Administración.** Dos administrativos son los encargados de las tareas administrativas y contables de la empresa.
3. **Oficina de proyectos**. Un responsable de área se encarga de la coordinación, gestión y tareas comerciales de los proyectos TI de la empresa.
4. **Sistemas**. Es la parte encargada de las infraestructuras TI tanto internas como Cloud y la componen cuatro ingenieros de sistemas y un responsable de área.
5. **Desarrollo**. Se divide a su vez en dos equipos de cinco personas cada uno además de un responsable de desarrollo que gestiona los equipos.

Tanto el departamento de dirección como el de administración gestionan sus procesos de forma interna, es decir, toda la información que gestionan y crean se realiza dentro de la empresa y únicamente de forma ocasional pueden hacer algún trámite telemático en alguna administración local o nacional. El responsable de la oficina de proyectos tiene un perfil más comercial y no sólo realiza su trabajo dentro de la empresa sino que por su trabajo tiene reuniones y entrevistas con clientes y proveedores, debido a esto utiliza herramientas de acceso de forma remota a Treval para gestionar la información.

El departamento de sistemas es el responsable de la información y sistemas de la empresa y el resto de departamentos, el órgano de dirección administración y la oficina de proyectos utilizan las herramientas y tecnologías de sistemas para el trabajo y la comunicación diaria, este departamento da soporte a clientes y a desarrollo para administrar las soluciones y entornos de desarrollo y pruebas de los proyectos.

Por último desarrollo se compone de dos equipos que a su vez pueden gestionar varios proyectos y desarrollan soluciones a medida y adaptadas a clientes y a la propia empresa Treval. Todos los procesos de desarrollo son internos y únicamente las soluciones que realizan se implantan en proveedores Cloud una vez finalizadas.

5.3.2. Infraestructura tecnológica

La infraestructura TI de la empresa se divide en tres grandes áreas:

1. Área de dirección, administración y oficina de proyectos gestionada por su propia red y que se comunica con los servidores del departamento de sistemas y con el exterior a través de su propio sistema de cortafuegos. Está compuesto de equipos de escritorio y un equipo multifunción compartido.

2. Área de desarrollo: compuesta por once equipos de escritorio y un equipo multifunción, acceden desde su propia red a los servicios del departamento de sistemas y al exterior desde el router de la empresa.

3. Área de sistemas: es la más importante y en ella trabajan los responsables del despliegue y servicios de la empresa y clientes. Disponen de varios servidores donde albergan las aplicaciones e información empresarial. Además gestionan los entornos de desarrollo y las actualizaciones de los sistemas.

La infraestructura está compuesta de:

- Red de comunicaciones ethernet dentro de la empresa.
- Equipos de escritorio con SO Windows instalado.
- Dos equipos multifunción.
- Tres equipos de cortafuegos más un router con sistema IDS.
- Servidor para desarrollo con Windows para entornos de prueba, testing y producción con control de versiones y herramientas de control de cambios.
- Servidor para dirección, administración y oficina de proyectos con Windows que contiene información y aplicaciones de estos departamentos.
- Servidor para gestión documental con Windows y sistema ECM Sharepoint para trabajo colaborativo y de documentación.
- Servidor de aplicaciones con Windows para trabajadores y usuarios externos que necesiten acceder a datos internos.
- Servidor de servicios con Windows para DNS, LDAP, Mail, etc.

5.4. Alcance del SGSI

Dentro del proyecto de implantación debemos definir el alcance o ámbito de nuestro SGSI, ya que es una parte importante y no debemos abarcar más de lo necesario. Una vez hemos definido los objetivos de nuestro proyecto en el apartado anterior observamos que nuestro SGSI se implantará en los procesos y servicios de las áreas de desarrollo y

sistemas ya que son las que dan soporte y servicio a toda la empresa incluidos los clientes y proveedores.

Estas áreas comprenden los procesos críticos de la empresa ya que se encargan de gestionar la información, comunicación, seguridad y proyectos de Treval.

La infraestructura empresarial de Treval también está incluida en la implantación del SGSI, toda la red equipos y sistemas de seguridad como IDS y cortafuegos además de los servidores ubicados dentro de la empresa. Las infraestructuras Cloud utilizadas para el despliegue de aplicaciones disponen de sus propias medidas de seguridad y certificación[1].

Quedan excluidas los demás departamentos de dirección, administración y oficina de proyectos.

[1] Azure,AWS

Capítulo 6

Análisis diferencial

El análisis de situación de la empresa respecto a la norma no es obligatorio según la ISO 27001 pero si aconsejable para entender dónde nos encontramos. El análisis diferencial nos permitirá evaluar el grado de cumplimiento de la norma y nos permitirá tener una versión preliminar de la **Declaración de aplicabilidad**.

La nomenclatura que se va a utilizar en este análisis es la siguiente:

- **Si**: Cumple con el requisito o control.
- **No**: No cumple con la aplicación del control.
- **Parcial**: El control está aplicado de manera parcial.
- **N/A**: No se aplica o no se utiliza.

Tabla 6.1: Análisis diferencial.

Objetivos	**Observaciones**	**Cumple**	**Justificación**
5. Política de seguridad			
5.1 Política de seguridad de la información			
5.1.1 Documento de política de seguridad de la información		No	Requerimiento ISO 27001
5.1.2 Revisión de la política de seguridad de la información		No	Requerimiento ISO 27001

Objetivos	Observaciones	Cumple	Justificación
6. Organización de la seguridad de la Información			
6.1 Organización interna			
6.1.1 Compromiso de la dirección con la seguridad de la información	Existen compromisos de medidas de seguridad.	Parcial	Requerimiento ISO 27001
6.1.2 Coordinación de la seguridad de la información	Ya existen controles de seguridad.	Parcial	Requerimiento ISO 27001
6.1.3 Asignación de responsabilidades para la seguridad de la información		No	Requerimiento ISO 27001
6.1.4 Procesos de autorización para los servicios de procesamiento de información		No	
6.1.5 Acuerdos sobre confidencialidad	Existen contratos con trabajadores, clientes y proveedores.	Si	Requerimiento legal
6.1.6 Contacto con las autoridades		No	Requerimiento legal e ISO
6.1.7 Contacto con grupos de interés especiales		No	
6.1.8 Revisión independiente de la seguridad de la información		No	Requerimiento legal e ISO

Objetivos	Observaciones	Cumple	Justificación
6.2 Terceras partes			
6.2.1 Identificación de los riesgos relacionados con las partes externas	Hay informes de riesgos derivados de los procesos externos.	Parcial	
6.2.2 Consideraciones de la seguridad cuando se trata con los clientes		Parcial	
6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes	Existen contratos de confidencialidad.	Si	

Objetivos	Observaciones	Cumple	Justificación
7. Gestión de activos			
7.1 Responsabilidad de los activos			
7.1.1 Inventario de activos		Si	Requerimiento ISO 27001
7.1.2 Propiedad de los activos		Si	Requerimiento ISO 27001
7.1.3 Uso aceptable de los activos		Si	Requerimiento ISO 27001
7.2 Clasificación de la información			
7.2.1 Directrices de clasificación		No	Requerimiento ISO 27001
7.2.2 Etiquetado y manejo de información		No	Requerimiento ISO 27001

Objetivos	Observaciones	Cumple	Justificación
8. Seguridad de la gestión de los recursos humanos			
8.1 Seguridad en actividades previas a la contratación			
8.1.1 Roles y responsabilidades	Todas las competencias están definidas.	Si	Requerimiento ISO 27001
8.1.2 Análisis y selección	Existe un análisis de requisitos para la selección de personal.	Si	
8.1.3 Términos y condiciones de empleo	Todos los empleados y proveedores tienen cláusulas de seguridad.	Si	
8.2 Seguridad durante el desempeño de funciones			
8.2.1 Responsabilidad de la dirección	Existen los documentos pero falta la revisión.	Parcial	

8.2.2 Educación, formación y concientización sobre la seguridad de la información		No	
8.2.3 Proceso disciplinario		No	
8.3 Finalización o cambio de empleo			
8.3.1 Responsabilidadades de fin de contrato	Existen procesos.	Si	
8.3.2 Restitución de activos	Existen procesos.	Si	
8.3.3 Eliminación de derechos de acceso	Existen procesos.	Si	

Objetivos	**Observaciones**	**Cumple**	**Justificación**
9. Seguridad física y del entorno			
9.1 Áreas seguras			
9.1.1 Perímetro de seguridad física		No	
9.1.2 Controles físicos de entrada		No	
9.1.3 Seguridad de oficinas, despachos y recursos		No	

9.1.4 Protección contra amenazas externas y ambientales		No	
9.1.5 Trabajo en áreas seguras		No	
9.1.6 Áreas de carga y acceso público	La oficina dispone de entrada de materiales y almacén.	Si	
9.2 Seguridad de los equipos			
9.2.1 Instalación y protección de los equipos		No	
9.2.2 Servicios de suministro	Los servidores disponen de SAI.	Si	
9.2.3 Seguridad del cableado	Ninguna parte de la infraestructura es pública.	Si	
9.2.4 Mantenimiento de los equipos	Existen contratos de mantenimiento de los servidores.	Si	
9.2.5 Seguridad de los equipos fuera de las instalaciones		No	
9.2.6 Seguridad en la reutilización o eliminación de los equipos		No	Requerimiento ISO 27001
9.2.7 Retiro de activos		No	

Objetivos	**Observaciones**	**Cumple**	**Justificación**

10. Gestión de las comunicaciones y las operaciones			
10.1 Procedimientos operativos y responsabilidades			
10.1.1 Documentación de los procedimientos de operación	El gestor documental lleva la gestión de operaciones.	Si	
10.1.2 Gestión del cambio	El gestor documental lleva la gestión de operaciones.	Si	
10.1.3 Segregación de tareas	Los procesos están definidos y documentados.	Si	
10.1.4 Separación de las instalaciones de desarrollo, pruebas y producción	La gestión de desarrollo y operaciones de sistemas está documentada y se realizan los procesos.	Si	
10.2 Gestión de los servicios suministrados por terceros			
10.2.1 Prestación del servicio		No	Requerimiento ISO 27001
10.2.2 Seguimiento y revisión de servicios de terceros		No	
10.2.3 Gestión de los cambios en servicios por terceras partes		No	
10.3 Planificación y aceptación del sistema			
10.3.1 Planificación de capacidades	Existen métricas de capacidades tanto internas como externas.	Si	

10.3.2 Aceptación del sistema	Existe control de nuevas versiones.	Si	
10.4 Protección frente a código malicioso y código móvil			
10.4.1 Medidas de control contra códigos maliciosos	Todos los equipos con antivirus.	Si	
10.4.2 Medidas de control contra software móvil	Existe control de acceso a la instalación de aplicaciones.	Si	
10.5 Copias de seguridad			
10.5.1 Copia de seguridad de la información	Control completo de las copias de seguridad y pruebas de restauración.	Si	
10.6 Gestión de la seguridad de la red			
10.6.1 Controles de red	Existe monitorización.	Si	
10.6.2 Seguridad de los servicios de la red	Existe monitorización.	Si	
10.7 Gestión de los soportes			
10.7.1 Gestión de los soportes extraíbles		No	Requerimiento legal
10.7.2 Retirada de los soportes		No	Requerimiento legal
10.7.3 Procedimientos para la utilización de la información		No	Requerimiento legal

10.7.4 Seguridad de la documentación del sistema		No	Requerimiento legal
10.8 Intercambio de información			
10.8.1 Políticas y procedimientos para el intercambio de la información	Existen procedimientos para el envío de información y procesos telemáticos.	Si	
10.8.2 Acuerdos para el intercambio		Si	
10.8.3 Soportes físicos en tránsito	La información utiliza medidas de seguridad.	Si	Requerimiento legal
10.8.4 Mensajería electrónica	El correo electrónico se gestiona desde la propia empresa.	Si	
10.8.5 Sistemas de información	Los diferentes sistemas como Sharepoint, SQL Server y otros incorporan medidas de seguridad.	Si	
10.9 Servicios de comercio electrónico			
10.9.1 Comercio electrónico		N/A	
10.9.2 Transacciones en línea		N/A	
10.9.3 Información disponible al público		N/A	
10.10 Seguimiento			

10.10.1 Registro de auditorías	Los sistemas disponen de registros.	Si	Requerimiento legal e ISO
10.10.2 Seguimiento del uso de los sistemas	Se revisan los registros del sistema	Si	
10.10.3 Protección de la información del registro	Existe un control de acceso a los registros.	Si	Requerimiento legal e ISO
10.10.4 Registros del administrador y del operador	Todos los sistemas tienen activado el control de registros.	Si	Requerimiento legal e ISO
10.10.5 Registro de fallas	Se analizan los registros de errores.	Si	
10.10.6 Sincronización de relojes	Todos los equipos están sincronizados.	Si	

Objetivos	**Observaciones**	**Cumple**	**Justificación**
11. Control de accesos			
11.1 Requisitos de negocio para el control de acceso			
11.1.1 Política de control de acceso	Existe y está documentada.	Si	Requerimiento ISO 27001
11.2 Gestión del acceso de los usuarios			
11.2.1 Registro de usuarios		No	Requerimiento legal
11.2.2 Gestión de privilegios	Se gestiona pero no se documenta.	Parcial	Requerimiento legal
11.2.3 Gestión de contraseñas para usuario	Existe política de gestión de contraseñas.	Si	Requerimiento legal

11.2.4 Revisión de los derechos de acceso de los usuarios	Se revisa cada cierto tiempo no estipulado.	Parcial	
11.3 Responsabilidad de los usuarios			
11.3.1 Uso de contraseñas	Se gestiona de forma automática.	Si	
11.3.2 Equipo de usuario desatendido	Existen procesos de bloqueos en todos los equipos.	Si	
11.3.3 Política de puesto de trabajo desatendido y bloqueo de pantalla		No	
11.4 Control de acceso a la red			
11.4.1 Política de uso de los servicios de red	Los usuarios no pueden acceder a recursos no asignados.	Si	Requerimiento ISO 27001
11.4.2 Autenticación de usuarios para conexiones externas	Acceso remoto controlado.	Si	
11.4.3 Identificación de los equipos en las redes		N/A	
11.4.4 Protección de los puertos de configuración y diagnóstico remoto		Si	

11.4.5 Separación en las redes	Existen métodos de control de acceso.	Si	
11.4.6 Control de conexión a las redes	Existen métodos de control de acceso.	Si	
11.4.7 Control de enrutamiento en la red	Existen métodos de control de enrutamiento.	Si	
11.5 Control de acceso al sistema operativo			
11.5.1 Procedimientos de conexión segura	Se dispone de contraseñas de acceso.	Si	
11.5.2 Identificación y autenticación de usuarios		Si	
11.5.3 Sistema de gestión de contraseñas	La gestión de cambio y complejidad de contraseñas se realiza de forma remota.	Si	
11.5.4 Uso de los servicios del sistema	Restringido.	Si	
11.5.5 Desconexión automática de sesión	Restringido.	Si	
11.5.6 Limitación del tiempo de conexión		No	
11.6 Control de acceso a información y aplicaciones			
11.6.1 Restricción de acceso a la información	Restricción a nivel de aplicación.	Si	

11.6.2 Aislamiento de sistemas sensibles		No	
11.7 Informática móvil y teletrabajo			
11.7.1 Informática y comunicaciones móviles	No están permitidos los accesos inalámbricos.	N/A	
11.7.2 Teletrabajo	No se contempla en el alcance.	N/A	

Objetivos	**Observaciones**	**Cumple**	**Justificación**
12. Adquisición, desarrollo y mantenimiento			
12.1 Requisitos de seguridad en los sistemas de información			
12.1.1 Análisis y especificación de los requisitos de seguridad		No	Requerimiento ISO 27001
12.2 Procesamiento correcto de las aplicaciones			
12.2.1 Validación de los datos de entrada	No se utilizan sistemas empresariales en sistemas y desarrollo.	N/A	
12.2.2 Control de procesamiento interno	No se utilizan sistemas empresariales en sistemas y desarrollo.	N/A	
12.2.3 Integridad del mensaje	No se utilizan sistemas empresariales en sistemas y desarrollo.	N/A	
12.2.4 Validación de los datos de salida	No se utilizan sistemas empresariales en sistemas y desarrollo.	N/A	
12.3 Controles criptográficos			

12.3.1 Política sobre el uso de controles criptográficos	Se utiliza controles para la comunicación de los sistemas con los proveedores cloud (PGP,VPN,SSL).	Si	
12.3.2 Gestión de claves	Las claves de los controles criptográficos se almacenan y gestionan.	Si	
12.4 Seguridad en los ficheros del sistema			
12.4.1 Control del software en producción	Existen controles.	Si	
12.4.2 Protección de los datos de prueba del sistema	Existe un ciclo de desarrollo de software.	Si	
12.4.3 Control de acceso al código fuente de los programas	Se gestiona todo el proceso.	Si	
12.5 Seguridad en los procesos de desarrollo y soporte			
12.5.1 Procedimientos de control de cambios	Existe un ciclo de desarrollo de software.	Si	Requerimiento ISO
12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	Se gestiona todo el proceso.	Si	
12.5.3 Restricciones en los cambios a los paquetes de software	Se gestiona todo el proceso.	Si	

12.5.4 Fuga de información		No	
12.5.5 Desarrollo de software contratado externamente		N/A	
12.6 Gestión de vulnerabilidades técnicas			
12.6.1 Control de vulnerabilidades técnicas	Se realizan test periódicamente.	Si	

Objetivos	**Observaciones**	**Cumple**	**Justificación**
13. Gestión de incidentes de seguridad			
13.1 Comunicación de eventos y debilidades			
13.1.1 Comunicación de eventos de seguridad de la información		No	
13.1.2 Comunicación de las debilidades de seguridad		No	
13.2 Gestión de incidencias			
13.2.1 Responsabilidades y procedimientos		No	
13.2.2 Aprendizaje debido a los incidentes de seguridad de la información		No	

13.2.3 Recogida de pruebas		No	Requerimiento legal

Objetivos	Observaciones	Cumple	Justificación
14. Gestión de la continuidad de negocio			
14.1 Aspectos de la seguridad de la información			
14.1.1 Inclusión de la seguridad de la inf. En el proceso de gestión de la continuidad del negocio		No	Requerimiento legal e ISO
14.1.2 Continuidad del negocio y evaluación de riesgos		No	Requerimiento legal e ISO
14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la inf.		No	Requerimiento legal e ISO
14.1.4 Marco de planificación de la continuidad del negocio		No	Requerimiento legal e ISO

14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio		No	Requerimiento legal e ISO

Objetivos	**Observaciones**	**Cumple**	**Justificación**
15. Conformidad			
15.1 Conformidad de los requisitos legales			
15.1.1 Identificación de legislación aplicable		No	Requerimiento legal
15.1.2 Derechos de propiedad intelectual		No	Requerimiento legal
15.1.3 Protección de los registros de la organización	Se gestionan de manera correcta.	Si	Requerimiento legal
15.1.4 Protección de los datos y privacidad de la información personal	Administración cumple con los requisitos.	Si	Requerimiento legal
15.1.5 Prevención del uso inadecuado de los dispositivos de tratamiento de la información		Si	Requerimiento legal

15.1.6 Regulación de los controles criptográficos	Se utiliza sistemas VPN, PGP, SSL en las comunicaciones.	Si	Requerimiento legal
15.2 Conformidad con políticas y normas de seguridad			
15.2.1 Conformidad con políticas y normas de seguridad	No siempre se realizan los controles establecidos.	Parcial	
15.2.2 Comprobación de la confirmidad técnica	Los sistemas empresariales disponen de documentación de cumplimiento.	Si	
15.3 Consideraciones sobre la auditoría			
15.3.1 Controles de auditoría de los sistemas de información	Las auditorias se planifican y registran.	Si	
15.3.2 Protección de las herramientas de auditoría de los sistemas de información	Existen controles de acceso.	Si	Requerimiento ISO 27001

Después de realizar el GAP Analysis podemos decir que nuestra empresa cumple con el 51.12 % de los requisitos en 68 controles, no cumple con el 33.08 % en 44 controles y sólo cumple de manera parcial en el 6 % de los casos.

Capítulo 7

Definición de la política de seguridad

7.1. Política de seguridad

Dentro de este apartado debemos decidir los criterios a seguir para que la confidencialidad, integridad y disponibilidad estén garantizados. La política de seguridad es un conjunto de normas y procedimientos de obligado cumplimiento para el tratamiento de los riesgos de seguridad empresariales. Nuestra empresa Treval entiende los riesgos que conlleva la seguridad de la información y por eso ha decidido implantar el SGSI basado en ISO 27001.

Todos los empleados de la organización deben de conocer, aceptar y cumplir dichas normas incluidos los que tengan una relación temporal así como clientes y proveedores que hagan uso de los sistemas o herramientas de la empresa. Este apartado corresponde con el **Documento de políticas de seguridad** de la norma.

7.2. Objetivos

Los objetivos que persigue Treval en la definición de la política de seguridad:

1. La información con la que trabaja Treval a través de sus procesos internos y externos es un aspecto muy importante dentro de la organización, por lo cual deben de tomarse las medidas que sean necesarias para garantizar su seguridad.

2. Todos los trabajadores y empleados externos a la empresa deben de conocer y aplicar las medidas de seguridad necesarias para asegurar la protección de la información.

3. Definir las responsabilidades de las personas dentro del marco de seguridad empresarial.

4. Definir e implementar sistemas de gestión de riesgos para impedir los problemas derivados de incidentes de seguridad.

5. Establecer los mecanismos legales que tenga que tomar la empresa para hacer cumplir la normativa de seguridad.

7.3. Alcance

Esta política de seguridad afecta a toda la información de la empresa, incluidos los sistemas de comunicaciones que sustentan la transferencia de información así como los aplicativos que la manipulan. Todos los empleados internos y externos que utilicen estos sistemas de información quedan incluidos en las políticas.

7.4. Políticas de seguridad

Las políticas de seguridad son las directrices y declaraciones de principios que seguirá la organización en materia de seguridad y se enumeran a continuación.

7.4.1. Referente al SGSI

- El documento de política del SGSI deberá ser aprobado por la dirección y publicado y comunicado a todos los empleados y terceras partes.
- La política de seguridad de la información se debería revisar con planificación o en el caso que se produzcan cambios significativos para asegurar la idoneidad, adecuación y la eficacia de la continuidad.

7.4.2. Organización

- Se debe definir todas las responsabilidades de la seguridad de la información.
- Debería de definirse e implantarse un proceso de autorización para la gestión de los nuevos recursos de información.
- Mantener contactos con las autoridades en cuanto a continuidad de negocio.
- Mantener contactos con grupos de interés especializados en seguridad de la información.
- Revisar de manera independiente los controles sobre seguridad de la información.

7.4.3. Gestión de activos

- La información debe estar clasificada según su valor, requisitos legales y criticidad para la organización.
- Desarrollar procedimientos para tratar la información según el esquema de clasificación de la organización.

7.4.4. Recursos humanos

- Todos los empleados internos y externos deberán recibir una formación adecuada y actualizada referente a las políticas y procedimientos de seguridad.
- Debe existir un proceso disciplinario para aquellos empleados que hayan provocado brechas de seguridad.

7.4.5. Seguridad física y del entorno

- Deberán de utilizarse sistemas perimetrales de seguridad para proteger las áreas correspondientes.
- Utilizar controles de entrada en las áreas críticas de la organización.
- Diseñar y aplicar medidas y procesos para daño por fuego, inundación y otros desastres naturales.
- Proteger los equipos de amenazas de seguridad y accesos no autorizados.
- Aplicar medidas de seguridad para los equipos utilizados fuera del lugar de trabajo.
- Todos los medios extraíbles deben ser comprobados antes de utilizar que no contienen o almacenan información sensible.
- No utilizar equipos e información fuera de la organización sin autorización previa.

7.4.6. Comunicaciones y operaciones

- Comprobar que los controles de seguridad y niveles de entrega se implantan y son mantenidos.
- Gestionar los cambios en la provisión de servicios incluido el mantenimiento y mejora de políticas.
- Crear procedimientos para soportes desmontables.
- Procedimientos para deshacerse de soportes desmontables.
- El sistema de documentación debe estar protegido de accesos no autorizados.

7.4.7. Control de accesos

- Procedimiento de registro formal de usuarios para conceder y revocar accesos a todos los sistemas.
- Adoptar política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables.
- Utilizar políticas de tiempo máximo de conexión a aplicaciones y sistemas críticos.
- Los sistemas sensibles deben de tener un entorno de ordenadores aislado.

7.4.8. Adquisición, desarrollo y mantenimiento

- Cuando se cambien los sistemas operativos deben revisarse las aplicaciones empresariales críticas para no existan efectos adversos.
- Debe evitarse la fuga de información.

7.4.9. Gestión de incidentes

- Los eventos de seguridad deben comunicarse de manera adecuada lo antes posible.
- Cualquier empleado interno o externo deberá anotar y comunicar brechas y debilidades en los sistemas de información.
- Definir las responsabilidades para la gestión de incidencias de información.
- Definir mecanismos para cuantificar los incidentes.
- Cuando un incidente de seguridad implique acciones legales deberán de recopilarse pruebas para conservarlas y utilizarlas posteriormente.

7.4.10. Continuidad de negocio

- Crear sistema de continuidad de negocio en toda la organización.
- Identificar eventos que provoquen interrupciones en los procesos de negocio y evaluarlos.
- Crear planes para asegurar la continuidad de los procesos.
- Mantener un único marco de referencia para la gestión de continuidad de negocio.
- Los planes de continuidad de negocio deben probarse y actualizarse.

7.4.11. Conformidad

- Todos los requisitos tanto legales como reglamentarios deben definirse, documentarse y mantenerse actualizados.
- Definir métodos y procesos para garantizar el cumplimiento de los requisitos legales.

Capítulo 8

Definición del enfoque del análisis de riesgo

Una de las tareas más difíciles en la evaluación de riesgos es la elección del enfoque para la elección de la metodología para el análisis de riesgos. Dicho enfoque persigue que la metodología esté alineada con los objetivos y políticas de dirección, estrategias de negocio y seguridad e la organización, y debe ser capaz de analizar procesos complejos y reducirlos a otros de fácil compresión.

Existen muchas metodologías de análisis de riesgo y aplicaciones que las soportan, la norma ISO 27001 no indica cual utilizar por lo que siguiendo la normativa nacional utilizaremos Magerit[1].

Magerit es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, además es posible también el uso de Pilar[2] que es una herramienta que implementa dicha metodología, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española.

[1]Revisión de la norma en administracionelectronica.gob.es
[2]Se puede descargar en www.ccn-cert.cni.es

Capítulo 9

Análisis de riesgos

9.1. Inventario de activos

Procedemos a identificar a los activos que están implicados en el alcance, así como sus propietarios, personas o entidades encargadas de controlar el activo en todo su ciclo de vida y garantizar su seguridad pero no tiene por qué tener el derecho de propiedad sobre este. Este apartado corresponde con el documento **Inventario de activos** de la norma.

Tabla 9.1: Inventario de activos.

Activo	**Descripción**	**Categoría**	**Ubicación**	**Propietario**
Personal	Técnico y de responsabilidad den desarrollo y sistemas	Personal	Dirección	Dirección
Documentación	Toda la documentación en papel	Soporte	Dirección	Dirección
Equipos PC	PC	Hardware	Desarrollo	Responsable de desarrollo
Servidores de Sistemas	Servidores que contiene los servicios de desarrollo, gestión, bases de datos y aplicaciones	Hardware	Sala de servidor	Responsable de Sistemas
Router	Dispositivo de enrutamiento	Hardware	Sala de servidor	Responsable de Sistemas
Cortafuegos	Sistemas IDS de seguridad	Hardware	Sala de servidor	Responsable de Sistemas
Impresoras	Multifunción	Hardware	Oficina principal	Responsable de Sistemas
Servicios cloud	Servicios de aplicativos a clientes	Servicios	Sistemas	Responsable de Sistemas

Datos de desarrollo	Control de código fuente, versiones, bases de datos, etc	Datos	Sistemas	Responsable de Sistemas
Correo electrónico	Datos de Mail	Datos	Sistemas	Responsable de Sistemas
Claves digitales	VPN, PGP, SSL, etc	Claves criptográficas	Sistemas	Responsable de Sistemas
S.O	Sistemas operativos	Aplicación	Sistemas	Responsable de Sistemas
Antivirus	Sistemas de seguridad	Aplicación	Sistemas	Responsable de Sistemas
App. de desarrollo	Software privativo de desarrollo	Aplicación	Sistemas	Responsable de Sistemas
Switch	Armario para toda la empresa	Hardware	Sistemas	Responsable de Sistemas
Backup	Sistemas de backup	Auxiliar	Sistemas	Responsable de Sistemas
Internet	Conexión a internet	Redes	Sistemas	Responsable de Sistemas
Red ethernet	Red de comunicación de la empresa	Redes	Sistemas	Responsable de Sistemas
CPD empresa	Sistema con SAI, sistema antiincendios, etc	Instalaciones	Sistemas	Responsable de Sistemas

9.2. Valoración de activos

Se valorarán los activos según una escala de puntuación de 0 (no aplicable/sin valor) a 4 (mucho valor). La valoración total será la suma aritmética de los cuatro valores. Este apartado corresponde con el documento **Valoración de activos** de la norma. La valoración de los activos en confidencialidad, integridad y disponibilidad quedaría de la siguiente manera:

Tabla 9.3: Valoración de activos.

Activo	**Conf.**	**Int.**	**Disp.**	**Total**
Servidores de Sistemas	2	3	4	**9**
Router	1	1	4	**6**
Cortafuegos	1	1	4	**6**
Equipos PC de desarrollo	1	2	3	**6**
Impresoras	1	1	4	**6**
Servicios cloud	2	4	4	**10**
Datos de desarrollo	4	4	1	**9**
Correo electrónico	4	4	2	**10**
Claves digitales	4	4	1	**9**
S.O	2	2	2	**6**
Antivirus	2	2	3	**6**
App. de desarrollo	2	2	2	**6**
Switch	1	1	4	**6**
Backup	3	3	3	**9**
Documentación	4	2	1	**7**
Internet	3	3	3	**9**
Red ethernet	3	3	3	**9**
CPD empresa	4	4	4	**12**
Personal	1	2	3	**6**

9.3. Identificación de amenazas

Procederemos a identificar las amenazas que pueden afectar a nuestros activos. Una amenaza es cualquier acción o acontecimiento que puede atentar contra nuestra seguridad. Las amenazas pueden ser de distintos tipos. El siguiente listado corresponde a un ejemplo del catálogo de amenazas de Magerit:

- Fuego.
- Daños por agua.
- Desastres naturales.
- Fuga de información.
- Introducción de falsa información.
- Alteración de la información.
- Corrupción de la información.
- Destrucción de información.
- Interceptación de información (escucha).
- Corte del suministro eléctrico.

- Condiciones inadecuadas de temperatura o humedad.
- Fallo de servicios de comunicaciones.
- Interrupción de otros servicios y suministros esenciales.
- Desastres industriales.
- Degradación de los soportes de almacenamiento de la información.
- Difusión de software dañino.
- Errores de mantenimiento / actualización de programas (software).
- Errores de mantenimiento / actualización de equipos (hardware).
- Caída del sistema por sobrecarga.
- Pérdida de equipos.
- Indisponibilidad del personal.
- Abuso de privilegios de acceso.
- Acceso no autorizado.
- Errores de los usuarios.
- Errores del administrador.
- Errores de configuración.
- Denegación de servicio.
- Robo.
- Indisponibilidad del personal.
- Extorsión Ingeniería social.

9.4. Valoración de riesgos por activo

El **nivel de riesgo** viene dado por el valor más alto para cada activo de:

Nivel de amenaza x Nivel de vulnerabilidad x Nivel de impacto

Tanto el nivel de vulnerabilidad como el nivel de amenaza se valorarán de 0 a 3 (no aplicado, bajo medio y alto). Debemos de calcular de cada activo para cada amenaza, para evitar poner todos los cálculos ya que el nivel de riesgo de cada activo de todas las amenazas posibles es bastante amplio se escogerá el valor más alto del cálculo de todas la amenazas. Este apartado resumido correspondería con el documento **Análisis de riesgos**

de la norma y el resultado de aquellos que superen el umbral formarían el documento de **Tratamiento de riesgos**.

Tabla 9.4: Tratamiento de riesgos.

Activo	**Amenaza**	**Impacto**	**Nivel de amenaza**	**Vulne.**	**Nivel de riesgo**
Servidores de Sistemas	Errores de usuario	9	2	3	54
Router	Fallo de comunicaciones	6	3	3	54
Cortafuegos	Fallo de comunicaciones	6	3	3	54
Equipos PC de desarrollo	Errores de usuario	6	2	3	36
Impresoras	Error de mantenimiento	6	2	2	24
Servicios cloud	Fallo de comunicaciones	10	3	2	60
Datos de desarrollo	Robo	9	3	3	81
Correo electrónico	Fallo de comunicaciones	10	2	2	40
Claves digitales	Robo	9	2	3	45
S.O	Error de mantenimiento	6	2	3	36
Antivirus	Error de mantenimiento	6	2		36
App. de desarrollo	Fallo de software	6	3	3	54
Switch	Fallo de comunicaciones	6	2	2	24
Backup	Errores de usuario	9	2	2	36
Documentación	Fuego	7	2	2	28

Internet	Fallo de comunicaciones	9	2	3	54
Red ethernet	Fallo de comunicaciones	9	2	2	36
CPD empresa	Fuego	12	2	3	72
Personal	Errores de usuario	6	3	3	54

9.5. Aceptación de dirección

Una vez hecho el análisis de riesgos se establece un valor de riesgo aceptable en 50 de manera que los activos que igualen o superen esta cifra serían los que se les aplicaría los controles de la norma. Los demás riesgos serán asumidos por la empresa ya que los riesgos están pendientes de aplicar y es la dirección quién debe de aprobar su implantación. De cualquier manera, se aplicarán los controles mínimos definidos en la declaración de aplicabilidad.

9.6. Declaración de aplicabilidad

A continuación elaboramos el documento de aplicabilidad que es el resumen de las decisiones que se han tomado en al análisis de riesgos. A diferencia del análisis diferencial estos controles son los elegidos para implementar de la norma ISO 27001 e incluyen los que ya están implementados en la organización. Este apartado corresponde con el documento **Declaración de aplicabilidad** de la norma.

Tabla 9.6: Declaración de aplicabilidad.

Objetivos	**Aplicable**	**Justificación**
5 Política de seguridad		
5.1 Política de seguridad de la información		
5.1.1 Documento de política de seguridad de la información	Aplicar	Requerimiento ISO 27001
5.1.2 Revisión de la política de seguridad de la información	Aplicar	Requerimiento ISO 27001

Objetivos	Aplicable	Justificación
6. Organización de la seguridad de la Información		
6.1 Organización interna		
6.1.1 Compromiso de la dirección con la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.2 Coordinación de la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.3 Asignación de responsabilidades para la seguridad de la información	Aplicar	Requerimiento ISO 27001
6.1.4 Procesos de autorización para los servicios de procesamiento de información	Aplicar	La dirección debe de gestionar los nuevos recursos.
6.1.5 Acuerdos sobre confidencialidad	Aplicado	Requerimiento legal
6.1.6 Contacto con las autoridades	Aplicar	Requerimiento legal e ISO
6.1.7 Contacto con grupos de interés especiales	Aplicar	La dirección y los responsables deben de mantener contactos con grupos de interés.

6.1.8 Revisión independiente de la seguridad de la información	Aplicar	Requerimiento legal e ISO
6.2 Terceras partes		
6.2.1 Identificación de los riesgos relacionados con las partes externas	Aplicado	El departamento de RRHH contempla este punto.
6.2.2 Consideraciones de la seguridad cuando se trata con los clientes	Aplicado	El departamento de RRHH contempla este punto.
6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes	Aplicado	El departamento de RRHH contempla este punto.

Objetivos	**Aplicable**	**Justificación**
7. Gestión de activos		
7.1 Responsabilidad de los activos		
7.1.1 Inventario de activos	Aplicado	Requerimiento ISO 27001
7.1.2 Propiedad de los activos	Aplicado	Requerimiento ISO 27001
7.1.3 Uso aceptable de los activos	Aplicado	Requerimiento ISO 27001
7.2 Clasificación de la información		

7.2.1 Directrices de clasificación	Aplicar	Requerimiento ISO 27001
7.2.2 Etiquetado y manejo de información	Aplicar	Requerimiento ISO 27001

Objetivos	**Aplicable**	**Justificación**
8. Seguridad de la gestión de los recursos humanos		
8.1 Seguridad en actividades previas a la contratación		
8.1.1 Roles y responsabilidades	Aplicado	Requerimiento ISO 27001
8.1.2 Análisis y selección	Aplicado	El departamento de RRHH contempla este punto.
8.1.3 Términos y condiciones de empleo	Aplicado	El departamento de RRHH contempla este punto.
8.2 Seguridad durante el desempeño de funciones		
8.2.1 Responsabilidad de la dirección	Aplicado	El departamento de RRHH contempla este punto.
8.2.2 Educación, formación y concientización sobre la seguridad de la información	Aplicar	La empresa debe de formar al personal.
8.2.3 Proceso disciplinario	Aplicar	El departamento de RRHH debe de crear un procedimiento para estos casos.
8.3 Finalización o cambio de empleo		
8.3.1 Responsabilidadades de fin de contrato	Aplicado	El departamento de RRHH contempla este punto.

8.3.2 Restitución de activos	Aplicado	El departamento de RRHH contempla este punto.
8.3.3 Eliminación de derechos de acceso	Aplicado	El departamento de RRHH contempla este punto.

Objetivos	**Aplicable**	**Justificación**
9. Seguridad física y del entorno		
9.1 Áreas seguras		
9.1.1 Perímetro de seguridad física	Aplicar	Deben de existir controles físicos de entrada.
9.1.2 Controles de acceso físico	Aplicar	Deben de existir controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos y recursos	Aplicar	Asegurar las oficinas de acuerdo a la actividad de la organización.
9.1.4 Protección contra amenazas externas y ambientales	Aplicar	Asegurar las oficinas de acuerdo a la actividad de la organización.
9.1.5 Trabajo en áreas seguras	Aplicar	Deben de existir controles físicos para áreas seguras.
9.1.6 Áreas de carga y acceso público	Aplicado	Existen los controles.
9.2 Seguridad de los equipos		

9.2.1 Instalación y protección de los equipos	Aplicar	Existen equipos que deben protegerse.
9.2.2 Servicios de suministro	Aplicado	Existen equipos que deben protegerse.
9.2.3 Seguridad del cableado	Aplicado	El armario de comunicaciones debe protegerse.
9.2.4 Mantenimiento de los equipos	Aplicado	Existen equipos que deben mantenerse.
9.2.5 Seguridad de los equipos fuera de las instalaciones	No	No se contempla el control de sistemas fuera de la empresa.
9.2.6 Seguridad en la reutilización o eliminación de los equipos	Aplicar	Requerimiento ISO 27001
9.2.7 Traslado de activos fuera de la organización	No	No se contempla el control de sistemas fuera de la empresa.

Objetivos	**Aplicable**	**Justificación**
10. Gestión de las comunicaciones y las operaciones		
10.1 Procedimientos operativos y responsabilidades		
10.1.1 Documentación de los procedimientos de operación	Aplicado	Existen procedimientos documentados.
10.1.2 Gestión del cambio	Aplicado	Existe gestión de cambios.

10.1.3 Segregación de tareas	Aplicado	El personal conoce sus funciones.
10.1.4 Separación de las instalaciones de desarrollo, pruebas y producción	Aplicado	Existe separación de entornos.
10.2 Gestión de los servicios suministrados por terceros		
10.2.1 Prestación del servicio	Aplicar	Requerimiento ISO 27001
10.2.2 Seguimiento y revisión de servicios de terceros	Aplicar	Se deben de controlar y revisar los servicios a terceros.
10.2.3 Gestión de los cambios en servicios por terceras partes	Aplicar	Se deben de controlar y revisar la gestión de cambios a terceros.
10.3 Planificación y aceptación del sistema		
10.3.1 Planificación de capacidades	Aplicado	Se gestiona la capacidad.
10.3.2 Aceptación del sistema	Aplicado	Se gestionan los sistemas.
10.4 Protección frente a código malicioso y código móvil		
10.4.1 Medidas de control contra códigos maliciosos	Aplicado	Se dispone de antivirus.

10.4.2 Medidas de control contra software móvil	Aplicado	Se dispone de antivirus.
10.5 Copias de seguridad		
10.5.1 Copia de seguridad de la información	Aplicado	Se dispone de sistema de copias.
10.6 Gestión de la seguridad de la red		
10.6.1 Controles de red	Aplicado	Sistemas de control de redes.
10.6.2 Seguridad de los servicios de la red	Aplicado	Se monitoriza el tráfico con sistemas IDS.
10.7 Gestión de los soportes		
10.7.1 Gestión de los soportes extraíbles	Aplicar	Requerimiento legal
10.7.2 Retirada de los soportes	Aplicar	Requerimiento legal
10.7.3 Procedimientos para la utilización de la información	Aplicar	Requerimiento legal
10.7.4 Seguridad de la documentación del sistema	Aplicar	Requerimiento legal
10.8 Intercambio de información		

10.8.1 Políticas y procedimientos para el intercambio de la información	Aplicado	Aplicadas en correo electrónico.
10.8.2 Acuerdos para el intercambio	Aplicado	Aplicadas en correo electrónico.
10.8.3 Soportes físicos en tránsito	Aplicado	Requerimiento legal
10.8.4 Mensajería electrónica	Aplicado	Aplicadas medidas de control.
10.8.5 Sistemas de información	Aplicado	Existen medidas de control para el intercambio entre organizaciones.
10.9 Servicios de comercio electrónico		
10.9.1 Comercio electrónico	No	No se utiliza.
10.9.2 Transacciones en línea	No	No se utiliza.
10.9.3 Información disponible al público	No	No se utiliza.
10.10 Seguimiento		
10.10.1 Registro de auditorías	Aplicado	Requerimiento legal e ISO
10.10.2 Seguimiento del uso de los sistemas	Aplicado	Se realizan auditorías.

10.10.3 Protección de la información del registro	Aplicado	Requerimiento legal e ISO
10.10.4 Registros del administrador y del operador	Aplicado	Requerimiento legal e ISO
10.10.5 Registro de fallas	Aplicado	Se registran los errores.
10.10.6 Sincronización de relojes	Aplicado	Se utilizan los relojes del sistema.

Objetivos	**Aplicable**	**Justificación**
11. Control de accesos		
11.1 Requisitos de negocio para el control de acceso		
11.1.1 Política de control de acceso	Aplicado	Requerimiento ISO 27001
11.2 Gestión del acceso de los usuarios		
11.2.1 Registro de usuarios	Aplicar	Requerimiento legal
11.2.2 Gestión de privilegios	Aplicar	Requerimiento legal
11.2.3 Gestión de contraseñas para usuario	Aplicar	Requerimiento legal
11.2.4 Revisión de los derechos de acceso de los usuarios	Aplicar	Aumentar el número de revisiones de accesos.
11.3 Responsabilidad de los usuarios		
11.3.1 Uso de contraseñas	Aplicado	Se fomenta el uso de buenas prácticas.

11.3.2 Equipo de usuario desatendido	Aplicado	Se fomenta el uso de buenas prácticas.
11.3.3 Política de puesto de trabajo desatendido y bloqueo de pantalla	Aplicar	Se debería de fomentar el uso de buenas prácticas.
11.4 Control de acceso a la red		
11.4.1 Política de uso de los servicios de red	Aplicado	Requerimiento ISO 27001
11.4.2 Autenticación de usuarios para conexiones externas	Aplicado	Gestión para el control de clientes a las aplicaciones de negocio.
11.4.3 Identificación de los equipos en las redes	No	No es necesario según dirección.
11.4.4 Protección de los puertos de configuración y diagnóstico remoto	Aplicado	Restricción a usuarios.
11.4.5 Separación en las redes	Aplicado	Existe separación en las redes de la empresa.
11.4.6 Control de conexión a las redes	Aplicado	No se comparten las redes y existe un control.

11.4.7 Control de enrutamiento en la red	Aplicado	Se controla y audita periódicamente.
11.5 Control de acceso al sistema operativo		
11.5.1 Procedimientos de conexión segura	Aplicado	Sistema de acceso mediante contraseñas.
11.5.2 Identificación y autenticación de usuarios	Aplicado	Las contraseñas son robustas.
11.5.3 Sistema de gestión de contraseñas	Aplicado	Sólo los administradores tienen acceso.
11.5.4 Uso de los servicios del sistema	Aplicado	Sólo los administradores tienen acceso.
11.5.5 Desconexión automática de sesión	Aplicado	Las sesiones se cierran automáticamente.
11.5.6 Limitación del tiempo de conexión	No	No es necesario este control.
11.6 Control de acceso a información y aplicaciones		
11.6.1 Restricción de acceso a la información	Aplicado	Existe un control de acceso a la información.
11.6.2 Aislamiento de sistemas sensibles	No	El coste es elevado para todos los equipos.
11.7 Informática móvil y teletrabajo		

11.7.1 Informática y comunicaciones móviles	No	No es necesario este control.
11.7.2 Teletrabajo	No	No es necesario este control.

Objetivos	**Aplicable**	**Justificación**
12. Adquisición, desarrollo y mantenimiento		
12.1 Requisitos de seguridad en los sistemas de información		
12.1.1 Análisis y especificación de los requisitos de seguridad	Aplicar	Requerimiento ISO 27001
12.2 Procesamiento correcto de las aplicaciones		
12.2.1 Validación de los datos de entrada	No	No es necesario este control.
12.2.2 Control de procesamiento interno	No	No es necesario este control.
12.2.3 Integridad del mensaje	No	No es necesario este control.
12.2.4 Validación de los datos de salida	No	No es necesario este control.
12.3 Controles criptográficos		
12.3.1 Política sobre el uso de controles criptográficos	Aplicado	Se utilizan sistemas de cifrado.
12.3.2 Gestión de claves	Aplicado	Se gestionan como información sensible.

12.4 Seguridad en los ficheros del sistema		
12.4.1 Control del software en producción	Aplicado	Sólo los administradores tienen acceso.
12.4.2 Protección de los datos de prueba del sistema	Aplicado	Existen controles de protección como sistemas de control de versiones.
12.4.3 Control de acceso al código fuente de los programas	Aplicado	Existen controles de protección como sistemas de control de versiones.
12.5 Seguridad en los procesos de desarrollo y soporte		
12.5.1 Procedimientos de control de cambios	Aplicado	Requerimiento ISO
12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	Aplicado	Se realizan controles.
12.5.3 Restricciones en los cambios a los paquetes de software	Aplicado	Se realizan controles.
12.5.4 Fuga de información	Aplicar	Se debería formar al personal.

12.5.5 Desarrollo de software contratado externamente	No	El software se desarrolla en la empresa y no se externaliza.
12.6 Gestión de vulnerabilidades técnicas		
12.6.1 Control de vulnerabilidades técnicas	Aplicado	Se realizan test de control.

Objetivos	**Aplicable**	**Justificación**
13. Gestión de incidentes de seguridad		
13.1 Comunicación de eventos y debilidades		
13.1.1 Comunicación de eventos de seguridad de la información	Aplicar	Requerimiento legal
13.1.2 Comunicación de las debilidades de seguridad	Aplicar	Requerimiento legal
13.2 Gestión de incidencias		
13.2.1 Responsabilidades y procedimientos	Aplicar	Requerimiento legal
13.2.2 Aprendizaje debido a los incidentes de seguridad de la información	Aplicar	Requerimiento legal
13.2.3 Recogida de pruebas	Aplicar	Requerimiento legal

Objetivos	Aplicable	Justificación
14. Gestión de la continuidad de negocio		
14.1 Aspectos de la seguridad de la información		
14.1.1 Inclusión de la seguridad de la inf. En el proceso de gestión de la continuidad del negocio	Aplicar	Requerimiento legal e ISO
14.1.2 Continuidad del negocio y evaluación de riesgos	Aplicar	Requerimiento legal e ISO
14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la inf.	Aplicar	Requerimiento legal e ISO
14.1.4 Estructura para la planificación de la continuidad del negocio	Aplicar	Requerimiento legal e ISO
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Aplicar	Requerimiento legal e ISO

Objetivos	Aplicable	Justificación

15. Conformidad		
15.1 Conformidad de los requisitos legales		
15.1.1 Identificación de legislación aplicable	Aplicar	Requerimiento legal
15.1.2 Derechos de propiedad intelectual	Aplicar	Requerimiento legal
15.1.3 Protección de los registros de la organización	Aplicado	Requerimiento legal
15.1.4 Protección de los datos y privacidad de la información personal	Aplicado	Requerimiento legal
15.1.5 Prevención del uso inadecuado de los dispositivos de tratamiento de la información	Aplicado	Requerimiento legal
15.1.6 Regulación de los controles criptográficos	Aplicado	Requerimiento legal
15.2 Conformidad con políticas y normas de seguridad		
15.2.1 Conformidad con políticas y normas de seguridad	Aplicado	Se realizan de forma periódica.

15.2.2 Comprobación de la confirmidad técnica	Aplicado	Se realizan de forma periódica.
15.3 Consideraciones sobre la auditoría		
15.3.1 Controles de auditoría de los sistemas de información	Aplicado	Se realizan de forma periódica.
15.3.2 Protección de las herramientas de auditoría de los sistemas de información	Aplicado	Requerimiento ISO 27001

Parte III

Implantación

Capítulo 10

Plan de tratamiento de riesgos

En esta etapa definiremos como se implementarán los controles del documento de aplicabilidad, se asignarán responsables y los recursos. Las prioridades en la gestión de los riesgos deben quedar especificadas. A continuación y utilizando como base el documento de **Declaración de aplicabilidad** el responsable de seguridad desarrollará el plan de tratamiento para Treval que corresponde al documento **Plan de tratamiento de riesgo**.

10.1. Plan de políticas de seguridad de la Información

Descripción

Corresponde al apartado 5 sobre las políticas de seguridad.

Objetivos

1. Documentos de políticas de seguridad de la información.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

La directiva junto a los responsables de departamentos de desarrollo y sistemas crearán y revisarán las diferentes políticas de seguridad, estas políticas afectarán no sólo a los departamentos de Treval también lo harán a los proveedores y clientes externos. Como responsable y coordinador del SGSI se nombrará a un consultor externo que ayudará en todas las etapas del proceso.

Todas las políticas creadas se publicarán y comunicarán a todo el personal afectado, los responsables de departamento serán los responsables de la difusión. Se creará un repositorio para almacenar la documentación utilizando el servidor ECM Sharepoint, los responsables de los departamentos serán los encargados de dar los accesos al repositorio de la documentación del SGSI.

Presupuesto

Tabla 10.1: Presupuesto de políticas de seguridad de la Información.

Descripción	Coste	Unidades	Subtotal
Horas de personal	30	20	600
		Total	2.000

10.2. Plan de la organización de la seguridad de la información

Descripción

Corresponde al apartado 6 sobre organización de la seguridad de la información.

Objetivos

1. Conseguir el compromiso de la dirección.
2. Coordinación departamental.
3. Roles y responsabilidades.
4. Procesos de autorizaciones.
5. Cooperación con las autoridades.
6. Contactos con grupos de interés.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

El gerente tendrá reuniones semanales o quincenales con los responsables de los departamentos en las cuales se tratarán temas relacionados con la seguridad, se propondrán ideas para la mejora o modificación de las políticas y se incentivarán medidas al resto del personal. Se adoptará por parte de la empresa un sistema de mejora por parte de los departamentos de desarrollo y sistemas para el control y registro de los sistemas de información y de los canales de comunicación respecto a las políticas de seguridad.

Se creará un puesto específico en el departamento de sistemas para el control y desarrollo de los sistemas de comunicación de la empresa tanto internos (red, cortafuegos, etc) como externos (internet y cloud). Esta persona será la responsable junto a los proveedores de comunicaciones de asegurar el funcionamiento y seguridad de los mismos. Este responsable estudiará las posibles inversiones en nuevos dispositivos con mejoras en la seguridad, el

dispositivo que se actualizará en la implantación será el router de comunicaciones que gestiona la seguridad de acceso a internet y que no cumple con las exigencias del responsable de proyecto.

Los responsables de departamentos y gerencia crearán vías de comunicación con cuerpos de seguridad a través de reuniones, colaboraciones y cursos de formación. La empresa además fomentará entre los empleados, sobre todo el responsable de sistemas de comunicación, el contacto y comunicación con grupos **reconocidos** en el ámbito de la seguridad.

Presupuesto

Tabla 10.2: Presupuesto de la organización de la seguridad de la información.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de personal	30	20	600
Router	1.000	1	1.000
		Total	1.600

10.3. Plan de gestión de activos

Descripción

Corresponde al apartado 7 sobre la gestión de activos.

Objetivos

1. Directrices de clasificación.
2. Etiquetado y manipulación de la información.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

Los responsables de departamentos utilizarán sistemas de almacenamiento físico que podrá ser de información sensible y no sensible, los responsables de departamento serán los encargados de controlar el acceso a la información más crítica.

En la medida de lo posible se intentará gestionar la información a través de Sharepoint y evitar el uso de documentación física ya que a través del gestor documental se puede controlar de forma más segura. El responsable de sistemas junto al responsable de comunicaciones creará los procesos de importación de documentos al gestor documental.

En el caso que hiciera falta se formaría al personal en el uso del gestor documental para el tratamiento diario de la información.

Presupuesto

Tabla 10.3: Presupuesto de gestión de activos.

Descripción	Coste	Unidades	Subtotal
Horas de personal	30	20	600
Formación	600	1	600
Archivadores con control de acceso	800	1	800
		Total	2.000

10.4. Plan de seguridad de los recursos humanos

Descripción

Corresponde al apartado 8 sobre la seguridad de Recursos Humanos.

Objetivos

1. Formación.
2. Creación de proceso disciplinario.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

Los responsables de departamentos junto al gerente y consultor externo decidirán la formación que el personal necesite para la nueva etapa de la empresa. Además se creará un plan de formación continua junto al consultor externo.

El responsable de comunicaciones recibirá formación adecuada a su nuevo cargo en materia de seguridad. Los clientes que utilicen servicios especiales de conexión y acceso a los recursos de la empresa a través de internet recibirán formación para actualizar conocimientos y se les dará acceso a la documentación necesaria a través del gestor documental para que puedan consultar todos los procesos nuevos.

El gerente y el responsable de administración crearán un proceso disciplinario para los empleados que provoquen alguna brecha de seguridad. El consultor externo completará el proceso ayudando en los aspectos legales del mismo.

Presupuesto

Tabla 10.4: Presupuesto de seguridad de los recursos humanos.

Descripción	Coste	Unidades	Subtotal
Horas de personal	30	40	1.200
Formación	300	1	300
Consultoría legal	800	1	800
		Total	2.300

10.5. Plan de seguridad física y del entorno

Descripción

Corresponde al apartado 9 sobre la seguridad física.

Objetivos

1. Perímetro físico de seguridad.
2. Controles físicos de entrada.
3. Seguridad de oficinas.
4. Amenazas externas y ambientales.
5. Trabajo en áreas seguras.
6. Protección de equipos.
7. Seguridad en la reutilización y eliminación de equipos.

Duración

La duración estimada es de treinta días para la realización de las tareas.

Tareas

El área crítica de la empresa es el CPD donde se encuentran los servidores de la empresa, el responsable de sistemas y el gerente junto al consultor externo seleccionarán a una empresa externa para realizar los cambios de infraestructura necesaria en el centro de datos y en la oficina.

Se construirá un recinto seguro para el control del CPD en donde se habilitarán medidas de control de acceso, el responsable de comunicaciones será el encargado de gestionar el control de accesos mediante tarjeta electrónica al CPD. El recinto a su vez dispondrá de medidas básicas contra amenazas externas como fuego o inundación.

El acceso a la oficina será restringido con control electrónico y el responsable de sistemas será el encargado de gestionar el control de acceso.

Todos los sistemas de comunicaciones como cortafuegos, router y switch se trasladarán al CPD para ubicarlos en áreas protegidas.

El responsable de sistemas junto al de comunicaciones creará y documentará el protocolo para la retirada de equipos de la empresa, se especificará como verificar que no existe riesgo de fuga de información y se indicará en su caso la destrucción de estos.

Presupuesto

Tabla 10.5: Presupuesto de seguridad física y del entorno.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de personal	30	80	2.400
Construcción de CPD y adecuación a normativa	60.000	1	60.000
Armario de comunicaciones	2.000	1	2.000
		Total	64.400

10.6. Plan de gestión de comunicaciones y operaciones

Descripción

Corresponde al apartado 10.

Objetivos

1. Prestación del servicio.
2. Monitoreo y revisión de los servicios por terceras partes.
3. Gestión de los cambios en servicios por terceras partes.
4. Gestión de los medios removibles.
5. Eliminación de los medios.
6. Procedimientos para el manejo de la información.
7. Seguridad de la documentación del sistema

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

El gerente y el responsable de sistemas comprobarán los acuerdos con el proveedor de internet para la posible mejora del servicio y el contrato de líneas dedicadas adicionales y servicios de seguridad para asegurar el servicio a clientes. El responsable de comunicaciones se encargará de comprobar el funcionamiento de las líneas y registrará todos los eventos e incidencias a través del gestor documental, el responsable de sistemas será el encargado de revisar estos registros y comunicar las incidencias al gerente.

El responsable de sistemas revisará los servicios con el proveedor cloud y comprobará que se cumple con los requisitos de seguridad, algunos ejemplos de conformidad en seguridad de proveedores cloud se pueden consultar en Azure y Amazon.

Tabla 10.6: Proveedores cloud.

Azure	**Amazon**
ISO 27001/27002	HIPAA
SOC 1/SSAE 16/ISAE 3402 y SOC 2	SOC 1/SSAE 16/ISAE 3402 (anteriormente, SAS70)
CCM de la Alianza de Seguridad en la Nube	SOC 2
FedRAMP	SOC 3
FISMA	PCI DSS nivel 1
CJIS del FBI (Azure Government)	ISO 27001
PCI DSS Level 1	FedRAMP(SM)
G-Cloud del Reino Unido	DIACAP y FISMA
Programa IRAP del gobierno de Australia Norma MTCS en Singapur HIPAA CDSA	ITAR
	FIPS 140-2
	CSA
	MPAA
Cláusulas según el modelo de la U. E.	
21 CFR Parte 11 de la Administración de Alimentos y Medicamentos (FDA) FERPA	
FIPS 140-2	
CCCPPF	
MLPS	

El responsable de sistemas creará los procesos para la gestión de soportes extraíbles donde documentará los procesos que se debe de seguir en caso de uso externo a las oficinas y entre departamentos. Esta documentación se publicará y dará acceso a todo el personal que utilice estos dispositivos a través del gestor documental. Sólo se permitirá el uso de puertos de comunicación para medios extraíbles a personal autorizado y se configurará para utilizar medios autorizados.

Los medios extraíbles serán proporcionados por la empresa y utilizarán técnicas de encriptación para impedir el robo de información. El responsable de sistemas será el encargado de controlar el acceso a estos medios.

Presupuesto

Tabla 10.7: Presupuesto de gestión de comunicaciones y operaciones.

Descripción	Coste	Unidades	Subtotal
Horas de personal	30	80	2.400
Consultoría legal de proveedores de servicios	1.000	1	1.000
Medios de almacenamiento seguros usb	223	5	1.115
		Total	4.515

10.7. Plan de control de accesos

Descripción

Corresponde al apartado 11 sobre el control de accesos.

Objetivos

1. Registro de usuario.
2. Gestión de privilegios.
3. Gestión de contraseñas.
4. Derechos de acceso.
5. Políticas de puestos de trabajo.

Duración

La duración estimada es de cinco días para la realización de las tareas.

Tareas

El responsable de sistemas creará perfiles para el control de accesos de los usuarios a través del sistema de identidades de Windows Server y gestionará los accesos a los servicios y aplicaciones. Además creará políticas de creación y mantenimiento de contraseñas. Todos los procesos se documentarán en el gestor documental y serán accesibles por el responsable de sistemas y comunicaciones.

El responsable de comunicaciones creará los procedimientos para la gestión de accesos a las comunicaciones de la empresa por el personal para el uso de la red e internet, además se documentarán los procesos en el gestor documental.

Los diferentes servicios del CPD se integrarán con el servicio de Active Directory de la empresa para la gestión centralizada de usuarios y privilegios de la empresa. De esta

manera la gestión de usuarios, derechos de acceso y contraseñas se podrán realizar a través del mismo gestor de identidades de Windows Server.

Se crearán políticas para la gestión de puestos de trabajo y se aplicarán a través de Active Directory de forma remota para los bloqueos de pantalla y solicitud de cambio de contraseñas.

Presupuesto

Tabla 10.8: Presupuesto de control de accesos.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de personal	30	80	2.400
		Total	2.400

10.8. Plan de adquisición, desarrollo y mantenimiento

Descripción

Corresponde al apartado 12 sobre adquisición, desarrollo y mantenimiento.

Objetivos

1. Análisis y especificación de los requisitos de seguridad.
2. Fugas de información.

Duración

La duración estimada es de cinco días para la realización de las tareas.

Tareas

La dirección y los responsables fomentarán el uso de la documentación sobre materia de seguridad para evitar riesgos y pérdidas de información.

Cada cierto tiempo y bajo las indicaciones del responsable de sistemas y comunicaciones se impartirá formación para mantener al personal actualizado en materia de seguridad.

Presupuesto

Tabla 10.9: Presupuesto de adquisición, desarrollo y mantenimiento.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de personal	30	50	1.500
		Total	1.500

10.9. Plan de gestión de incidentes

Descripción

Corresponde al apartado 13 sobre la gestión de incidentes.

Objetivos

1. Reporte sobre los eventos de seguridad de la información.
2. Reportes sobre las debilidades de la seguridad.
3. Responsabilidades y procedimientos.
4. Aprendizaje debido a los incidentes de seguridad de la información.
5. Recolección de evidencias.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

El responsable de comunicaciones creará los procesos necesarios para gestionar los eventos en los servicios de seguridad como router y cortafuegos, la mayoría de estos procesos funcionarán de manera autónoma y no será necesario adquirir nuevo material. Los procedimientos deberán incluir el protocolo en caso de que existe un incidente de seguridad y se tenga que tomar medidas extraordinarias que incluyan la comunicación a cuerpos de seguridad y recopilación de pruebas.

El departamento de administración modificará los contratos con proveedores y clientes para incluir cláusulas para que de manera obligatoria estos avisen sobre posibles problemas de seguridad en los servicios prestados, de esta manera no sólo se mejora la comunicación en materia de seguridad sino la imagen de la propia empresa.

Presupuesto

Tabla 10.10: Presupuesto de gestión de incidentes.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de personal	30	50	1.500
Consultoría legal	800	1	800
		Total	2.300

10.10. Plan de gestión de continuidad

Descripción

Corresponde al apartado 14 sobre la gestión de continuidad de negocio.

Objetivos

1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
2. Continuidad del negocio y evaluación de riesgos.
3. Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.
4. Estructura para la planificación de la continuidad del negocio.
5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

Duración

La duración estimada es de diez días para la realización de las tareas.

Tareas

El responsable de sistemas creará un plan de contingencia para asegurar el funcionamiento de infraestructura y servicios y asegurar su disponibilidad.

El responsable de comunicaciones será el encargado de crear el plan de contingencia de las redes de la empresa y asegurar su funcionamiento.

El responsable de desarrollo creará un plan de contingencia para asegurar los servicios en producción y asegurar el correcto funcionamiento de las aplicaciones.

El personal implicado en el plan de continuidad recibirá la formación adecuada dependiendo de las necesidades, el consultor del SGSI será el encargado de gestionar el proceso.

Presupuesto

Tabla 10.11: Presupuesto de gestión de continuidad.

Descripción	**Coste**	**Unidades**	**Subtotal**
Horas de responsables de departamentos	30	100	3.000
Formación de continuidad de negocio	600	1	600
		Total	3.600

10.11. Plan de conformidad

Descripción

Corresponde al apartado 15 sobre conformidad.

Objetivos

1. Identificación de legislación aplicable.
2. Derechos de propiedad intelectual.

Duración

La duración estimada es de cinco días para la realización de las tareas.

Tareas

Para garantizar el cumplimiento de requisitos legales sobre el uso de materiales con derechos de propiedad intelectual el personal implicado recibirá formación adecuada en la legislación vigente.

Presupuesto

Tabla 10.12: Presupuesto de conformidad.

Descripción	**Coste**	**Unidades**	**Subtotal**
Curso formación requisitos legales LSSI, LOPD	1.000	1	1.000
		Total	1.000

Capítulo 11

Implementación del plan

Después de definir los planes de tratamiento de riesgos el responsable gestionará los proyectos de implantación. Estos deberán llevarse a cabo en los plazos propuestos del proyecto que inicialmente son de cuatro meses.

Tabla 11.1: Plan de trabajo de implementación.

Planes	**Duración**	**Responsable**
5 Plan de políticas de seguridad de la información	10 días	
Revisión de las políticas	5 días	Dirección y responsables de departamento
Creación de los procesos de difusión	5 días	Responsable de sistemas
6 Plan de la organización de la seguridad de la información	10 días	
Implantar sistema de mejora a través de gestor documental	4 días	Responsable de sistemas
Selección de personal para responsable de comunicaciones	5 días	Administración
Reuniones de la directiva con cuerpos de seguridad	1 día	Dirección
7 Plan de gestión de activos	10 días	
Instalar armarios seguros para documentación física	1 día	Responsables de departamento
Crear políticas de creación y migración de documentos al sistema ECM	6 días	Responsable de sistemas
Formación en gestor documental	3 días	Consultor externo
8 Plan de seguridad de los recursos humanos	10 días	
Formación	6 días	Consultor externo
Creación de proceso disciplinario	4 días	Administración, gerencia y consultoría legal

9 Plan de seguridad física y del entorno	30 días	
Propuestas de trabajo para ampliación de CPD	2 días	Dirección y responsable de sistemas
Ampliación de CPD	15 días	Empresa externa
Traslado de armario de comunicaciones al CPD	3 días	Empresa externa
Instalación de sistema de controles de acceso	6 días	Empresa externa
Creación y documentación de procesos para la retirada de equipos	4 días	Responsable de sistemas y consultor externo
10 Plan de gestión de comunicaciones y operaciones	10 días	
Revisión de contratos con empresas externas	5 días	Responsable de sistemas y comunicaciones
Creación los procesos para la gestión de soportes extraíbles	3 días	Responsable de sistemas
Adquisición de material de medios extraíbles	2 días	Responsable de sistemas
11 Plan de control de accesos	5 días	
Migración de políticas de usuario al gestor de identidades	3 días	Responsable de sistemas
Creación y documentación de procesos en seguridad de comunicaciones	2 días	Responsable de comunicaciones
12 Plan de adquisición, desarrollo y mantenimiento de los sistemas de información	5 días	
Creación de políticas de uso sobre seguridad de la información	5 días	Dirección y responsable de sistemas
13 Plan de gestión de incidentes	5 días	
Modificación de contratos	2 días	Administración y consultoría legal
Creación de procesos para gestión incidentes de seguridad	3 días	Responsable de comunicaciones
14 Plan de gestión de continuidad	10 días	
Plan de contingencia de infraestructura	2 días	Responsable de sistemas y consultor externo

Plan de contingencia de desarrollo	2 días	Responsable de desarrollo
Plan de contingencia de comunicaciones	2 días	Responsable de comunicaciones
Formación en gestión de la continuidad	4 días	Consultor externo
15 Plan de conformidad	5 días	
Formación en materia legal	5 días	Consultor externo
Total días	110 días	

El tiempo total calculado corresponde a días hábiles por lo tanto se puede demorar cinco meses y medio de los cuatro planificados. El coste total del proyecto se detalla a continuación y en el que se puede observar que la mayor parte del presupuesto se centra en la mejora del CPD que es la base sobre la que trabaja Treval:

Tabla 11.3: Coste total del proyecto.

Planes	**Coste**
5 Plan de políticas de seguridad de la información	2.000
6 Plan de la organización de la seguridad de la información	1.600
7 Plan de gestión de activos	2.000
8 Plan de seguridad de los recursos humanos	2.300
9 Plan de seguridad física y del entorno	64.400
10 Plan de gestión de comunicaciones y operaciones	4.515
11 Plan de control de accesos	2.400
12 Plan de adquisición, desarrollo y mantenimiento	1.500
13 Plan de gestión de incidentes	2.300
14 Plan de gestión de continuidad	3.600
15 Plan de conformidad	1.000
Total	87.615

Parte IV

Conclusiones

Capítulo 12

Resumen

Es evidente que la seguridad de la información juega un papel importante en las organizaciones y es un activo a tener en cuenta. Con la llegada de las nuevas tecnologías esta información se encuentra más expuesta a amenazas y no sólo a nivel empresarial sino que afecta a cualquier persona que haga uso de las tecnologías de la información.

Para proteger estos activos es necesario garantizar todas las dimensiones de la seguridad como el acceso, integridad, disponibilidad, autenticidad, confidencialidad y conservación de la información. Otro aspecto a tener en cuenta dentro de las organizaciones son los Sistemas de Información y Comunicaciones, son los encargados de almacenar, procesar y transmitir la información y que deben de protegerse frente a las amenazas ya que son la base de las Tecnologías de la información.

Para intentar proteger los activos frente a las amenazas se debe de aplicar controles y hacerlo durante todo el ciclo de vida de la información, desde que entra al sistema hasta que se elimina.

Actualmente las tecnologías de la información sirven de soporte a la mayoría de procesos de nuestra vida diaria y se encuentran en todos los ámbitos que podamos imaginar y es necesario confiar en el correcto funcionamiento de estas tecnologías. Para garantizar este funcionamiento es adecuado la aplicación de normas y estándares, la certificación en estas normas no supone que un producto no este exento de errores o de un mal funcionamiento pero garantiza un cierto grado de calidad al tener que someterse a una serie de auditorías y controles.

Dentro del mundo de las normas y certificaciones podemos encontrar las aprobadas por organismos como ISO o AENOR y también algunos marcos de buenas prácticas como ITIL y COBIT. Además, también existen las normas de cumplimiento como LOPD y LSI, pero una de las normas más importantes es la ISO 27001, este Sistema de Gestión de Seguridad de la Información proporciona unas directrices claras sobre materia de gestión de la seguridad.

Treval teniendo en cuenta las necesidades en materia de seguridad ha decidido la implantación de este SGSI, sobre todo al ser una empresa que se sustenta en las TIC y proporciona servicios tecnológicos a clientes en los que la información juega un papel im-

portante.

Tal y como se ha descrito en el comienzo del trabajo esta implantación abarca las dos primeras fases del ciclo de vida de Deming. Dentro de la primera fase se ha definido el plan de seguridad y especificado el alcance del proyecto, después se ha realizado el Gap Analysis que no es un requerimiento de la norma pero ayuda a establecer la hoja de ruta del proyecto. Gracias al análisis diferencial se ha podido ver el estado de Treval respecto a la norma y ha ayudado a crear las políticas de seguridad.

Después de definir la metodología de análisis de riesgos entramos en la parte más importante de la primera fase en donde realizamos el inventario de activos e identificamos los riesgos y amenazas. Para terminar volvemos a definir el documento de aplicabilidad para concretar los controles que sean necesarios implantar.

En la segunda fase y utilizando el documento de **Declaración de aplicabilidad** como referencia crearemos los planes de tratamiento definidos y por último creamos el plan de trabajo para la implantación. Una vez visto el resultado podemos asegurar que casi todo el trabajo se ha centrado en mejorar las instalaciones y adecuar los procesos de seguridad de la información dentro de la organización a través de actividades formativas y la creación de nuevos procesos.

Podemos concluir este trabajo sugiriendo aplicar las dos fases restantes del ciclo de Deming para completar totalmente la norma, para ello se deberá revisar el SGSI así como la efectividad de los controles, además se realizarán auditorías periódicas para evaluar la eficacia y eficiencia del sistema. En la última fase nos centraremos en implantar planes de mejora y acciones correctivas y preventivas.

Bibliografía

[1] *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes* de Ana Gómez Fernández y Luis Andrés Álvarez. Editorial Aenor, 2012.

[2] *Implantación de un SGSI según ISO 27001* de Cristina Merino Bada y Ricardo Cañizares Sales. Editorial FC, 2011.

[3] ISO 27001 en Wikipedia, http://es.wikipedia.org/wiki/ISO/IEC_27001.

[4] Sistema de la seguridad de la información en Wikipedia, http://es.wikipedia.org/wiki/Sistema_de_gestión_de_la_seguridad_de_la_información.

[5] AENOR, https://www.aenor.es/AENOR/certificacion/seguridad/seguridad_27001.asp.

[6] http://www.iso27000.es.

[7] http://www.iso27001standard.com/es.

[8] Asociación Española para el Fomento de la Seguridad de la Información, https://www.ismsforum.es/iso27001.

[9] Implantación de un SGSI en la empresa, https://www.incibe.es.

[10] Audisec, http://audisec.es.

[11] Metodología Magerit, http://administracionelectronica.gob.es.