Proceso de adecuación de la seguridad de la información en una pequeña empresa

Nombre estudiante: José Sureda Uceda

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre consultor: Arsenio Tortajada Gallego

Centro: Universitat Oberta de Catalunya

Fecha de entrega: 20 de diciembre 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	***Proceso de adecuación de la seguridad de la información en una pequeña empresa***
Nombre del autor:	***José Sureda Uceda***
Nombre del consultor:	***Arsenio Tortajada Gallego***
Fecha entrega (mm/aaaa):	*12/2019*
Área del Trabajo Final:	***Sistema de Gestión de Seguridad de la Información***
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo

Estudios recientes en ciberseguridad confirman que las pequeñas y medianas empresas no están gestionando adecuadamente la seguridad de sus sistemas informáticos y, en consecuencia, los datos que con ellos se procesan, vitales para su existencia y funcionamiento normal. Las entidades más pequeñas no invierten los recursos necesarios ni prestan la suficiente atención a la gestión de la seguridad de la información. Sin embargo, los riesgos a los que están expuestas son los mismos que cualquier gran empresa. El robo de credenciales, la fuga de información reservada, la pérdida de un dispositivo o el incumplimiento de leyes, son ejemplos con los que se puede encontrar cualquier empresa. En ciberseguridad existe el dogma que la seguridad 100% no existe, pero sí es posible aprender a gestionar los riesgos. Este proyecto, a través de un caso real, muestra todo el proceso por el cual una pequeña empresa con pocos recursos es capaz de instaurar una cultura de seguridad en toda la organización, transformando su vulnerable gestión de la información en un sistema mucho más robusto, eficaz y con mayores garantías en la protección de sus datos. Este objetivo se ha conseguido usando estándares y metodologías reconocidas a nivel internacional como las normas ISO/IEC 27001, ISO/IEC 27002, el marco de trabajo MAGERIT, el Ciclo de Deming y el Modelo de Madurez de la Capacidad. Educar y concienciar en materia de seguridad de la información son la clave para que las pequeñas empresas afronten con las mejores garantías los riesgos a las que están expuestas.

Abstract

Recent cybersecurity studies prove that small and medium-sized companies are not managing properly the security of their computer systems, therefore the data processing, which is vital for its existence and normal functioning. Small entities do not invest in the necessary resources and do not pay enough attention to information security management. Nevertheless, they are exposed to the same risks as big companies are. Credential theft, leakage of reserved information, the loss of a device or the breach of laws are examples of actions that any company can suffer. In cybersecurity there is a dogma which contemplates that 100% security does not exist, even though it is possible to learn how to manage the risks. This paper, through a real case, presents how to help a small company with few resources to set up a security culture around it. This is a transformation of its vulnerable information management with a stronger and more efficient system to ensure the data protection. The target has been reached by using internationally recognised standards and methodologies such as ISO/IEC 27001, ISO/IEC 27002 requirements, the MAGERIT framework, the Deming Cycle and the Capability Maturity Model. Educating and raising awareness in data security are the key for small companies to face the risks they are exposed to with the best warranties.

Palabras clave (entre 4 y 8):

ciberseguridad, información reservada, datos, riesgos, ISO/IEC 27001, ISO/IEC 27002, MAGERIT, pequeña empresa

Índice

Índice de figuras

Índice de tablas

1. Introducción

1.1 Contexto

La incorporación de las nuevas tecnologías en las empresas y organizaciones ha generado que éstas procesen sus datos a través de un amplio abanico de dispositivos, todos ellos con la posibilidad de interconectarse mediante redes locales o remotas. Este gran conglomerado de información virtual que se ha creado, es una atracción no sólo para los delincuentes que han encontrado nuevas formas de llevar a cabo sus actividades ilegales, si no también, para todo tipo de entidades que pretenden la captura de información por el poder que ésta representa. De aquí que actualmente se hable y se oigan más a menudo noticias relacionadas con el robo de datos, ciberataques, malware o fugas de información entre otras.

Ante esta situación muchas empresas y organizaciones han cambiado su visión y filosofía a la hora de tratar la seguridad de su información, prestando la importancia que se merece. No obstante, la realidad, tal y como reflejan diversos estudios, es que existe un número aún mayor de entidades, principalmente microempresas y PYMES, que no abordan el tema con la suficiente responsabilidad y seriedad.

Hoy en día las pequeñas empresas tratan un volumen alto de información, que además, resulta ser un activo importante para el negocio. Sin embargo, muchas de estas entidades no son conscientes de los riesgos de seguridad a las que están expuestos sus datos. Este hecho puede provocar situaciones indeseables que van desde la exposición de credenciales de usuario, caída de servicios, crisis de reputación, pasando por las importantes sanciones que puede acarrear el incumplimiento de las normativas y leyes vigentes.

Las grandes empresas tienen el potencial para dedicar una parte importante de su presupuesto a protegerse, pero esto no está al alcance de las empresas más modestas. Es cierto que a más seguridad los costes y los recursos

aumentan considerablemente, no obstante, hay medidas básicas que pueden aplicarse sin hacer grandes inversiones y que además, permiten mejorar el nivel de seguridad de la información. Esta visión es la que hay que hacer llegar a las microempresas, PYMES y autónomos con el fin de cambiar el pensamiento de asociar la seguridad con costes elevados. En muchos casos, los empresarios y directivos lanzan esta afirmación desconociendo las pérdidas y el impacto para su organización, en el caso de producirse un incidente de seguridad de la información.

Otra idea que necesita ser erradicada es la de creer que por ser una entidad pequeña y sin una gran repercusión a nivel nacional o internacional, no se está en el punto de mira de un ataque informático. En realidad, toda información que se sustenta en las TIC (Tecnologías de la Información y las Comunicaciones) es susceptible de sufrir un incidente, ya sea provocado o por accidente, en alguna de sus dimensiones principales: **disponibilidad, integridad** y **confidencialidad**.

Por otro lado, son muchas las PYMES que por desconocimiento, falta de capacidad o por la inexistencia de políticas y procesos adecuados, resuelven los incidentes relacionados con la seguridad de la información de forma arbitraria.

Estos hechos están relacionados con la situación que muestran algunas de las estadísticas de estudios más recientes en materia de la ciberseguridad:

- A lo largo del año 2018, sólo en España se registraron al menos 120.000 incidentes de ciberseguridad, siendo las pequeñas y medianas empresas las mayores afectadas[1].

- El 99,8% del tejido empresarial español no se considera un objetivo atractivo para un ciberataque[2], según el informe de la empresa The Cocktail Analysis “*Panorama Actual de la Ciberseguridad en España*” y elaborado para Google.

- El 53 % de las pequeñas y medianas empresas en España, reconoció haber sido víctima de un ciberataque en 2017, según el informe SMB Cybersecurity Report de Cisco[1]. En realidad, según Helena Rifà, directora del máster universitario en Seguridad de las TIC de la Universitat Oberta de Catalunya (UOC), el porcentaje de las que han sido atacadas puede superar el 80%, aunque no salen a la luz por temas de imagen y reputación.

- Las microempresas españolas son las que menos porcentaje de su presupuesto total de TIC destinan a ciberseguridad (6,5%)[3].

- El impacto medio de un ataque oscila entre los 20.000 y los 50.000 euros[1].

1.2 Justificación y pretensiones del proyecto

La situación actual de las pequeñas empresas y el modo en que hacen frente a la seguridad de la información es la motivación de este Trabajo Fin de Máster o TFM. Hay dos cuestiones fundamentales y relacionadas entre sí que requieren la aplicación de medidas urgentes. En primer lugar, las pequeñas empresas representan el 45% del total en España, según los últimos datos extraídos del Ministerio de Trabajo, Migraciones y Seguridad Social en octubre de 2019[4]. Si añadimos los autónomos la cifra aumenta hasta el 98,9%.

Empresas por tamaño	Número de empresas	Tasa de variación %	
		intermensual	Interanual
Autónomos[1] (PYME sin asalariados)	**1.539.708**		**-0,68**
PYME (1-249 asalariados)	**1.314.060**	**-0,68**	**-0,15**
Microempresas (1-9 asalariados)	1.133.756	-0,59	-0,43
Pequeñas (10-49 asalariados)	154.816	-1,26	1,50
Medianas (50-249 asalariados)	25.488	-1,00	2,89
Grandes (250 o más asalariados)	4.855	0,56	3,45
Total empresas	**2.858.623**		**-0,43**

Figura 1: Empresas inscritas en la Seguridad Social y autónomos

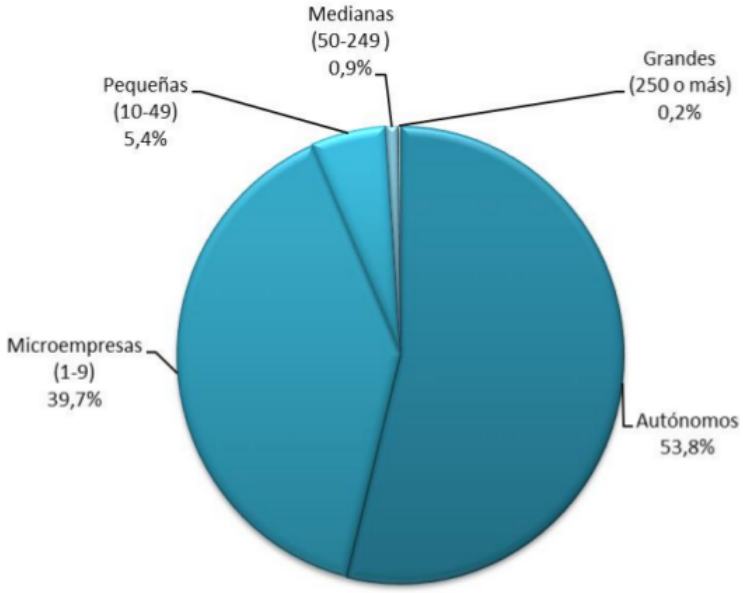

Figura 2: Distribución según el tipo de empresa

En segundo lugar, tal como indican las estadísticas anteriores, las pequeñas y medianas empresas son las más afectadas por incidentes de ciberseguridad. Estos motivos hacen que sea necesario cambiar el enfoque y la actitud que actualmente existe en las pequeñas empresas y la solución pasa, primeramente, por educar y concienciar a sus dirigentes.

La finalidad de este proyecto es definir un modelo que pueda extrapolarse a otras empresas y ser usado como guía para mejorar el estado de seguridad de su información. El producto ha sido desarrollado a partir de un caso real para obtener las máximas garantías de fiabilidad y semejanza a un escenario típico. Su uso puede ser válido para cualquier organización, aunque evidentemente se deberá adecuar a las características, objetivos y recursos de cada caso.

Este TFM analizará la situación de una microempresa en relación a la seguridad de la información, para que el equipo directivo sea consciente de cuál es su estado actual. El resultado final les permitirá tomar las medidas necesarias dentro de las posibilidades de la entidad para, finalmente, obtener una mejora en la seguridad de la información a nivel global. La propuesta para conseguir este objetivo es implantar un **Sistema de Gestión de la Seguridad de la Información** o **SGSI**.

Debido a que la empresa objeto de estudio es una entidad real, se mantendrá su anonimato para respetar su privacidad y no poner en compromiso información confidencial. Desde ahora se hará referencia a ella con el nombre ficticio "*TurisTech Balear*" o los términos "*la entidad*", "*la organización*" o "*la empresa*".

1.2 Objetivos del Trabajo

El trabajo fin de máster especializado en Sistemas de Gestión de Seguridad de la Información pretende conseguir los siguientes objetivos:

Generales:

- Concienciar a las microempresas y PYMES para que integren la seguridad de la información en su modelo de negocio, evitando tratarla como una cuestión que afecte sólo a ciertos departamentos o proyectos.

- Transmitir a las empresas y organizaciones la importancia de conocer cual es su estado de protección de la seguridad de la información, en relación a los estándares y la normativa legal vigente.

- Educar sobre los beneficios que puede aportar a las empresas y organizaciones la implantación de un Sistema de Gestión de Seguridad de la Información.

Específicos:

- Describir el estado inicial y final de TurisTech Balear en relación a la seguridad de la información.

- Crear la documentación que requiere un SGSI y que sea accesible para todos los trabajadores.

- Implantar en la empresa una metodología para gestionar los riesgos.

- Obtener una lista de proyectos que la empresa tendrá que desarrollar para situar el estado inicial de seguridad a los niveles definidos en el Plan Director. Siendo el objetivo reducir los riesgos a los que están expuestos los activos de la empresa.

- Realizar una auditoría interna de cumplimiento de la ISO/IEC 27002:2013.

- Documentar y presentar a la dirección los resultados finales obtenidos.

- Definir las líneas a seguir para conseguir establecer una “cultura de seguridad” dentro de la organización.

- Que el SGSI resultado del TFM pueda ser usado, si así lo encuentra oportuno la entidad, para conseguir la certificación ISO/IEC 27001.

1.3 Enfoque y método seguido

Si bien, en TurisTech Balear se aplican ciertos procesos para gestionar la seguridad de la información, estos resultan insuficientes para completar el TFM porque hay muchos aspectos que simplemente no se contemplan, por ejemplo, un análisis de riesgos o la ejecución de auditorías. El modelo actual de gestión no permitirá alcanzar los objetivos indicados en el apartado 1.2, por ello se ha acordado substituirlo por otro.

La estrategia acordada consiste en implantar un SGSI a través de un Plan Director de Seguridad, fundamentado en los siguientes elementos:

- El estándar internacional ISO/IEC 27001:2013[11] e ISO/IEC 27002:2013[12]. La primera de ellas contiene las especificaciones para la implantación del SGSI y la segunda, una guía de buenas prácticas para la selección, implantación y gestión de controles de seguridad. Éstos se utilizan para evaluar el estado del cumplimiento de la empresa

frente a la norma. Actualmente son dos estándares con gran difusión y aceptación a escala internacional.

- El marco de trabajo MAGERIT[13]. Se utiliza para el análisis y la gestión de los riesgos, aspecto clave en un SGSI. Ésta metodología esta reconocida en el inventario elaborado por ENISA (*Agencia de Seguridad de las Redes y de la Información de la Unión Europea*) https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

- La metodología PDCA[14] o ciclo de Deming. Se trata de un método de gestión iterativo de cuatro pasos (Plan, Do, Check, Act) utilizado para el control y la mejora continua de procesos y productos. La ISO 27001 en su apartado 10.2 indica: "*la organización deberá mejorar continuamente la idoneidad, adecuación y efectividad de la información del sistema de gestión de seguridad*".

Además de su reconocimiento internacional, estos estándares y metodologías han sido materia de estudio durante la realización del máster, lo cual ofrece una mayor garantía de que el alumno haga un buen uso y aplicación en el TFM. Con este nuevo enfoque es muy probable que se cumplan todos los objetivos establecidos, además de garantizar que la gestión de la seguridad de la información se realiza acorde a unos estándares y metodologías reconocidas a nivel mundial.

1.4 Planificación del Trabajo

1.4.1 Recursos utilizados

Para la elaboración del trabajo se han utilizado los siguientes recursos:

- Ordenador portátil HP Pavilion con procesador Intel© CoreTM i5 a 2.27 GHz, 8 GB de memoria RAM y un disco duro de 500 GB.

- Sistema operativo Linux Mint 18.1 Cinnamon 64-bits.
- Monitor auxiliar LG 21 pulgadas.
- Disco duro externo USB 2.0 WD Elementos 500 GB, para almacenar copias de seguridad de la documentación generada.
- Software de ofimática LibreOffice versión 5.1.6.2.
- Software Visual Paradigm Online Diagram versión gratuita.
- Software Project Libre versión 1.9.1.

1.4.2 Organización tareas

Para que el proyecto sea más manejable se ha dividido en un conjunto de etapas, cada una de las cuales con una fecha de fin que representa un hito en el tiempo y en la que se tendrá que hacer una entrega. Las fases a ejecutar son las siguientes:

- Fase 1. Situación actual: Contextualización, objetivos y análisis diferencial.
- Fase 2. Sistema de gestión documental.
- Fase 3. Análisis de riesgos.
- Fase 4. Propuesta de proyectos.
- Fase 5. Auditoría de cumplimiento de la ISO/IEC 27002:2013.
- Fase 6. Presentación de resultados y entrega de informes.

1.4.2 Dedicación

Cualquier proyecto de cierta envergadura y con un número elevado de tareas, requiere que éstas queden claramente definidas, asignadas y organizadas en el tiempo. El periodo definido para la ejecución del TFM es de unos 3 meses aproximadamente, iniciándose el 18/09/2019 y finalizando el 20/12/2019.

Al inicio del proyecto se hizo una estimación del volumen de horas de dedicación, considerando una media de 84 horas al mes (3 horas al día). Esto dio un total aproximado de 252 horas para el desarrollo completo del proyecto.

Una vez completadas las 6 fases del TFM los cálculos se han ajustado bastante a las previsiones iniciales. Si se suman las horas del diagrama de Gantt (figura 3) da un total de 196 horas pero esta cantidad no es real, pues hay que añadirle un 25% más. Esta discrepancia se debe porque al inicio del proyecto se definió un horario de trabajo diario en la aplicación Project Libre para poder ir anotando las tareas. Pero en realidad, hubo días donde se imputaron más horas, así que finalmente el total se queda en unas 245 horas.

	Nombre	Trabajo	Inicio	Terminado
1	**Fase previa. Inicio semestre**	**3 horas**	**18/09/19 17:30**	**19/09/19 18:30**
2	Presentación y lectura del enunciado	1 hora	18/09/19 17:30	18/09/19 18:30
3	Organización tareas	1 hora	18/09/19 18:30	18/09/19 19:30
4	Recopilación e impresión de normas y guías	1 hora	19/09/19 17:30	19/09/19 18:30
5	**Fase 1. Situación actual**	**33,5 horas**	**19/09/19 17:30**	**4/10/19 19:30**
6	Selección empresa. Inicio desarrollo fase 1	2 horas	19/09/19 17:30	19/09/19 19:30
7	**Reunión con dirección**	**2 horas**	**20/09/19 17:30**	**20/09/19 19:30**
8	Definir alcance y objetivos Plan Director Seguri...	2 horas	20/09/19 17:30	20/09/19 19:30
9	Desarrollo fase 1	29 horas	21/09/19 17:30	3/10/19 19:30
10	Preparación y entrega fase 1	0,5 horas	4/10/19 19:00	4/10/19 19:30
11	**Fase 2. Sistema de gestión documental**	**27,5 horas**	**5/10/19 8:00**	**18/10/19 19:30**
12	Inicio desarrollo fase 2	6 horas	5/10/19 8:00	6/10/19 11:00
13	**Reunión con dirección**	**2 horas**	**7/10/19 17:30**	**7/10/19 19:30**
14	Política de seguridad y procedimiento de audit...	2 horas	7/10/19 17:30	7/10/19 19:30
15	Desarrollo fase 2	6 horas	8/10/19 17:30	10/10/19 19:30
16	**Reunión con dirección**	**2 horas**	**11/10/19 17:30**	**11/10/19 19:30**
17	Procedimiento revisión por Dirección, Gestión r...	2 horas	11/10/19 17:30	11/10/19 19:30
18	Desarrollo fase 2	11 horas	12/10/19 17:30	17/10/19 19:30
19	Preparación y entrega fase 2	0,5 horas	18/10/19 19:00	18/10/19 19:30
20	**Fase 3. Análisis de riesgos**	**46,5 horas**	**19/10/19 8:00**	**8/11/19 19:30**
21	Inicio desarrollo fase 3	6 horas	19/10/19 8:00	20/10/19 11:00
22	**Reunión con dirección**	**2 horas**	**21/10/19 17:30**	**21/10/19 19:30**
23	Inventario de activos y valoración	2 horas	21/10/19 17:30	21/10/19 19:30
24	Desarrollo fase 3	14 horas	22/10/19 17:30	27/10/19 11:00
25	**Reunión con dirección**	**2 horas**	**28/10/19 17:30**	**28/10/19 19:30**
26	Análisis de amenazas y definir umbral de riesgo	2 horas	28/10/19 17:30	28/10/19 19:30
27	Desarrollo fase 3	22 horas	29/10/19 17:30	7/11/19 19:30
28	Preparación y entrega fase 3	0,5 horas	8/11/19 19:00	8/11/19 19:30
29	**Fase 4. Propuestas de proyectos**	**25,5 horas**	**9/11/19 11:00**	**22/11/19 19:30**
30	Inicio desarrollo fase 4	2 horas	9/11/19 11:00	10/11/19 10:00
31	**Reunión con dirección**	**2 horas**	**11/11/19 17:30**	**11/11/19 19:30**
32	Definir plan de proyectos	2 horas	11/11/19 17:30	11/11/19 19:30
33	Desarrollo fase 4	21 horas	12/11/19 18:30	21/11/19 19:30
34	Preparación y entrega fase 4	0,5 horas	22/11/19 19:00	22/11/19 19:30
35	**Fase 5. Auditoria de cumplimiento**	**30,5 horas**	**23/11/19 8:00**	**6/12/19 19:30**
36	Inicio desarrollo fase 5	6 horas	23/11/19 8:00	24/11/19 11:00
37	**Reunión con dirección**	**2 horas**	**25/11/19 17:30**	**25/11/19 19:30**
38	Planificación auditoria	2 horas	25/11/19 17:30	25/11/19 19:30
39	Desarrollo fase 5	22 horas	26/11/19 17:30	5/12/19 19:30
40	Preparación y entrega fase 5	0,5 horas	6/12/19 19:00	6/12/19 19:30
41	**Fase 6. Presentación de resultados e infor...**	**29,5 horas**	**7/12/19 8:00**	**20/12/19 19:30**
42	Desarrollo fase 6	28 horas	7/12/19 8:00	18/12/19 19:30
43	**Reunión con dirección**	**1 hora**	**19/12/19 18:30**	**19/12/19 19:30**
44	Presentación de resultados a la dirección	1 hora	19/12/19 18:30	19/12/19 19:30
45	Preparación y entrega fase 6	0,5 horas	20/12/19 19:00	20/12/19 19:30

Figura 3: Planificación temporal TFM

1.5 Resumen de productos obtenidos

Al finalizar cada fase se han obtenido los siguientes productos:

- Fase 1. Descripción y situación actual de la empresa objeto de estudio, el alcance del Plan Director de Seguridad y un análisis diferencial.

- Fase 2. Esquema documental ISO/IEC 27001:2013, es decir, aquella documentación requerida en un SGSI basado en esta norma.

- Fase 3. Un Informe de análisis de riesgos.

- Fase 4. La planificación de proyectos que deberá ejecutar la empresa.

- Fase 5. Auditoría de cumplimiento de la ISO/IEC 27002:2013.

- Fase 6. Presentación de los resultados.

1.6 Resumen del resto de capítulos

Capítulo 2. Situación actual: Contextualización, objetivos y análisis diferencial

En este capítulo se describe la empresa y los motivos de su elección a partir de la cual se ha confeccionado el Plan Director de Seguridad. También se define el alcance del SGSI y finalmente un análisis diferencial que muestra el estado actual de la entidad enfrente a la norma ISO/IEC 27002:2013.

Capítulo 3. Sistema de gestión documental

Implantar un SGSI requiere una documentación donde queden definidos los procedimientos a seguir para gestionar la seguridad de la información. La ISO/IEC 27001:2013 describe cuáles son estos documentos necesarios para cumplir con dicha norma.

Capítulo 4. Análisis de riesgos

El primer paso para la gestión de los riesgos consiste en realizar un análisis que identifique los activos que hay que proteger, las amenazas a las cuales están expuestos y el impacto que pueden tener sobre ellos. En esta fase también se define otro aspecto importante, el nivel de riesgo aceptable que la dirección ha aprobado.

Capítulo 5. Propuesta de proyectos

En este apartado se pueden consultar aquellos proyectos que contienen las mejoras planteadas a partir del análisis de riesgos, con el objetivo de eliminar o minimizar las amenazas a las que están expuestos los activos. Cada proyecto irá acompañado de una cuantificación económica y temporal.

Capítulo 6. Auditoría de cumplimiento de la ISO/IEC 27001:2013

Este capítulo se centra en el proceso de ejecución y el resultado de la auditoría de cumplimiento efectuado en la empresa. Se trata de evaluar los controles implantados en los proyectos definidos en la sección anterior, siendo el resultado un informe de las "*No Conformidades*" y las observaciones oportunas.

Capítulo 7. Presentación de resultados y entrega de informes

Superados todos los capítulos anteriores llega el momento de hacer la presentación del Plan de Implementación del SGSI. En esta fase se preparan los informes y la documentación necesaria de cara la dirección, así como la entrega del proyecto completo.

2. Situación actual: Contextualización, objetivos y análisis diferencial

2.1 Contextualización

La empresa TurisTech Balear SL se dedica al desarrollo de software y servicios especializados en el sector turístico. Se trata de una organización pequeña de pocos trabajadores y relativamente joven, puesto que solo han pasado 4 años desde que se constituyó. Esto hace que a día de hoy todavía existan aspectos a mejorar y otros por introducir.

En la actividad diaria de la empresa se genera y procesa información considerada como crítica, ya sea porque es vital para el funcionamiento del negocio o porque está regulada por ley. Por ejemplo, se pueden encontrar datos personales de sus empleados, de los clientes, de terceros, pagos con tarjetas de crédito o facturas electrónicas.

Actualmente, a pesar de que se aplican ciertas medidas de seguridad y que hay una persona a cargo de estas tareas, no existe una política de seguridad aprobada por la dirección. En consecuencia, por nombrar algunos ejemplos, los trabajadores no tienen bien claro las pautas de actuación ante un incidente de seguridad. Tampoco conocen lo que pueden hacer y lo que no con la información que manipulan, ni está estipulado el uso de los diferentes recursos de la empresa. Estas situaciones, en muchos casos, se resuelven sin seguir unos procedimientos bien definidos. Por otro lado, es necesario identificar debidamente los activos críticos y se desconocen, o al menos no está documentado, las amenazas y el impacto que pueden tener sobre los activos.

La decisión de implantar un Sistema de Gestión de la Seguridad de la Información o SGSI tiene una doble función. De una parte, conocer, gestionar y reducir los posibles riesgos que pueden afectar a la seguridad de la información de la empresa. Y de otra, validar que todos los procesos con información sujeta

a reglamentos y leyes están debidamente gestionados según su legislación, y en caso contrario, saber qué medidas se deben aplicar.

La certificación del SGSI según la norma ISO/IEC 27001:2013 no está definido como objetivo a corto o medio plazo.

2.2 Descripción de la empresa

2.2.1 Ubicaciones físicas

Las dependencias físicas están formadas por una única sede ubicada en Palma de Mallorca. Se trata de una primera planta de unos 60 m² distribuidos en una recepción, una sala de reuniones, el área principal de trabajo, baños y una habitación pequeña que realiza la función de almacén.

El teletrabajo está permito en la empresa, por lo que se considera que el domicilio de cada trabajador es una ubicación física a tener en cuenta de cara al alcance del Sistema de Gestión de Seguridad de la Información.

2.2.2 Plantilla

Está compuesta por los dos fundadores de la entidad y tres empleados en nómina, siendo su perfil el siguiente:

- 1 Ingeniero en Telecomunicaciones.
- 2 Ingenieros Técnicos en Informática.
- 1 Técnico de Grado Superior en Diseño de Aplicaciones Web.
- 1 Técnico de Grado Superior en Sistemas.

La modalidad del teletrabajo esa permitida sólo si el empleado cumple los siguientes criterios: Llevar un año y medio contratado para que tenga interiorizados los métodos y la dinámica de trabajo. Haber asumido su rol y que haya adquirido cierto nivel de autonomía en la organización y ejecución de tareas.

2.2.3 Modelo de negocio

Los clientes utilizan los servicios y aplicaciones que la propia empresa desarrolla mediante una modalidad SaaS. El soporte lógico y los datos se alojan en los servidores que tiene TurisTech Balear, los cuales son contratados a una empresa externa.

La actividad fundamental de la compañía se centra en el desarrollo de productos y servicios de tipo software orientados al sector turístico, siendo los principales clientes cadenas hoteleras y hoteles rurales. Los servicios más destacados son:

- **MBE**. Aplicación modular para los hoteles y hoteles rurales que les permite gestionar todas las tareas relacionadas con sus reservas. Los módulos principales que aquí son objeto de estudio son:

  - **Motor de reservas**. Se trata de un sistema web que permite a los clientes finales consultar hoteles, disponibilidad, tipo de habitaciones y servicios, para finalmente realizar una reserva.

  - **CRS**. Aplicación que los hoteles utilizan para gestionar diferentes aspectos del negocio, por ejemplo las tarifas, los precios, la disponibilidad o las reservas de los clientes finales.

- **Sistema de precheck-in**. Éste proyecto está en desarrollo y su función será permitir optimizar uno de los procesos más críticos en los hoteles, como es la recepción de los clientes y el procedimiento que conlleva.

- **Desarrollo web**. La empresa ofrece a sus clientes la posibilidad de contratar el servicio para diseñar su Web corporativas.

- **MBE-CM Sistema de integraciones**. Los hoteles y hoteles rurales exponen sus servicios en una gran variedad de entornos como touroperadores, agencias de viaje tradicionales y también de tipo online.

En la mayoría de los casos la información que circula entre los diferentes canales es heterogénea y por lo tanto, es necesario aplicar una serie de procesos para que los datos que llegan a los sistemas de los clientes sea válida y adecuada.

- **Soporte y formación**. Los clientes reciben formación para aquellos productos que contratan así como documentación específica. También se les ofrece un soporte de primer nivel para atender y resolver incidencias con los servicios y aplicaciones.

Los servicios que son objeto de estudio y de aplicación en el Sistema de Gestión de Información, son **MBE** y **MBE-CM**.

2.2.4 Clientes

Actualmente todos los clientes están ubicados en las Islas Baleares siendo mayoritariamente cadenas hoteleras y en menor grado hoteles rurales. Estos clientes contratan los servicios y aplicaciones que se encuentran implantados en servidores Cloud, que TurisTech Balear tiene contratados en una empresa externa con modalidad IaaS.

Para los clientes la información que les supone más valor y que se puede considerar como crítica son las reservas que realizan los usuarios, las cuales son procesadas y enviadas a sus destinos (hoteles) a través de las diferentes aplicaciones de TurisTech Balear.

2.3 Organigrama

Cómo se ha visto en el apartado anterior la compañía es una empresa sencilla a nivel organizativo e infraestructuras. Muchas de las funciones las realizan los propios fundadores, pero como se pretende que este proyecto sirva de ejemplo para cualquier pequeña empresa, se ha considerado que se tenían que separar las principales funciones en departamentos.

El organigrama queda de la siguiente forma:

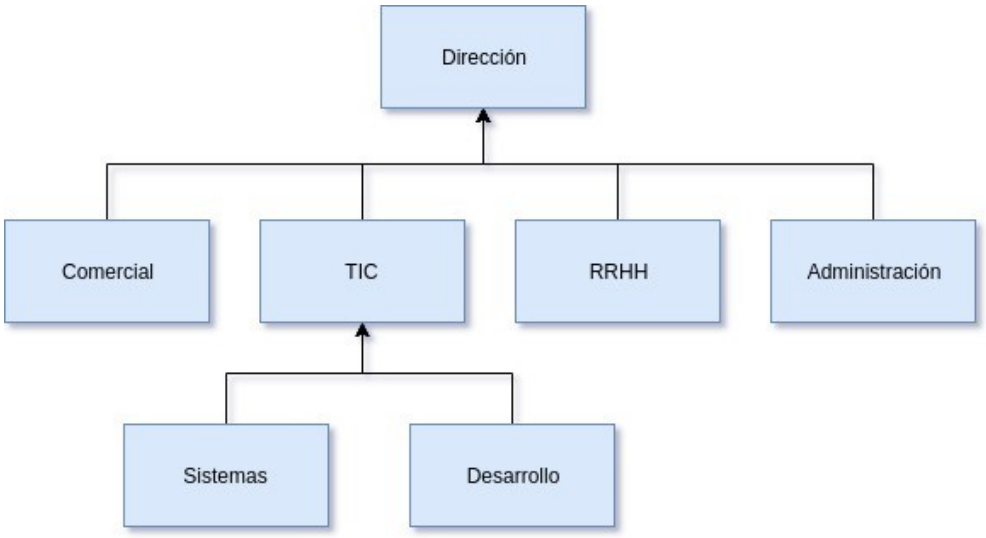

Figura 4: Organigrama de la empresa

Se describen de forma resumida cada uno de los departamentos:

- **Dirección**. Compuesta por los dos fundadores de la empresa, de los cuales dependen todas las decisiones que se toman a nivel organizativo y funcional de cada departamento.

- **Comercial**. Uno de los fundadores se encarga de atender, mantener y ampliar la cartera de clientes.

- **TIC**.

  - **Sistemas**. Este departamento es el encargado de mantener toda la infraestructura informática (hardware y software) de la empresa, así como de la gestión de las copias de seguridad. Está compuesto por un empleado y uno de los fundadores.

  - **Desarrollo**. Las funciones de desarrollo y mantenimiento de los diferentes servicios y productos descritos anteriormente es llevado a cabo por dos empleados y uno de los fundadores.

- **RRHH**. Todos los procesos de este departamento como la contratación de personal, la gestión de ausencias o la gestión de nóminas son distribuidas entre los dos fundadores.

- **Administración**. En este caso las tareas también se reparten entre los dos fundadores y además, se cuenta con el asesoramiento de una empresa externa para la elaboración y presentación de la documentación fiscal, así como de la seguridad social.

2.5 Infraestructura tecnológica

La empresa no dispone de un CPD (Centro de Procesamiento de datos) en sus dependencias, en su lugar la infraestructura de servidores se encuentra de forma online mediante un servicio IaaS contratado a una empresa externa. Tampoco existe una topología de red de área local (LAN) en la sede central para interconectar todos los equipos. Esto es posible porque la información y las aplicaciones compartidas se encuentran en repositorios y puntos remotos, que cada trabajador puede acceder desde cualquier lugar con acceso a Internet. Esta particularidad, junto con el hecho que la plantilla es pequeña, permite tener una infraestructura de sistemas simplificada, la cual se describe a continuación de forma resumida y sin profundizar en los detalles técnicos.

2.4.1 Hardware

En las instalaciones de la organización se encuentran los siguientes componentes:

- Una linea ADSL.
- Un router.
- Un ordenador personal.
- Dos portátiles
- Una impresora/fotocopiadora

Cada trabajador dispone en su domicilio de una área de trabajo compuesta de:

- Un router ADSL.
- Un portátil.

Como se ha comentado anteriormente, la empresa dispone sus servidores en una infraestructura en Cloud que contrata a empresas externas. El mantenimiento y gestión de estos equipos las lleva a cabo el Departamento de Sistemas interno. La siguiente figura muestra la representación conceptual de la infraestructura tecnológica descrita:

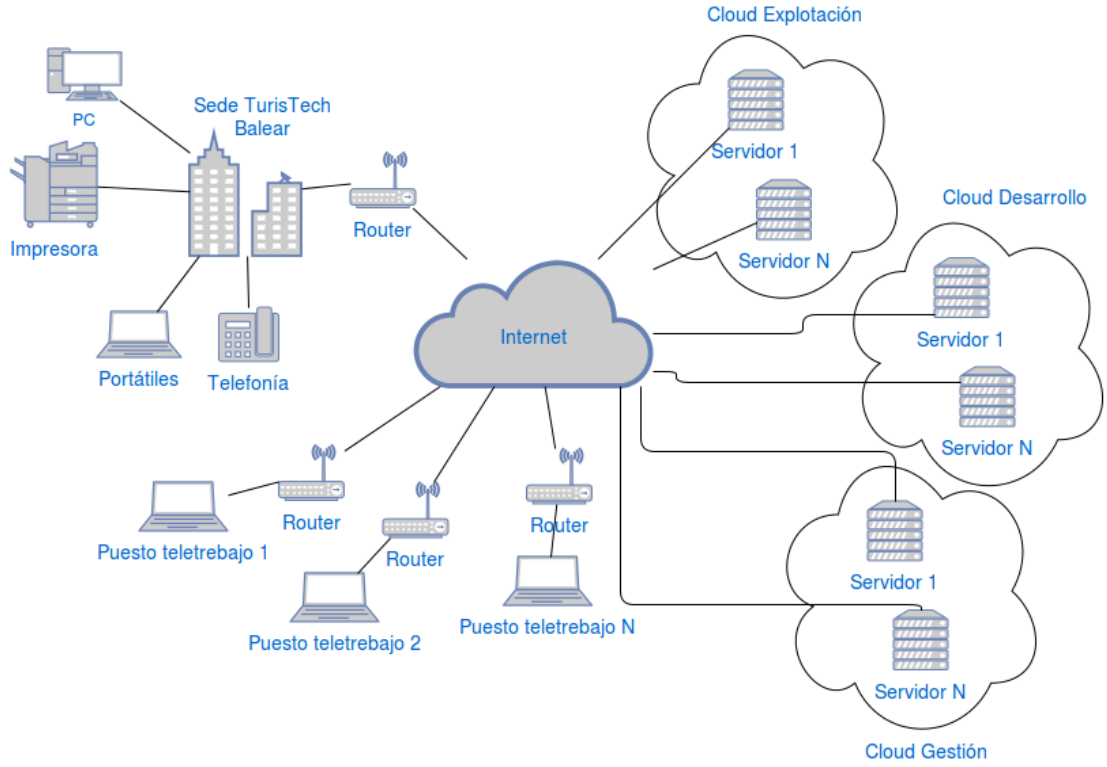

Figura 5: Infraestructura de la empresa

Como se puede observar, los servidores se encuentra distribuidos en tres Cloud distintos con lo que se consigue separar los entornos según su función. Esta parte de la infraestructura TIC es la más crítica, pues posee toda la información y los componentes lógicos que permiten la actividad diaria de la empresa.

Los empleados del departamento TIC que necesitan conectarse remotamente con los servidores, por ejemplo, para realizar tareas de mantenimiento de los

equipos y de gestión, se conectan a ellos mediante un terminal y el protocolo SSH (Secure Shell). Esto permite crear conexiones a través de las cuales los datos enviados y recibidos durante la sesión se transfieren de forma cifrada.

Seguidamente se describen las funciones de cada Cloud:

- **Cloud de explotación**. Compuesto por varios servidores que contienen los diferentes servicios y aplicaciones que los clientes contratan, junto con las bases de datos correspondientes.

- **Cloud de desarrollo**. En este entorno están los servidores que se utilizan para realizar el desarrollo, el mantenimiento y las pruebas de los distintos servicios, aplicaciones y bases de datos.

- **Cloud de gestión**. Aquí se ubican varios servidores muy importantes para la organización, como el servidor *Owncloud* que almacena toda la documentación que se genera en los diferentes proyectos. Un servidor *Git* para almacenar todo el código fuente, uno para la facturación y por último, el de monitoreo de los diferentes servicios y procesos.

2.4.2 Software

En relación al software interno la empresa mantiene una filosofía de usar, siempre que sea posible, proyectos Open Source o Software Libre.

Se resumen algunas de las aplicaciones y software utilizado en la empresa.

- Sistemas operativos:
  - Todos los portátiles que usan los empleados y el ordenador personal situado en la sede, disponen de un sistema operativo Linux Mint con versión mínima 18.1 Cinnamon 64-bit.

  - Los servidores están equipados con un sistema operativo Linux Debian Stretch.

- Gestión y planificación de proyectos:
  - Redmine

- Tareas ofimáticas:
  - LibreOffice

- Desarrollo:
  - Eclipse
  - Java
  - PHP
  - Apache Tomcat
  - Apache ActiveMQ
  - Apache Camel
  - Git

- Bases de datos:
  - BaseX
  - PostgreSQL

- Monitoreo de sistemas:
  - Icinga

- Comunicaciones:
  - Slack
  - Mozilla Thunderbird

2.5 Alcance del Plan Director de Seguridad

El alcance de un SGSI es un requisito de la norma ISO/IEC 27001:2013 descrito en la cláusula 4.3, que define aquellos procesos, áreas organizativas, emplazamientos y activos que quedan contemplados dentro de los límites del sistema de gestión.

Como ya se ha comentado, TurisTech Balear es una microempresa con un nivel de organización e infraestructuras bastante sencillo. La organización está distribuida en pocas áreas en las que un mismo empleado puede realizar funciones en varias de ellas. Teniendo en cuenta esta situación se acuerda con la dirección que el alcance del Plan Director de Seguridad abarque todos los activos de información de la empresa, cualquiera que sea la forma de soporte, así como los procesos y sistemas que los apoyan.

En concreto el alcance estará compuesto de:

- Los sistemas y equipos ubicados en la sede.
- Las zonas y equipos donde se realiza el teletrabajo.
- Los servidores ubicados en los sistemas Cloud.
- Todos los empleados de las distintas áreas de la empresa.
- Los servicios MBE y MBE-CM prestados a clientes.

2.6 Análisis diferencial

El paso previo a la implantación del SGSI consiste en revisar el estado inicial de la seguridad de la información existente en la empresa, en relación a los controles de seguridad definidos en la ISO/IEC 27002:2013. Posteriormente, con la información obtenida en el análisis, se realiza una valoración para conocer el grado de implantación que posee la entidad en contraste con el estándar.

Para realizar la valoración se ha usado la tabla que se describe a continuación basada en el Modelo de Madurez de la Capacidad (CMM)[5]. Consiste en establecer para cada control de la norma ISO/IEC 27002:2013 uno de los niveles definidos en la tabla 1 según su estado de implantación en la organización.

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

Tabla 1: Modelo de madurez de la capacidad CMM

2.6.1 Resultado del análisis

A partir del análisis diferencial se elabora una tabla que contiene los 14 capítulos principales de la norma ISO/IEC 27002:2013, junto con los porcentajes que reflejan su grado de implantación en la empresa. Hay que recordar que la entidad no tiene como objetivo la certificación del SGSI, lo que permite que los capítulos se puedan implantar según su prioridad y/o los objetivos y necesidades de la compañía.

En el Anexo I se pueden consultar los 14 capítulos desglosados con sus 114 controles revisados.

Capítulo	Valoración	Nivel CMM
5 Políticas de seguridad de la información	0 %	L0
6 Organización de la seguridad de la información	14,5 %	L1
7 Seguridad relativa a los recursos humanos	1,7 %	L0
8 Gestión de activos	16,7 %	L1
9 Control de acceso	38 %	L1
10 Criptografia	30 %	L1
11 Seguridad física y del entorno	50 %	L2
12 Seguridad de las operaciones	55,4 %	L2
13 Seguridad de las comunicaciones	37,5 %	L1
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	48,3 %	L2
15 Relación con proveedores	50 %	L2
16 Gestión de incidentes de seguridad de la información	7,1 %	L1
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	30 %	L1
18 Cumplimiento	13 %	L1

Tabla 2: Situación actual según ISO/IEC 27002:2013

Como se puede apreciar en la tabla anterior, los capítulos con mayor grado de implementación son aquellos que están relacionados con procesos y actividades más técnicas. Esto resulta lógico teniendo en cuenta que TurisTech Balear es una empresa tecnológica, que por naturaleza, estos aspectos se encuentran más asumidos e interiorizados.

Por otro lado, los capítulos con peor puntuación son los que tienen que ver con temas de gestión, documentación, organización y cumplimiento. Aunque todos los capítulos son importantes, el apartado *5 Políticas de Seguridad* o el *16 Gestión de Incidentes de Seguridad de la Información*, son fundamentales de cara a la implantación de un Sistema de Gestión de la Información basado en la norma ISO/IEC 27001:2013. Este hecho refleja que hace falta un mayor compromiso y dedicación en general, pero sobretodo por parte de la dirección.

Lo positivo de esta situación inicial es que ya existen medidas y procesos que son aprovechables. Es cierto que hay apartados que mejorar y otros donde hay una carga de trabajo importante debido a su bajo nivel inicial, pero en general, se puede decir que no se trata de una empresa con un grado de madurez inexistente o muy bajo, lo cual requeriría un esfuerzo aun mayor.

Seguidamente se sintetizan los resultados obtenidos mediante una serie de gráficos que facilitan su comprensión.

La figura 6 muestra de qué forma están distribuidos los controles por cada nivel CMM. De los 114 controles analizados no hay ninguno en los niveles “Gestionado” ni “Optimizado”, y sólo un 4% se encuentra “Definido”. Esta situación refleja un alto recorrido de mejora y un grado de madurez medio-bajo en lo que respecta a la seguridad de la Información.

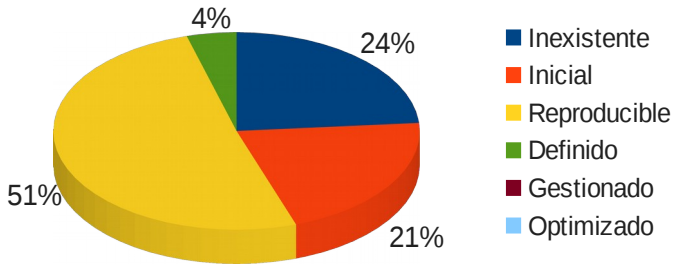

Figura 6: Distribución de controles ISO/IEC 27002:2013

En el siguiente gráfico de barras se puede observar el porcentaje de cumplimiento inicial por áreas. Destacan negativamente los bajos valores de las áreas 5 Políticas de seguridad de la información, 7 Seguridad relativa a los recursos humanos y 16 Gestión de incidentes de seguridad de la información, en las cuales se deberá hacer un esfuerzo importante para alcanzar unos niveles adecuados.

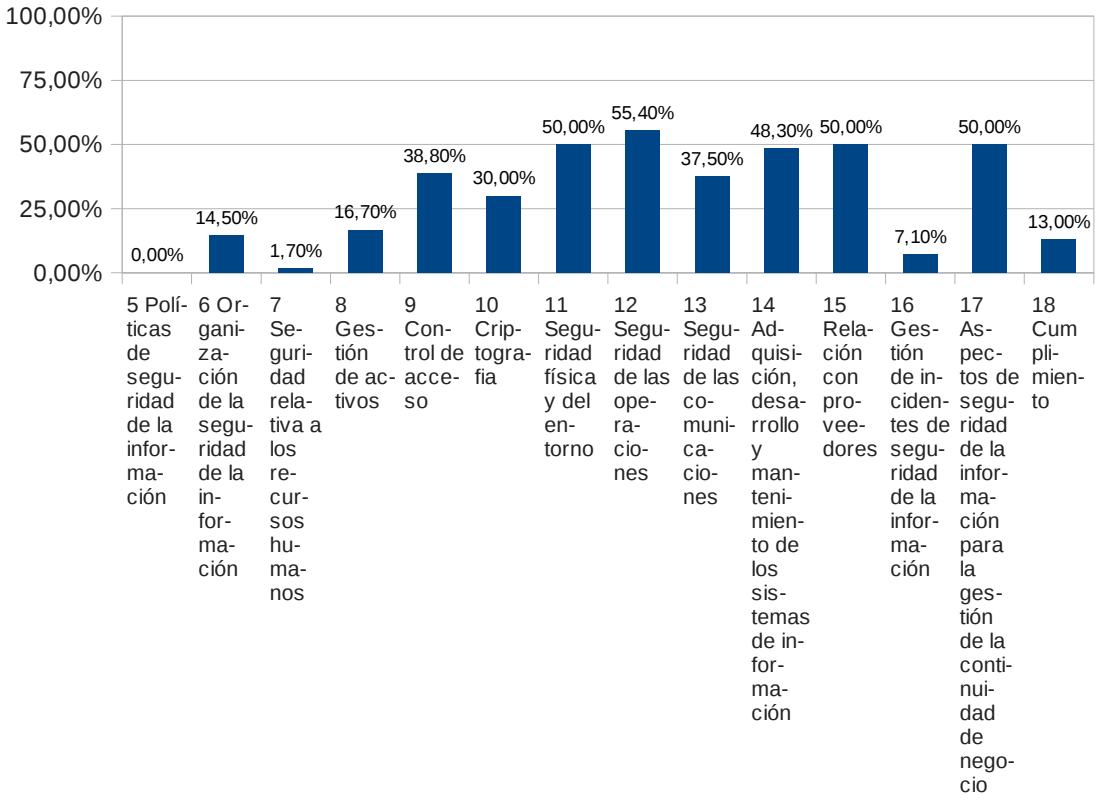

Figura 7: Cumplimiento inicial por áreas

Como aspecto positivo, resaltar que hay varias áreas con valores próximos al 50%, lo que permitirá que normalizando lo que ya se está realizando de forma intuitiva puedan llegar a un nivel de madurez “Definido” (L3). Del total de 114 controles que dispone la norma ISO/IEC 27002:2013, sólo se han detectado 3 que no son de aplicación y que se comentan en la Declaración de Aplicabilidad (Anexo VII).

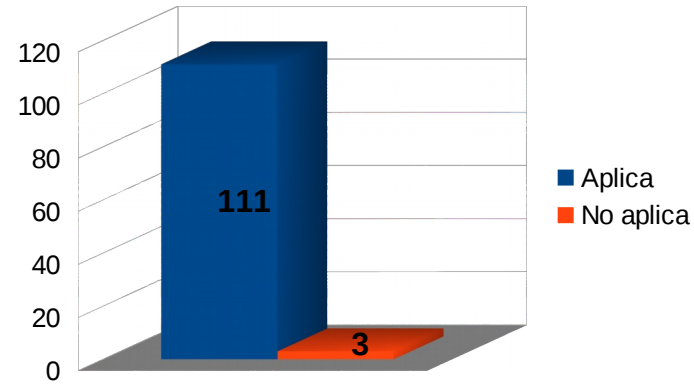

Figura 8: Controles de aplicación

Por último está el análisis GAP que permite ver las diferencias entre dos puntos de referencia. Con la dirección se ha acordado que la situación deseada que la empresa pretende obtener es el nivel L3 (Proceso definido) de madurez, de los controles ISO/IEC 27002:2013. La figura 6 muestra la situación actual de la entidad, color morado, respecto al objetivo, en naranja. Como se puede apreciar, hay una gran distancia entre ambos estados lo que evidencia que queda mucho trabajo por hacer.

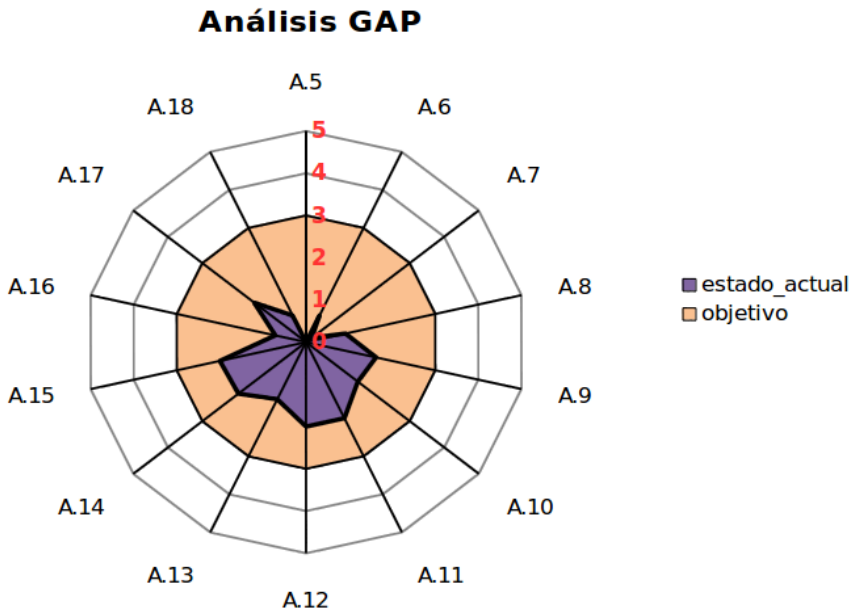

Figura 9: Resultado análisis GAP. Estado actual y objetivo de la empresa

3. Sistema de Gestión Documental

3.1 Introducción

El volumen de información que generan las compañías actuales crece de forma exponencial, originando que las empresas den cada vez más importancia a los sistemas de gestión documental. Estos sistemas consisten en controlar de un modo eficiente y sistemático la creación, la recepción, el mantenimiento, la utilización y la disposición de los documentos.

La gestión documental es un aspecto fundamental para la conformidad con la norma ISO/IEC 27001, la cual se basa el SGSI a implantar en TurisTech Balear.

En la seguridad de la información se suele utilizar la pirámide jerárquica de documentos que indica la forma de organizarlos. En la cima se sitúan los documentos de mayor importancia y más generalizados. El nivel de concreción y detalle aumenta a medida que se baja en los niveles de la pirámide, por eso la documentación situada en los escalones inferiores está más orientada a personal especializado. De forma general, un documento de nivel superior se desarrolla en los de nivel inferior.

Figura 10: Pirámide de documentos

3.2 Política de seguridad

En un sistema de gestión de la seguridad el estándar más importante es el documento que define la Política de Seguridad de la Información, situándose en el nivel más alto de la pirámide jerárquica.

El principal objetivo de dicho documento es establecer las directrices en seguridad de la información, alineadas con los objetivos del negocio y la legislación aplicable. La dirección de la organización debe conocer, aprobar y comprometerse con la política de seguridad.

La política de seguridad se encuentra definida en el Anexo II.

3.3 Procedimiento de Auditorías Internas

Este procedimiento (Anexo III) tiene como objetivo determinar la conformidad y eficacia del Sistema de Gestión de Seguridad de la Información, en base a criterios y lineamientos para planificar, preparar, ejecutar y registrar las auditorías internas de seguridad. A partir de los informes generados en las auditorías será posible verificar si se cumplen las disposiciones preestablecidas con respecto a la norma ISO/IEC 27001 y a los objetivos fijados en la empresa.

3.4 Gestión de Indicadores

Los indicadores son métricas generales que permiten evaluar la eficiencia y la eficacia de un SGSI. La efectividad de estos sistemas está proporcionalmente relacionada con la efectividad de los controles implantados en la organización, siendo los indicadores el medio para obtener esta información.

Con los resultados de los indicadores es posible realizar un informe periódico sobre como se está desarrollando la gestión de la seguridad de los sistemas de información. Es importante que el indicador asegure la fiabilidad de la medición y que se sea un proceso repetible.

Consultar el Anexo IV para ver los indicadores definidos para el SGSI de TurisTech Balear.

3.5 Procedimiento de Revisión por Dirección

Este procedimiento (ver Anexo V) permite establecer los criterios y requisitos para la revisión por parte de la alta dirección, con la finalidad de determinar si el Sistema de Gestión de Seguridad de la Información cumple con los requisitos de la norma ISO/IEC 27001:2013 y el marco legal aplicable.

La dirección de la organización debe revisar de forma periódica las cuestiones más importantes que van sucediendo en relación al Sistema de Gestión de Seguridad de la Información. Resulta imprescindible que los directivos estén al corriente de la conveniencia, adecuación y eficacia del sistema para poder aplicar mejoras o efectuar cambios allá donde sea necesario.

3.6 Gestión de Roles y Responsabilidades

La implantación de un Sistema de Gestión de Seguridad de la Información y los procesos que en él se definen, genera la necesidad de establecer roles y responsabilidades. Sin estos, se corre el riesgo que la gestión y la ejecución de las tareas en materia de seguridad sea incorrecta o poco eficaz. Es por ello que una de las primeras tareas a realizar en la implantación del SGSI es formar una estructura interna con responsabilidad directa sobre la seguridad de la información, que permita crear, mantener, supervisar y mejorar el sistema.

Las personas tanto internas como externas con acceso a la información de la empresa, deben conocer cuales son sus funciones y las responsabilidades que deben asumir en materia de la seguridad.

El Anexo VI contiene los roles y responsabilidades asignados en TurisTech Balear, SL.

3.7 Metodología de Análisis de Riesgos

Los Sistemas de Gestión de Seguridad de la Información que se implantan bajo la norma ISO/IEC 27001, tienen como requerimiento realizar un análisis de riesgos. Esta herramienta permite obtener una visión objetiva y priorizada de los riesgos a los que está expuesta una organización.

Si bien, cada entidad puede plantear su propio método, la mejor opción es utilizar una metodología ya definida (ahorra tiempo y esfuerzos), reconocida (aporta fiabilidad) y contrastada (esta validada).

Para realizar el análisis de riesgos de la empresa TurisTech Balear se ha elegido la metodología MAGERIT (ver Anexo VII) en su versión 3.0.

3.8 Declaración de Aplicabilidad

La Declaración de Aplicabilidad o SoA (del inglés Statement of Applicability) es un requisito del estándar ISO/IEC 27001:2013 que deben cumplir las entidades que pretendan certificar dicha norma. Las que no persigan este objetivo no tienen porque redactarlo, no obstante, se recomienda su utilización como forma de mantener un registro y control de las medidas de seguridad que son aplicadas dentro del Sistema de Gestión de Seguridad de la Información.

La Declaración describe cada control que es aplicable y los que no junto con una justificación. También puede indicar si las medidas se encuentran implementadas o no, convirtiendo el documento en una guía muy útil para las auditorías.

La Declaración de Aplicabilidad de la empresa TurisTech Balear, SL se puede consultar en el Anexo VIII.

4. Análisis de Riesgos

4.1 Introducción

Como se ha comentado en el capítulo 3, la metodología que se usará para realizar el análisis de riesgos es MAGERIT v3.0 (ver Anexo VII). La información incluida en este capítulo se ha extraído de la documentación oficial del método.

En el "*Libro I – Método"*[6] de la versión 3.0 de MAGERIT podemos encontrar la siguiente definición: "*el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados".* Estas pautas consisten en:

1. Determinar los activos relevantes para la organización, su interrelación y su valor en el sentido de qué perjuicio (coste) supondría su degradación.

2. Determinar a qué amenazas están expuestos los activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Cabe destacar que el proceso de análisis de riesgos da como resultado una información y no una medida de seguridad como tal. No obstante, gracias a esta información, a la organización le resultará más fácil protegerse frente a situaciones que representen un riesgo.

A partir de los pasos indicados anteriormente aparecen una serie de elementos y relaciones entre ellos que se resumen en la figura 11[6]:

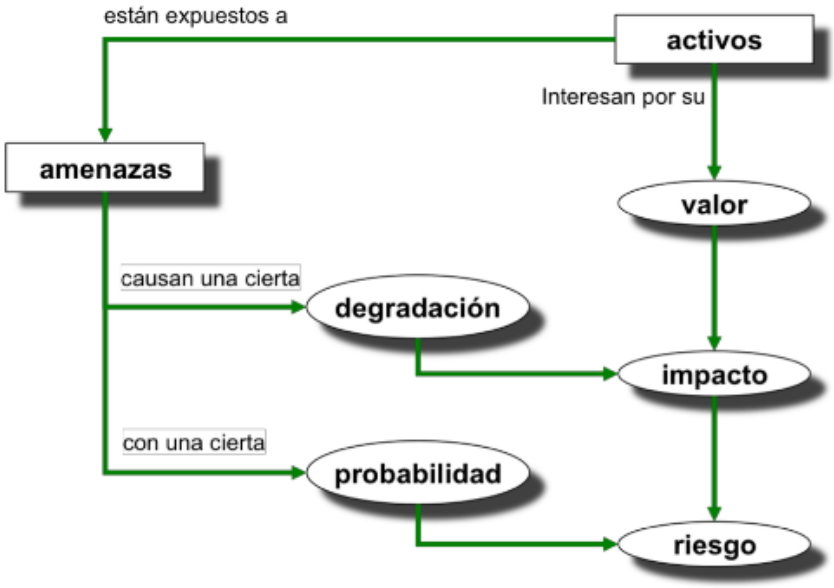

Figura 11: Elementos del análisis de riesgos

4.1.1 Activo

Son todos los componentes, funcionalidades o servicios del sistema de información de la organización esenciales para la actividad del negocio y susceptibles a ser atacados, provocando unas consecuencias en la entidad. Estos pueden agruparse en distintas categorías tal como se describe en el apartado 4.2 de éste capítulo.

Los activos pueden depender de otros llegando a formar un árbol o grafo de dependencias, en el cual la seguridad de los nodos de niveles superiores se ve afectada por los nodos inferiores. De aquí surge el concepto de “dependencias entre activos” que es la medida en que un activo “superior” se ve afectado por uno “inferior”.

4.1.2 Amenaza

Causa potencial de un incidente que puede causar daños a los activos de una organización impidiendo que funcionen correctamente. Las amenazas pueden

tener un origen natural, industrial, por errores o fallos no intencionados, y finalmente, por ataques intencionados.

4.1.3 Vulnerabilidad

Es una debilidad o fallo en un activo de información que pone en riesgo su seguridad, al permitir que una amenaza pueda comprometer la integridad, disponibilidad o confidencialidad de la información.

Las vulnerabilidades pueden darse por diversas causas, por ejemplo, por fallos de diseño, por codificación insegura, por falta de mantenimiento, carencia de procedimientos, poca capacitación en materia de seguridad en las personas, o bien, simples errores de configuración.

4.1.4 Impacto

Se refiere a la medida del daño sobre el activo provocado por la materialización de una amenaza, fruto de una vulnerabilidad.

4.2 Inventario de activos

La primera fase del análisis de riesgos consiste en realizar un inventario de los activos del sistema de información que son imprescindibles para la entidad. No es una tarea fácil e incluso puede llegar a ser abrumadora en aquellas organización más complejas y de mayor tamaño, debido al gran volumen de activos que pueden llegar a gestionar.

Independientemente del tipo y organización, en un sistema de información hay 2 activos esenciales: la información que maneja y los servicios que presta. A partir de estos, quedan subordinados otro conjunto de activos que MAGERIT los clasifica según los siguientes ámbitos:

- **Instalaciones** [L]. Se incluyen los lugares físicos donde se hospedan los sistemas de información y comunicaciones.

- **Hardware** [HW]. Componentes físicos que soportan de forma directa o indirecta los servicios que presta la organización. Contienen los datos y las aplicaciones informáticas responsables del procesado o transmisión de datos.

- **Aplicación** (software) [SW]. Hace referencia a los programas, aplicaciones y desarrollos.

- **Datos** (información) [D]. Permiten a una organización prestar sus servicios y son almacenados en equipos o soportes de información.

- **Redes** [COM]. Se centra siempre en elementos o medios de transporte de datos de un sitio a otro. Se incluyen tanto las instalaciones dedicadas como servicios de comunicaciones contratados a terceros.

- **Servicios** [S]. Son aquellas funciones o servicios internos que cubren las necesidades de los usuarios.

- **Equipamiento auxiliar** [AUX]. Elementos que sirven de soporte a los sistemas de información sin estar directamente relacionados con los datos.

- **Personal** [P]. Son aquellas personas relacionadas con los sistemas de información.

Hay que tener presente que los activos de información van cambiando con el tiempo y lo que no es importante para hoy puede llegar a serlo en un futuro. Por este motivo, es recomendable revisar y mantener el inventario en períodos de tiempo establecidos.

Para consultar el inventario de activos ver el Anexo IX.

4.3 Valoración de activos

Una vez elaborado el inventario de activos se procede con la segunda fase, que consiste en ejecutar una valoración de cada uno de ellos, ya sea de forma cualitativa, cuantitativa o una combinación de ambas. Para realizar esta tarea, es necesario definir una escala de valores en la cual situar cada uno de los elementos que se van a analizar.

La metodología MAGERIT, en su "*Libro III – Guía de Técnicas"*[10], define una escala de valores que puede aplicarse en diferentes escenarios, por ejemplo, la valoración de los activos, la magnitud del impacto o la magnitud del riesgo.

- **MB**: muy bajo
- **B**: bajo
- **M**: medio
- **A**: alto
- **MA**: muy alto

No obstante, para realizar una valoración económica estos valores no permiten precisar el coste de un activo, por ello, se les ha asociado unos rangos cuantitativos dando como resultado la tabla 3. Ésta especifica el valor estimado utilizado para todos los activos, la valoración de los cuales se corresponde con uno de los rangos económicos definidos:

Valor	ID	Rango	Valor estimado
Muy alto	MA	Valor > 100.000 €	200.000 €
Alto	A	50.000 € < valor > 100.000 €	75.000 €
Medio	M	10.000 € < valor > 50.000 €	30.000 €
Bajo	B	1.000 € < valor > 10.000 €	5.000 €
Muy bajo	MB	< 1.000 €	1.000 €

Tabla 3: Valores estimados para los activos

Para asignar el valor estimado a cada uno de los activos se han tenido en consideración los siguientes factores:

- **El valor de reposición**. Cuánto le cuesta a la organización reponer un activo en caso de pérdida o inutilidad.

- **El valor de configuración**. Corresponde al tiempo que pasa desde que se adquiere un nuevo activo hasta que está en las mismas condiciones de uso que el anterior. Se estipula un precio de 50 euros por hora de reparación o configuración.

- **El valor de uso**. Hace referencia a la pérdida que sufre la empresa durante el tiempo que no puede utilizar el activo. Para este factor hay que tener en cuenta que la empresa no tiene establecido con sus clientes ningún acuerdo de nivel de servicio o SLA (del inglés *Service Level Agraement*). No obstante, de cara a la empresa sí que existen unas pérdidas que corresponden al tiempo que el activo no produce. El valor acordado con la dirección es de 50 euros por hora sin uso.

Adicionalmente, hay que tener en cuenta la jerarquía de los activos según la dependencia existente entre ellos. Éste árbol o grafo muestra de arriba a abajo las dependencias entre activos, mientas que de abajo hacia arriba refleja la propagación del daño en caso de materializarse una amenaza.

Para facilitar la identificación de estas dependencias, tal como refleja la figura 12, se han definido un conjunto de capas en las que se agrupan los activos. Se observa como las personas afectan a todos los niveles:

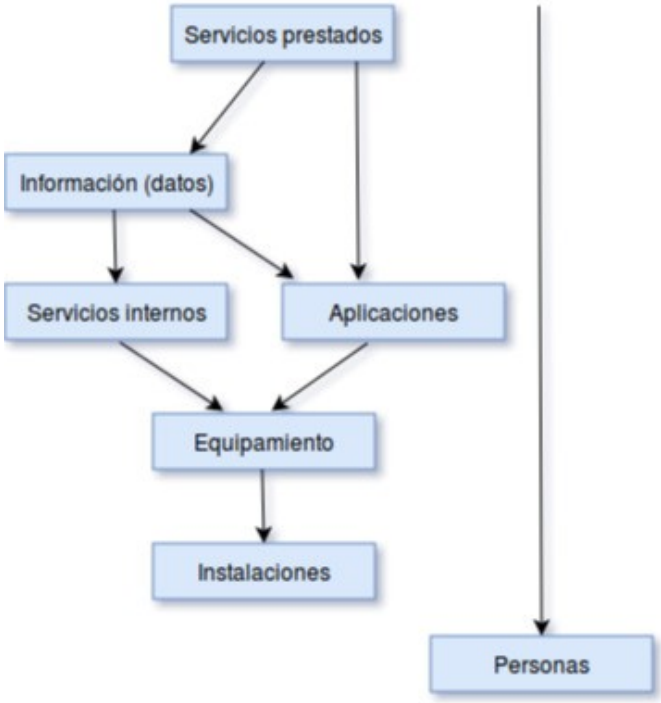

Figura 12: Organización de activos por capas

La tabla 4 muestra la valoración según los ámbitos definidos (el análisis detallado puede verse en Anexo X). Como puede observarse, los activos más valiosos para la organización, económicamente hablando, corresponden al ámbito Hardware, Aplicación, Datos y Personal. Esta situación tiene su lógica teniendo en cuenta el perfil tecnológico y el tipo de negocio de la empresa. El resto de activos, aunque importantes para la entidad, no tienen el mismo carácter crítico pues pueden ser reparados o sustituidos de una forma relativamente fácil y/o rápida.

Ámbito	Valor total €
[L] Instalaciones	10.000
[HW] Hardware	612.000
[SW] Aplicación (Software)	533.000
[D] Datos	677.000
[COM] Redes	3.000
[S] Servicios	4.000
[AUX] Equipamiento auxiliar	10.000
[P] Personal	270.000

Tabla 4: Valor total de activos por ámbito

La siguiente figura representa la misma información de forma gráfica.

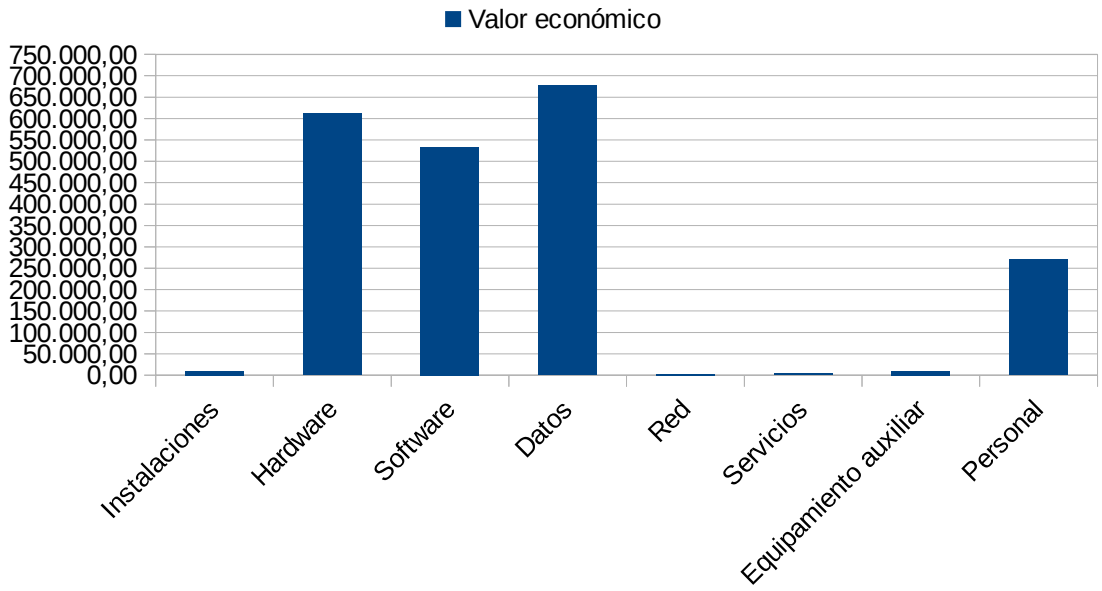

Figura 13: Valor económico de los activos

Algunos ámbitos presentan valores muy bajos como las Instalaciones, la Red o los Servicios, debido a que no hay un volumen alto de activos o una fuerte dependencia hacia ellos. Por ejemplo, así como en otras empresas similares las instalaciones tienen un gran valor, no es el mismo caso en TurisTech Balear al no disponer de servidores y CPD en sus propias dependencias. Algo similar ocurre con el ámbito Red, al no tener implantada una topología de red local donde conectar y compartir distintos recursos y todo lo que ello implica.

4.4 Dimensiones

Según la criticidad de la información que contienen los activos pueden verse afectadas una o más dimensiones de la seguridad, que tradicionalmente se han dividido en:

- **Disponibilidad [D]**: Valor cualitativo o cuantitativo que determina la importancia que tiene la ausencia del activo o no poder usarlo.

- **Integridad [I]**: Valor cualitativo o cuantitativo que determina las repercusiones que tendría para el negocio la manipulación del activo, ser total o parcialmente falsos o, incluso, que sean incompletos.

- **Confidencialidad [C]**: Valor cualitativo o cuantitativo que determine el grado de daño que causaría el acceso a información confidencial sin autorización.

Además, MAGERIT contempla dos dimensiones que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos:

- **Autenticidad [A]**: Valor cualitativo o cuantitativo que determina la necesidad de garantizar que un individuo o sistema es quien dice ser. Normalmente está relacionado con los accesos a sistemas y servicios.

- **Trazabilidad [T]**: Valor cualitativo o cuantitativo que determina la importancia de saber que acciones y usos se le da a un activo, así como quien las realiza y en que momentos.

Cada dimensión de seguridad afectada se adscribirá a uno de los niveles definidos en la taba 5.

Valor		Criterio
10	Muy Alto [MA]	Daño muy grave
7-9	Alto [A]	Daño grave
4-6	Medio [M]	Daño importante
1-3	Bajo [B]	Daño menor
0	Muy Bajo [MB]	Daño irrelevante

Tabla 5: Valores de criticidad para las dimensiones de seguridad

Seguidamente, para cada nivel definido se concreta su significado y las implicaciones que tienen. De esta forma será posible valorar los activos en relación a las dimensiones de seguridad y los criterios establecidos.

a) **Muy Alto [MA] (daño muy grave)**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las

dimensiones de seguridad, supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados, ya sean internos o externos. Se entenderá por perjuicio muy grave:

1. La anulación de la capacidad de la organización para llevar a cabo sus funciones fundamentales y que éstas sigan desempeñándose, parando la actividad principal del negocio.

2. Que los activos de la organización sufran un daño muy grave e incluso irreparable.

3. El incumplimiento total de varias leyes y/o regulaciones.

4. Causar un perjuicio muy grave a algún individuo interno o externo, de difícil o imposible reparación.

b) **Alto [A] (daño grave)**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados, ya sean internos o externos. Se entenderá por perjuicio grave:

1. La reducción de la capacidad de la organización para atender a algunas de sus obligaciones fundamentales, pero no hay parada del negocio.

2. Que los activos de la organización sufran un daño grave que sea difícil de reparar.

3. El incumplimiento total de una ley o regulación.

4. Causar un perjuicio grave a algún individuo interno o externo de difícil reparación.

c) **Medio [M] (daño importante)**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio importante sobre las funciones de la organización, sobre sus activos o los individuos internos. Se entenderá por perjuicio medio:

1. La reducción significativa de la capacidad de la organización para atender de forma eficaz a algunas de las obligaciones básicas, aunque estas puedan seguir desempeñándose.

2. Que los activos de la organización sufran un daño significativo y su reparación requiera cierto esfuerzo.

3. El incumplimiento parcial de alguna ley o regulación que sea posible subsanar.

4. Causar un perjuicio moderado a algún individuo interno de difícil reparación.

d) **Bajo [B] (daño menor)**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio menor sobre las funciones de la organización, sobre sus activos o los individuos internos. Se entenderá por perjuicio menor:

1. Una reducción menor en la capacidad de la organización para atender a algunas de las obligaciones corrientes, pero pueden seguir ejecutándose con normalidad.

2. Que los activos de la organización sufran un daño menor y su recuperación resulte fácil.

3. El incumplimiento parcial de alguna normativa interna que sea posible subsanar.

4. Causar un perjuicio menor a algún individuo interno de fácil reparación.

e) **Muy Bajo [MB] (daño irrelevante)**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad no suponen un perjuicio sobre las funciones de la organización, sobre sus activos o los individuos internos. Se entenderá por perjuicio irrelevante:

1. Cuando el daño no repercute en la capacidad de la organización para atender a todas sus obligaciones y puedan seguir ejecutándose con total normalidad.

2. Que los activos de la organización sufran un daño que no requiera de una solución a corto o medio plazo.

3. Cuando no afecta a ninguna ley o regulación ni a la normativa interna que sean de aplicación en la organización.

4. Cuando el incidente no resulta molesto para los individuos internos o externos y no requiere ningún tratamiento.

4.4 Resumen de valoración

A partir de la información obtenida hasta ahora, es posible generar una tabla resumen que refleje la importancia o participación que tienen los activos en la cadena de valor de los servicios, así como su criticidad en las dimensiones de seguridad de la información. Para su valoración se usarán las categorías “Muy alta”, “Alta”, “Media”, “Baja” o “Irrelevante”, a la vez que se asignará a cada dimensión un valor entre 0 y 10, según la tabla 5 descrita anteriormente.

Según la valoración obtenida, el 45% de los activos está catalogado con una importancia “Alta” o “Muy alta”, a los que la organización deberá prestar una atención especial.

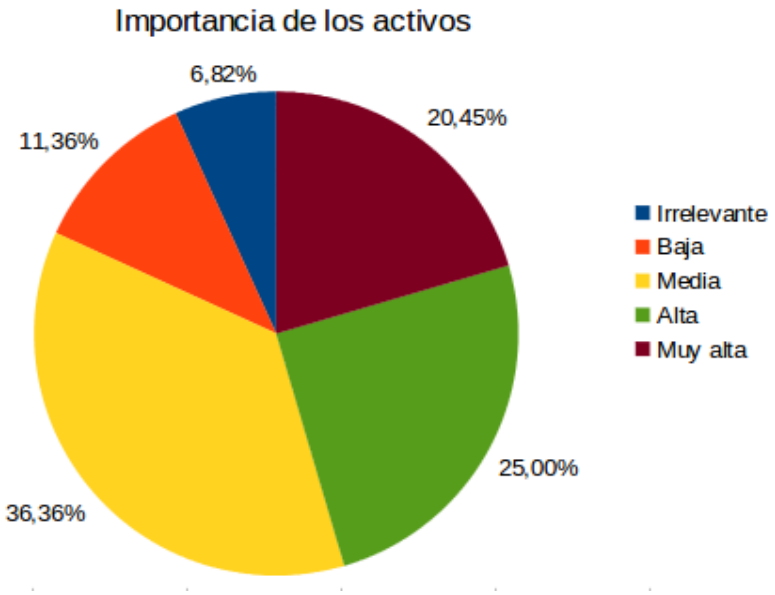

Figura 14: Distribución según importancia del activo

Para consultar la tabla resumen de valoración ver el Anexo XI.

4.5 Análisis de amenazas

Según la definición que se puede encontrar en la norma UNE 71504:2008: “*una amenaza es la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización*”.

Los activos de información de TurisTech Balear están expuestos a un conjunto de amenazas, las cuales deben ser identificadas y evaluadas para conocer su probabilidad de ocurrencia. Para realizar éste análisis se ha utilizado una lista de amenazas comunes definidas por la metodología MAGERIT, así como una tabla que mapea la frecuencia a un número de veces por año.

Las amenazas se clasifican de la siguiente forma (para más detalle ver el apartado 3.4 del Anexo VII):

- Desastres naturales [N].
- De origen industrial [I].
- Errores y fallos no intencionados [E].
- Ataques intencionados [A].

Para determinar la tasa de probabilidad de materialización de una amenaza se ha utilizado la tabla 6, basada en el modelo habitual de usar 1 año como referencia. Se incluye la columna “Valor mapa” que se utilizará más adelante para poder crear un mapa de calor al del riesgo.

Vulnerabilidad	ID	Rango	Valor	Valor mapa
Frecuencia muy alta	FMA	1 vez al día	100	5
Frecuencia alta	FA	1 vez al mes	10	4
Frecuencia media	FM	1 vez al año	1	3
Frecuencia baja	FB	1 vez cada varios años	0,1	2
Frecuencia muy baja	FMB	1 vez cada varias décadas	0,01	1

Tabla 6: Clasificación de la vulnerabilidad

Se ha optado por usar los rangos finales de FB (varios años) y FMB (varias décadas) en lugar de indicar como máximo un rango de 1 año, porque se considera que la ocurrencia de ciertas amenazas de forma anual no entra dentro de la normalidad, al menos para la entidad aquí tratada. Por ejemplo, pueden pasar décadas sin que ocurra un incendio, una inundación o un robo.

A modo de resumen se comentan las amenazas identificadas con mayor probabilidad de producirse según su ámbito:

Ámbito	Amenaza	Frecuencia
[L] Instalaciones	[N.*] Desastres naturales (rayo, tormenta eléctrica) [I.2] Daños por agua (industrial accidental o provocado) [A.18] Destrucción de información	1 vez cada varios años
[HW] Hardware	[I.6] Corte del suministro eléctrico [E.2] Errores del administrador [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos	1 vez al año
[SW] Aplicación (Software)	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios	1 vez al año

	[E.2] Errores del administrador [E.21] Errores de mantenimiento / actualización de programas (software)	
[D] Datos	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración	1 vez al año
[COM] Redes	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador [E.24] Caída del sistema por agotamiento de recursos	1 vez al año
[S] Servicios	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.24] Caída del sistema por agotamiento de recursos	1 vez al año
[AUX] Equipamiento auxiliar	[I.6] Corte del suministro eléctrico	1 vez al año
[P] Personal	[E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal (ausencia por enfermedad, altercados públicos)	1 vez al año

Tabla 7: Listado de principales amenazas por ámbito

El análisis completo de las amenazas puede consultarse en el Anexo XII.

4.6 Evaluación del impacto potencial

Con la información obtenida en la tabla de análisis de amenazas y la valoración de los activos es posible calcular el impacto potencial. Éste representa el daño que se produce a un activo derivado de la materialización de una amenaza. Tal como se describe en apartado 3.6 del Anexo VII el cálculo del impacto potencial se realiza de la siguiente forma:

Impacto potencial = Valor activo x Porcentaje de impacto

Los niveles de impacto y porcentajes asociados para la empresa quedan definidos en la tabla 8.

Impacto	Valor	Valor mapa
Muy alto	100%	5
Alto	75%	4
Medio	50%	3
Bajo	20%	2
Muy bajo	5%	1

Tabla 8: Niveles de impacto

Al igual que en la tabla 6, se incluye la columna “Valor mapa” para facilitar la creación de un mapa de calor del riesgo.

La evaluación del impacto potencial resulta de gran importancia a la hora de priorizar los planes de acción. Además, permite valorar la eficacia de las contramedidas aplicadas para reducir el riesgo, según varía el valor del impacto.

El resultado del impacto potencial puede consultarse en el Anexo XIII.

4.7 Nivel de riesgo aceptable y riesgo residual

El “*umbral de riesgo aceptable”* es el nivel máximo de riesgo que la empresa está dispuesta a soportar. Todo valor que supere dicho umbral deberá ser gestionado hasta situarlo por debajo del límite establecido. Esto se consigue aplicando un conjunto de controles o salvaguardas que permitirán reducir el riesgo. No obstante, la eliminación total del riesgo no es posible quedando un remanente que se conoce como “*riesgo residual”*. Para reducir o mitigar los riesgos pueden aplicarse diferentes acciones, por ejemplo:

- Instalar productos y equipos o contratar servicios.
- Establecer controles de seguridad.
- Mejorar los procedimientos.
- Cambiar o adecuar el entorno.
- Incluir métodos de detección temprana.
- Implantar un plan de contingencia y continuidad.
- Realizar formación y sensibilización.

El nivel de tolerancia del riesgo se ha establecido en base a criterios de coste-beneficio, con los que se busca mantener un equilibro entre el coste de protección y el de exposición. El objetivo es no gastar más en protección de lo

que representa recuperarse de una situación adversa. La figura 15 representa gráficamente esta situación[7]:

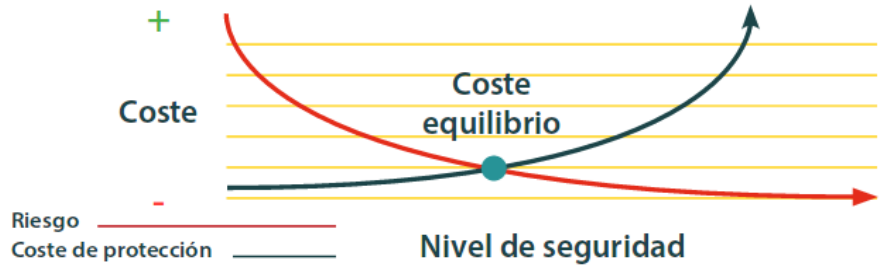

Figura 15: Umbral de riesgo aceptable

Además del coste del propio activo se han tenido en consideración los siguientes criterios:

- Los daños personales.
- Las pérdidas financieras.
- El incumplimiento de leyes y reglamentos.
- La interrupción del servicio.
- La pérdida de imagen y reputación.
- La disminución del rendimiento.

Según los criterios anteriores y la información obtenida en el análisis de riesgos, la dirección de TurisTech Balear ha acordado y aprobado que el umbral del riesgo esté situado en el **valor 7**. A partir de este nivel establecido es posible calcular el riesgo para cada activo según lo indicado en el apartado 3.7 del Anexo VII, en el que se define la siguiente fórmula:

Riesgo intrínseco = Impacto potencial x Vulnerabilidad (Frecuencia amenaza)

Hay que tener en cuenta que MAGERIT interpreta las vulnerabilidades como la frecuencia de ocurrencia de una amenaza.

A modo de resumen, la figura 11 muestra el riesgo calculado para cada activo mediante un mapa de calor, correspondiente al producto de las columnas “Valor mapa” de las tablas 6 y 8. Este sistema permite identificar el riesgo de una forma más fácil y visual. Para ello se ha utilizado la matriz de la tabla 9, que consiste en asignar un color para los distintos rangos de valores obtenidos con la fórmula del riesgo:

Probabilidad					
Muy alta (5)	5	**10**	15	**20**	**25**
Alta (4)	4	8	**12**	16	**20**
Media (3)	3	6	9	**12**	15
Baja (2)	2	4	6	8	**10**
Muy baja (1)	1	2	3	4	5
	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy Alto (5)
			Impacto		

Tabla 9: Matriz del riesgo

- 1-4 = riesgo muy bajo (azul claro)
- 5-9 = riesgo bajo (verde)
- 10-12 = riesgo medio (azul)
- 15-16 = riesgo alto (amarillo)
- 20-25 = riesgo muy alto (rojo)

Como se puede observar en la figura 16, según los cálculos realizados y la matriz anterior no se han identificado activos con un nivel de riesgo muy alto (color rojo) estando la mayoría de ellos entre los rangos bajo y medio.

Por otro lado, existen muchos activos que sí superan el umbral del riesgo establecido por la entidad, los cuales se identifican en la figura 17. Éstos deberán ser gestionados según los controles que se definan.

Todos los cálculos pueden consultarse en la hoja de cálculo adjunta con el nombre: *TFM_MISTIC_Josep_Sureda_PAC3.ods*

Activo	Mapa calor riesgo				
	[A]	[C]	[I]	[D]	[T]
Oficina	0	0	0	2	0
Puestos teletrabajo	0	0	0	2	0
Portátiles	0	6	6	6	0
Routers	0	8	8	8	0
Impresoras	0	4	4	4	0
Ordenadores de mesa	0	6	4	4	0
Servidores Cloud explotación	0	10	10	10	0
Servidores Cloud desarrollo	0	10	10	10	0
Servidores Cloud gestión	0	10	10	10	0
Sistema operativo Linux Mint	4	4	4	4	0
Sistema operativo Debian	6	6	8	8	0
PostgreSQL	6	10	10	10	0
Apache Tomcat	6	6	6	10	0
Apache Camel	6	6	6	6	0
Apache ActiveMQ	6	8	6	10	0
Java	6	8	8	6	0
Redmine	6	8	6	8	0
LibreOffice	0	0	0	4	0
Sistema de backup	6	8	8	8	0
BaseX	6	10	10	10	0
Eclipse (entorno de desarrollo integrado)	0	0	0	4	0
Icinga (monitoreo de sistemas)	6	4	4	8	0
Sistema MBE	8	10	10	10	0
Sistema MBE-CM Integraciones	8	10	10	10	0
Copias de seguridad	4	10	10	10	6
Registros de actividad	8	6	6	6	8
Documentación departamental	4	10	10	10	6
Código fuente MBE, MBE-CM	8	10	10	10	8
Archivos de configuración MBE, MBE-CM	6	8	8	10	6
Bases de datos MBE, MBE-CM	8	10	10	10	8
ADSL (voz y datos)	2	2	2	4	0
Red inalámbrica WIFI	2	4	2	2	0
Móviles	0	2	2	2	0
Correo electrónico corporativo	6	8	4	4	4
SSH protocolo para acceso a servidores	8	8	8	6	4
Git	8	8	8	8	8
Slack	6	4	0	4	0
Sistema eléctrico	0	0	0	2	0
Sistema contra incendios	0	0	0	2	0
Administradores de sistemas	0	8	8	8	0
Desarrolladores	0	8	8	8	0
Contratistas especializados	0	8	8	8	0
Directivos	0	8	8	8	0
Comerciales	0	8	8	8	0
Administrativos	0	8	6	6	0

Figura 16: Mapa de calor del riesgo

Activo	Umbral riesgo > 7				
	[A]	[C]	[I]	[D]	[T]
Oficina	0	0	0	2	0
Puestos teletrabajo	0	0	0	2	0
Portátiles	0	6	6	6	0
Routers	0	8	8	8	0
Impresoras	0	4	4	4	0
Ordenadores de mesa	0	6	4	4	0
Servidores Cloud explotación	0	10	10	10	0
Servidores Cloud desarrollo	0	10	10	10	0
Servidores Cloud gestión	0	10	10	10	0
Sistema operativo Linux Mint	4	4	4	4	0
Sistema operativo Debian	6	6	8	8	0
PostgreSQL	6	10	10	10	0
Apache Tomcat	6	6	6	10	0
Apache Camel	6	6	6	6	0
Apache ActiveMQ	6	8	6	10	0
Java	6	8	8	6	0
Redmine	6	8	6	8	0
LibreOffice	0	0	0	4	0
Sistema de backup	6	8	8	8	0
BaseX	6	10	10	10	0
Eclipse (entorno de desarrollo integrado)	0	0	0	4	0
Icinga (monitoreo de sistemas)	6	4	4	8	0
Sistema MBE	8	10	10	10	0
Sistema MBE-CM Integraciones	8	10	10	10	0
Copias de seguridad	4	10	10	10	6
Registros de actividad	8	6	6	6	8
Documentación departamental	4	10	10	10	6
Código fuente MBE, MBE-CM	8	10	10	10	8
Archivos de configuración MBE, MBE-CM	6	8	8	10	6
Bases de datos MBE, MBE-CM	8	10	10	10	8
ADSL (voz y datos)	2	2	2	4	0
Red inalámbrica WIFI	2	4	2	2	0
Móviles	0	2	2	2	0
Correo electrónico corporativo	6	8	4	4	4
SSH protocolo para acceso a servidores	8	8	8	6	4
Git	8	8	8	8	8
Slack	6	4	0	4	0
Sistema eléctrico	0	0	0	2	0
Sistema contra incendios	0	0	0	2	0
Administradores de sistemas	0	8	8	8	0
Desarrolladores	0	8	8	8	0
Contratistas especializados	0	8	8	8	0
Directivos	0	8	8	8	0
Comerciales	0	8	8	8	0
Administrativos	0	8	6	6	0

Figura 17: Activos que superan el umbral de riesgo

En la figura 18 pueden observarse las dimensiones más afectadas:

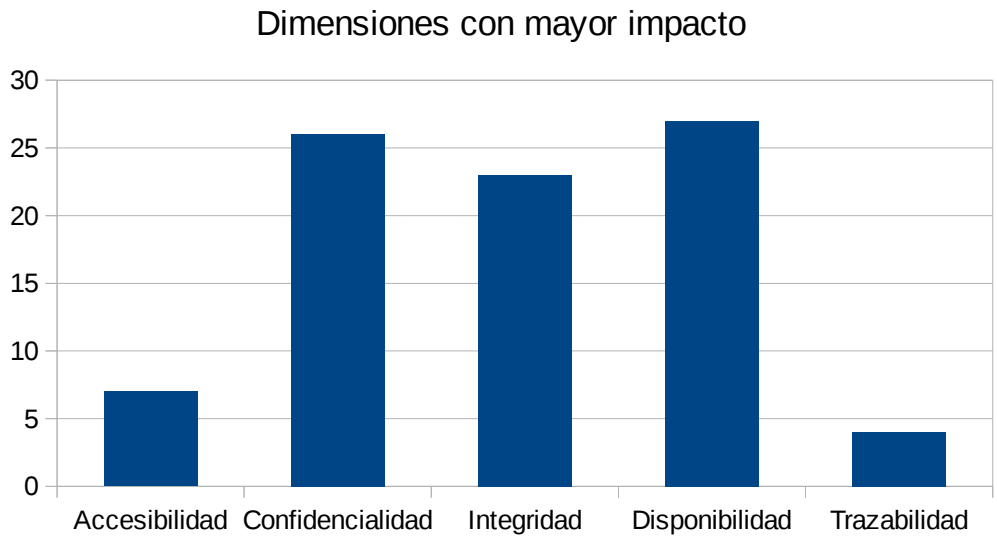

Figura 18: Dimensiones con mayor impacto

4.8 Resumen de riesgos

A partir de los resultados obtenidos en las secciones anteriores se describen de forma resumida los riesgos principales a los que está expuesta la empresa. A cada riesgo se le ha asignado un identificador para poder hacer un seguimiento directo en las acciones correctivas que vayan a aplicarse, facilitando así su trazabilidad. El conjunto de activos que superan el umbral de riesgo han sido agrupados según el tipo de riesgo al que están expuestos.

ID Riesgo	**R001 – Configuración y mantenimiento de routers**
Ámbito	[HW] Hardware
Descripción	La gestión que actualmente se está realizando en los routers de la oficina y de teletrabajo no es el adecuado, por lo que existe un alto riesgo de convertirse en vectores de ataque
Recomendación	Es necesario definir los procedimientos para gestionar y mantener la seguridad de estos equipos. Por ejemplo establecer el nivel de cifrado adecuado o definir una política de contraseñas

ID Riesgo	R002 – Mantenimiento de los servidores
Ámbito	[HW] Hardware
Descripción	Los servidores Cloud, principalmente el de explotación, son una pieza clave para la disponibilidad de los servicios prestados
Recomendación	Es necesario contar con una plan de continuidad en caso de que estos equipos sufran un incidente grave. Puede contener por ejemplo una valoración de tener un segundo servidor o incluso un estudio de mercado con otros proveedores Revisar los contratos con el proveedor para validar que el mantenimiento y los SLA son adecuados a las necesidades de la empresa

ID Riesgo	R003 – Mantenimiento y configuración del software
Ámbito	[SW] Software
Descripción	Este riesgo afecta a un conjunto de activos que pueden tratarse de forma global como uno sólo por la función que realizan, los cuales permiten exponer los servicios a los clientes. Va desde los sistemas operativos de los servidores (Debian), el software relacionado con el desarrollo (Apache Tomcat, Java, Sistema MBE y MBE-CM) el de almacenamiento (Apache ActiveMQ, BaseX, PostgreSQL) y el de monitorización (Icinga). Un error de configuración o estar desactualizados puede provocar un grave riesgo
Recomendación	Definir y documentar los procesos de mantenimiento y configuración de todos el software indicado. Deben mantenerse al día en relación a los “parches” y/o actualizaciones existentes, tanto a nivel de software propio como de terceros.

ID Riesgo	R004 – Mantenimiento y configuración de datos críticos
Ámbito	[D] Datos
Descripción	El código fuente, los registros de actividad, la documentación departamental, las bases de datos y los ficheros de configuración, son sin duda el conjunto de activos con mayor riesgo para la empresa
Recomendación	Revisar que los procedimientos existentes de copias de seguridad son los adecuados para que en cualquier momento sea posible restaurar toda la información requerida Definir una política de control de acceso a los recursos y sistemas de la entidad, así como implantar un sistema de registros (logs) que permitan en todo momento hacer el seguimiento de quien, como y cuando se accede a la información crítica Estudiar la posibilidad de cifrar la información que así lo requiera

ID Riesgo	R005 – Mantenimiento y configuración servicios internos
Ámbito	[S] Servicios
Descripción	La empresa no tiene muchos servicios internos pero los que usa pueden ser un foco de riesgos. Estos son: SSH, con el cual el administrador y los desarrolladores se conectan a los servidores Correo electrónico, con el que a veces se envían datos que pueden tener carácter privado Git, todo el código fuente se sube a un repositorio
Recomendación	Definir los procesos de configuración, mantenimiento y protección de las claves de dichos servicios Si no se está haciendo, analizar la posibilidad del cifrado de los mensajes electrónicos Activar sistemas para detectar malware y accesos no autorizados

ID Riesgo	R006 – Falta de procedimientos de seguridad en RRHH
Ámbito	[P] Personal
Descripción	Al ser pocos empleados el departamento de RRHH es uno de los más descuidados en relación a la seguridad de la información. No hay establecida una cultura de seguridad y hay muchos procedimientos por definir e implantar.
Recomendación	Se deberían implantar planes de formación y concienciación dirigidos a los empleados para que conozcan el modo en cómo se clasifica la información según su criticidad, qué usos pueden hacer con ella y de qué forma pueden tratarla Se deberían conocer los procedimientos a seguir en caso de producirse un incidente de seguridad de la información Por último, se recomienda que la empresa establezca procedimientos en las altas y bajas de personal.

4.9 Gestión de riesgos

En la gestión de riesgos hay dos tareas principales a realizar: el análisis de riesgos y el tratamiento de los riesgos. La primera de ellas se ha completado en este mismo capítulo, la segunda, se llevará a cabo en el capítulo 5.

El tratamiento de los riesgos consiste en describir las acciones y medidas que se llevarán a cabo para mitigar la situación de riesgo. Generalmente, para tratar el riesgo las empresas optan por una de estas tres opciones:

- Evitarlo o eliminarlo. Se puede sustituir el activo por otro que no se vea afectado por la amenaza, o bien, eliminando la actividad que produce el riesgo.

- Reducirlo. Se aplican las medidas oportunas para disminuir el nivel de riesgo por debajo del umbral aprobado por la organización. En este caso hay dos opciones:

    - Reducir la probabilidad o frecuencia de ocurrencia, por ejemplo aplicando medidas preventivas.

- Reducir el impacto de la amenaza estableciendo controles.

- Transferirlo. Si la empresa no puede hacerse cargo o no tiene la capacidad para tratar el riesgo, puede contratar a un tercero para que se ocupe de él.

- Aceptarlo. En este caso se asume el riesgo, ya sea porque está por debajo del umbral o porque los costes de su tratamiento no pueden ser asumidos por la entidad. También puede ocurrir que aunque el impacto sea elevado su probabilidad de ocurrencia sea muy baja.

5. Propuestas de proyectos

5.1 Introducción

Éste capítulo describe los proyectos que la empresa llevará a cabo a corto, medio y largo plazo con dos objetivos fundamentales. De un lado, reducir el riesgo de aquellos activos que superan el nivel de umbral establecido, obtenido en el análisis de riesgos (capítulo 4). Y de otro, mejorar el cumplimento de las áreas de la ISO/IEC 27002:2013 que están por debajo del nivel L3 del Modelo de Madurez de la Capacidad, según el análisis diferencial inicial (capítulo 2).

Los proyectos planteados pretenden mejorar la seguridad de la información a nivel general y no sólo aquellas áreas o procesos de perfil técnico. Hay que tener en cuenta que al tratarse de una pequeña entidad con pocos recursos, tanto económicos como humanos, las pretensiones deben ir acorde a esta situación y se han evitado propuestas inalcanzables para la entidad. Se ha prestado especial atención a la integración de estos proyectos en la planificación actual de la empresa, para evitar que interfieran de forma notable en el desarrollo de las tareas en curso o que estén por empezar.

El planteamiento inicial de la compañía consiste en ejecutar los proyectos en un plazo de **tres años** y de forma progresiva. En el tercer año se han planificado menos proyectos para disponer de un margen de tiempo, por si fuera necesario ajustar la planificación de los dos primeros años. La estrategia a seguir es crear proyectos que mejoren principalmente el nivel de cumplimiento de los controles ISO/IEC 27002:2013 que se obtuvo en en el análisis diferencial. De forma colateral, estas mejoras se verán reflejadas en aquellos activos con un nivel de riesgo superior al umbral establecido.

Los criterios que se han tenido en cuenta a la hora de definir los proyectos y establecer la prioridad de ejecución a corto, medio y largo plazo, son:

- Resultado del análisis diferencial respecto a la ISO/IEC 27002:2013.

- Nivel de riesgo obtenido en el análisis de riesgos.
- Coste económico del proyecto.
- Recursos requeridos en el proyecto.
- Aplicar el concepto “quick wins” (acciones que con menor esfuerzo proporcionan mejoras más amplias).

5.2 Proyectos propuestos

A continuación se resumen todos los proyectos en materia de seguridad de la información que la empresa ejecutará en los próximos tres años, a partir del 07/01/2020. Se trata de una planificación abierta que se revisará de forma temporal permitiendo así su reorganización. Incluso si hace falta, se podrán eliminar o añadir proyectos según las necesidades y los objetivos que se cumplan.

Los costes de los proyectos se han calculado con una estimación en horas a un precio de 50 euros cada una, a los que habrá que añadir los recursos materiales y/o externos que puedan ser necesarios.

ID Proyecto	PR001
Título	Integración de la seguridad de la información en la gestión de proyectos y el teletrabajo
Descripción	Este proyecto está pensado para mejorar tres aspectos relacionados con la organización de la seguridad de la información de la empresa y que actualmente no son contemplados debidamente. Por un lado la seguridad de la información debe considerarse como un proceso integrado dentro del modelo de negocio, y no como una necesidad del departamento tecnológico o un requisito de ciertas tareas. Por otro, no existen medidas de seguridad específicas en el teletrabajo, lo que puede suponer un eslabón débil en la cadena de seguridad. Y en tercer lugar no existe una política de seguridad para los dispositivos móviles. Este proyecto define e implanta los controles para la gestión de estos tres apartados
Responsable	La dirección, el responsable de seguridad y los encargados de las diferentes áreas organizativas
Estimación tiempo/horas	1 mes / 20 horas
Período	07/01/2020 al 07/02/2020

Ámbitos objetivo del AARR **Riesgos a mitigar**	Afecta a todos en general R001, R002, R003, R004, R005 y R006
Dominios ISO/IEC 27002:2013 relacionados	6.1.5 Seguridad de la información en la gestión de proyectos 6.2.1 Política de dispositivos móviles 6.2.2 Teletrabajo
Recursos **Valoración costes asociados**	Personal interno 1.000 euros
Objetivos principales	• Documentar las directrices para integrar la seguridad de la información en la gestión de proyectos • Defefinir una política para dispositivos móviles • Garantizar la seguridad en el teletrabajo
Punto de control	• Revisión anual de la documentación

ID Proyecto	PR002
Título	Plan de gestión de activos
Descripción	El análisis de riesgos ha permito identificar los activos principales de la empresa. Es necesario que se clasifiquen, etiqueten y se les asigne un responsable a cada uno de ellos. Por otro lado hay que definir como se deben gestionar los medios extraíbles que contienen información
Responsable	La dirección y encargados de las diferentes áreas organizativas
Estimación tiempo/horas	2 meses / 40 horas
Período	10/02/2020 al 10/04/2020
Ámbitos objetivo del AARR **Riesgos a mitigar**	Afecta a todos en general R001, R002, R003, R004, R005 y R006
Dominios ISO/IEC 27002:2013 relacionados	8.1 Responsabilidad sobre los activos 8.2 Clasificación de la información 8.3 Manipulación de los soportes
Recursos **Valoración costes asociados**	Personal interno 2.000 euros
Objetivos	• Asignar los responsables de los activos • Clasificar y etiquetar la información • Definir los procesos para gestionar los soportes
Punto de control	• Revisión trimestral del plan de gestión de activos

ID Proyecto	PR003
Título	Plan de continuidad de los servicios MBE y MBE-CM
Descripción	Actualmente no existe un plan de continuidad para los casos en los que un incidente afecte a la disponibilidad de los servicios prestados a los clientes. Tampoco están documentados los procedimientos a seguir para el mantenimiento de los equipos y sistemas relacionados. Este proyecto describe como establecer, documentar, implementar y mantener los procedimientos y controles para asegurar el nivel de continuidad de los servicios prestados a los clientes si se produce un incidente
Responsable	Responsable de seguridad, director TIC y la dirección
Estimación tiempo/horas	3 meses / 60 horas
Período	10/04/2020 al 10/07/2020
Ámbitos objetivo del AARR **Riesgos a mitigar**	[HW] Hardware, [SW] Software y [D] Datos R001, R002, R003 y R004
Dominios ISO/IEC 27002:2013 relacionados	17.1 Continuidad de la seguridad de la información 17.2 Redundancias
Recursos **Valoración costes asociados**	Personal interno, replicar servidor de explotación 3.000 + 2.400 = 5.400 euros
Objetivos	• Definir un plan de continuidad de los servicios críticos • Obtener una documentación con los procedimientos de mantenimiento y sustitución (cuando sea necesario) de los sistemas, equipos y software implicados en la disponibilidad de los servicios MBE y MBE-CM
Punto de control	• Revisión anual del plan de continuidad • Revisión semestral de parches y actualizaciones del software incluido en el proyecto • Alertas de avisos ante caídas de sistemas y equipos

ID Proyecto	PR004
Título	Revisión del cumplimiento de LOPDGDD
Descripción	El proyecto identificará cuales son los procesos y servicios de la empresa que se ven afectados por la ley LOPDGDD y adecuará todos aquellos que no estén acorde a la normativa
Responsable	Responsable de seguridad, delegado de protección de datos
Estimación tiempo/horas	1 mes / 30 horas

Período	13/07/2020 al 13/08/2020
Ámbitos objetivo del AARR **Riesgos a mitigar**	[D] Datos y [S] Servicios R004 y R005
Dominios ISO/IEC 27002:2013 relacionados	18.1 Cumplimiento de los requisitos legales y contractuales
Recursos **Valoración costes asociados**	Personal interno + Asesoramiento legal externo 1.500 + 300 = 1.800 euros
Objetivos	• Evitar posibles sanciones por incumplimiento de las leyes vigentes • Proporcionar tranquilidad y confianza a los clientes en relación al tratamiento de sus datos personales • Mejorar el umbral de riesgo de los elementos del área de Datos y Servicios
Punto de control	• Revisión anual de la normativa vigente

ID Proyecto	PR005
Título	Gestión de incidentes de seguridad de la información
Descripción	Se documentarán los procedimientos y acciones a realizar ante un incidente de seguridad. Entre otras cosas se identificarán las personas involucradas y sus responsabilidades, cómo notificar los eventos, los canales de comunicación a usar, así como la recopilación y aprendizaje de los incidentes
Responsable	Responsable de seguridad, director TIC y la dirección
Estimación tiempo/horas	3 meses / 60 horas
Período	07/09/2020 al 07/12/2020
Ámbitos objetivo del AARR **Riesgos a mitigar**	Afecta a todos en general R001, R002, R003, R004, R005 y R006
Dominios ISO/IEC 27002:2013 relacionados	16.1 Gestión de incidentes de seguridad de la información y mejoras
Recursos **Valoración costes asociados**	Personal interno 3.000 euros
Objetivos	Obtener un modelo aprobado conocido y divulgado en la empresa de gestión interna de los incidentes de seguridad, que principalmente describa: • los sistemas a implantar para la detección de incidentes y/o puntos débiles • los procedimientos a seguir la notificación y respuesta del incidente • los procedimientos para la recopilación y aprendizaje

Punto de control	• Revisar el documento anualmente • Los avisos de detección de incidentes

ID Proyecto	PR006
Título	Gestión de seguridad en las comunicaciones
Descripción	Documentar los procedimientos y acciones para asegurar el intercambio de información entre distintos actores, así como fortalecer las seguridad en las conexiones entre los sistemas y los equipos usados
Responsable	Responsable de seguridad y el director TIC
Estimación tiempo/horas	10 días / 15 horas
Período	11/01/2021 al 29/01/2021
Ámbitos objetivo del AARR **Riesgos a mitigar**	[HW] Hardware y [S] Servicios R001, R002 y R005
Dominios ISO/IEC 27002:2013 relacionados	13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red 13.2.1 Políticas y procedimientos de intercambio de información 13.2.3 Mensajería electrónica
Valoración costes asociados	750 euros
Objetivos	• Asegurar la protección de la información en las redes y los recursos de tratamiento de la información como el correo electrónico y el servicio Git • Mejorar la seguridad en los routers de la oficina, los puestos de teletrabajo y el protocolo SSH usado para conectarse con los servidores
Punto de control	• Revisar el documento, los estándares y protocolos usados anualmente • Modificar las contraseñas de los distintos sistemas (routers, accesos a servidores) cada tres meses

ID Proyecto	PR007
Título	Plan de gestión de accesos
Descripción	Se establecerá y documentará una política de control de acceso basada en los requisitos de la empresa y de seguridad de la información
Responsable	Responsable de seguridad, la dirección y responsables de las

	diferentes áreas
Estimación tiempo/horas	2 meses / 40 horas
Período	01/02/2021 al 01/04/2021
Ámbitos objetivo del AARR **Riesgos a mitigar**	[S] Servicios, [SW] Software, [HW] Hardware y [Personal] R001, R002, R005 y R006
Dominios ISO/IEC 27002:2013 relacionados	9.1 Política de control de acceso 9.2 Gestión de acceso de usuario 9.3 Responsabilidades del usuario 9.4 Control de acceso a sistemas y aplicaciones
Valoración costos asociados	2.000 euros
Objetivos	• Gestionar que los distintos sistemas y su información sólo es accesible a los usuarios autorizados
Punto de control	• Revisar los accesos cada 6 meses y en las altas, bajas de personal

ID Proyecto	PR008
Título	Plan de formación y concienciazión en materia de seguridad de la información
Descripción	Este proyecto describirá los planes de formación a realizar temporalmente, para proveer de los conocimientos necesarios en materia de seguridad de la información y concienciación sobre los riesgos asociados con las tecnologías. Los empleados, a nivel de usuario, deben conocer y aplicar un conjunto de buenas prácticas en el uso de todo tipo de dispositivos y de la información que tratan. Por otro lado, están los desarrolladores y administradores de sistemas que deberán recibir formación específica a su especialidad Como las formaciones se realizarán en horario laboral, con el fin de interferir le menor posible en la jornada normal, los planes se ejecutarán en pocas sesiones de 1 o 2 días, con una duración entre 2 y 4 horas máximo
Responsable	Responsable de seguridad y director de recursos humanos
Estimación tiempo/horas	Preparación de 3 sesiones: 2 meses / 32 horas
Período	Preparación sesiones: 05/04/2021 al 04/06/2021 Ejecución sesiones: entre el 07 y el 30 de junio 2020
Ámbitos objetivo del AARR **Riesgos a mitigar**	[P] Personal R006

Dominios ISO/IEC 27002:2013 relacionados	7.2. Durante el empleo
Recursos **Valoración costos asociados**	Personal interno Preparación y asistencia de las sesiones: 1 sesión 6h para los administradores + 12h de preparación = 900 euros 1 sesión 6h para desarrolladores + 12h preparación = 900 euros 1 sesión 4h empleados en general + 8h preparación = 600 euros Total 2.400 euros
• **Objetivos**	• Diseñar los distintos programas de formación tanto generales como específicos según las áreas organizativas • Promover una cultura de seguridad de la información • Asegurar que los empleados conocen, entienden y cumplen las normas y las medidas de protección en materia de seguridad adoptadas por la empresa, advirtiéndoles de los riesgos y repercusiones que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance
Punto de control	• Revisar anualmente las necesidades de formación

ID Proyecto	PR009
Título	Plan de mejora del sistema de monitorización y registros de eventos
Descripción	Actualmente los registros (logs), se centran principalmente en los flujos de negocio para detectar errores de ejecución. No obstante, es necesario crear nuevos registros que puedan ser de ayuda en la detección, análisis y tratamiento de un incidente de seguridad de la información
Responsable	Responsable de seguridad y el director TIC
Estimación tiempo/horas	1 mes / 30 horas
Período	01/07/2021 al 30/07/2021
Ámbitos objetivo del AARR **Riesgos a mitigar**	Afecta a todos en general R001, R002, R003, R004, R005 y R006
Dominios ISO/IEC 27002:2013 relacionados	12.4 Registros y supervisión
Recursos **Valoración costos asociados**	Personal interno 1.500 euros
Objetivos	• Mejorar los sistemas actuales eliminando información innecesaria y así optimizar el espacio ocupado por los

	registros • Segregar la información de los registros según su ámbito o finalidad para facilitar su análisis • Incluir nuevos registros relacionados con la seguridad de la información que sean de ayuda en el tratamiento de los incidentes ocurridos • Definir los procedimientos necesarios para la revisión efectiva de los registros • Implantar un sistema de alertas de incidentes
Punto de control	• Los avisos del sistema de alertas de incidentes

ID Proyecto	PR010
Título	Plan de cumplimiento normativa PCI DSS SAQ A-EP
Descripción	PCI DSS es la normativa internacional de seguridad para todas las entidades que almacenan, procesan o transmiten datos de titulares de tarjeta o datos sensibles de autentificación. La empresa tiene delegado a terceros el proceso de pago por tarjetas pero son cada vez más los que exigen la certificación del cuestionario SAQ A-EP. Mediante este proyecto se aplicarán las medidas necesarias para cumplir con todos los requisitos de dicho cuestionario
Responsable	Responsable de seguridad, el director TIC, la dirección
Estimación tiempo/horas	3 meses / 50 horas
Período	01/09/2021 al 01/12/2021
Ámbitos objetivo del AARR **Riesgos a mitigar**	[D] Datos y [S] Servicios R004 y R005
Dominios ISO/IEC 27002:2013 relacionados	18.1 Cumplimiento de los requisitos legales y contractuales
Recursos **Valoración costos asociados**	Personal interno + Asesoramiento legal externo 2.500 + 500 = 3.000 euros
Objetivos	• Analizar el entorno de cumplimiento (flujos de pagos con tarjetas) • Plan de acción. Adecuar las no conformidades detectadas según los controles del cuestionario SAQ-EP de la normativa PCI DSS • Elaboración del SAQ
Punto de control	• Revisión anual del cumplimiento de los controles del cuestionario

ID Proyecto	PR011
Título	Plan de mejora de los sistemas criptográficos
Descripción	El proyecto consiste en el desarrollo e implementación de una política sobre el uso de controles criptográficos para proteger la información
Responsable	Responsable de seguridad y el director TIC
Estimación tiempo/horas	1 mes / 30 horas
Período	09/01/2022 al 09/02/2022
Ámbitos objetivo del AARR **Riesgos a mitigar**	[D] Datos y [S] Servicios R004 y R005
Dominios ISO/IEC 27002:2013 relacionados	10.1.1 Política de uso de los controles criptográficos 10.1.2 Gestión de claves
Recursos **Valoración costos asociados**	Personal interno 1.500 euros
Objetivos	• Definir los procedimientos para la generación, uso, mantenimiento y protección de las claves • Establecer períodos de tiempo para la revisión, actualización o cambio de los estándares usados • Establecer períodos de tiempo para revisar que se usan los servicios criptográficos según la legislación vigente de cada momento
Punto de control	• Revisión anual de la política • Instaurar un sistema de alertas de caducidad de claves y certificados

ID Proyecto	PR012
Título	Procedimiento de gestión de altas y bajas de personal
Descripción	El proyecto pretende ser una fuente de información para la dirección y el departamento de recursos humanos para que en todo momento conozca los procedimientos a seguir en la contratación y despido de personal. Entre otras cosas se cubrirán aspectos como la concesión o revocación de permisos, los comunicados o la creación de un documento de confidencialidad
Responsable	La dirección y el director de recursos humanos
Estimación tiempo/horas	1 mese / 20 horas

Período	14/02/2022 al 14/03/2022
Ámbitos objetivo del AARR **Riesgos a mitigar**	[P] Personal R006
Dominios ISO/IEC 27002:2013 relacionados	7.1 Antes del empleo 7.3 Finalización del empleo o cambio en el puesto de trabajo
Recursos **Valoración costos asociados**	Personal interno 1.000 euros
Objetivos	• Definir y documentar el procedimiento para la gestión de la contratación y despido de personal
Punto de control	• Revisión anual de altas y bajas

Las siguientes tablas muestran un resumen de los proyectos a realizar en los próximos 3 años, junto con el período de ejecución y los costes asociados:

PROYECTOS A CORTO PLAZO - AÑO 2020				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Organización interna de la seguridad de la información y el teletrabajo	1 mes	07/01/2020	07/02/2020	1.000 €
Plan de gestión de activos	2 meses	10/02/2020	10/04/2020	2.000 €
Plan de continuidad de los servicios MBE y MBE-CM	3 meses	10/04/2020	10/07/2020	5.400 €
Revisión del cumplimiento de LOPDGDD	1 mes	13/07/2020	13/08/2020	1.800 €
Gestión de incidentes de seguridad de la información	3 meses	07/09/2020	07/12/2020	3.000 €
			Total	**13.200 €**

Tabla 10: Proyectos propuestos año 2020

PROYECTOS A MEDIO PLAZO - AÑO 2021				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Gestión de seguridad en las comunicaciones	10 días	11/01/2021	29/01/2021	750 €
Plan de gestión de accesos	2 meses	01/02/2021	10/04/2020	2.000 €
Plan de formación y concienciazión en materia de seguridad de la información	3 meses	05/04/2021	30/06/2021	2.400 €
Plan de mejora del sistema de monitorización y registros de eventos	1 mes	01/07/2021	30/07/2021	1.500 €
Plan de cumplimiento normativa PCI DSS SAQ A-EP	3 meses	01/09/2021	01/12/2021	3.000 €
			Total	**9.650 €**

Tabla 11: Proyectos propuestos año 2021

PROYECTOS A LARGO PLAZO - AÑO 2022				
Proyecto	**Duración**	**Inicio**	**Fin**	**Coste**
Plan de mejora de los sistemas criptográficos	1 mes	09/01/2022	09/02/2022	1.500 €
Procedimiento de gestión de altas y bajas de personal	1 mes	14/02/2022	14/03/2022	1.000 €
			Total	**2.500 €**

Tabla 12: Proyectos propuestos año 2022

5.3 Evolución del riesgo

La ejecución de todos los proyectos propuestos terminará, con toda probabilidad, con la disminución del impacto de materialización de las amenazas identificadas, lo que conllevará a una mejora del nivel de riesgo que se obtuvo inicialmente. Las siguientes figuras muestran una estimación del nivel que se podría conseguir en cada uno de los activos, si todos los proyectos cumplen sus objetivos. Como puede observarse, los activos que en el primer análisis de riesgos superaban el umbral establecido ahora se encuentran por debajo.

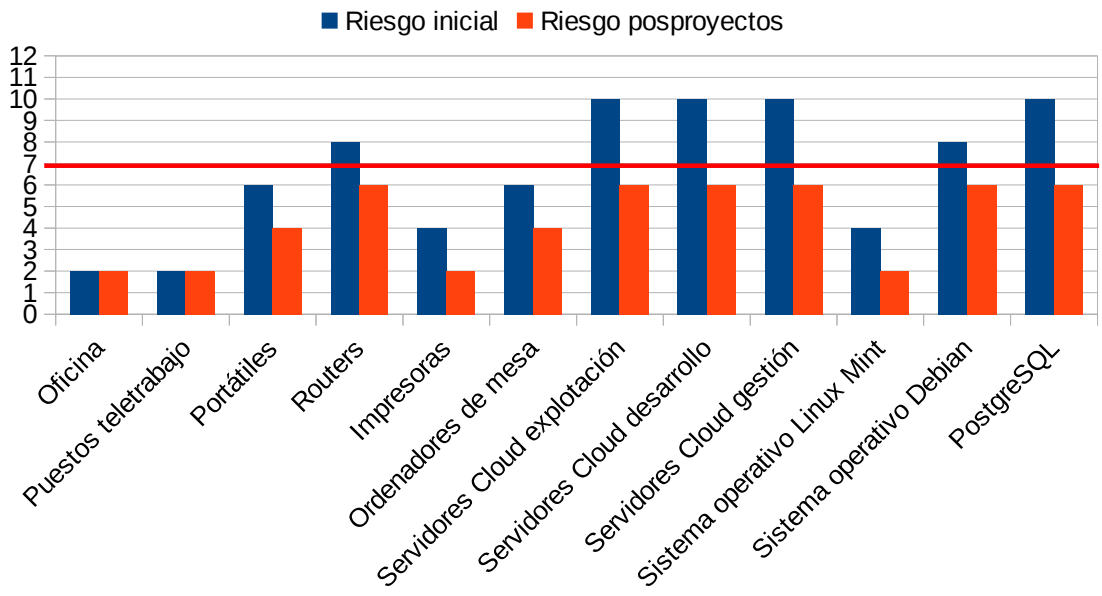

Figura 19: Comparativa del riesgo de los activos

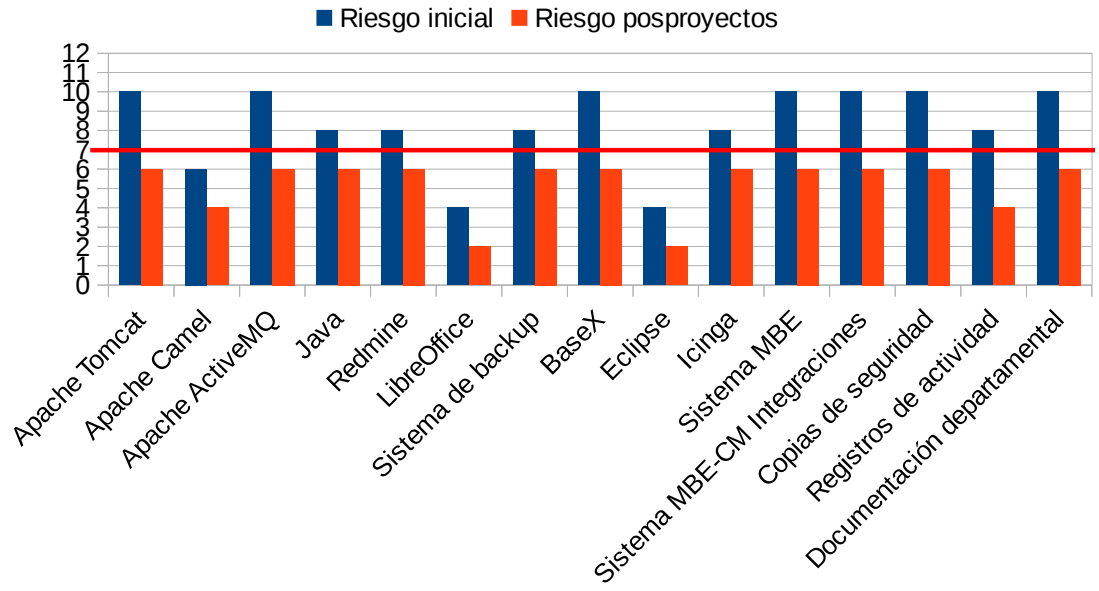

Figura 20: Comparativa del riesgo de los activos (continuación)

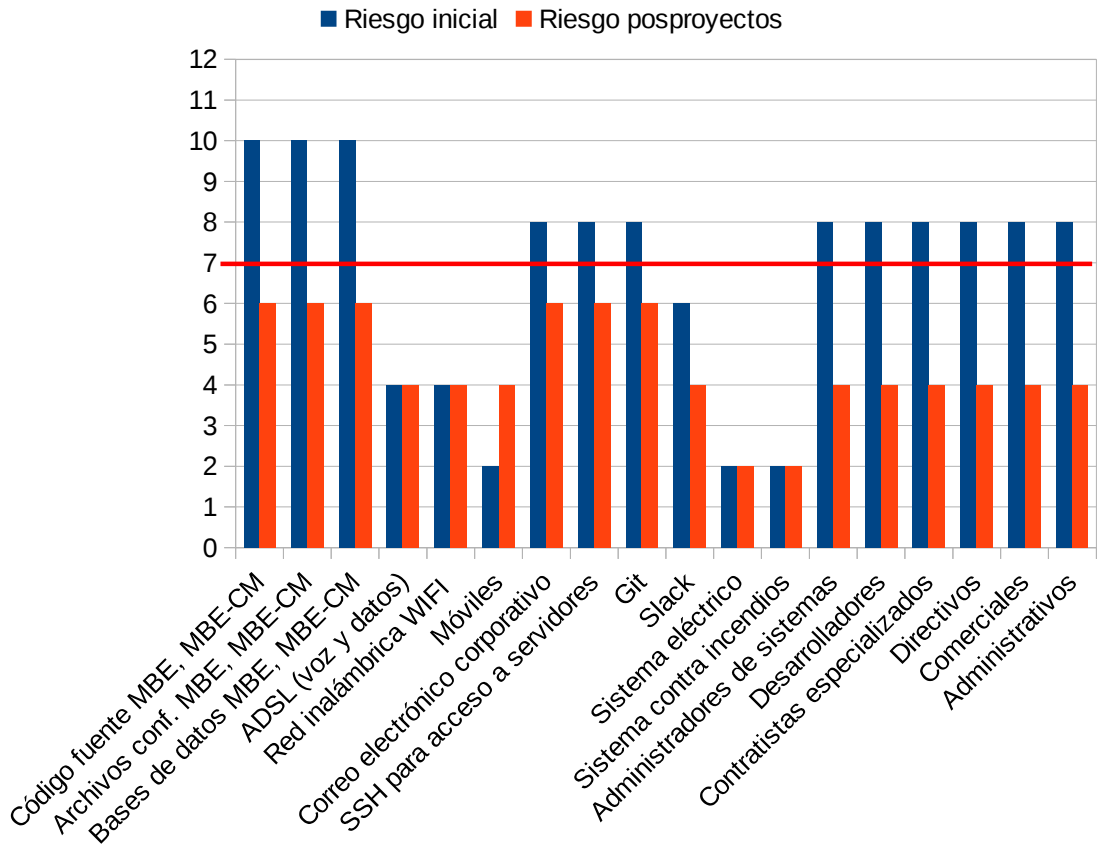

Figura 21: Comparativa del riesgo de los activos (continuación)

5.4 Evolución del nivel de cumplimiento ISO/IEC 27002

Por lo que respecta al cumplimiento de la norma ISO/IEC 27002:2013, gracias a los proyectos propuestos y de la gestión documental que se ha instaurado (Política de Seguridad, Procedimiento de Auditorias, Gestión de indicadores, etc.) ha sido posible obtener una gran mejora en casi todos los dominios según se aprecia en la tabla 13. En la comparativa puede apreciarse que de los 14 capítulos que conforman la norma, 12 reflejan un avance positivo.

La mayoría de dominios han evolucionado hasta situarse en el nivel L3 CMM, objetivo que se estableció inicialmente. Los que han quedado por debajo y los que no han sufrido cambios serán tratados en futuras propuestas durante el tercer año (2022), según se vayan cumpliendo los proyectos propuestos.

Capítulo	Valoración inicial	Valoración posproyectos
5 Políticas de seguridad de la información	0 %	90 %
6 Organización de la seguridad de la información	14,5 %	90 %
7 Seguridad relativa a los recursos humanos	1,7 %	90 %
8 Gestión de activos	16,7 %	90 %
9 Control de acceso	38 %	90 %
10 Criptografía	30 %	90 %
11 Seguridad física y del entorno	50 %	70 %
12 Seguridad de las operaciones	55,4 %	68,57 %
13 Seguridad de las comunicaciones	37,5 %	67,1 %
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	48,3 %	48,3 %
15 Relación con proveedores	50 %	50 %
16 Gestión de incidentes de seguridad de la información	7,1 %	90 %
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	30 %	90 %
18 Cumplimiento	13 %	90 %

Tabla 13: Comparativa ISO/IEC 27002:2013 inicial y posproyectos

Los siguientes gráficos proporcionan una visión general de como ha variado el nivel de madurez respecto al estado inicial que se obtuvo en el análisis diferencial del capítulo 2.

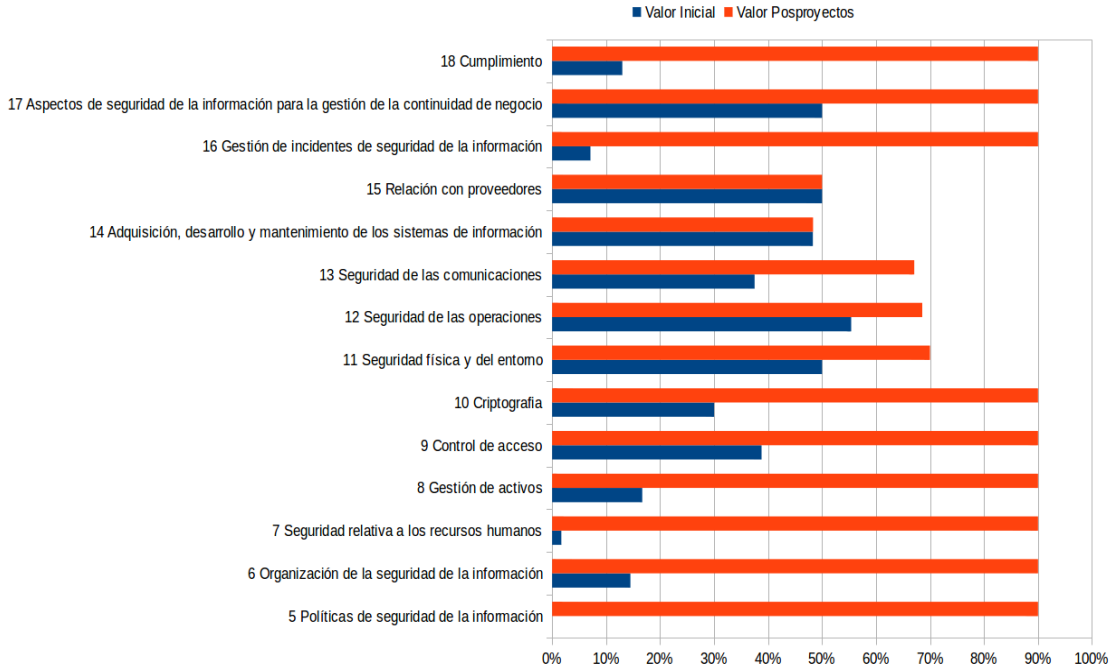

Figura 22: Capítulos ISO/IEC 27002 inicio y posproyectos

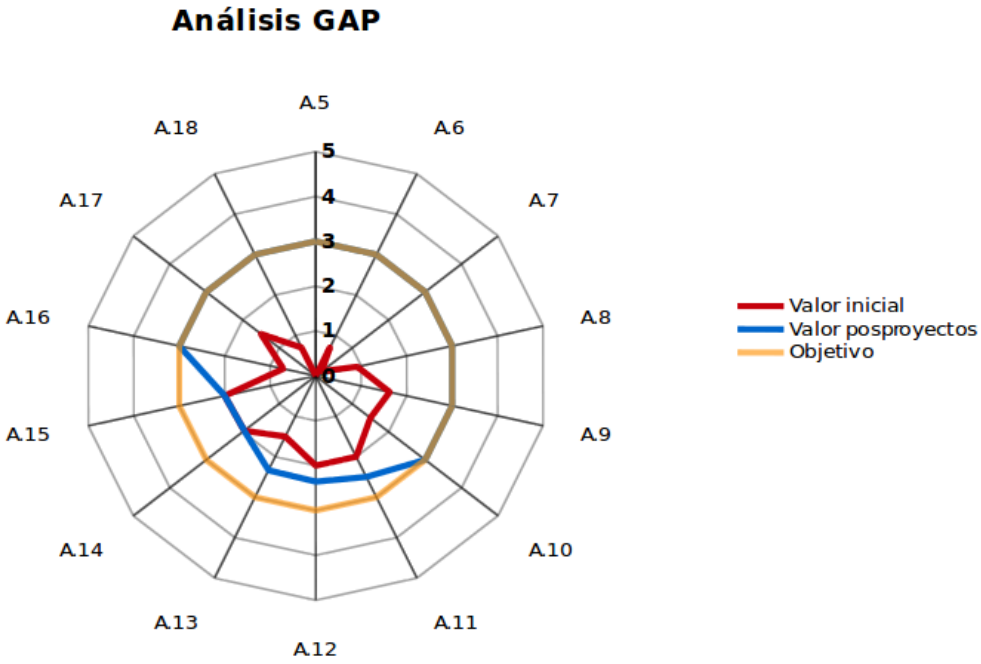

Figura 23: Comparativa GAP inicio y posproyectos

6. Auditoría de cumplimiento

6.1 Introducción

Al comienzo del TFM se comentó que los SGSI basados en la norma ISO/IEC 27001 se rigen por un proceso iterativo de calidad, siendo el más conocido el Ciclo de Deming o PDCA (por sus siglas en inglés *Plan, Do, Check, Act*).

Figura 24: Ciclo de Deming

Las auditorías internas se realizan en la fase Verificar (*Check)* siendo el medio que tiene la organización para comprobar y valorar si el Sistema de Gestión de Seguridad de la Información está conforme a la norma ISO/IEC 27001. Los informes generados en las auditorías proporcionan la información que permite analizar como evoluciona el sistema, así como detectar aquellas áreas que necesitan acciones correctivas.

En las auditorías se usa el concepto de No Conformidad para indicar que se incumplen uno o varios controles de la norma ISO/IEC 27002:2013, o bien, una política o normativa interna. Una No Conformidad puede ser Mayor o Menor, pero en ambos casos se indica que es necesario aplicar acciones de corrección. Por otro lado está el concepto de Observación, que es una recomendación que la organización puede tener en consideración o no.

6.2 Resumen de resultados de la auditoría

El proceso de auditoría se inició el 01/04/2022, una vez ejecutados todos los proyectos propuestos en el capítulo 5, y terminó el 18/05/2022 con la presentación del informe de resultados. En él quedan constatadas las mejoras descritas en el capítulo anterior, pero también revela la existencia de *No Conformidades* en relación a la ISO/IEC 27002:2013. Éstas deberán ser gestionadas por la empresa para que puedan ser corregidas, de forma que todos los dominios lleguen a un nivel L3 CMM que es el mínimo al que se pretende situar el SGSI implantado.

El informe de auditoría se puede consultar en el Anexo XV pero a modo de resumen se describen algunos datos de interés:

Resultado	Encontradas	Plazo de corrección
No Conformidades Mayores	4	Entre 1 y 3 meses
No Conformidades Menores	2	6 meses
Observaciones	3	1 año

Tabla 14: Resultados de la Auditoría

Las categorías de la norma que se ven afectadas por No Conformidades son:

- 12.1 Procedimientos y responsabilidades operacionales (No Conformidad Menor). Es necesario documentar procedimientos para poder gestionar debidamente los cambios aplicados en los entornos de producción y ciertos recursos que afectan a servicios prestados.

- 12.2 Protección contra el software maliciosos (malware) (No Conformidad Mayor). Se ha comprobado que los equipos no cuentan con ningún tipo de sistema de protección ante este tipo de programas, ni hay procedimientos definidos para su tratamiento.

- 13.2 Intercambio de información (No Conformidad Mayor). La entidad no cumple con la sección 7.9 de la Política de Seguridad interna, al no

disponer de acuerdos que deberían usarse tanto con el personal interno como con terceros.

- 14.2 Seguridad en el desarrollo y en los procesos de soporte (No Conformidad Mayor). Falta definir una política de desarrollo seguro para que el personal correspondiente pueda consultar y seguir sus procedimientos.

- 14.3 Datos de prueba (No Conformidad Menor). Los datos que se usan en los entornos de prueba proceden de los sistemas de producción. Si no se gestionan debidamente podrían provocar incidentes como una fuga de información, por lo que se deberían establecer normas y autorizaciones para tratar debidamente los datos.

- 15.1 Seguridad en las relaciones con proveedores y 15.2 Gestión de la provisión de servicios del proveedor (No Conformidad Mayor). No existen políticas de seguridad para las relaciones con proveedores, tal y como exige el dominio 15.1.1 de la norma ISO/IEC 27002:2013. Para la entidad éste es un punto importante pues los servicios que se prestan están ubicados en servidores Cloud contratados a terceros.

7. Presentación de resultados y entrega de informes

7.1 Introducción

Una vez finalizadas todas las fases del proyecto se ha procedido a recopilar la información generada y elaborar los informes a presentar a la Dirección. A partir de ellos la empresa podrá analizar y valorar los resultados que le ayudarán a tomar las decisiones que crea oportunas, con el fin de seguir mejorando el Sistema de Gestión de Seguridad de la Información.

7.2 Entregas

- Resumen ejecutivo (se adjunta documento)
- Presentación del Proyecto (se adjunta fichero con diapositivas)
- Video defensa del Proyecto (se adjunta fichero)
- Memoria completa del Proyecto (documento presente)

8. Conclusiones

La ejecución de este trabajo ha dejado claro desde un principio que la participación de la Dirección es un punto clave en la implantación de un SGSI y que sin ella, resultaría prácticamente imposible.

El análisis de riesgos es una de las fases más importantes, sino la que más, en el desarrollo, mantenimiento y evolución del sistema de gestión. Identificar y valorar incorrectamente los riesgos puede provocar que se tomen malas decisiones y/o apliquen medidas inadecuadas.

Todas las metodologías existentes para la gestión de riesgos tienen sus ventajas e inconvenientes, por ello se recomienda que en las primeras fases se analice cuál de ellas se ajusta mejor a las características y objetivos de la organización.

Las pequeñas empresas que pretendan implantar un SGSI deberán prestar especial atención a los objetivos y proyectos que se definan en el Plan Director. Generalmente estas entidades suelen disponer de pocos recursos, siendo muy importante establecer metas alcanzables. Si éstas no se consiguen generarán frustración y desánimo, conduciendo el sistema de gestión al fracaso.

Las auditorias resultan imprescindibles para la mejora continua del sistema de gestión de la seguridad de la información.

A nivel de objetivos generales, se han completado de forma satisfactoria los que se establecieron inicialmente. Los empleados y principalmente la dirección, han tomado conciencia de la importancia de gestionar adecuadamente la información y los activos que la procesan. En este aspecto los planes de formación han sido de gran ayuda. Por lo que respecta a los objetivos específicos, la división y planificación del proyecto en diversas fases ha contribuido a la consecución de cada uno de ellos.

La certificación ISO/IEC 27001:2013 no entraba en los planes iniciales y actualmente se sigue pensando igual. No obstante, la empresa analizará su conveniencia una vez que el SGSI haya adquirido un mayor grado de madurez.

Precisamente, el nivel de madurez de la seguridad de la información conseguido en la empresa según el modelo CMM, ha mejorado considerablemente, pero hay que resaltar que no se ha logrado llegar al nivel L3 que se pretendía en todas las áreas. Esta situación se debe a la limitación en la ejecución de proyectos en el tercer año, para disponer de un margen de tiempo por si se producían retrasos en los planes propuestos. Por este motivo algunas áreas de la ISO/IEC 27002:2013 no reflejan mejoras o éstas no han sido suficientes.

Las seis fases con las que se dividió este TFM y las tareas programadas se han ejecutado según la planificación. No obstante, la previsión de horas ha variado respecto al principio pues ha hecho falta un 25% más, para completar todas las tareas en los plazos establecidos.

En cuanto a la metodología aplicada se considera que las normas ISO y el Ciclo de Deming son adecuados para la empresa y los objetivos establecidos. El mayor inconveniente se ha encontrado en la elaboración del análisis de riesgos siguiendo el método MAGERIT. El hecho de tener que estimar el valor económico de los activos teniendo en cuenta el árbol de dependencias, ha supuesto un gran trabajo.

Como líneas de trabajo futuras y de mejora se prevé:

- Analizar si otras metodologías para el análisis de riesgos pueden ser más adecuadas, o bien, si se sigue apostando por MAGERIT sopesar el uso de la herramienta PILAR la cual implementa ésta metodología. En los 3 meses disponibles para realizar el TFM no ha sido posible invertir tiempo en el aprendizaje y aplicación de este software.

- Definir un nuevo Plan Director de Seguridad con el objetivo de mejorar el nivel CMM al que se ha llegado. Para ello será necesario especificar nuevos proyectos para tratar las siguientes áreas de la norma ISO/IEC 27002:

    - Seguridad física y del entorno.
    - Seguridad de las operaciones.
    - Seguridad de las comunicaciones.
    - Adquisición, desarrollo y mantenimiento de los sistemas de información.
    - Relación con los proveedores.

- La empresa tiene previsto prestar servicios y soluciones en distintos Ayuntamientos por lo que será necesario disponer, en aquellos casos que sea requerido, de las debidas Certificaciones de Conformidad con el Esquema Nacional de Seguridad (ENS) y de Interoperabilidad (ENI).

Se cierra este capítulo sabiendo que TurisTech Balear a conseguido establecer una cultura de la seguridad en toda la organización. Ahora es una empresa mucho menos vulnerable a las amenazas en la seguridad de la información y en caso que ocurra un incidente, tiene mayor capacidad de reacción. Además, ofrece una imagen más profesional y de confianza a sus clientes.

9. Glosario

AARR. Acrónimo de análisis de riesgos.

Activo. En seguridad de la información, componente o funcionalidad de un sistema que tiene valor para su propietario y que es susceptible de ser atacado.

Amenaza. Causa potencial de un incidente que puede provocar daños a un sistema u organización.

Auditoría de seguridad. Estudio y examen independiente del historial y actividades de un sistema con la finalidad de comprobar su idoneidad.

Autenticidad. En seguridad de la información, propiedad o característica consistente en que una entidad es quien dice ser o que garantiza la fuente de la que proceden los datos.

Ciber. Prefijo que alude a las redes informáticas y tecnologías virtuales.

Ciberataque. Cualquier tipo de acción ofensiva sobre sistemas de información.

Ciberseguridad. Conjunto de políticas, estrategias, metodologías y herramientas que pueden utilizarse para proteger los activos de una organización y a los usuarios que usan los sistemas de información.

Ciclo de Deming. Estrategia basada en la mejora continua de la calidad que se puede usar en los sistemas de gestión.

Cloud. Se refiere a los sistemas de computación y servicios en la nube que se prestan generalmente a través de la red Internet.

CMM. Siglas del ingés *Capability Maturity Model* (Modelo de Madurez de Capacidades). Modelo que permite la evaluación de los procesos de una organización.

Confidencialidad. En seguridad de la información, propiedad o característica consistente en garantizar que la información no se revela a individuos, entidades o procesos no autorizados.

CPD. Siglas de *Centro de Proceso de Datos*. Salas o edificios que albergan equipos informáticos, además de mecanismos de control eléctrico, ambiental, de incendios, acceso y vigilancia.

Declaración de Aplicabilidad. Documento que exige la norma ISO/IEC 27001, el cual contiene la lista de controles de seguridad que son aplicables en un sistema de información.

Delegado de datos. Persona responsable de supervisar el cumplimiento de la normativa en materia de protección de datos personales.

Disponibilidad. En seguridad de la información, propiedad o característica consistente en asegurar que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando lo requieran.

ENI. *Esquema Nacional de Interoperabilidad*. Normativa que regula la toma de decisiones tecnológicas para garantizar la interoperabilidad de los sistemas de información entre las distintas administraciones.

ENS. *Esquema Nacional de Seguridad*. Ley que recoge los derechos de las personas en sus relaciones con las Administraciones Públicas en lo relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

GAP. Del inglés *Gap Analysis* (análisis de brecha). En seguridad de la información se refiere a la técnica que permite identificar la distancia entre el estado actual de seguridad de la empresa y el objetivo establecido.

IaaS. Siglas del inglés *Infrastructure as a Service* (infraestructura como servicio). Servicio de tipo Cloud donde se proveen recursos de informática física como procesamiento y almacenamiento.

Impacto. En seguridad de la información, consecuencia que sobre un activo tiene la materialización de una amenaza.

Integridad. En seguridad de la información, propiedad o característica que previene la modificación o destrucción no autorizadas de datos.

ISO. Del inglés *International Organization for Standardization* (Organización Internacional de Normalización). Se trata de una organización no gubernamental compuesta por diversas entidades nacionales que crea estándares a nivel mundial.

IEC. Siglas del inglés *International Electrotechnical Commission* (Comisión Electrotécnica Internacional). Organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

ISO/IEC 27001. Estándar para la seguridad de la información aprobado y publicado por las entidades ISO e IEC, que describe como gestionar la seguridad de la información en las empresas y organizaciones.

ISO/IEC 27002. Estándar para la seguridad de la información aprobado y publicado por las entidades ISO e IEC que especifica un conjunto de buenas prácticas.

LOG. Término en inglés que se refiere a la grabación de un registro de eventos o acciones ocurridas en un sistema informático.

LOPD. *Ley Orgánica de Protección de Datos*, ley española que tiene por objeto garantizar y proteger el tratamiento y los derechos de los datos personales.

LOPDGDD. *Ley Orgánica de Protección de Datos y Garantía de Derechos Personales*. Ley española que adapta la LOPD a las disposiciones del RGPD del Parlamento Europeo.

LSSI-CE. Ley española que regula los *Servicios de la Sociedad de la Información y del Comercio Electrónico* a través de Internet.

MAGERIT. Siglas de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.

Malware. Término del inglés compuesto por las palabras *malicious* y *software* que engloba todo tipo de programa o código informático malicioso, cuya función es dañar un sistema o causar un mal funcionamiento.

Monitoreo. Véase LOG.

PCI DSS. Estándar de seguridad de datos para la industria de tarjetas de pago.

PDCA. Se refiere a las fases del *Ciclo de Deming* en inglés: Plan, Do, Check, Act.

Plan Director de Seguridad. Conjunto de objetivos, proyectos y actividades en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta una organización.

RGPD. *Reglamento General de Protección de Datos* elaborado por el Parlamento Europeo.

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

SaaS. Siglas del inglés *Software as a Service* (programa como servicio). Servicio de tipo Cloud donde se proveen recursos de informática lógica como programas y aplicaciones.

Salvaguarda. Procedimiento o mecanismo tecnológico que reduce el riesgo.

Seguridad de la Información. Conjunto de medidas preventivas y reactivas con el fin de proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

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

Sistema de Gestión de la Seguridad de la Información. Conjunto de acciones relacionadas entre ellas que permiten conseguir un objetivo de negocio relacionados con la seguridad de la información.

SoA. Siglas el inglés *Statement Of Applicability* (Declaración de Aplicabilidad).

TIC. De las siglas *Tecnologías de la Información y Comunicación*.

Trazabilidad. En seguridad de la información, propiedad o característica que permite realizar el seguimiento de las acciones que se realizan en un sistema de información, relacionándolas con un individuo, entidad o proceso de forma inequívoca.

Vulnerabilidad. En seguridad de la información, defecto o debilidad en de un activo que puede ser aprovechada por una amenaza.

10. Bibliografía

[1] https://www.uoc.edu/portal/es/news/actualitat/2019/161-ciberseguridad-pymes.html (21/11/2019).

[2] https://elderecho.com/google-concienciara-ciberseguridad-las-pymes-espanolas (21/11/2019).

[3] https://www.hiscox.es/10-realidades-sobre-ciberseguridad-pymes (21/11/2019).

[4] http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-octubre2019.pdf (11/11/2019). Ministerio de Trabajo, Migraciones y Seguridad Social .

[5] https://www.sei.cmu.edu/ (25/09/2019). Modelo creado por la Carnegie Mellon University para el SEI.

[6] Dirección General de Modernización Administrativa. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método*. Ministerio de Hacienda y Administraciones Públicas, Madrid, (2012).

[7] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf. (28/10/2019). *Gestión de riesgos. Una guía de aproximación para el empresario*.

[8] Cruz, D y Garre, S. *Sistema de gestión de la seguridad de la información*. Material docente de la UOC. Eureca Media SL, Barcelona, (2011)

[9] Dirección General de Modernización Administrativa. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II Catálogo de Elementos*. Ministerio de Hacienda y Administraciones Públicas, Madrid, (2012).

[10] Dirección General de Modernización Administrativa. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III Guía de Técnicas*. Ministerio de Hacienda y Administraciones Públicas, Madrid, (2012).

[11] https://www.iso.org/standard/54534.html (06/12/2019).

[12] https://www.iso.org/standard/54533.html (06/12/2019).

[13] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (06/12/2019).

[14] https://en.wikipedia.org/wiki/PDCA (06/12/2019).

Anexo I. Análisis diferencial ISO/IEC 27002:2013

La siguiente tabla muestra el estado inicial de la empresa en relación a los 114 puntos de control de la norma ISO/IEC 27002:2013.

N/A = No aplica

Controles	Valoración
5 Políticas de seguridad de la información	**0%**
5.1 Directrices de gestión de la seguridad de la información	0%
5.1.1 Políticas para la seguridad de la información	0%
5.1.2 Revisión de las políticas para la seguridad de la información	0%
6 Organización de la seguridad de la información	**14,5%**
6.1 Organización interna.	4,00%
6.1.1 Roles y responsabilidades en seguridad de la información	10%
6.1.2 Segregación de tareas	0%
6.1.3 Contacto con las autoridades	0%
6.1.4 Contacto con grupos de interés especial	0%
6.1.5 Seguridad de la información en la gestión de proyectos	10%
6.2 Los dispositivos móviles y el teletrabajo	25%
6.2.1 Política de dispositivos móviles	0%
6.2.2 Teletrabajo	50%
7 Seguridad relativa a los recursos humanos	**1,7%**
7.1 Antes del empleo	5,00%
7.1.1 Investigación de antecedentes	10%
7.1.2 Términos y condiciones del empleo	0%
7.2 Durante el empleo	0%
7.2.1 Responsabilidades de gestión	0%
7.2.2 Concienciación, educación y capacitación en seguridad de la información	0%
7.2.3 Proceso disciplinario	0%
7.3 Finalización del empleo o cambio en el puesto de trabajo	0%
7.3.1 Responsabilidades ante la finalización o cambio	0%
8 Gestión de activos	**16,7%**
8.1 Responsabilidad sobre los activos	40%
8.1.1 Inventario de activos	50%
8.1.2 Propiedad de los activos	50%
8.1.3 Uso aceptable de los activos	10%
8.1.4 Devolución de activos	50%

8.2 Clasificación de la información	0%
8.2.1 Clasificación de la información	0%
8.2.2 Etiquetado de la información	0%
8.2.3 Manipulado de la información	0%
8.3 Manipulación de los soportes	10%
8.3.1 Gestión de soportes extraíbles	10%
8.3.2 Eliminación de soportes	10%
8.3.3 Soportes físicos en tránsito	10%
9 Control de acceso	**38,8%**
9.1 Requisitos de negocio para el control de acceso	25%
9.1.1 Política de control de acceso	0%
9.1.2 Acceso a las redes y a los servicios de red	50%
9.2 Gestión de acceso de usuario	30%
9.2.1 Registro y baja de usuario	50%
9.2.2 Provisión de acceso de usuario	50%
9.2.3 Gestión de privilegios de acceso	50%
9.2.4 Gestión de la información secreta de autenticación de usuarios	10%
9.2.5 Revisión de los derechos de acceso de usuario	10%
9.2.6 Retirada o reasignación de los derechos de acceso	10%
9.3 Responsabilidades del usuario	50%
9.3.1 Uso de la información secreta de autenticación	50%
9.4 Control de acceso a sistemas y aplicaciones	50%
9.4.1 Restricción del acceso a la información	50%
9.4.2 Procedimientos seguros de inicio de sesión	50%
9.4.3 Sistema de gestión de contraseñas	50%
9.4.4 Uso de utilidades con privilegios de sistemas	10%
9.4.5 Control de acceso al código fuente de los programas	90%
10 Criptografia	**30%**
10.1 Controles criptográficos	30%
10.1.1 Política de uso de los controles criptográficos	10%
10.1.2 Gestión de claves	50%
11 Seguridad física y del entorno	**50%**
11.1 Áreas seguras	50%
11.1.1 Perímetro de seguridad física	50%
11.1.2 Controles físicos de entrada	50%
11.1.3 Seguridad de oficinas, despachos y recursos	50%
11.1.4 Protección contra las amenazas externas y ambientales	50%
11.1.5 El trabajo en áreas seguras	N/A
11.1.6 Áreas de carga y descarga	N/A
11.2 Seguridad de los equipos	50%

11.2.1 Emplazamiento y protección de equipos	50%
11.2.2 Instalaciones de suministro	50%
11.2.3 Seguridad del cableado	50%
11.2.4 Mantenimiento de los equipos	50%
11.2.5 Retirada de materiales propiedad de la empresa	50%
11.2.6 Seguridad de los equipos fuera de las instalaciones	50%
11.2.7 Reutilización o eliminación segura de equipos	50%
11.2.8 Equipo de usuario desatendido	50%
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	50%
12 Seguridad de las operaciones	**55,4%**
12.1 Procedimientos y responsabilidades operacionales	70%
12.1.1 Documentación de procedimientos de operación	90%
12.1.2 Gestión de cambios	50%
12.1.3 Gestión de capacidades	50%
12.1.4 Separación de los recursos de desarrollo, prueba y operación	90%
A.12.2 Protección contra el software malicioso (malware)	50%
12.2.1 Controles contra el código malicioso	50%
12.3 Copias de seguridad	90%
12.3.1 Copias de seguridad de la información	90%
12.4 Registros y supervisión	37,5%
12.4.1 Registro de eventos	50%
12.4.2 Protección de la información de registro	50%
12.4.3 Registros de administración y operación	50%
12.4.4 Sincronización del reloj	0%
12.5 Control del software en explotación	90%
12.5.1 Instalación del software en explotación	90%
12.6 Gestión de la vulnerabilidad técnica	50%
12.6.1 Gestión de las vulnerabilidades técnicas	50%
12.6.2 Restricción en la instalación de software	50%
12.7 Consideraciones sobre la auditoria de sistemas de información	0%
12.7.1 Controles de auditoria de sistemas de información	0%
13 Seguridad de las comunicaciones	**37,5%**
13.1 Gestión de la seguridad de las redes	50%
13.1.1 Controles de red	50%
13.1.2 Seguridad de los servicios de red	50%
13.1.3 Segregación en redes	50%
13.2 Intercambio de información	25%
13.2.1 Políticas y procedimientos de intercambio de información	0%
13.2.2 Acuerdos de intercambio de información	0%
13.2.3 Mensajería electrónica	50%

13.2.4 Acuerdos de confidencialidad o no revelación	50%
14 Adquisición, desarrollo y mantenimiento de los sistemas de información	**48,3%**
14.1 Requisitos de seguridad en los sistemas de información	50%
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	50%
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	50%
14.1.3 Protección de las transacciones de servicios de aplicaciones	50%
14.2 Seguridad en el desarrollo y en los procesos de soporte	45%
14.2.1 Política de desarrollo seguro	50%
14.2.2 Procedimiento de control de cambios en sistemas	50%
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	50%
14.2.4 Restricciones a los cambios en los paquetes de software	N/A
14.2.5 Principios de ingeniería de sistemas seguros	50%
14.2.6 Entorno de desarrollo seguro	50%
14.2.7 Externalización del desarrollo de software	10%
14.2.8 Pruebas funcionales de seguridad de sistemas	50%
14.2.9 Pruebas de aceptación de sistemas	50%
14.3 Datos de prueba	50%
14.3.1 Protección de los datos de prueba	50%
15 Relación con proveedores	**50%**
15.1 Seguridad en las relaciones con proveedores	50%
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	50%
15.1.2 Requisitos de seguridad en contratos con terceros	50%
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	50%
15.2 Gestión de la provisión de servicios del proveedor	50%
15.2.1 Control y revisión de la provisión de servicios del proveedor	50%
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	50%
16 Gestión de incidentes de seguridad de la información	**7,1%**
16.1 Gestión de incidentes de seguridad de la información y mejoras	7,1%
16.1.1 Responsabilidades y procedimientos	10%
16.1.2 Notificación de los eventos de seguridad de la información	10%
16.1.3 Notificación de puntos débiles de la seguridad	10%
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	10%
16.1.5 Respuesta a incidentes de seguridad de la información	10%
16.1.6 Aprendizaje de los incidentes de seguridad de la información	0%
16.1.7 Recopilación de evidencias	0%
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**50%**
17.1 Continuidad de la seguridad de la información	10%

17.1.1 Planificación de la continuidad de la seguridad de la información	10%
17.1.2 Implementar la continuidad de la seguridad de la información	10%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	10%
17.2 Redundancias	90%
17.2.1 Disponibilidad de los recursos de tratamiento de la información	90%
18 Cumplimiento	**13%**
18.1 Cumplimiento de los requisitos legales y contractuales	26%
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	10%
18.1.2 Derechos de propiedad intelectual (DPI)	50%
18.1.3 Protección de los registros de la organización	50%
18.1.4 Protección y privacidad de la información de carácter personal	10%
18.1.5 Regulación de los controles criptográficos	10%
18.2 Revisiones de la seguridad de la información	0%
18.2.1 Revisión independiente de la seguridad de la información	0%
18.2.2 Cumplimiento de las políticas y normas de seguridad	0%
18.2.3 Comprobación del cumplimiento técnico	0%

Anexo II. Política de Seguridad

POLÍTICA DE SEGURIDAD

Elaboración y revisado: ***Área de mejora y procesos***	Aprobado: ***Comité de Dirección***
	Firmado: J.S.XX ***Director del Comité de Dirección***

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Responsable de seguridad	08/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Justificación

TurisTech Balear SL y sus representantes Don J. S. XXX y Don T. C. XXX, como directores y gerentes de la empresa son conscientes de la importancia que tiene la seguridad de la información para la compañía y sus clientes. La información de la empresa representa un activo, el cual se expone a riesgos y amenazas que pueden producirse desde dentro o fuera de la organización, ya sea de forma intencionada o accidental. El hecho que ocurran puede generar pérdidas materiales y económicas, daños en la imagen institucional y en la confianza de los clientes, infracciones legales o vulnerar derechos de terceros.

Por todo lo anterior se decide implantar un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual requiere definir su documento estándar por excelencia: "*Política de Seguridad de la Información*".

2. Objetivos

La Política de Seguridad de la Información tiene como objetivos:

- Establecer los criterios y directrices generales sobre la gestión de Seguridad de la Información aplicables en TurisTech Balear SL en los cuales se basan las demás políticas, normas y procedimientos.

- Proporcionar orientación y apoyo en las acciones sobre la Gestión de Seguridad de la Información, de acuerdo a las normas de la empresa y la legislación vigente.

- Sensibilizar y concienciar a todo el personal de TurisTech Balear SL en materia de seguridad de la información.

3. Alcance y vigencia

Esta Política se dirige a todos los empleados, trabajadores eventuales, en prácticas, contratistas, consultores y proveedores que tengan acceso a los

recursos y servicios que contengan y/o procesen información de la empresa. También se aplicará a todos los ordenadores, dispositivos, redes, aplicaciones y sistemas operativos que son propiedad de la empresa o bien son contratados a terceros.

La Política de Seguridad de la Información y todo su contenido tendrán vigencia a contar desde su fecha de aprobación y puesta en marcha.

Este documento será revisado anualmente y se modificará cuando el Comité de Seguridad de la Información lo considere pertinente para la mejora continua de la misma.

4. Aprobación y difusión

La Dirección debe conocer, aprobar y firmar el contenido, así como hacer saber de su compromiso con esta Política al resto de la compañía. Por ello, cuando se apruebe, será la Dirección la encargada de difundirla para que todo el personal tenga claro quien es el promotor principal. Esta difusión se realizará también a terceras partes con acceso a la información de TurisTech Balear SL

5. Cumplimiento legal y estándares de seguridad

La presente Política se regirá por la siguiente legislación y normas de seguridad:

- Reglamento General de Protección de Datos (RGPD) de 27 de abril de 2016 del Parlamento Europeo y del Consejo.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)

- Norma de seguridad de datos de la Industria de tarjetas de pago (PCI DSS – SAQ A-EP)

- ISO/IEC 27001:2013. Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la información – Requisitos.

- ISO/IEC 27002:2013. Tecnología de la Información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.

6. Sanciones

El incumplimiento de las políticas definidas por la empresa TurisTech Balear SL dará derecho a ésta a ejercer las acciones civiles, penales y administrativas que correspondan contra el infractor, así como a la terminación de los posibles contratos existentes entre ambas partes.

Las medidas de disciplina como resultado de una violación de la seguridad informática será gestionada por la Dirección en colaboración con el responsable del Departamento de Seguridad Informática y de Recursos Humanos.

7. Normas

7.1 Normativa de seguridad de equipos

Los equipos son una parte fundamental para la organización pues son el medio para almacenar y gestionar la información. Por ello el departamento TIC debe velar para que todos los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas en caso de incendio, robo, inundaciones, fallos eléctricos y otros factores que puedan inutilizar la infraestructura informática.

I. El departamento TIC tendrá un inventario actualizado de todos los equipos y dispositivos que son propiedad de la empresa.

II. Para el traslado, retirada o destrucción de cualquier equipo, periférico o dispositivo que sea propiedad de la empresa, será necesario contar con el consentimiento del responsable del departamento TIC.

III. Los equipos propiedad de TurisTech Balear SL deben usarse solamente para las actividades propias de la empresa, por lo tanto los usuarios no deben utilizarlos para asuntos personales. En caso que un empleado utilice un equipo o dispositivo de su propiedad deberá contar con la autorización del responsable del departamento TIC, y además, se aplicarán las medidas necesarias para asegurar que los entornos laboral y personal están totalmente independizados.

IV. Todo equipo de TurisTech Balear SL así como los que sean de propiedad de los empleados pero que sean usados para la actividad de la empresa, deberá estar ubicado en una área que cumpla con los requerimientos de seguridad física y condiciones ambientales adecuadas. Se mantendrán alejados de la luz directa del Sol, humedades y contactos con líquidos.

V. No se permite el uso de dispositivos de almacenamiento extraíble como memorias USB, CD o DVD sin conocer su procedencia y sin haberlo analizado anteriormente con las herramientas adecuadas y en un equipo específico ajeno sin conexión a la red interna o Internet.

VI. Se aplicarán las medidas de seguridad necesarias para bloquear los equipos cuando sus usuarios se ausenten. Los usuarios no deben dejar las sesiones abiertas mientras el equipo no este atendido. Estas pautas deberán aplicarse tanto a los dispositivos móviles como a los equipos fijos.

VII. Se deben implantar sistemas de protección de los equipos portátiles y dispositivos extraíbles, cuando las instalaciones se encuentran cerradas, por ejemplo, usar armarios o cajas de seguridad con cierre electrónico.

VIII. En la oficina se instalará y mantendrá un sistema de alarma conectado con las autoridades policiales.

IX. En la oficina se instalará y mantendrá un sistema de interrupción de suministro eléctrico.

X. Se definirán períodos de tiempo para realizar las revisiones, la limpieza y el mantenimiento de los equipos. Estas tareas y las de reparación serán realizadas por el personal de mantenimiento autorizado.

7.2 Normativa de seguridad de usuarios

Los usuarios son aquellas personas que utilizan equipos, dispositivos y recursos de red, ya sean de su propiedad o de la organización, con acceso a la información de la empresa. Por ello es necesario definir las restricciones, autorizaciones, denegaciones, roles y perfiles de usuario, así como todo lo necesario que permita mantener un buen nivel de seguridad informática.

I. Corresponde a los usuarios el responsabilizarse y cumplir con la normativa de la empresa, procedimientos y estándares relacionados con la seguridad informática.

II. Los permisos a usuarios son personales e intransferibles y deberán adecuarse a las funciones que desempeñen. La solicitud se realizará al responsable de su departamento, o en su defecto, al Administrador o Responsable del Departamento de Seguridad Informática.

III. Los usuarios deben renovar periódicamente su clave de acceso a los diferentes sistemas, quedando totalmente prohibido el intento de violación de los controles establecidos; El uso sin autorización de los activos informáticos; Acceder a servicios informáticos utilizando cuentas o contraseñas de otros usuarios, aún con la autorización del propietario de la misma.

IV. Los usuarios son responsables de las actividades que se realicen con sus credenciales. Si se detectan irregularidades tienen que informar de inmediato al responsable del Departamento de Seguridad Informática.

7.3 Normativa de seguridad de contraseñas

Las contraseñas son el mecanismo principal que usa la empresa para el control de acceso a la información, aplicaciones y diversos sistemas. Es por ello que todos los usuarios deberán prestar la debida atención en cumplir está Política.

I. Los usuarios deberán usar contraseñas que sean difíciles de adivinar, para ello se evitará el uso de información de la vida personal o profesional como la matricula de su vehículo, nombres de personas, direcciones, fechas señaladas, teléfonos, etc.

II. No se usaran contraseñas con una secuencia de caracteres que esté parcialmente compuesta de una fecha o factor predecible, por ejemplo «34ENE» en enero, «34FEB» en febrero y así sucesivamente. Tampoco hay que usar contraseñas similares o idénticas a las utilizadas anteriormente.

III. Las contraseñas tendrán un mínimo de 8 caracteres combinando letras en mayúsculas, minúsculas, números y signos de puntuación.

IV. Con la finalidad de asegurar que una contraseña comprometida no se esté utilizando en los distintos sistemas de acceso, deberán cambiarse en un intervalo máximo de 60 días.

V. Las contraseñas no se han de almacenar en ningún medio legible como ficheros de texto, macros de aplicaciones, teclas de función de un terminal, equipos sin un sistema de control de acceso u otras formas que puedan ser descubiertas por personas o sistemas sin autorización. Tampoco deben anotarse en papel y dejarse a la vista.

VI. En el momento que un usuario sospeche que su contraseña o contraseñas han sido comprometidas, deberá cambiarse de inmediato e informar al responsable del departamento TIC.

7.4 Normativa de control de acceso

I. Los roles, perfiles y privilegios concedidos a los usuarios serán asignados y revisados por los administradores de los diferentes servicios, aplicaciones y sistemas de forma periódica para evitar accesos no autorizados.

II. La Dirección de la compañía se reserva cualquier derecho a revocar los privilegios de sistemas de cualquier usuario en el momento que crea oportuno.

7.5 Normativa de desarrollo y uso de software

La principal actividad de TurisTech Balear SL es el desarrollo de distintos servicios y aplicaciones, por lo que el software generado es uno de sus principales activos. Por otro lado, se hace uso de software de terceras partes para la realización de distintas tareas.

I. Los empleados, trabajadores eventuales o en prácticas, contratistas y consultores que estén prestando un servicio de desarrollo de software para la compañía, ceden exclusivamente a esta los derechos de patentes, reproducción u otra propiedad intelectual del producto creado.

II. Todos los programas y documentación generados o facilitados por los empleados, trabajadores eventuales o en prácticas, contratistas y consultores a beneficio de la empresa se consideran propiedad de la compañía.

III. En ningún caso los empleados, trabajadores eventuales o en prácticas, contratistas y consultores podrán copiar el software de la compañía en algún tipo de soporte y transferirlo a terceras partes sin la autorización de la Dirección del departamento TIC.

IV. Se deberán separar los entornos de desarrollo de los de producción para evitar problemas de disponibilidad o fallos en el servicio. Se evitará que los datos e información de los entornos de desarrollo, así como el código fuente estén disponibles para los entornos de producción.

V. Queda estrictamente prohibido el uso, instalación, reproducción, cesión, transformación o comunicación pública de programas informáticos, así como de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial, sin la correspondiente autorización y/o licencia.

VI. Se definirán procedimientos para ejecutar instalaciones de software en cualquier dispositivo de la organización o que sea usado para su actividad. Se valorará la necesidad de actualización o instalación y en caso de ser necesario, cualquier software será probado primero en entornos de prueba y aislados de los de explotación.

7.6 Normativa de copias de seguridad

I. Toda información de relevancia y que suponga un activo para TurisTech Balear SL debe contar con su respectiva copia de seguridad y almacenarla durante un tiempo determinado.

II. El propietario de la información, junto con el administrador de sistemas y con la supervisión del responsable del departamento TIC, son los encargados de la creación y seguimiento de las copias de seguridad.

7.7 Normativa de teletrabajo

I. El permiso de teletrabajo será concedido por la dirección basándose en la antigüedad del empleado, mínimo un año y medio, su grado de adquisición de los métodos y la dinámica de trabajo, así como del nivel de autonomía en la organización y ejecución de tareas.

II. La concesión del teletrabajo dependerá en parte de la conformidad de ciertas normativas y estándares relacionados con la seguridad informática.

III. El departamento TIC proporcionará los medios y protocolos seguros para que los empleados puedan conectarse desde sus casas a los diferentes equipos y sistemas de la empresa.

IV. El departamento TIC mantendrá un registro de la custodia de los activos que abandonan la organización y realizará evaluaciones de riesgo de las instalaciones donde serán utilizados.

7.8 Normativa de la seguridad en la red corporativa

I. En relación a las conexiones internas, TurisTech Balear SL actualmente no tiene interconectados los equipos existentes, por lo que no dispone de una topología de red interna. Este punto será revisado y actualizado en caso de crearse esta infraestructura.

II. La empresa mantiene conexiones externas entre los equipos internos y los diferentes servicios Cloud que tienen contratados. Estas conexiones se deberán realizar usando protocolos de seguridad que permitan cifrar la información que se intercambie. Actualmente el protocolo que se usa es SSH (Secure Shell).

7.9 Normativa sobre terceras partes

I. Sólo se permite el acceso a la información interna de la compañía cuando exista una necesidad de su conocimiento demostrable, cuando se haya firmado un acuerdo de no revelar, o cuando haya sido autorizado expresamente por el responsable de la información o de la dirección de la compañía.

II. Si TurisTech Balear SL requiere de servicios de terceras partes para procesar y/o alojar su información, éste tendrá que aceptar las normas establecidas por la empresa. Cuando por algún motivo no se pueda cumplir con

las normas, ya sea de forma parcial o completa, el Comité de Seguridad de la Información elaborará un informe detallando los riesgos e impacto que puedan derivar, el cual deberá ser revisado y firmado por el Comité de Dirección.

7.10 Normativa de incidentes de seguridad de la información y vulnerabilidades

I. Se deberá informar al Departamento TIC ante cualquier aparición de virus, programas sospechosos, intentos de intromisión en los sistemas y equipos de la empresa o los que son usados para su actividad.

II. Las actividades que supongan una amenaza para las medidas de seguridad de la empresa o que sean ilegales se considerarán como una violación grave de la normativa interna de la compañía.

III. El Responsable de Seguridad será el encargado de contactar con las autoridades en aquellos casos donde fuera necesario, por ejemplo si se sospecha que se pueda haber infringido la ley.

IV. Con el fin de poder analizar y gestionar vulnerabilidades se llevará un registro de activos de información.

V. Se monitorizarán los sistemas y procesos que puedan arrojar información valiosa para la toma de decisiones en cuanto a la identificación de vulnerabilidades técnicas.

7.11 Normativa de clasificación de la información

La compañía ha adoptado un sistema de clasificación de la información formado por cuatro grupos.

I. Toda información bajo el control de la empresa, ya sea generada interna o externamente, se incluirá en una de las categorías siguientes:

- **Secreta**. Información que sólo puede conocerla el propietario de la misma como podrían ser contraseñas o claves criptográficas.

- **Confidencial**. Engloba aquella información accesible unicamente por un grupo cerrado de personas, por ejemplo, un informe de auditoría, cifras de negocio o un listado de clientes.

- **Uso interno**. Aplica a información menos sensible, que se pretende sea de uso interno de TurisTech Balear SL.

- **Pública**. Cualquier persona puede tener acceso a la información de la empresa ya sea digital o en papel.

II. Los empleados de TurisTech Balear SL tendrán que conocer las definiciones del punto I, así como los procedimientos a seguir para la seguridad de la información según a la categoría que pertenezca.

III. Según esta normativa la “información sensible” es aquella que pertenece a la categoría Secreta o Confidencial.

IV. Los empleados de la compañía deberán firmar una cláusula de confidencialidad al incorporarse a la plantilla.

7.12 Normativa para la continuidad del negocio

I. Anualmente se realizará un análisis de riesgos (AARR), que permitirá conocer el estado actual de los activos de la empresa en relación a las amenazas y el impacto que éstas pueden provocar.

II. La Dirección, junto con los responsables de cada área organizativa, deberán revisar el AARR y establecer los mecanismos necesarios para afrontar con garantías los incidentes de seguridad de la información que puedan ocurrir.

Para ello se definirá un Plan de Contingencia y Continuidad del Negocio, el cual será periódicamente revisado y aprobado por la Dirección.

7.13 Normativa de cumplimiento

I. El Responsable de Seguridad y el Delegado de Protección de Datos (pueden ser la misma persona) se encargarán de revisar anualmente, o cuando así lo requieran las leyes en materia de la seguridad de la información, que las actividades y servicios de la empresa cumplen con la normativa legal vigente. Al detectar algún incumplimiento legal lo comunicarán en la menor brevedad a la Dirección para adoptar las medidas y soluciones correspondientes.

II. Los responsables y directivos de las diferentes áreas realizarán revisiones periódicas del cumplimiento de las políticas y normas internas de su ámbito. Para ello se aplicarán métodos y/o herramientas que ayuden a la medición, detección y evaluación.

Anexo III. Procedimiento de Auditorias Internas

PROCEDIMIENTO DE AUDITORIAS INTERNAS A LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE TURISTECH BALEAR SL

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	12/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivos

Establecer los lineamientos y el procedimiento a seguir para la planificación, realización y cierre de auditorías internas al Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001:2013.

2. Alcance

Este procedimiento es aplicable a los procesos comprendidos dentro del alcance del Plan Director.

El presente documento es administrado por el Departamento TIC y es una fuente de consulta para todo el personal de las áreas comprendidas en su alcance.

3. Documentos de referencia

Norma ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

Norma ISO/IEC 27002:2013. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

4. Condiciones

I. Las auditorías internas se realizarán para poder determinar el grado en que el SGSI está implementado y mantenido de forma óptima, si cumple con la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013 y los requisitos propios de la empresa. Estas formarán parte del Programa Anual de Auditoría el cual será aprobado por el Comité de Dirección dentro del primer trimestre de cada año.

II. Las auditorías internas se realizarán a intervalos planificados (al menos una vez al año) y el alcance podrá ser parcial o integral, aunque en el plazo máximo de tres años debe quedar auditado el SGSI de forma completa.

III. El equipo auditor podrá estar formado por uno o varios auditores dependiendo de la complejidad y alcance de la auditoría. También podrán intervenir auditores en formación y expertos técnicos. Los auditores podrán ser empleados de la entidad, o en caso necesario, contratados a terceros.

IV. Los auditores deberán mantener la objetividad e imparcialidad durante la realización de la auditoría y no podrán auditar aquellos procesos donde haya intervenido en cualquier fase de su desarrollo y creación.

V. El Responsable de Seguridad de la Información será el encargado de crear el equipo auditor y garantizará que el proceso de auditoría se ejecute siguiendo el Procedimiento de Auditoría Interna.

VI. El responsable y los empleados del proceso o área objeto de la auditoria, deberán poner a disposición del equipo auditor los medios necesarios para su correcta ejecución. Facilitarán el acceso a las instalaciones y documentos relevantes y cooperarán con los auditores para asegurar el éxito de la auditoría.

VII. Los hallazgos de la auditoría se clasificarán y tratarán de la siguiente forma:

Tipo de hallazgo	Tratamiento
No Conformidad Mayor	Ausencia o fallo en implantar y mantener uno o más controles de la ISO/IEC 27002:2013, que afecta a la capacidad del sistema de gestión
No Conformidad Menor	Ausencia o fallo en implantar y mantener uno o más controles de la ISO/IEC 27002:2013, pero no afecta a la capacidad del sistema de gestión
Observaciones	Acción de mejora que la organización puede considerar o no. Se constituye como una recomendación pero su repetición y no corrección puede derivar en una No Conformidad.

5. Descripción del procedimiento

Las auditorías deberán realizarse siguiendo un procedimiento compuesto de tres fases: Planificación, Ejecución, Resultados y Seguimiento.

5.1 Planificación

I. Se define si la auditoría programada será realizada por personal de la empresa o externo.

II. Si el equipo auditor lo forma personal interno el Comité de Seguridad de la empresa designará al auditor líder, auditores y técnicos si son requeridos y se notificará el resultado a las partes involucradas.

III. El equipo auditor y auditado establecerán el alcance y objetivos de la auditoría.

IV. La dirección deberá dar su apoyo y compromiso para la realización de la acción de auditoría, la cual si es interna se redactará y firmará la carta de auditoría.

V. El equipo auditor deberá definir el Plan de Auditoría, determinando de forma detallada los siguientes puntos:

- Plazos temporales:
  - Fechas de inicio y fin de los períodos de prueba.
  - Periodos del día para realizar las pruebas.
  - Periodicidad del plan de auditoría.

- Establecer vías y procedimientos de comunicación con el auditado.

- Crear un inventario de las políticas corporativas que afecten a la auditoría.

- Documentar las pruebas y sus objetivos, indicando como se realizarán y las herramientas o requisitos específicos necesarios.

5.2 Ejecución

I. Se realizará la reunión de apertura con el personal involucrado para hacer las presentaciones en caso de ser un equipo externo, informar de los horarios, los responsables y los procesos a auditar.

II. El equipo auditor recolectará toda la información necesaria para preparar la ejecución de las pruebas identificadas en el Plan de Auditoria.

III. Una vez recopilada la información previa, se ejecutarán las pruebas de auditoría y documentarán los hallazgos y su clasificación. Si es necesario se podrán realizar entrevistas con el personal de la área afectada, así como visitas para observar in situ el modo en que operan los sistemas de información.

IV. Finalizado el punto anterior se procederá a analizar toda la información recopilada en la ejecución de la auditoría y se elaborará el Informe de Auditoría Interna.

5.3 Resultados

I. Se realizará una reunión con la Dirección y los responsables de los procesos y/o áreas objeto de la auditoría, para presentar el Informe de Auditoría Interna y sus resultados.

5.4 Seguimiento

I. Una vez finalizada la auditoría y entregado el informe, el auditado es el responsable de adoptar y aplicar las medidas que se recomienden.

II. El Comité de Seguridad de la Información planificará las acciones correctivas a ejecutar. En esta tarea podrá participar el equipo auditor si así lo requiere el Comité.

Anexo IV. Gestión de indicadores

GESTIÓN DE INDICADORES

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	13/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivos

Con en el fin de mantener actualizado el Sistema de Gestión de la Información, es necesario tener un modo para poder evaluarlo. Los indicadores permiten controlar el funcionamiento, la eficacia y eficiencia de las medidas de seguridad de la información implantadas. Por ello, es imprescindible definir e implantar indicadores que proporcionen esta información.

2. Alcance

Este procedimiento es aplicable a todos los controles de la norma ISO/IEC 27002:2013 que son de aplicación. No se definirán métricas para cada uno de ellos, sino que se agruparán en indicadores de alto nivel y que intenten cubrir la mayor parte de la norma.

3. Indicadores

ID indicador de control	IC01
Nombre de indicador	Política de la seguridad de la información
Descripción	Indica si la entidad tiene definida y actualizada una política de seguridad de la información
Controles de seguridad ISO/IEC 27002:2013 relacionados	5.1.1 Políticas para la seguridad de la información 5.1.2 Revisión de las políticas para la seguridad de la información
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Frecuencia de medición	Anual
Valor objetivo **Valor umbral**	Número de revisiones = 1 Número de revisiones < 1
Responsable de la medición	Responsable de Seguridad de la Información y el Comité de Dirección

ID indicador de control	IC02
Nombre de indicador	Seguridad de la información en proyectos
Descripción	Indica el grado de inclusión de la seguridad de la información dentro de la gestión de proyectos
Controles de seguridad ISO/IEC 27002:2013 relacionados	6.1.5 Seguridad de la información en la gestión de proyectos
Fórmula de medición	Total proyectos / Proyectos que incluyen un análisis de riesgos de la seguridad de la información
Unidades de medida	Porcentaje de Proyectos
Frecuencia de medición	Anual
Valor objetivo **Valor umbral**	Proyectos que incluyen análisis de riesgos de seguridad de la información = 100% Proyectos que incluyen análisis de riesgos de seguridad de la información < 90%
Responsable de la medición	Responsable de Seguridad de la Información

ID indicador de control	IC03
Nombre de indicador	Capacitación y formación en seguridad de la información
Descripción	Revisa si todos los empleados han recibido un plan de formación en materia de la seguridad de la información
Controles de seguridad ISO/IEC 27002:2013 relacionados	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Fórmula de medición	Total empleados que han realizado el plan de formación / Total empleados
Unidades de medida	Porcentaje de empleados
Frecuencia de medición	Anual
Valor objetivo **Valor umbral**	Porcentaje de empleados = 100% Porcentaje de propietarios < 75%
Responsable de la medición	Responsable de Seguridad de la Información y Departamento de RRHH

ID indicador de control	IC04
Nombre de indicador	Gestión de inventario de activos
Descripción	Revisión del inventario de activos del sistema de información
Controles de seguridad ISO/IEC 27002:2013 relacionados	8.1.1 Inventario de activos
Fórmula de medición	Revisiones inventario / año
Unidades de medida	Número revisiones
Frecuencia de medición	Anual
Valor objetivo	Número de revisiones = 1
Valor umbral	Número de revisiones < 1
Responsable de la medición	Comité de Seguridad de la Información

ID indicador de control	IC05
Nombre de indicador	Gestión de los propietarios de los activos
Descripción	Revisa la relación entre los activos identificados y sus propietarios, los cuales son sus responsables Cada activo debe tener asignado un propietario
Controles de seguridad ISO/IEC 27002:2013 relacionados	8.1.2 Propiedad de los activos
Fórmula de medición	Número de propietarios / activos
Unidades de medida	Porcentaje de propietarios
Frecuencia de medición	Trimestral
Valor objetivo	Porcentaje de propietarios = 100%
Valor umbral	Porcentaje de propietarios < 100%
Responsable de la medición	Comité de Seguridad de la Información

ID indicador de control	IC06
Nombre de indicador	Clasificación de la información
Descripción	Revisa si los activos están debidamente clasificados
Controles de seguridad ISO/IEC 27002:2013 relacionados	8.2.1 Clasificación de la información
Fórmula de medición	Total de activos clasificados / Total de activos
Unidades de medida	Porcentaje de activos
Frecuencia de medición	Semestral
Valor objetivo	Porcentaje activos clasificados = 100%
Valor umbral	Porcentaje activos clasificados < 80%
Responsable de la medición	El responsable del activo

ID indicador de control	IC07
Nombre de indicador	Política de control de acceso
Descripción	Revisa si la entidad tiene definida y actualizada una política de acceso a la información, así como las directrices y normas para controlar los accesos a los diferentes sistemas de la entidad
Controles de seguridad ISO/IEC 27002:2013 relacionados	9 Control de acceso
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Frecuencia de medición	Anual
Valor objetivo	Número de revisiones = 1
Valor umbral	Número de revisiones < 1
Responsable de la medición	Comité de Seguridad de la Información

ID indicador de control	IC08
Nombre de indicador	Criptografía
Descripción	Revisa el grado de cifrado de la información clasificada como confidencial
Controles de seguridad ISO/IEC 27002:2013 relacionados	10.1 Controles criptográficos
Fórmula de medición	Revisar si la información confidencial esta cifrada
Unidades de medida	Cifrada / No cifrada
Frecuencia de medición	Anual
Valor objetivo	Información confidencial = Cifrada
Valor umbral	Información confidencial = No cifrada
Responsable de la medición	Responsable de Seguridad de la Información

ID indicador de control	IC09
Nombre de indicador	Copias de seguridad
Descripción	Revisa si la entidad tiene definida y actualizada las normas y directrices de copias de seguridad para la información que lo requiera
Controles de seguridad ISO/IEC 27002:2013 relacionados	12.3.1 Copias de seguridad de la información
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Frecuencia de medición	Anual
Valor objetivo	Número de revisiones = 1
Valor umbral	Número de revisiones < 1
Responsable de la medición	Responsable de Seguridad de la Información

ID indicador de control	IC10
Nombre de indicador	Disponibilidad de los servicios de proveedores
Descripción	Muestra el grado de cumplimiento de los acuerdos de nivel de servicio o SLA de los proveedores
Controles de seguridad ISO/IEC 27002:2013 relacionados	15.1.1 Política de seguridad de la información en las relaciones con los proveedores 15.2.1 Control y revisión de la provisión de servicios del proveedor
Fórmula de medición	Disp = 100 x (T – Tc) / T Disp = 100% de disponibilidad del servicios T = tiempo total mensual Tc = tiempo con pérdida de disponibilidad
Unidades de medida	Disponibilidad
Frecuencia de medición	Mensual
Valor objetivo **Valor umbral**	Disponibilidad = 99% Disponibilidad < 95%
Responsable de la medición	Comité de Seguridad de la Información

ID indicador de control	IC11
Nombre de indicador	Control de incidentes de seguridad de la información y continuidad del negocio
Descripción	Revisa la relación entre los incidentes ocurridos y los que se han resuelto
Controles de seguridad ISO/IEC 27002:2013 relacionados	16.1.5 Respuesta a incidentes e seguridad de la información 16.1.7 Recopilación de evidencias 17.1.2 Implementar la continuidad de la seguridad de la información 17.2.1 Disponibilidad de los recursos de tratamiento de la información
Fórmula de medición	Número de incidentes resueltos / Número de incidentes ocurridos
Unidades de medida	Porcentaje de incidentes
Frecuencia de medición	Mensual

Valor objetivo	Porcentaje de incidentes resueltos = 90%
Valor umbral	Porcentaje de incidentes resueltos < 70%
Responsable de la medición	Responsable de Seguridad de la Información

ID indicador de control	IC12
Nombre de indicador	Cumplimiento legal y normativo
Descripción	Verifica el grado de cumplimiento de las distintas leyes y normativas que afectan a la seguridad de la información
Controles de seguridad ISO/IEC 27002:2013 relacionados	18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales 18.1.2 Derechos de propiedad intelectual (DPI) 18.1.3 Protección de los registros de la organización 18.1.4 Protección y privacidad de la información de carácter personal
Fórmula de medición	Revisar si los procesos cumplen las distintas leyes y normativas
Unidades de medida	Cumple / No cumple
Frecuencia de medición	Anual
Valor objetivo	Ley / Normativa = Cumple
Valor umbral	Ley / Normativa = No cumple
Responsable de la medición	Comité de Seguridad de la Información

Anexo V. Procedimiento de Revisión por la Dirección

PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	15/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivos

Establecer los criterios y requisitos para la revisión por parte de la Dirección, con la finalidad de determinar si el Sistema de Gestión de Seguridad de la Información (SGSI) cumple con los requisitos de la norma ISO/IEC 27001:2013 y la Política de Seguridad definida. Así mismo, asegurar la trazabilidad, conveniencia, eficacia, eficiencia y efectividad del SGSI.

2. Alcance

Es de aplicación a todas las revisiones realizadas del Sistema de Gestión de Seguridad de la Información por la dirección.

3. Procedimiento

I. Las revisiones del Sistema de Gestión de Seguridad de la Información (SGSI) de TurisTech Balear SL se realizarán anualmente, pudiéndose realizar con más frecuencia según las circunstancias y si la dirección lo considera oportuno por el nivel de eficacia e implantación del Sistema.

II. Con la periodicidad estipulada para la realización del SGSI, el Responsable de Seguridad de la Información y el Comité de Dirección realizarán un análisis y valoración de la información y los datos proporcionados por el Sistema de Gestión de Seguridad de la Información, al menos con respecto a los siguientes puntos:

- Resultados de auditorías.
- Estado de las acciones correctivas y preventivas.
- Analizar los resultados de los indicadores de control.
- Analizar los problemas e incidentes reportados y su tratamiento.
- Analizar los recursos asignados al SGSI.
- Acciones de seguimiento de las revisiones anteriores por la dirección.
- Cambios que podrían afectar al SGSI.

- Recomendaciones de mejora.
- Realimentación de los clientes.

III. En base al análisis realizado, el Responsable de Seguridad de la Información emitirá un Informe de Revisión por la Dirección fechado y firmado por ella, que será sometido a la aprobación de la Gerencia, quedando evidencia de dicha aprobación mediante su fechado y firma. En este informe se incluyen las conclusiones sobre cada uno de los puntos tratados así como las acciones de mejora propuestas por la Gerencia.

IV. El Responsable de Seguridad de la Información verificará la eficacia de las soluciones adoptadas en base a los informes presentados en la próxima Revisión de la Dirección. En el caso de resultar no eficaz, se decidirá un nuevo planteamiento a seguir, o incluso se podrá desestimar.

Anexo VI. Gestión de roles y responsabilidades

GESTIÓN DE ROLES Y RESPONSABILIDADES

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	15/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivo

Definir los roles, responsabilidades y funciones de las personas que formarán la estructura interna con responsabilidad directa sobre la seguridad de la información, con el fin de facilitar la implantación del Sistema de Gestión de Seguridad de la Información.

2. Alcance

Este documento va dirigido a la alta dirección de la organización.

3. Roles y responsabilidades

4.1 Comité de Dirección

Está formado por los dos gerentes de la empresa que al mismo tiempo son sus fundadores. Las funciones directivas que desempeñan son las siguientes:

- Director de Administración y TIC
- Director de RRHH y Comercial

Las funciones de dicho comité son[8]:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
- Nombrar los miembros del Comité de Seguridad de la Información y darle soporte, dotándoles de los recursos necesarios y establecer sus directrices de trabajo.
- Aprobar la política, las normas y responsabilidades generales en materia de seguridad de la información.

- Determinar el umbral de riesgo aceptable en materia de seguridad.

- Analizar riesgos posibles introducidos por cambios en las funciones o en el funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.

- Aprobar el Plan de Seguridad de la Información, que recoge los principales proyectos e iniciativas en la materia.

- Hacer el seguimiento del cuadro de mando de la seguridad de la información.

4.3 Comité de Seguridad de la Información

Está formado por un grupo de responsables de la empresa que tomarán las decisiones en materia de seguridad de la información de forma consensuada. Los integrantes son:

- Director TIC.

- Responsable de Seguridad Informática.

Sus funciones son[8]:

- Ejecutar las directrices del Comité de Dirección.

- Asignar roles y funciones en materia de seguridad.

- Presentar al Comité de Dirección, las políticas, normas y responsabilidades de seguridad de la información para su aprobación.

- Validar el mapa de riesgos y las acciones de mitigación que ha propuesto el Responsable de Seguridad de la Información.

- Validar el Plan Director de Seguridad de la información y presentarlo a aprobación al Comité de Dirección, supervisar y hacer el seguimiento de su implantación.

- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.

- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.

- Revisar las incidencias más destacadas.

- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

4.4 Responsable de Seguridad de la información

Esta persona será la encargada de coordinar las acciones para garantizar la seguridad de la información sea cual sea su formato y durante todo su ciclo de vida, de forma que se proteja en términos de confidencialidad, privacidad, integridad, disponibilidad, autenticidad y trazabilidad.

Las funciones principales de esta figura son[8]:

- Implantar las directrices del Comité de Seguridad de la Información.

- Elaborar, promover y mantener una política de seguridad de la información y proponer anualmente objetivos en materia de seguridad de la información.

- Desarrollar y mantener el documento de *Organización de la seguridad de la información* en colaboración con el área de organización o recursos humanos, en el cual se recoja quien asume cada una de las

responsabilidades en seguridad y también una descripción detallada de las funciones y dependencias.

- Desarrollar con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.

- Actuar como punto central en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa, etc.), con el fin de gestionar la seguridad de la información de manera global.

- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones para mejorar y mitigar el riesgo, de acuerdo con el umbral aceptable que ha definido el Comité de Dirección. Elevar el mapa de riesgos y el plan de seguridad de la información al Comité de Seguridad de la Información.

- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de las aplicaciones.

- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas y metodológicas. Esta revisión ha de permitir proponer o actualizar el plan de seguridad de la información e incorporarle todas las acciones preventivas, correctivas y de mejora que se hayan detectado. Una vez el Comité de Seguridad de la Información ha aprobado este plan y el presupuesto, el Responsable de Seguridad de la Información ha de gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.

- Coordinar acciones con las áreas de negocio para elaborar y gestionar un plan de continuidad de negocio para la compañía, basado en el

análisis de riesgos y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.

- Velar por el cumplimiento de la normativa legal aplicable y coordinar las actuaciones necesarias con las unidades responsables.

- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios, etc.), hacer el seguimiento de las incidencias de seguridad y escalarlos al Comité de Seguridad de la Información si procede.

- Elaborar y mantener un plan de concienciación y formación del personal en materia de seguridad de la información, en colaboración con el departamento de recursos humanos.

- Hacer el seguimiento de las incidencias, revisarlas y escalarlas al Comité de Seguridad de la Información si procede.

- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El Responsable de Seguridad de la Información ha de analizar y mantener actualizado el cuadro de mando y presentarlo al Comité de Seguridad de la Información con la periodicidad que se establezca.

4.5 Delegado de Protección de Datos

Esta figura es un elemento del Reglamento General de Protección de Datos (RGPD) aprobado por el Parlamento Europeo, en el cual se define la persona encargada del cumplimiento de la normativa de la protección de datos en las organizaciones. Este rol puede ser asumido por una persona interna o externa a la entidad, que en este caso y por la similitud de tareas podría recaer en el Responsable de Seguridad de la Información.

Las funciones principales son:

- Asesoramiento a los directivos y el personal de la organización.
- Supervisión del cumplimiento normativo.
- Cooperación y enlace con las autoridades de control AEPD y los ciudadanos que quieran ejercer sus derechos.

4.6 Personal en general

Quedan incluidas en este perfil todas aquellas personas de la organización y externas, no incluidas en las categorías anteriores y que tengan acceso a la información de la compañía. Su principal función es respetar y cumplir con la Política de Seguridad, las normas y las directrices definidas por la empresa, así como las leyes vigentes en materia de seguridad de la información.

Anexo VII. Metodología de Análisis de Riesgos

METODOLOGÍA DE ANÁLISIS DE RIESGOS

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	16/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivo

Definir la metodología que TurisTech Balear SL usará para realizar el análisis de riesgos, a partir del cual se identificarán los riesgos a que esta expuesta la organización desde el punto de vista de la seguridad y que pueden afectar al desarrollo normal del negocio.

2. Alcance

El procedimiento abarca todos aquellos activos que son de valor para la empresa y que son susceptibles a amenazas.

3. Metodología

Entre las diferentes posibilidades existentes TurisTech Balear SL ha optado por usar la metodología MAGERIT en su versión 3.0. El nombre son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. El Consejo Superior de Administración Electrónica es quién ha elaborado y promueve esta metodología.

Su elección se debe a las siguientes causas:

- Se trata de un método contrastado.
- Está alineado con la norma ISO/IEC 27001:2013.
- Se puede aplicar a cualquier tipo de organización.
- Cuenta con una documentación que facilita su comprensión y aplicación.
- Aunque no es imprescindible, es posible usar una herramienta EAR (Entorno de Análisis de Riesgos) que facilita la implementación de MAGERIT.

La metodología MAGERIT se compone de un conjunto de fases que definen un proceso, que tiene como punto final elaborar e identificar todos los riesgos de una organización.

3.1 Fase 1. Recogida de datos y procesos de información

Es uno de los puntos más importantes de toda la metodología, pues es donde se define el alcance del análisis y por tanto, repercutirá directamente al esfuerzo para ejecutar el proceso.

Los riesgos pueden interferir y afectar en los procesos de la empresa, por ello es necesario analizar e identificar los procesos que se llevan a cabo y cual de ellos son críticos para la entidad.

3.2 Fase 2. Establecimiento de parámetros

Consiste en establecer los parámetros a partir de los cuales se obtendrán los resultados del análisis. Estos deben ser usados durante todo el proceso, ya que de no hacerlo así no se podrán comparar los resultados.

Los parámetros a identificar son:

- **Valor de los activos**. Tiene como objetivo fijar una valoración económica a cada uno de los activos del alcance del análisis. Para poder hacerlo hay que tener en consideración:

    - El valor de reposición. Cuanto le cuesta a la organización reponer un activo en caso de pérdida o inutilidad.

    - El valor de configuración. Corresponde al tiempo que pasa desde que se adquiere un nuevo activo hasta que está en las mismas condiciones de uso que el anterior.

- El valor de uso. Hace referencia a la pérdida que sufre la empresa durante el tiempo que no puede utilizar el activo.

Para realizar la valoración de activos se usará la siguiente tabla:

Valor	ID	Rango	Valor estimado
Muy alto	MA	Valor > 100.000 €	200.000 €
Alto	A	50.000 € < valor > 100.000 €	75.000 €
Medio	M	10.000 € < valor > 50.000 €	30.000 €
Bajo	B	1.000 € < valor > 10.000 €	5.000 €
Muy bajo	MB	< 1000 €	1.000 €

- **Vulnerabilidad**. En MAGERIT las vulnerabilidades se interpretan como la frecuencia de ocurrencia de una amenaza. Para realizar la valoración es necesario establecer una escala de valores y traducirla a números, que se obtienen a partir de una estimación anual.

Vulnerabilidad = frecuencia estimada / días del año

Vulnerabilidad	ID	Rango	Valor
Frecuencia muy alta	FMA	1 vez al día	100
Frecuencia alta	FA	1 vez al mes	10
Frecuencia media	FM	1 vez al año	1
Frecuencia baja	FB	1 vez cada varios años	0,1
Frecuencia muy baja	FMB	1 vez cada varios siglos	0,01

- **Impacto**. El método entiende por impacto a la medida del porcentaje del valor del activo que se pierde en caso de que se produzca una incidencia sobre este activo. Los niveles de impacto y los porcentajes asociados para la empresa son los siguientes:

Impacto	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

- **Efectividad del control de seguridad**. Éste parámetro indica que porcentaje del riesgo se reduce por la aplicación de una medida de seguridad. Bien porque se disminuye la frecuencia de ocurrencia (vulnerabilidad) o por el impacto que provoca el riesgo. La clasificación queda de la siguiente forma:

Efectividad sobre el impacto / vulnerabilidad	Valor
Muy alta	95%
Alta	75%
Media	50%
Baja	30%
Muy baja	10%

Según estos valores la organización espera reducir la vulnerabilidad o el impacto un 95% aplicando la mejor medida de seguridad para un determinado riesgo.

3.3 Fase 3. Análisis de activos

Esta etapa tiene como objetivo identificar los activos que tiene la organización y que se encuentran dentro del alcance del análisis. Deben seleccionarse aquellos que supongan un necesidad para la actividad del negocio. Se consideran como activos los siguientes puntos:

- **Activos físicos**. Engloba a todo tipo de hardware que se utilice en la organización: ordenadores, servidores, portátiles, teléfonos móviles, impresoras, routers, etc.

- **Activos lógicos**. Entran en esta categoría todos los elementos de tipo software como sistemas operativos, aplicaciones, scripts, etc.

- **Activos de personal**. Son las personas que tienen asignado un perfil o rol dentro de la empresa y que desempeñan una función, por ejemplo, el

responsable de recursos humanos, administrador de sistemas, desarrollador web, etc.

- **Activos de entorno e infraestructura**. Abarca todos los componentes que son necesarios para que el resto de activos funcione correctamente: sistemas de climatización, generadores, armarios, fuentes de alimentación, cableados, etc.

- **Activos intangibles**. Se refiere a aspectos como la imagen corporativa, credibilidad, confianza de los clientes y en general aquellos activo que no son monetarios ni tienen presencia física, pero que aportan valor a la entidad.

3.4 Fase 4. Análisis de amenazas

Las amenazas son escenarios que ocurren y que pueden afectar a los activos de la empresa, causándoles cierto grado de daño pudiendo llegar a inutilizarlos.

El método MAGERIT en su *Libro II – Catálogo de Elementos*[9]*, capítulo 5* clasifica las amenazas en cuatro grupos:

- **Desastres naturales [N]**. Son los accidentes que pueden ocurrir sin intervención del ser humano:

  - [N.1] Fuego.
  - [N.2] Daños por agua.
  - [N.*] Desastres naturales.

- **De origen industrial [I]**. Pueden ocurrir de forma accidental o deliberada como escapes, fugas, contaminación, explosiones, etc.

  - [I.1] Fuego.
  - [I.2] Daños por agua.

- [I.*] Desastres industriales.
- [I.3] Contaminación mecánica.
- [I.4] Contaminación electromagnética.
- [I.5] Avería de origen físico o lógico.
- [I.6] Corte de suministro eléctrico.
- [I.7] Condiciones inadecuadas de temperatura o humedad.
- [I.8] Fallo de servicios de comunicaciones.
- [I.9] Interrupción de otros servicios y suministros esenciales.
- [I.10] Degradación de los soportes de almacenamiento de información.
- [I.11] Emanaciones electromagnéticas.

- **Errores y fallos no intencionados [E]**. Los que se generan por errores o fallos no intencionales causados por las personas en los procesos de diseño o implementación de los productos.

  - [E.1] Errores de los usuarios.
  - [E.2] Errores del administrador.
  - [E.3] Errores de monitorización (log).
  - [E.4] Errores de configuración.
  - [E.7] Deficiencias en la organización.
  - [E.8] Difusión de software dañino.
  - [E.9] Errores de [re-]encaminamiento.
  - [E.10] Errores de secuencia.
  - [E.15] Alteración accidental de la información.
  - [E.18] Destrucción de información.
  - [E.19] Fugas de información.
  - [E.20] Vulnerabilidades de los programas.
  - [E.21] Errores de mantenimiento / actualización de programas.
  - [E.23] Errores de mantenimiento / actualización de equipos.
  - [E.24] Caída del sistema por agotamiento de recursos.

- [E.25] Pérdida de equipos.
- [E.28] Indisponibilidad del personal.

- **Ataques intencionados [A]**. Fallos deliberados causados por las personas. Las personas con acceso a los sistemas de información pueden ser causa de problemas intencionados para obtener un bien indebidamente, o bien, con la intención de generar daños y perjuicios.

  - [A.3] Manipulación de los registros de actividad (log).
  - [A.4] Manipulación de la configuración.
  - [A.5] Suplantación de la identidad del usuario.
  - [A.6] Abuso de privilegios de acceso.
  - [A.7] Uso no previsto.
  - [A.8] Difusión de software dañino.
  - [A.9] [Re-]encaminamiento de mensajes.
  - [A.10] Alteración de secuencia.
  - [A.11] Acceso no autorizado.
  - [A.12] Análisis de tráfico.
  - [A.13] Repudio.
  - [A.14] Interceptación de información (escucha).
  - [A.15] Modificación deliberada de la información.
  - [A.18] Destrucción de información.
  - [A.19] Divulgación de información.
  - [A.22] Manipulación de programas.
  - [A.23] Manipulación de los equipos.
  - [A.24] Denegación de servicio.
  - [A.25] Robo.
  - [A.26] Ataque destructivo.
  - [A.27] Ocupación enemiga.
  - [A.28] Indisponibilidad del personal.
  - [A.29] Extorsión.

- [A.30] Ingeniería social (picaresca).

3.5 Fase 5. Establecimiento de vulnerabilidades

La metodología MAGERIT no requiere la definición de una lista de las vulnerabilidades, pero sí hay que tenerlas en cuenta para estimar la frecuencia de ocurrencia de una determinada amenaza sobre un activo.

3.6 Fase 6. Valoración del impacto

Cuando una amenaza aprovecha una vulnerabilidad determinada en un activo provoca, como consecuencia, un impacto sobre él. Para el análisis del impacto hay que tener en consideración los aspectos siguientes:

- El resultado de la materialización de una amenaza sobre un activo.
- El efecto en cadena o daño colateral que puede provocar el impacto en un activo al conjunto de activos relacionados.
- El valor económico representativo de las pérdidas producidas en cada activo.
- Las pérdidas cuantitativas o cualitativas.

Conociendo el valor de los activos en sus distintas dimensiones y la degradación que causan las amenazas, es posible calcular el impacto potencial que estas tendrían sobre el sistema.

Impacto potencial = Valor activo x Porcentaje de impacto

3.7 Fase 7. Análisis de riesgos intrínsecos

Con los elementos definidos hasta ahora es posible calcular el riesgo intrínseco, que para MAGERIT, representa la situación actual con la que se encuentra la organización teniendo en cuenta las medidas de seguridad implantadas. El análisis se realiza mediante la siguiente fórmula:

Riesgo intrínseco = Impacto potencial x Vulnerabilidad

3.8 Fase 8. Influencia de los controles de seguridad

En esta fase se clasifican los tipos de controles de seguridad que se aplicarán más adelante en la gestión de riesgos:

- Preventiva. Son aquellas que reducen la frecuencia de ocurrencia y se puede expresar con la fórmula:

  Nueva vulnerabilidad = Vulnerabilidad x Porcentaje de disminución de vulnerabilidad

- Correctiva. Medidas que reducen el impacto de las amenazas.

  Nuevo impacto = Impacto x Porcentaje de disminución del impacto

3.9 Fase 9. Análisis de riesgos efectivos

Con los controles de seguridad seleccionados en el paso anterior, se procede a realizar un estudio de como se han reducido los riesgos después de aplicar dichas medidas a cada una de las amenazas detectadas. Para ellos se aplica el siguiente cálculo:

Riesgo Efectivo = Valor efectivo × Nueva vulnerabilidad × Nuevo impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución del impacto) = Riesgo intrínseco ×

Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución del impacto

3.10 Fase 10. Gestión de riesgos

La última etapa de la metodología MAGERIT consiste en seleccionar la mejor solución de seguridad de la lista de controles, que permitan reducir los riesgos de la organización. Para ello la entidad realizará esta tarea siguiendo un plan de acción que tenga en cuenta la siguiente información:

- Establecer prioridades, de forma que los riesgos que primero se reduzcan sean los más críticos para la empresa.

- Analizar la relación coste-beneficio que conlleva implantar cada medida de seguridad.

- A partir del análisis coste-beneficio, seleccionar los controles de seguridad que la organización ha de implantar para situar los riesgos por debajo del umbral establecido.

- Asignar los responsables de la organización que ejecutarán la implantación de los controles seleccionados.

- Por último proceder a la implantación de los controles de seguridad, ya sean técnicos, organizativos o procedimentales.

Anexo VIII. Declaración de Aplicabilidad

DECLARACIÓN DE APLICABILIDAD

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	17/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Índice

1. Objetivo

Identificar los controles necesarios para gestionar los riesgos que afectan a la Seguridad de la Información que han sido identificados y valorados en TurisTech Balear SL, indicando si resultan de aplicación o no en la empresa.

2. Alcance

Este documento hace referencia al estándar ISO/IEC 27001, en concreto a la sección 6.1.3, apartado d) donde se fija como requisito su elaboración y al anexo A de dicha norma. Su alcance afecta a:

- Los sistemas y equipos ubicados en la sede de TurisTech Balear SL.
- Las zonas y equipos donde se realiza el teletrabajo.
- Los servidores ubicados en los sistemas Cloud contratados.
- Todos los empleados de las distintas áreas de la empresa.

El documento va dirigido a la alta dirección de la organización pues es su deber conocer y aprobar el documento.

3. Declaración de Aplicabilidad

La siguiente tabla muestra los controles que son aplicables y los que no, indicando, para estos últimos, el motivo de su exclusión.

Control ISO/IEC 27002:2013	Aplica	Justificación
5 Políticas de seguridad de la información		
5.1 Directrices de gestión de la seguridad de la información		
5.1.1 Políticas para la seguridad de la información	Sí	Necesario para la gestión de seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información	Sí	Necesario para la gestión de seguridad de la información
6 Organización de la seguridad de la información		
6.1 Organización interna.		

6.1.1 Roles y responsabilidades en seguridad de la información	Sí	Requisito de la Política de Seguridad
6.1.2 Segregación de tareas	Sí	Requerimiento del negocio
6.1.3 Contacto con las autoridades	Sí	Requisito de la Política de Seguridad
6.1.4 Contacto con grupos de interés especial	Sí	Mejorar la gestión de incidencias de seguridad
6.1.5 Seguridad de la información en la gestión de proyectos	Sí	Requerimiento del negocio
6.2 Los dispositivos móviles y el teletrabajo		
6.2.1 Política de dispositivos móviles	Sí	Necesario para la gestión de seguridad de la información
6.2.2 Teletrabajo	Sí	Requisito de la Política de Seguridad
7 Seguridad relativa a los recursos humanos		
7.1 Antes del empleo		
7.1.1 Investigación de antecedentes	Sí	Requerimiento del negocio
7.1.2 Términos y condiciones del empleo	Sí	Requerimiento del negocio
7.2 Durante el empleo		
7.2.1 Responsabilidades de gestión	Sí	Requisito de la Política de Seguridad
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Sí	Requisito de la Política de Seguridad
7.2.3 Proceso disciplinario	Sí	Requisito de la Política de Seguridad
7.3 Finalización del empleo o cambio en el puesto de trabajo		
7.3.1 Responsabilidades ante la finalización o cambio	Sí	Requerimiento del negocio
8 Gestión de activos		
8.1 Responsabilidad sobre los activos		
8.1.1 Inventario de activos	Sí	Requerido para el análisis de riesgos
8.1.2 Propiedad de los activos	Sí	Requerido para el análisis de riesgos
8.1.3 Uso aceptable de los activos	Sí	Requisito de la Política de Seguridad
8.1.4 Devolución de activos	Sí	Requerimiento del negocio
8.2 Clasificación de la información		
8.2.1 Clasificación de la información	Sí	Requerimiento del negocio
8.2.2 Etiquetado de la información	Sí	Requerimiento del negocio
8.2.3 Manipulado de la información	Sí	Requerimiento del negocio
8.3 Manipulación de los soportes		
8.3.1 Gestión de soportes extraíbles	Sí	Requerimiento del negocio
8.3.2 Eliminación de soportes	Sí	Requerimiento del negocio
8.3.3 Soportes físicos en tránsito	Sí	Requerimiento del negocio

9 Control de acceso		
9.1 Requisitos de negocio para el control de acceso		
9.1.1 Política de control de acceso	Sí	Requisito de la Política de Seguridad
9.1.2 Acceso a las redes y a los servicios de red	Sí	Requisito de la Política de Seguridad
9.2 Gestión de acceso de usuario		
9.2.1 Registro y baja de usuario	Sí	Requisito de la Política de Seguridad
9.2.2 Provisión de acceso de usuario	Sí	Requisito de la Política de Seguridad
9.2.3 Gestión de privilegios de acceso	Sí	Requisito de la Política de Seguridad
9.2.4 Gestión de la información secreta de autenticación de usuarios	Sí	Requisito de la Política de Seguridad
9.2.5 Revisión de los derechos de acceso de usuario	Sí	Requisito de la Política de Seguridad
9.2.6 Retirada o reasignación de los derechos de acceso	Sí	Requisito de la Política de Seguridad
9.3 Responsabilidades del usuario		
9.3.1 Uso de la información secreta de autenticación	Sí	Requisito de la Política de Seguridad
9.4 Control de acceso a sistemas y aplicaciones		
9.4.1 Restricción del acceso a la información	Sí	Requisito de la Política de Seguridad
9.4.2 Procedimientos seguros de inicio de sesión	Sí	Requisito de la Política de Seguridad
9.4.3 Sistema de gestión de contraseñas	Sí	Requisito de la Política de Seguridad
9.4.4 Uso de utilidades con privilegios de sistemas	Sí	Requisito de la Política de Seguridad
9.4.5 Control de acceso al código fuente de los programas	Sí	Requisito de la Política de Seguridad
10 Criptografia		
10.1 Controles criptográficos		
10.1.1 Política de uso de los controles criptográficos	Sí	Requerimiento del negocio
10.1.2 Gestión de claves	Sí	Requerimiento del negocio
11 Seguridad física y del entorno		
11.1 Áreas seguras		
11.1.1 Perímetro de seguridad física	Sí	Requerimiento del negocio
11.1.2 Controles físicos de entrada	Sí	Requerimiento del negocio
11.1.3 Seguridad de oficinas, despachos y recursos	Sí	Requerimiento del negocio
11.1.4 Protección contra las amenazas externas y ambientales	Sí	Requerimiento del negocio

11.1.5 El trabajo en áreas seguras	No	La empresa no cuenta con áreas seguras
11.1.6 Áreas de carga y descarga	No	La empresa no cuenta con zonas de carga y descarga
11.2 Seguridad de los equipos		
11.2.1 Emplazamiento y protección de equipos	Sí	Requisito de la Política de Seguridad
11.2.2 Instalaciones de suministro	Sí	Requerimiento del negocio
11.2.3 Seguridad del cableado	Sí	Requerimiento del negocio
11.2.4 Mantenimiento de los equipos	Sí	Requisito de la Política de Seguridad
11.2.5 Retirada de materiales propiedad de la empresa	Sí	Requisito de la Política de Seguridad
11.2.6 Seguridad de los equipos fuera de las instalaciones	Sí	Requisito de la Política de Seguridad
11.2.7 Reutilización o eliminación segura de equipos	Sí	Requisito de la Política de Seguridad
11.2.8 Equipo de usuario desatendido	Sí	Requisito de la Política de Seguridad
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Sí	Requerimiento del negocio
12 Seguridad de las operaciones		
12.1 Procedimientos y responsabilidades operacionales		
12.1.1 Documentación de procedimientos de operación	Sí	Requerimiento del negocio
12.1.2 Gestión de cambios	Sí	Requerido para el análisis de riesgos y las auditorias
12.1.3 Gestión de capacidades	Sí	Requerimiento del negocio
12.1.4 Separación de los recursos de desarrollo, prueba y operación	Sí	Requisito de la Política de Seguridad
A.12.2 Protección contra el software malicioso (malware)		
12.2.1 Controles contra el código malicioso	Sí	Necesario para la gestión de seguridad de la información
12.3 Copias de seguridad		
12.3.1 Copias de seguridad de la información	Sí	Requisito de la Política de Seguridad
12.4 Registros y supervisión		
12.4.1 Registro de eventos	Sí	Necesario para la gestión de los incidentes de seguridad de la información y las auditorías
12.4.2 Protección de la información de registro	Sí	Necesario para evitar manipulaciones de los registros o su información
12.4.3 Registros de administración y operación	Sí	Necesario para la gestión de los incidentes de seguridad de la información y las auditorías

12.4.4 Sincronización del reloj	Sí	Necesario para la gestión de los incidentes de seguridad de la información y las auditorías
12.5 Control del software en explotación		
12.5.1 Instalación del software en explotación	Sí	Requisito de la Política de Seguridad
12.6 Gestión de la vulnerabilidad técnica		
12.6.1 Gestión de las vulnerabilidades técnicas	Sí	Requisito de la Política de Seguridad
12.6.2 Restricción en la instalación de software	Sí	Requisito de la Política de Seguridad
12.7 Consideraciones sobre la auditoria de sistemas de información		
12.7.1 Controles de auditoria de sistemas de información	Sí	Requerido por el Procedimiento de Auditorias
13 Seguridad de las comunicaciones		
13.1 Gestión de la seguridad de las redes		
13.1.1 Controles de red	Sí	Requisito de la Política de Seguridad
13.1.2 Seguridad de los servicios de red	Sí	Requisito de la Política de Seguridad
13.1.3 Segregación en redes	Sí	Requisito de la Política de Seguridad
13.2 Intercambio de información		
13.2.1 Políticas y procedimientos de intercambio de información	Sí	Requerimiento del negocio
13.2.2 Acuerdos de intercambio de información	Sí	Requerimiento del negocio
13.2.3 Mensajería electrónica	Sí	Requerimiento del negocio
13.2.4 Acuerdos de confidencialidad o no revelación	Sí	Requerimiento del negocio
14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
14.1 Requisitos de seguridad en los sistemas de información		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Sí	Requerimiento del negocio
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	Sí	Requerimiento del negocio
14.1.3 Protección de las transacciones de servicios de aplicaciones	Sí	Requerimiento del negocio
14.2 Seguridad en el desarrollo y en los procesos de soporte		
14.2.1 Política de desarrollo seguro	Sí	Requisito de la Política de Seguridad
14.2.2 Procedimiento de control de cambios en sistemas	Sí	Requisito de la Política de Seguridad
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Sí	Requisito de la Política de Seguridad
14.2.4 Restricciones a los cambios en los paquetes de software	Sí	Requisito de la Política de Seguridad

14.2.5 Principios de ingeniería de sistemas seguros	Sí	Requerimiento del negocio
14.2.6 Entorno de desarrollo seguro	Sí	Requerimiento del negocio
14.2.7 Externalización del desarrollo de software	Sí	Requerimiento del negocio
14.2.8 Pruebas funcionales de seguridad de sistemas	Sí	Requerimiento del negocio
14.2.9 Pruebas de aceptación de sistemas	Sí	Requerimiento del negocio
14.3 Datos de prueba		
14.3.1 Protección de los datos de prueba	Sí	Requerimiento del negocio
15 Relación con proveedores		
15.1 Seguridad en las relaciones con proveedores		
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Sí	Requisito de la Política de Seguridad
15.1.2 Requisitos de seguridad en contratos con terceros	Sí	Requisito de la Política de Seguridad
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Sí	Requerimiento del negocio
15.2 Gestión de la provisión de servicios del proveedor		
15.2.1 Control y revisión de la provisión de servicios del proveedor	Sí	Requerimiento del negocio
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Sí	Requerido para el análisis de riesgos
16 Gestión de incidentes de seguridad de la información		
16.1 Gestión de incidentes de seguridad de la información y mejoras		
16.1.1 Responsabilidades y procedimientos	Sí	Requisito de la Política de Seguridad
16.1.2 Notificación de los eventos de seguridad de la información	Sí	Requisito de la Política de Seguridad
16.1.3 Notificación de puntos débiles de la seguridad	Sí	Requisito de la Política de Seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Sí	Requisito de la Política de Seguridad
16.1.5 Respuesta a incidentes de seguridad de la información	Sí	Requisito de la Política de Seguridad
16.1.6 Aprendizaje de los incidentes de seguridad de la información	Sí	Requisito de la Política de Seguridad
16.1.7 Recopilación de evidencias	Sí	Requisito de la Política de Seguridad
17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio		
17.1 Continuidad de la seguridad de la información		
17.1.1 Planificación de la continuidad de la seguridad de la información	Sí	Requerimiento del negocio
17.1.2 Implementar la continuidad de la seguridad de la información	Sí	Requerimiento del negocio
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Sí	Requerimiento del negocio

17.2 Redundancias		
17.2.1 Disponibilidad de los recursos de tratamiento de la información	Sí	Requerimiento del negocio
18 Cumplimiento		
18.1 Cumplimiento de los requisitos legales y contractuales		
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Sí	Requerimiento del negocio y las leyes vigentes
18.1.2 Derechos de propiedad intelectual (DPI)	Sí	Requerimiento del negocio y las leyes vigentes
18.1.3 Protección de los registros de la organización	Sí	Requerimiento del negocio y las leyes vigentes
18.1.4 Protección y privacidad de la información de carácter personal	Sí	Requerimiento del negocio y las leyes vigentes
18.1.5 Regulación de los controles criptográficos	Sí	Requerimiento del negocio y las leyes vigentes
18.2 Revisiones de la seguridad de la información		
18.2.1 Revisión independiente de la seguridad de la información	Sí	Requerimiento del negocio
18.2.2 Cumplimiento de las políticas y normas de seguridad	Sí	Requisito de la Política de Seguridad
18.2.3 Comprobación del cumplimiento técnico	Sí	Requisito de la Política de Seguridad

Anexo IX. Inventario de activos

INVENTARIO DE ACTIVOS

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	27/10/2019	Pendiente de revisión	Elaboración de la versión inicial

INVENTARIO DE ACTIVOS		
[L] Instalaciones		**Cantidad**
L.1	Oficina	1
L.2	Puestos teletrabajo	4
[HW] Hardware		**Cantidad**
HW.1	Portátiles	5
HW.2	Routers	5
HW.3	Impresoras	1
HW.4	Ordenadores de mesa	1
HW.5	Servidores Cloud explotación	2
HW.6	Servidores Cloud desarrollo	1
HW.7	Servidores Cloud gestión	1
[SW] Aplicación (software)		**Cantidad**
SW.1	Sistema operativo Linux Mint	6
SW.2	Sistema operativo Debian	4
SW.3	PostgreSQL	6
SW.4	Apache Tomcat	6
SW.5	Apache Camel	5
SW.6	Apache ActiveMQ	5
SW.7	Java	6
SW.8	Redmine	1
SW.9	LibreOffice	5
SW.10	Sistema de backup	4
SW.11	BaseX	5
SW.12	Eclipse (entorno de desarrollo integrado)	3
SW.13	Icinga (monitoreo de sistemas)	1
SW.14	Sistema MBE	3
SW.15	Sistema MBE-CM Integraciones	3
[D] Datos / Información		**Cantidad**
D.1	Copias de seguridad	4
D.2	Registros de actividad	4
D.3	Documentación departamental	1
D.4	Código fuente MBE, MBE-CM	1
D.5	Archivos de configuración MBE, MBE-CM	1
D.6	Bases de datos MBE, MBE-CM	1
[COM] Redes		**Cantidad**
COM.1	ADSL (voz y datos)	5
COM.2	Red inalámbrica WIFI	5
COM.3	Móviles	2
[S] Servicios		**Cantidad**

S.1	Correo electrónico corporativo	1
S.2	SSH protocolo para acceso a servidores	1
S.3	Git	1
S.4	Slack	1
[AUX] Equipamiento auxiliar		**Cantidad**
AUX.1	Sistema eléctrico	1
AUX.2	Sistema contra incendios	1
[P] Personal		**Cantidad**
P.1	Administradores de sistemas	1
P.2	Desarrolladores	3
P.3	Contratistas especializados	1
P.4	Directivos	2
P.5	Comerciales	1
P.6	Administrativos	1

Anexo X. Valoración económica de activos

VALORACIÓN ECONÓMICA DE ACTIVOS

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	28/10/2019	Pendiente de revisión	Elaboración de la versión inicial

Las siguientes tablas muestran el valor de cada activo según el ámbito al que pertenece, siguiendo los criterios establecidos de valoración indicados en el apartado *4.3 Valoración de activos* de la memoria.

VALORACIÓN INSTALACIONES [L]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
L.1	Oficina	1	Bajo	5.000
L.2	Puestos teletrabajo	4	Bajo	5.000
				10.000

Tanto la oficina como los puestos de trabajo en remoto son espacios sencillos y con pocos elementos, que básicamente son los que ha tenido que incorporar la entidad, por ejemplo, el mobiliario o rótulos. La oficina no dispone de CPD, ya que los servidores se encuentran alojados en un servicio Cloud y los puestos de teletrabajo sólo requieren un escritorio y una silla. El portátil, la línea ADSL y el router se valoran en el apartado Hardware [HW] y Red [COM]

VALORACIÓN HARDWARE [HW]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
HW.1	Portátiles	5	Bajo	5.000
HW.2	Routers	5	Muy bajo	1.000
HW.3	Impresoras	1	Muy bajo	1.000
HW.4	Ordenadores de mesa	1	Bajo	5.000
HW.5	Servidores Cloud explotación	2	Muy alto	200.000
HW.6	Servidores Cloud desarrollo	1	Muy alto	200.000
HW.7	Servidores Cloud gestión	1	Muy alto	200.000
				612.000

Como se ha comentado en capítulos anteriores, los servidores son contratados a una empresa externa en modalidad IaaS.

VALORACIÓN SOFTWARE [SW]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
SW.1	Sistema operativo Linux Mint	6	Muy bajo	1.000
SW.2	Sistema operativo Debian	4	Medio	30.000
SW.3	PostgreSQL	6	Medio	30.000
SW.4	Apache Tomcat	6	Medio	30.000
SW.5	Apache Camel	5	Medio	30.000
SW.6	Apache ActiveMQ	5	Medio	30.000
SW.7	Java	6	Medio	30.000
SW.8	Redmine	1	Medio	30.000
SW.9	LibreOffice	5	Muy bajo	1.000
SW.10	Sistema de backup	4	Muy alto	200.000
SW.11	BaseX	5	Medio	30.000
SW.12	Eclipse (entorno de desarrollo integrado)	3	Muy bajo	1.000
SW.13	Icinga (monitoreo de sistemas)	1	Medio	30.000
SW.14	Sistema MBE	3	Medio	30.000
SW.15	Sistema MBE-CM Integraciones	3	Medio	30.000
				533.000

El software que actualmente utiliza la empresa es Open Source y/o Software Libre sin costes de licencias, o bien, se ha desarrollado en la propia empresa, de aquí que el coste de reposición sea 0.

VALORACIÓN DATOS [D]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
D.1	Copias de seguridad	4	Muy bajo	1.000
D.2	Registros de actividad	4	Muy bajo	1.000
D.3	Documentación departamental	1	Alto	75.000
D.4	Código fuente MBE, MBE-CM	1	Muy alto	200.000
D.6	Archivos de configuración MBE, MBE-CM	1	Muy alto	200.000
D.7	Bases de datos MBE, MBE-CM	1	Muy alto	200.000
				677.000

Para la valoración del código fuente, las bases de datos, los archivos de configuración y la documentación departamental, se ha realizado una estimación de horas invertidas en su desarrollo y un precio por hora.

VALORACIÓN REDES [COM]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
COM.1	ADSL (voz y datos)	5	Muy bajo	1.000
COM.2	Red inalámbrica WIFI	5	Muy bajo	1.000
COM.3	Móviles	2	Muy bajo	1.000
				3.000

VALORACIÓN SERVICIOS [S]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
S.1	Correo electrónico corporativo	1	Muy bajo	1.000
S.3	SSH protocolo para acceso a servidores	1	Muy bajo	1.000
S.4	Git	1	Muy bajo	1.000
S.5	Slack	1	Muy bajo	1.000
				4.000

VALORACIÓN EQUIPAMIENTO AUXILIAR [AUX]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimad €**
AUX.1	Sistema eléctrico	1	Bajo	5.000
AUX.2	Sistema contra incendios	1	Bajo	5.000
				10.000

Se valora el sistema eléctrico y contra incendios de la oficina, quedando excluidos el de los puestos de teletrabajo pues no son parte de la organización.

VALORACIÓN PERSONAL [P]				
ID	**Activo**	**Cantidad**	**Valor**	**Valor estimado €**
P.1	Administradores de sistemas	1	Medio	30.000
P.2	Desarrolladores	3	Alto	75.000
P.3	Contratistas especializados	1	Medio	30.000
P.4	Directivos	2	Alto	75.000
P.5	Comerciales	1	Medio	30.000
P.6	Administrativos	1	Medio	30.000
				270.000

En cuanto al personal su valoración se basa en los factores siguientes:

- Cantidad media de entrevistas. Se estima unas 10 entrevistas hasta que se encuentra el perfil requerido.

- Coste hora entrevista. 50 €.

- Coste formación. Se calculan unas 4 horas durante 20 días a un coste de 50 € la hora.

Anexo XI. Resumen importancia y criticidad de los activos

RESUMEN IMPORTANCIA Y CRITICIDAD DE LOS ACTIVOS

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	30/10/2019	Pendiente de revisión	Elaboración de la versión inicial

			ASPECTOS CRÍTICOS				
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones	Oficina	Baja	1	5	1	1	1
[L] Instalaciones	Puestos teletrabajo	Baja	1	5	1	1	1
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[HW] Hardware	Portátiles	Media	4	6	4	4	4
[HW] Hardware	Routers	Media	7	8	7	8	3
[HW] Hardware	Impresoras	Irrelevante	0	1	1	1	0
[HW] Hardware	Ordenadores de mesa	Baja	2	6	2	2	2
[HW] Hardware	Servidores Cloud explotación	Muy alta	8	10	10	10	8
[HW] Hardware	Servidores Cloud desarrollo	Muy alta	8	10	10	10	8
[HW] Hardware	Servidores Cloud gestión	Muy alta	8	10	10	10	8
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[SW] Aplicación	Sistema operativo Linux Mint	Baja	3	1	1	1	1
[SW] Aplicación	Sistema operativo Debian	Alta	6	6	7	8	7
[SW] Aplicación	PostgreSQL	Alta	6	10	10	10	6
[SW] Aplicación	Apache Tomcat	Alta	6	6	6	10	7
[SW] Aplicación	Apache Camel	Media	4	4	4	5	3
[SW] Aplicación	Apache ActiveMQ	Alta	6	8	6	10	4
[SW] Aplicación	Java	Alta	6	8	8	5	6
[SW] Aplicación	Redmine	Media	4	8	6	8	5
[SW] Aplicación	LibreOffice	Irrelevante	0	0	0	1	0
[SW] Aplicación	Sistema de backup	Media	4	8	8	8	4
[SW] Aplicación	BaseX	Alta	6	10	10	10	6
[SW] Aplicación	Eclipse (entorno de desarrollo integrado)	Irrelevante	0	0	0	1	0
[SW] Aplicación	Icinga (monitoreo de sistemas)	Media	6	3	3	8	8
[SW] Aplicación	Sistema MBE	Muy alta	9	10	10	10	8
[SW] Aplicación	Sistema MBE-CM Integraciones	Muy alta	9	10	10	10	8
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[D] Datos	Copias de seguridad	Alta	2	10	10	10	4
[D] Datos	Registros de actividad	Media	9	4	4	4	9
[D] Datos	Documentación departamental	Alta	2	10	10	10	5
[D] Datos	Código fuente MBE, MBE-CM	Muy alta	8	10	10	10	8
[D] Datos	Archivos de configuración MBE, MBE-CM	Alta	5	7	9	10	5
[D] Datos	Bases de datos MBE, MBE-CM	Muy alta	8	10	10	10	8
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[COM] Redes	ADSL (voz y datos)	Media	2	4	4	6	4
[COM] Redes	Red inalámbrica WIFI	Media	2	6	4	4	4

[COM] Redes	Móviles	Baja	0	4	1	1	1
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[S] Servicios	Correo electrónico corporativo	Media	5	8	1	3	3
[S] Servicios	SSH protocolo para acceso a servidores	Media	9	8	8	4	2
[S] Servicios	Git	Alta	7	8	8	8	7
[S] Servicios	Slack	Baja	4	3	0	3	0
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[AUX] Equipamiento auxiliar	Sistema eléctrico	Media	0	0	8	8	0
[AUX] Equipamiento auxiliar	Sistema contra incendios	Media	0	0	8	8	0
ÁMBITO	**ACTIVO**	**VALOR**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[P] Personal	Administradores de sistemas	Alta	7	8	8	8	5
[P] Personal	Desarrolladores	Alta	7	8	8	8	5
[P] Personal	Contratistas especializados	Media	7	7	8	8	5
[P] Personal	Directivos	Muy alta	9	9	9	9	9
[P] Personal	Comerciales	Alta	6	8	8	8	5
[P] Personal	Administrativos	Media	6	8	6	6	5

Anexo XII. Análisis de amenazas

ANÁLISIS DE AMENAZAS

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	03/11/2019	Pendiente de revisión	Elaboración de la versión inicial

De las amenazas descritas en el apartado 3.4 del Anexo VII, se identifican las más significativas para la organización.

AMENAZAS INSTALACIONES [L]						
ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
L.1 Oficina					20%	
L.2 Puestos teletrabajo					20%	
[N.1] Fuego (natural accidental)	0,01				20%	
[N.2] Daños por agua (natural accidental)	0,01				20%	
[N.*] Desastres naturales (rayo, tormenta eléctrica, terremoto)	0,1				5%	
[I.1] Fuego (industrial accidental o provocado)	0,01				20%	
[I.2] Daños por agua (industrial accidental o provocado)	0,1				20%	
[A.18] Destrucción de información	0,1				20%	

AMENAZAS HARDWARE [HW]						
ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
HW.1 Portátiles			100%	100%	100%	
HW.2 Routers			100%	100%	100%	
HW.3 Impresoras			100%	100%	100%	
HW.4 Ordenadores de mesa			100%	100%	100%	
HW.5 Servidores Cloud explotación			100%	100%	100%	
HW.6 Servidores Cloud desarrollo			100%	100%	100%	
HW.7 Servidores Cloud gestión			100%	100%	100%	
[N.1] Fuego (accidental natural)	0,01				100%	
[N.2] Daños por agua (accidental natural)	0,01				100%	
[N.*] Desastres naturales (rayo, tormenta eléctrica, terremoto)	0,1				75%	
[I.1] Fuego (industrial accidental o provocado)	0,01				100%	
[I.2] Daños por agua (industrial accidental o provocado)	0,1				100%	
[I.3] Contaminación mecánica (polvo, suciedad)	0,01				20%	
[I.5] Avería de origen físico o lógico	0,1				50%	
[I.6] Corte del suministro eléctrico	1				100%	
[E.2] Errores del administrador	1		50%	50%	50%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1				50%	

[E.24] Caída del sistema por agotamiento de recursos	1				50%	
[E.25] Pérdida de equipos	0,01		20%		20%	
[A.6] Abuso de privilegios de acceso	0,1		100%	100%	100%	
[A.23] Manipulación de los equipos	0,01		50%		100%	
[A.25] Robo	0,1		100%		100%	
[A.26] Ataque destructivo (vandalismo)	0,01				100%	

AMENAZAS APLICACIÓN [SW]						
ACTIVO	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
SW.1 Sistema operativo Linux Mint		100%	100%	100%	100%	
SW.2 Sistema operativo Debian		100%	100%	100%	100%	
SW.3 PostgreSQL		100%	100%	100%	100%	
SW.4 Apache Tomcat		100%	100%	100%	100%	
SW.5 Apache Camel		100%	100%	100%	100%	
SW.6 Apache ActiveMQ		100%	100%	100%	100%	
SW.7 Java		100%	100%	100%	100%	
SW.8 Redmine		100%	100%	100%	100%	
SW.9 LibreOffice		100%	100%	100%	100%	
SW.10 Sistema de backup		100%	100%	100%	100%	
SW.11 BaseX		100%	100%	100%	100%	
SW.12 Eclipse (entorno de desarrollo integrado)		100%	100%	100%	100%	
SW.13 Icinga (monitoreo de sistemas)		100%	100%	100%	100%	
SW.14 Sistema MBE		100%	100%	100%	100%	
SW.15 Sistema MBE-CM Integraciones		100%	100%	100%	100%	
[I.5] Avería de origen físico o lógico	1				50%	
[E.1] Errores de los usuarios	1		20%	20%	20%	
[E.2] Errores del administrador	1		50%	50%	50%	
[E.8] Difusión de software dañino	0,1		50%	50%	50%	
[E.9] Errores de [re-]encaminamiento	0,1		20%			
[E.10] Errores de secuencia	0,01			20%		
[E.15] Alteración accidental de la información	0,1			20%		
[E.18] Destrucción de información	0,1				20%	
[E.19] Fugas de información	0,01		50%			
[E.20] Vulnerabilidad de los programas (software)	0,1		50%	50%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	1			75%	75%	
[A.5] Suplantación de la identidad del	0,01	100%	50%	50%		

usuario						
[A.6] Abuso de privilegios de acceso	0,01		100%	100%	100%	
[A.7] Uso no previsto	0,01		5%	5%	5%	
[A.8] Difusión de software dañino	0,1		100%	100%	100%	
[A.9] [Re-]encaminamiento de mensajes	0,01		50%			
[A.10] Alteración de secuencia	0,01			50%		
[A.11] Acceso no autorizado	0,01		100%	50%		
[A.15] Modificación deliberada de la información	0,01			100%		
[A.18] Destrucción de información	0,01				100%	
[A.19] Divulgación de información	0,01		75%			
[A.22] Manipulación de programas	0,01		50%	50%	50%	

AMENAZAS DATOS [D]						
ACTIVO	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
D.1 Copias de seguridad		100%	100%	100%	100%	100%
D.2 Registros de actividad		100%	100%	100%	100%	100%
D.3 Documentación departamental		100%	100%	100%	100%	100%
D.4 Código fuente MBE, MBE-CM		100%	100%	100%	100%	100%
D.5 Archivos de configuración MBE, MBE-CM		100%	100%	100%	100%	100%
D.6 Bases de datos MBE, MBE-CM		100%	100%	100%	100%	100%
[E.1] Errores de los usuarios	1		20%	20%	20%	
[E.2] Errores del administrador	1		50%	50%	50%	
[E.3] Errores de monitorización (log)	1					20%
[E.4] Errores de configuración	1			20%		
[E.15] Alteración accidental de la información	0,1			20%		
[E.18] Destrucción de información	0,1				20%	
[E.19] Fugas de información	0,01		50%			
[A.3] Manipulación de los registros de actividad (log)	0,01					100%
[A.4] Manipulación de la configuración	0,01		20%	50%	50%	
[A.5] Suplantación de la identidad del usuario	0,01	100%	100%	100%		
[A.6] Abuso de privilegios de acceso	0,01		100%	100%	100%	
[A.11] Acceso no autorizado	0,01		100%	50%		
[A.15] Modificación deliberada de la información	0,01			100%		
[A.18] Destrucción de información	0,01				100%	
[A.19] Divulgación de información	0,01		75%			

AMENAZAS RED [COM]						
ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
COM.1 ADSL (voz y datos)		20%	20%	20%	20%	
COM.2 Red inalámbrica WIFI		20%	20%	20%	20%	
COM.3 Móviles		20%	20%	20%	20%	
[I.8] Fallo de servicios de comunicaciones	1				100%	
[E.2] Errores del administrador	1		20%	20%	20%	
[E.9] Errores de [re-]encaminamiento	0,1		20%			
[E.10] Errores de secuencia	0,01			20%		
[E.15] Alteración accidental de la información	0,1			20%		
[E.18] Destrucción de información	0,1				20%	
[E.19] Fugas de información	0,01		20%			
[E.24] Caída del sistema por agotamiento de recursos	1				20%	
[A.5] Suplantación de la identidad del usuario	0,01	20%	20%	20%		
[A.6] Abuso de privilegios de acceso	0,01		20%	20%	20%	
[A.7] Uso no previsto	0,01		5%	5%	5%	
[A.9] [Re-]encaminamiento de mensajes	0,01		20%			
[A.10] Alteración de secuencia	0,01			20%		
[A.11] Acceso no autorizado	0,01		20%	20%		
[A.12] Análisis de tráfico	0,01		20%			
[A.14] Interceptación de información (escucha)	0,01		20%			
[A.15] Modificación deliberada de la información	0,01			20%		
[A.19] Divulgación de información	0,01		20%			
[A.24] Denegación de servicio	0,1				20%	

AMENAZAS SERVICIOS [S]						
ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
S.1 Correo electrónico corporativo		100%	100%	100%	100%	100%
S.2 SSH protocolo para acceso a servidores		100%	100%	100%	100%	100%
S.3 Git		100%	100%	100%	100%	100%
S.4 Slack		100%	100%	100%	100%	100%
[E.1] Errores de los usuarios	1		20%	20%	20%	
[E.2] Errores del administrador	1		50%	50%	50%	
[E.9] Errores de [re-]encaminamiento	0,1		20%			

[E.10] Errores de secuencia	0,01			20%		
[E.15] Alteración accidental de la información	0,1			20%		
[E.18] Destrucción de información	0,1				20%	
[E.19] Fugas de información	0,01		20%			
[E.24] Caída del sistema por agotamiento de recursos	1				20%	
[A.5] Suplantación de la identidad del usuario	0,01	100%	20%	20%		
[A.6] Abuso de privilegios de acceso	0,01		20%	20%	20%	
[A.7] Uso no previsto	0,01		5%	5%	5%	
[A.9] [Re-]encaminamiento de mensajes	0,01		100%			
[A.10] Alteración de secuencia	0,01			100%		
[A.11] Acceso no autorizado	0,01		100%	20%		
[A.13] Repudio	0,01					100%
[A.15] Modificación deliberada de la información	0,01			100%		
[A.18] Destrucción de información	0,01				100%	
[A.19] Divulgación de información	0,01		100%			
[A.24] Denegación de servicio	0,1				100%	

AMENAZAS EQUIPAMIENTO AUXILIAR [AUX]						
ACTIVO	**FRECUENCIA**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
AUX.1 Sistema eléctrico			0%		5%	
AUX.2 Sistema contra incendios			0%		5%	
[N.1] Fuego (accidental natural)	0,01				5%	
[N.2] Daños por agua (accidental natural)	0,01				5%	
[N.*] Desastres naturales (rayo, terremoto)	0,1				5%	
[I.1] Fuego (industrial accidental o provocado)	0,01				5%	
[I.2] Daños por agua (industrial accidental o provocado)	0,1				5%	
[I.3] Contaminación mecánica (polvo, suciedad)	0,01				5%	
[I.5] Avería de origen físico	0,1				5%	
[I.6] Corte del suministro eléctrico	1				5%	
[I.7] Condiciones de temperatura o humedad	0,1				5%	
[A.23] Manipulación de los equipos	0,01		0%		5%	
[A.26] Ataque destructivo (vandalismo)	0,01				5%	

AMENAZAS PERSONAL [P]						
ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
P.1 Administradores de sistemas			100%	100%	100%	
P.2 Desarrolladores			100%	100%	100%	
P.3 Contratistas especializados			100%	100%	100%	
P.4 Directivos			100%	100%	100%	
P.5 Comerciales			100%	100%	100%	
P.6 Administrativos			100%	100%	100%	
[E.7] Deficiencias en la organización	1				25%	
[E.19] Fugas de información	0,01		100%			
[E.28] Indisponibilidad del personal (ausencia por enfermedad, altercados públicos)	1				10%	
[A.28] Indisponibilidad del personal (deliberado, huelgas, bajas no justificadas, absentismo laboral, ...)	0,1				10%	
[A.29] Extorsión	0,01		100%	100%	100%	
[A.30] Ingeniería social	0,01		100%	100%	100%	

Anexo XIII. Análisis del impacto potencial

ANÁLISIS DEL IMPACTO POTENCIAL

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	04/11/2019	Pendiente de revisión	Elaboración de la versión inicial

[L] Instalaciones															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Oficina	1	5	1	1	1				20		0	0	0	0,2	0
Puestos teletrabajo	1	5	1	1	1				20		0	0	0	0,2	0

[HW] Hardware															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Portátiles	4	6	4	4	4		100	100	100		0	6	4	4	0
Routers	7	8	7	8	3		100	100	100		0	8	7	8	0
Impresoras	0	1	1	1	0		100	100	100		0	1	1	1	0
Ordenadores de mesa	2	6	2	2	2		100	100	100		0	6	2	2	0
Servidores Cloud explotación	8	10	10	10	8		100	100	100		0	10	10	10	0
Servidores Cloud desarrollo	8	10	10	10	8		100	100	100		0	10	10	10	0
Servidores Cloud gestión	8	10	10	10	8		100	100	100		0	10	10	10	0

[SW] Software															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Sistema operativo Linux Mint	3	1	1	1	1	100	100	100	100		3	1	1	1	0
Sistema operativo Debian	6	6	7	8	7	100	100	100	100		6	6	7	8	0
PostgreSQL	6	10	10	10	6	100	100	100	100		6	10	10	10	0
Apache Tomcat	6	6	6	10	7	100	100	100	100		6	6	6	10	0
Apache Camel	4	4	4	5	3	100	100	100	100		4	4	4	5	0
Apache ActiveMQ	6	8	6	10	4	100	100	100	100		6	8	6	10	0
Java	6	8	8	5	6	100	100	100	100		6	8	8	5	0

Redmine	4	8	6	8	5	100	100	100	100		4	8	6	8	0
LibreOffice	0	0	0	1	0	100	100	100	100		0	0	0	1	0
Sistema de backup	4	8	8	8	4	100	100	100	100		4	8	8	8	0
BaseX	6	10	10	10	6	100	100	100	100		6	10	10	10	0
Eclipse (entorno de desarrollo integrado)	0	0	0	1	0	100	100	100	100		0	0	0	1	0
Icinga (monitoreo de sistemas)	6	3	3	8	8	100	100	100	100		6	3	3	8	0
Sistema MBE	9	10	10	10	8	100	100	100	100		9	10	10	10	0
Sistema MBE-CM Integraciones	9	10	10	10	8	100	100	100	100		9	10	10	10	0

[D] Datos															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Copias de seguridad	2	10	10	10	4	100	100	100	100	100	2	10	10	10	4
Registros de actividad	9	4	4	4	9	100	100	100	100	100	9	4	4	4	9
Documentación departamental	2	10	10	10	5	100	100	100	100	100	2	10	10	10	5
Código fuente MBE, MBE-CM	8	10	10	10	8	100	100	100	100	100	8	10	10	10	8
Archivos de configuración MBE, MBE-CM	5	7	9	10	5	100	100	100	100	100	5	7	9	10	5
Bases de datos MBE, MBE-CM	8	10	10	10	8	100	100	100	100	100	8	10	10	10	8

[COM] Red															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
ADSL (voz y datos)	2	4	4	6	4	20	20	20	20		0,4	0,8	0,8	1,2	0
Red inalámbrica WIFI	2	6	4	4	4	20	20	20	20		0,4	1,2	0,8	0,8	0
Móviles	0	4	1	1	1	20	20	20	20		0	0,8	0,2	0,2	0

[S] Servicios															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Correo electrónico corporativo	5	8	1	3	3	100	100	100	100	100	5	8	1	3	3
SSH protocolo para acceso a servidores	9	8	8	4	2	100	100	100	100	100	9	8	8	4	2
Git	7	8	8	8	7	100	100	100	100	100	7	8	8	8	7
Slack	4	3	0	3	0	100	100	100	100	100	4	3	0	3	0

[AUX] Equipamiento auxiliar															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Sistema eléctrico	0	0	8	8	0		0		5		0	0	0	0,4	0
Sistema contra incendios	0	0	8	8	0		0		5		0	0	0	0,4	0

[P] Personal															
ACTIVO	Valor activo					Impacto materialización %					Impacto potencial				
	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Administradores de sistemas	7	8	8	8	5		100	100	100		0	8	8	8	0
Desarrolladores	7	8	8	8	5		100	100	100		0	8	8	8	0
Contratistas especializados	7	7	8	8	5		100	100	100		0	7	8	8	0
Directivos	9	9	9	9	9		100	100	100		0	9	9	9	0
Comerciales	6	8	8	8	5		100	100	100		0	8	8	8	0
Administrativos	6	8	6	6	5		100	100	100		0	8	6	6	0

Anexo XIV. Análisis del riesgo

ANÁLISIS DEL RIESGO

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Comité de Seguridad de la información	06/11/2019	Pendiente de revisión	Elaboración de la versión inicial

[L] Instalaciones											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Oficina	0	0	0	0,2	0	0,1	0	0	0	0,02	0
Puestos teletrabajo	0	0	0	0,2	0	0,1	0	0	0	0,02	0

[HW] Hardware											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Portátiles	0	6	4	4	0	1	0	6	4	4	0
Routers	0	8	7	8	0	1	0	8	7	8	0
Impresoras	0	1	1	1	0	1	0	1	1	1	0
Ordenadores de mesa	0	6	2	2	0	1	0	6	2	2	0
Servidores Cloud explotación	0	10	10	10	0	1	0	10	10	10	0
Servidores Cloud desarrollo	0	10	10	10	0	1	0	10	10	10	0
Servidores Cloud gestión	0	10	10	10	0	1	0	10	10	10	0

[SW] Software											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Sistema operativo Linux Mint	3	1	1	1	0	1	3	1	1	1	0
Sistema operativo Debian	6	6	7	8	0	1	6	6	7	8	0
PostgreSQL	6	10	10	10	0	1	6	10	10	10	0
Apache Tomcat	6	6	6	10	0	1	6	6	6	10	0
Apache Camel	4	4	4	5	0	1	4	4	4	5	0
Apache ActiveMQ	6	8	6	10	0	1	6	8	6	10	0
Java	6	8	8	5	0	1	6	8	8	5	0
Redmine	4	8	6	8	0	1	4	8	6	8	0
LibreOffice	0	0	0	1	0	1	0	0	0	1	0
Sistema de backup	4	8	8	8	0	1	4	8	8	8	0
BaseX	6	10	10	10	0	1	6	10	10	10	0
Eclipse (entorno de desarrollo integrado)	0	0	0	1	0	1	0	0	0	1	0
Icinga (monitoreo de sistemas)	6	3	3	8	0	1	6	3	3	8	0
Sistema MBE	9	10	10	10	0	1	9	10	10	10	0
Sistema MBE-CM Integraciones	9	10	10	10	0	1	9	10	10	10	0

[D] Datos											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Copias de seguridad	2	10	10	10	4	1	2	10	10	10	4
Registros de actividad	9	4	4	4	9	1	9	4	4	4	9
Documentación departamental	2	10	10	10	5	1	2	10	10	10	5
Código fuente MBE, MBE-CM	8	10	10	10	8	1	8	10	10	10	8
Archivos de configuración MBE, MBE-CM	5	7	9	10	5	1	5	7	9	10	5
Bases de datos MBE, MBE-CM	8	10	10	10	8	1	8	10	10	10	8

[COM] Red											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
ADSL (voz y datos)	0,4	0,8	0,8	1,2	0	1	0,4	0,8	0,8	1,2	0
Red inalámbrica WIFI	0,4	1,2	0,8	0,8	0	1	0,4	1,2	0,8	0,8	0
Móviles	0	0,8	0,2	0,2	0	1	0	0,8	0,2	0,2	0

[S] Servicios											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Correo electrónico corporativo	5	8	1	3	3	1	5	8	1	3	3
SSH protocolo para acceso a servidores	9	8	8	4	2	1	9	8	8	4	2
Git	7	8	8	8	7	1	7	8	8	8	7
Slack	4	3	0	3	0	1	4	3	0	3	0

[AUX] Equipamiento auxiliar											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Sistema eléctrico	0	0	0	0,4	0	1	0	0	0	0,4	0
Sistema contra incendios	0	0	0	0,4	0	1	0	0	0	0,4	0

[P] Personal											
ACTIVO	Impacto potencial					Frecuencia amenaza	Riesgo				
	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
Administradores de sistemas	0	8	8	8	0	1	0	8	8	8	0
Desarrolladores	0	8	8	8	0	1	0	8	8	8	0
Contratistas especializados	0	7	8	8	0	1	0	7	8	8	0
Directivos	0	9	9	9	0	1	0	9	9	9	0
Comerciales	0	8	8	8	0	1	0	8	8	8	0
Administrativos	0	8	6	6	0	1	0	8	6	6	0

Anexo XV. Auditoría de Cumplimiento

Informe de Auditoria TurisTech Balear

Mayo / 2022

Auditores UOC, SL
C/ Vista Alegre, 27
07009 Palma de Mallorca
971000000

Cliente auditoria: TurisTech Balear,S.L.

Historial de versiones del documento

Versión	Autor	Fecha	Estado	Acciones
1.0	Auditores UOC SL	16/05/2022	Definitivo	Elaboración de la versión inicial

Índice

1. Resumen ejecutivo

1.1 Introducción

De acuerdo con el Plan de Auditorias anual de la empresa TurisTech Balear SL, el Auditado, que se aprobó en el mes de octubre de 2019 por el Comité de Seguridad de la Información, la empresa Auditores UOC SL procedió a realizar una auditoría de primera parte del estado actual del Sistema de Gestión de Seguridad de la Información implantado en TurisTech Balear SL.

El personal interno del Auditado que está capacitado para realizar la auditoría, ha participado de una forma u otra en casi todos los elementos que son objeto de la audición. Con el fin de mantener la objetividad e independencia de la auditoría y siguiendo las indicaciones del punto tercero, capítulo 4, del documento Procedimiento de Auditorias Internas, la tarea fue encargada a la entidad Auditores UOC SL.

1.2 Plan de Auditoría y Metodología

Cronograma

01/04/2022 – Reunión inicial y recogida de documentación.
04/04/2022 al 22/04/2022 – Auditoria documental.
25/04/2022 al 29/04/2022 – Auditoria *in situ*:

Fecha	Auditoría *in situ*	Objeto de auditoria	Representantes de la entidad
25/04/2022	Instalaciones del auditado	Departamentos de Dirección y Administración	La Dirección y el responsable de Administración
26/04/2022	Instalaciones del auditado	Departamento Comercial y Recursos Humanos	Responsable de RRHH y del dpto. Comercial
27/04/2022	Instalaciones del auditado	Departamento TIC	Responsable del dpto. TIC y sus trabajadores
28/04/2022	Puestos de teletrabajo	Departamento TIC	Trabajadores afectados
29/04/2022	Puestos de teletrabajo	Departamento TIC	Trabajadores afectados

02/05/2022 al 16/05/2022 – Elaboración del informe de la Auditoría.

18/05/2022 – Presentación del informe de la Auditoría.

Criterios

Para elaborar el presente informe se usaron los términos y definiciones establecidos en el documento Procedimiento de Auditorias Internas aprobado por la Dirección del Auditado, los cuales, se tuvieron en cuenta para la posterior formulación de los planes de mejoramiento, a saber:

Tipo de hallazgo	Tratamiento
No Conformidad Mayor	Ausencia o fallo en implantar y mantener uno o más controles de la ISO/IEC 27002:2013, afectando a la capacidad del sistema de gestión
No Conformidad Menor	Ausencia o fallo en implantar y mantener uno o más controles de la ISO/IEC 27002:2013, pero no afecta a la capacidad del sistema de gestión
Observaciones	Acción de mejora que la organización puede considerar o no. Se constituye como una recomendación de mejora. No obstante, su repetición y no tratamiento puede derivar en una No Conformidad

A su vez, cada hallazgo se clasificó según los siguientes niveles de criticidad:

- 1 Informativa. Se recomienda que se gestione y que no sea ignorada, pero puede ser asumida por la entidad después de ser evaluada en un análisis de riesgos.

- 2 Baja. Puede ser gestionada en la próxima configuración planificada, pero no puede ser ignorada ni asumida por la entidad.

- 3 Media. El cliente tiene que gestionar la solución según sus procedimientos, pero no puede ser ignorada ni asumida por la entidad.

- 4 Alta. Se tiene que resolver en la mayor brevedad posible. Programar una parada.

- 5 Crítica. Se tiene que aplicar una solución inmediata.

Metodología

La auditoría se realizó con la modalidad de caja blanca, lo cual significa que TurisTech Balear facilitó toda la información necesaria para el acceso a los distintos sistemas, servicios y procesos a auditar.

Equipo auditor

El equipo auditor estuvo formado por personal perteneciente a la empresa Auditores UOC SL:

- Arsenio Tortajada Gallego como auditor jefe.
- José Sureda Uceda como auditor.

1.3 Conclusiones

Según la información que se pudo recopilar el equipo auditor obtuvo los siguientes resultados:

No Conformidades Mayores	No Conformidades Menores	Observaciones
4	2	3

Considerando que:

- La entidad TurisTech Balear incumple ciertas políticas internas y algunos controles de la norma ISO/IEC 27002:2013. Los detalles de las No Conformidades quedan detalladas en el capítulo 5, *Hallazgos de auditoría,* de este mismo documento.

1.4 Recomendaciones

Seguir las indicaciones descritas para cada uno de los hallazgos del capítulo 5 de este mismo informe.

2. Objetivo de la auditoría

Evaluar la efectividad de los controles, políticas, normas y/o procedimientos establecidos por el auditado para la implantación, mantenimiento y mejora de su Sistema de Gestión de Seguridad de la Información. La correcta administración de los riesgos y efectuar las recomendaciones necesarias en pro del mejoramiento continuo del proceso, lo cual redundará en el cumplimiento de los objetivos de la entidad.

3. Alcance

El equipo auditor realizó la Auditoría a los departamentos de Dirección, Administración, Recursos Humanos, Comercial y de TIC, a los puestos donde se realiza teletrabajo y a todos los dominios incluidos en el documento de Declaración de Aplicabilidad.

4. Marco legal y normativa de referencia

Norma ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

Norma ISO/IEC 27002:2013. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

Normativa interna del Auditado: Política de Seguridad, Procedimiento de Auditorías Internas, Análisis de Riesgos y declaración de Aplicabilidad.

5. Hallazgos de auditoría

Seguidamente se describen las No Conformidades que se detectaron a partir de las pruebas realizadas por el equipo auditor.

ID Hallazgo	HA0001
Resultado	**Observaciones**
Categoría principal	11.1 Áreas seguras
Controles ISO/IEC 27002:2013 afectados	11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada 11.1.3 Seguridad de oficinas, despachos y recursos 11.1.4 Protección contra las amenazas externas y ambientales
Evidencia	• No existen sistemas que alerten de accesos no autorizados en la oficina, donde se encuentran los portátiles y PCs de los empleados, así como información en papel y/o en dispositivos extraíbles • El acceso principal a la oficina así como las puertas interiores donde están los equipos y documentación física, no disponen de cerraduras reforzadas • Revisión de los accesos a las instalaciones
Recomendación	• Instalar un sistema de alarma conectada con los autoridades policiales • Cambiar el sistema de cerradura de las puertas de acceso a la sala de equipos y documentación
Nivel de gravedad **Plazo corrección**	1 - Informativa 1 año

ID Hallazgo	HA0002
Resultado	**No Conformidad Menor**
Categoría principal	12.1 Procedimientos y responsabilidades operacionales
Controles ISO/IEC 27002:2013 afectados	12.1.2 Gestión de cambios 12.1.3 Gestión de capacidades
Evidencia	• No existe una documentación que defina los procedimientos para la gestión de cambios. Por ejemplo la aprobación formal de subidas a producción ni de vuelta a estados anteriores (rollback) • No existen procedimientos definidos para la gestión de los recursos. En ocasiones se han producido cuellos de botella en algunos servicios, así como la ocupación completa de espacios de almacenamiento • Entrevistas con el personal
Recomendación	• Documentar los procedimientos para la gestión de cambios y de capacidades • Implantar sistemas que permitan detectar con tiempo

	suficiente las capacidades y estados de los recursos y servicios
Nivel de gravedad **Plazo corrección**	2 - Baja 6 meses

ID Hallazgo	HA0003
Resultado	**No Conformidad Mayor**
Categoría principal	12.2 Protección contra el software malicioso (malware)
Controles ISO/IEC 27002:2013 afectados	12.2.1 Controles contra el código malicioso
Evidencia	• Los equipos portátiles y servidores no cuentan con sistemas de protección y detección de malware • Aunque existe una política que define los procesos para la instalación de software en general, no hay una que describa la gestión y el tratamiento del malware • Entrevistas con el personal
Recomendación	• Definir una política de protección contra software malicioso y de recuperación en caso de infección • Instalar sistemas de protección en los distintos equipos • Implantar un plan de formación para la concienciación del usuario
Nivel de gravedad **Plazo corrección**	4 - Alta 1 mes

ID Hallazgo	HA0004
Resultado	**Observaciones**
Categoría principal	13.1 Gestión de la seguridad de las redes
Controles ISO/IEC 27002:2013 afectados	13.1.3 Segregación en redes
Evidencia	• Los servidores que prestan servicios ya se encuentran segregados en distintas redes pero no está debidamente documentado • Se revisan los segmentos de redes existentes
Recomendación	• Definir los procedimientos de segregación de las redes
Nivel de gravedad **Plazo corrección**	1 - Informativa 1 año

ID Hallazgo	HA0005
Resultado	**No Conformidad Mayor**
Categoría principal	13.2 Intercambio de información
Controles ISO/IEC 27002:2013 afectados	13.2.2 Acuerdos de intercambio de información 13.2.4 Acuerdos de confidencialidad o no revelación
Evidencia	• No existen acuerdos para el intercambio de información entre departamentos de la propia organización y con terceros según se requiere en la Política de Seguridad • La organización tampoco dispone de acuerdos de confidencialidad o no revelación • Entrevistas con el personal
Recomendación	• Establecer los acuerdos para la transferencia de información dentro de la organización y con terceros • Documentar los acuerdos de confidencialidad, un modelo dirigido a los empleados y otro para entidades externas
Nivel de gravedad **Plazo corrección**	3 - Media 3 meses

ID Hallazgo	HA0006
Resultado	**Observaciones**
Categoría principal	14.1 Requisitos de seguridad en los sistemas de información
Controles ISO/IEC 27002:2013 afectados	14.1.1 Análisis de requisitos y especificaciones de seguridad de la información 14.1.2 Asegurar los servicios de aplicaciones en redes públicas 14.1.3 Protección de las transacciones de servicios de aplicaciones
Evidencia	• La organización, aunque tienen en cuenta los aspectos de seguridad de los controles anteriores a la hora de diseñar nuevas funcionalidades, no cuenta con los procesos definidos y documentados • Entrevistas con el personal
Recomendación	• Documentar los requisitos de seguridad en los sistemas de información
Nivel de gravedad **Plazo corrección**	1 - Informativa 1 año

ID Hallazgo	HA0007
Resultado	**No Conformidad Mayor**
Categoría principal	14.2 Seguridad en el desarrollo y en los procesos de soporte

Controles ISO/IEC 27002:2013 afectados	14.2.1 Política de desarrollo seguro 14.2.2 Procedimiento de control de cambios en sistemas 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 14.2.5 Principios de ingeniería de sistemas seguros 14.2.6 Entorno de desarrollo seguro 14.2.7 Externalización del desarrollo de software 14.2.8 Pruebas funcionales de seguridad de sistemas 14.2.9 Pruebas de aceptación de sistemas
Evidencia	• No existe una política de desarrollo seguro. Todo el ciclo de vida del desarrollo de software se realiza de forma similar y reproducible, pero de forma intuitiva y todo depende del grado de conocimiento de los desarrolladores • No existen planes de formación para el desarrollo seguro y de buenas prácticas • No existen procedimientos ni controles formales para la gestión de cambios • Las pruebas tras efectuar los cambios se dejan bajo la responsabilidad de cada desarrollador. No existen procesos de pruebas debidamente definidos • Se aplican patrones de diseño del software pero sin estar documentados los procesos • No están definidos los acuerdos en los casos donde haya que externalizar desarrollos • Entrevistas con el personal
Recomendación	• Documentar una política de desarrollo seguro que alcance todos los puntos indicados en este hallazgo
Nivel de gravedad **Plazo corrección**	3 - Media 3 meses

ID Hallazgo	HA0008
Resultado	**No Conformidad Menor**
Categoría principal	14.3 Datos de prueba
Controles ISO/IEC 27002:2013 afectados	14.3.1 Protección de los datos de prueba
Evidencia	• Los datos de prueba son una copia exacta del entorno de explotación, pero no existen procedimientos para gestionar su retirada o modificación
Recomendación	• Documentar las directrices para proteger los datos que se usan en las pruebas. La repetición de esta situación podría llegar a derivar en una No Conformidad Mayor
Nivel de gravedad **Plazo corrección**	2 - Baja 6 meses

ID Hallazgo	HA0009
Resultado	**No Conformidad Mayor**
Categoría principal	15.1 Seguridad en las relaciones con proveedores 15.2 Gestión de la provisión de servicios del proveedor
Controles ISO/IEC 27002:2013 afectados	15.1.1 Política de seguridad de la información en las relaciones con los proveedores 15.1.2 Requisitos de seguridad en contratos con terceros 15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones 15.2.1 Control y revisión de la provisión de servicios del proveedor 15.2.2 Gestión de cambios en la provisión del servicio del proveedor
Evidencia	• No existe ninguna política para las relaciones con los proveedores, en este caso los que prestan el servicio Cloud donde se alojan los servidores • No existen planes de auditorias en los servicios contratados • Los empleados desconocen si existen contratos con terceros y de qué forma les afectan a ellos • El administrador de sistemas no tiene claro cuáles son las medidas de seguridad que el proveedor aplica en los entornos Cloud ni los acuerdos de provisión el servicio • Entrevistas con el personal
Recomendación	• Definir una política para las relaciones con proveedores • Definir un plan de auditoria de los servicios contratados • Implantar sistemas que permitan gestionar los servicios contratados, por ejemplo para la recogida de incidentes, incumplimientos de SLA o información para las auditorias
Nivel de gravedad **Plazo corrección**	3 - Media 3 meses