Elaboración de un Plan de Implementación de la ISO/IEC 27001:2017 para una empresa de servicios

Nombre Estudiante: Jacopo Bianchi Porro

Programa: Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: junio 2022

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2017 para una empresa de servicios*
Nombre del autor:	*Jacopo Bianchi Porro*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	06/2022
Titulación::	Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Castellano*
Palabras clave	*ISO27001, Riesgos, Seguridad*

Resumen del Trabajo (máximo 250 palabras)

La información es hoy uno de los principales activos de las organizaciones: protegerla y garantizar su confidencialidad, integridad y disponibilidad es una tarea muy importante. Para una empresa que ofrece servicios de consultoría sobre (entre otro) la seguridad laboral, la medicina ocupacional y los cursos de formación para los empleados, la obtención de la certificación ISO 27001 no solo permite garantizar que se alcanza un nivel adecuado de seguridad de la información, sino es obligatoria por ley (en Italia) para trabajar con las administraciones públicas y también, aunque informalmente, con los bancos.

Reduciendo el alcance de la certificación al software desarrollado internamente y utilizado por consultores (una aplicación Windows y dos web App), y partiendo de una situación en la que parte de los procedimientos son el resultado de la experiencia y no están codificados (por lo tanto ya presentes, al menos parcialmente, aunque no siempre aplicados o controlados) se ha conseguido establecer un plan de acción que le permita estar lista para la certificación en menos de un año.

El trabajo permitió aumentar sensiblemente el nivel de madurez del cumplimiento de los requisitos de ISO/IEC 27001 e ISO/IEC 27002 pasando de una situación crítica a otra sin duda satisfactoria, que sin embargo debe ser vista como un punto de partida y no de llegada: hay que mejorar los controles menos maduros, realizar revisiones y auditorías periódicas, buscar ajustamientos contra nuevas amenazas y, posiblemente, ampliar el alcance del sistema gestión de seguridad de la información.

Abstract (in English, 250 words or less):

Information is today one of the main assets of organizations: protecting it and guaranteeing its confidentiality, integrity and availability is a very important task. For a company that offers consulting services on (among others) occupational safety, occupational medicine and training courses for employees, obtaining ISO 27001 certification not only ensures that is achieved an adequate level of safety in the information, but it is mandatory by law (in Italy) to work with public administrations and also, albeit informally, with banks.

Reducing the scope of the certification to the software developed internally and used by consultants (one Windows application and two web Apps), and starting from a situation in which part of the procedures are the result of experience and are not codified (therefore present, at least partially, although not always applied or controlled) it has been possible to establish an action plan that allows to be ready for certification in less than a year.

The work made possible to significantly increase the maturity level of compliance with the requirements of ISO/IEC 27001 and ISO/IEC 27002, moving from a critical situation to another undoubtedly satisfactory one, which, however, should be seen as a starting point and not an arrival point: it is necessary to improve less mature controls, carry out periodic reviews and audits, to seek adjustments against new threats and, possibly, to expand the scope of the information security management system.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Este Trabajo Final de Master se centrará en la elaboración de un plan de implementación de la ISO/IEC 27001:2017 (se trata de la ISO/IEC 27001:2013 con dos correcciones de 2014 y 2015, implementada en Italia en 2017[1]) para una empresa de servicios del norte de Italia en la cual el autor ha trabajado durante 17 años, que desarrolla unos software para servicios de consultoría sobre la seguridad laboral, la prevención de riesgos laborales, la gestión de impactos ambientales, la medicina ocupacional, los cursos de formación para los empleados.
Todos estos programas pueden tratar datos personales; todavía mientras una parte de ellos son utilizados - en general - solo por los trabajadores internos, unas de las plataformas web realizadas pueden estar disponibles para los clientes, para que puedan elaborar datos sin la intervención de los consultores de la empresa.
En la imagen siguiente se puso una esquematización (simplificada) de la estructura:

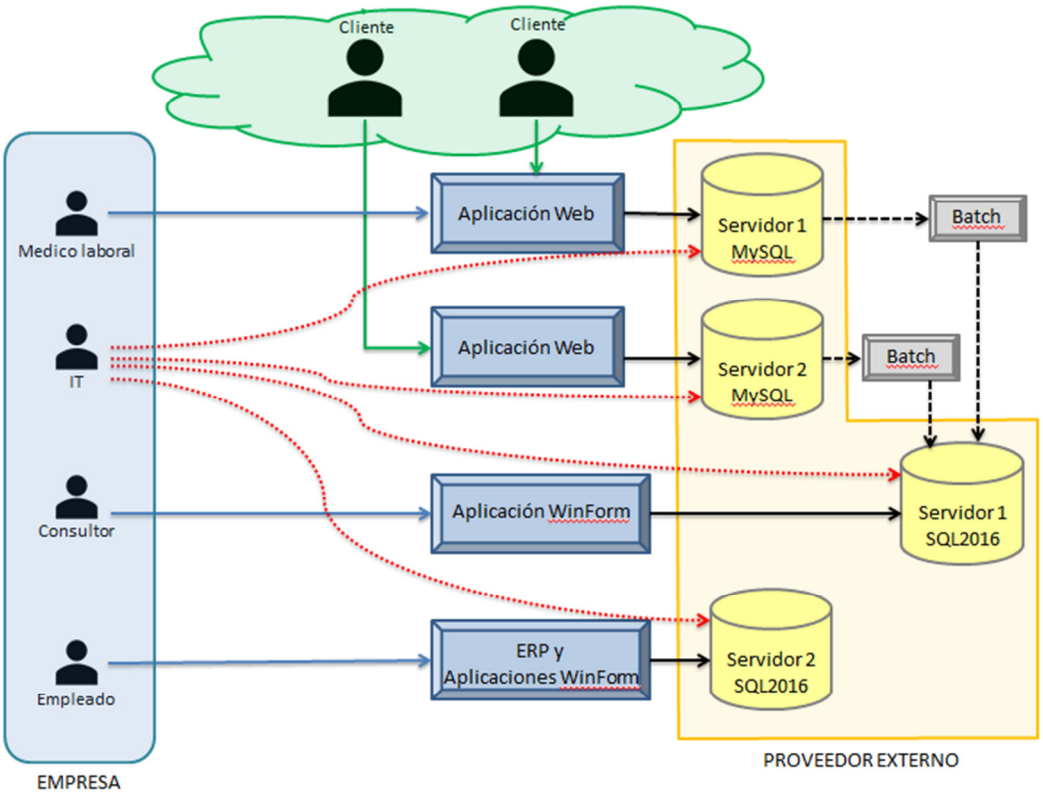


Imagen 1: Esquema de la estructura de la organización de la empresa

Aunque todos estos software, gestionando datos sensibles (o pudiendo hacerlo), deben por supuesto cumplir con el RGPD y con las leyes italianas, no es necesaria la certificación ISO/IEC 27001. Todavía esta es requerida cuando los clientes son administraciones públicas o bancos: por esto es necesario implementar un análisis y un consecuente plan de acción para poder obtener la certificación y no perder clientes.

1.2 Objetivos del Trabajo

El objetivo final del trabajo es aquello de implementar un plan de acción para obtener en el menor tiempo posible la certificación ISO/IEC 27001: esto significa elegir bien cuáles deben ser los activos que deben entrar en el alcance del análisis excluyendo aquellos que pueden ser considerados como "superfluos". Esto no significa que no deberán nunca ser objetos de una futura auditoría, sino que en este momento la prioridad de las acciones a realizarse debe darse a aquellas que sirven para no perder potenciales clientes.
Consecuentemente, el primer objetivo a llevar a cabo es aquello de circunscribir el alcance de la certificación; será luego necesario realizar un análisis preciso de la situación actual con las fortalezas y debilidades, individuar las correcciones y finalmente establecer un plan de mantenimiento periódico.

1.3 Planificación del Trabajo

Para la elaboración del trabajo se seguirá la planificación sugerida, aunque el autor podrá sucesivamente adaptarla a las necesidades de revisiones, de profundizaciones u otras sugerencias recibidas por el consultor.
En la **fase 1** se completará la introducción al proyecto, la selección de la empresa, la definición de los objetivos y un análisis diferencial de la misma empresa con respecto la ISO/IEC 27001+ISO/IEC 27002.
En la **fase 2** se elaborarán la Política de Seguridad, la declaración de aplicabilidad y la documentación del SGSI.
Durante la **tercera fase** se elaborará una metodología de análisis de riesgos, es decir identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.
La **fase 4** será constituida por la evaluación de los proyectos que la empresa deberá llevar a cabo para alinearse con los objetivos planteados en el Plan Director, con su cuantificación económica y temporal.
En la **fase 5** se evaluarán controles, madurez y nivel de cumplimiento.
Finalmente en la **fase 6**, que se concluirá con la entrega del proyecto final y su presentación, se consolidarán los resultados obtenidos durante el proceso de análisis y se realizarán los informes.

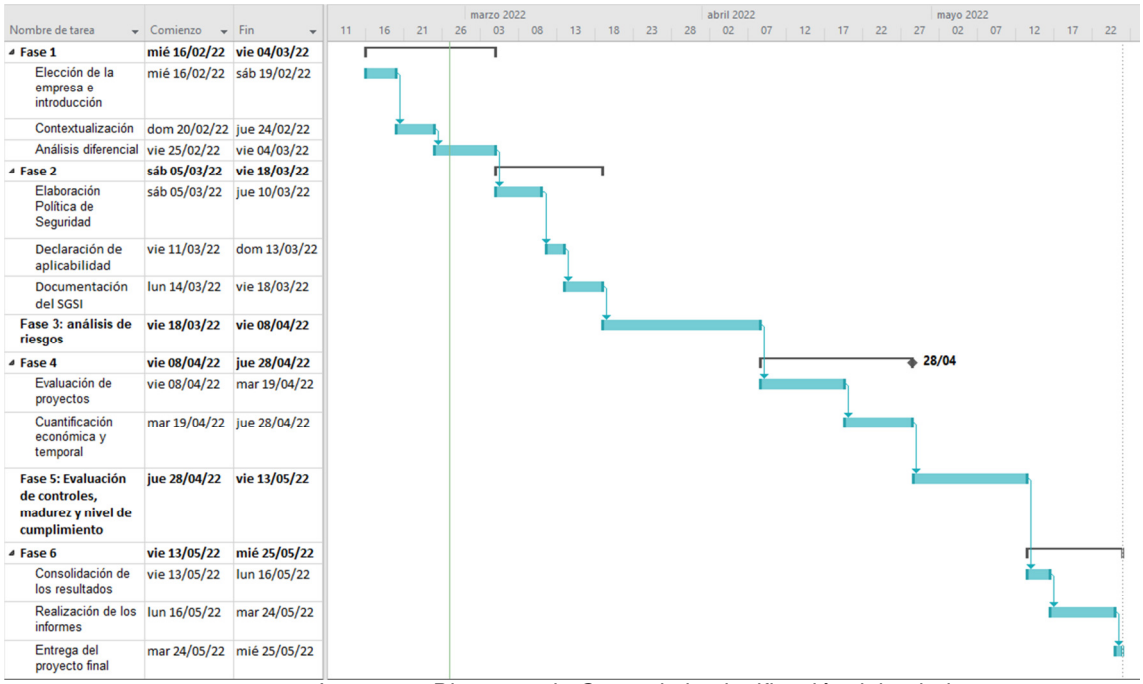


Imagen 2: Diagrama de Gannt de la planificación del trabajo

1.4 Breve descripción de los otros capítulos de la memoria

En el **capítulo 2** se hace un breve resumen de las principales características del estándar ISO 27001 y del código de mejores prácticas ISO 27002, mientras el **capítulo 3** incluye una descripción de la empresa elegida y la definición del alcance del análisis siguiente.

Los resultados del análisis diferencial, que permite entender cuál es la situación inicial en la que se encuentra la empresa, ocupa el **capítulo 4** (la tabla completa del análisis se incluye en el anexo 1).

2. Conociendo ISO 27001 e ISO/IEC 27002

Dado que ISO 27000 es una serie de normas iniciadas por ISO para garantizar la seguridad y la protección dentro de las organizaciones de todo el mundo, vale la pena conocer la diferencia entre ISO 27001 e ISO 27002, dos de las normas de la serie ISO 27000.

El estándar ISO 27001 garantiza la seguridad de la información y la protección de datos en las organizaciones: es muy importante para las organizaciones comerciales porque su certificación es reconocida en todo el mundo como una indicación de que el sistema de gestión de seguridad de la información está alineado con las mejores prácticas de seguridad en la protección de sus clientes y de la información confidencial contra las amenazas.
En efecto el objetivo principal de la norma es proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). En la mayoría de las empresas, las decisiones sobre la adopción de este tipo de normas las toma la alta dirección. Además, la necesidad de contar con este tipo de sistema de seguridad de la información para la organización surge de diversos factores tales como metas y objetivos organizacionales, requerimientos de seguridad, tamaño y estructura de la organización, etc.
En la versión anterior del estándar en 2005, se desarrolló sobre la base del ciclo PDCA, el modelo Plan-Do-Check-Act para estructurar procesos y esto fue de manera de reflejar los principios establecidos por las directrices de la OCDE. La nueva versión enfatiza la medición y evaluación de la efectividad del desempeño organizacional en SGSI. También se ha incluido un apartado basado en la externalización y se da más énfasis a la seguridad de la información en las organizaciones.
La versión más reciente de la norma en Italia es UNI CEI EN ISO/IEC 27001:2017 (publicada el 30 de marzo de 2017), que no es otra que la versión de 2013 con dos correcciones (emitidas por ISO en 2014 y 2015):

- requisito A.8.1.1: el inventario, clasificación y tratamiento de los "activos" ahora también se refiere a la "información" con la que están asociados los activos.
- requisito 6.1.3: la Declaración de Aplicabilidad debe especificar si se implementan o no los "controles necesarios", y no solo los controles a los que se refiere el Anexo A.

La ISO 27002, por otro lado, es un estándar complementario que se enfoca en los controles de seguridad de la información que las organizaciones pueden optar por implementar. Estos controles se enumeran en el Anexo A de ISO 27001; sin embargo, mientras que el Anexo A simplemente describe cada control en una o dos frases, ISO 27002 dedica en promedio una página a cada control, lo que los hace extremadamente fáciles de entender e implementar. El estándar, de hecho, explica cómo funciona cada control, cuál es su objetivo y cómo se puede implementar. La ISO 27002 es, por lo tanto, extremadamente útil como norma complementaria a la ISO 27001 porque, si esta norma entrara en los detalles de la ISO 27002, se volvería innecesariamente larga y complicada. En cambio, simplemente proporcionando un resumen de cada aspecto de un sistema de

gestión de seguridad de la información y dejando recomendaciones específicas en algunos estándares adicionales, se mantiene optimizado y fácil de entender.
Nacida originalmente como estándar ISO 17799, que se basa en el código de prácticas para la seguridad de la información, es una colección de "mejores prácticas" que se pueden adoptar para cumplir con los requisitos del estándar ISO / IEC 27001.

La versión existente del estándar se publicó en 2013 como ISO 27002: 2013 y tiene, además de los apartados introductorios, 14 dominios, 35 objetivos de seguridad y 114 controles. En detalle son[2]:

- Políticas de seguridad de la información (1 objetivo, 2 controles)
- Organización de la seguridad de la información (2 objetivos, 7 controles)
- Seguridad relativa a los recursos humanos (3 objetivos, 6 controles)
- Gestión de activos (3 objetivos, 10 controles)
- Controles de acceso (4 objetivos, 14 controles)
- Criptografía (1 objetivo, 2 controles)
- Seguridad física y del entorno (2 objetivos, 15 controles)
- Seguridad de las operaciones (7 objetivos, 14 controles)
- Seguridad de las comunicaciones (2 objetivos, 7 controles)
- Adquisición, desarrollo y mantenimiento de los sistemas de información (3 objetivos, 13 controles)
- Relaciones con proveedores (2 objetivos, 5 controles)
- Gestión de incidentes de seguridad de la información (1 objetivo, 7 controles)
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio (2 objetivos, 4 controles)
- Cumplimiento (2 objetivos, 8 controles)

Siendo una simple colección de recomendaciones, la norma ISO/IEC 27002 no es certificable.

A pesar del hecho que este trabajo se desarrollará teniendo en cuenta la ISO 27002:2013, es necesario destacar que el 15 de febrero de 2022 se publicó la nueva edición de la norma ISO/IEC 27002. Aunque los requisitos de ISO/IEC 27001:2013 (párrafos 4 – 10), no han sido modificados, que solo se han actualizado los controles de seguridad listados en ISO/IEC 27001:2013, Anexo A, y que el número de controles disminuyó de 114 a 93 (se han definido 11 nuevos controles y se han emparejado otros, eliminando algunos de los que más se percibían como duplicados, dado que el mismo control “genérico” se expresaba varias veces en diferentes contextos de riesgo), hay que tener en cuenta que los controles están organizados en 4 secciones en lugar de las 14 anteriores. En efecto ahora están agregados por "macro-temas” que coinciden con los 4 pilares tradicionales asociados a la seguridad de la información:

- controles organizacionales (37 controles)
- controles físicos (14 controles)
- controles de personas (8 controles)
- controles tecnológicos (34 controles)

La nueva edición adopta la nueva definición de control de la ISO 31000, es decir “Medida que mantiene y/o modifica el riesgo”: esta definición resuelve una crítica que a menudo se planteó sobre la versión anterior, que no incluía la capacidad de un control limitado únicamente al mantenimiento de un riesgo.

Además, cada control ahora está asociado con cinco atributos importantes, a los que se asocian valores específicos:

- Tipo de control (Preventivo, Detectivo, Correctivo);
- Propiedades de seguridad de la información (Confidencialidad, Integridad, Disponibilidad);
- Conceptos de ciberseguridad (Identificar, Proteger, Detectar, Responder y Restaurar);
- Capacidades operativas: Gobierno, gestión de activos, protección de la información, seguridad de recursos humanos, seguridad física, seguridad de redes y sistemas, seguridad de aplicaciones, configuración segura, gestión de identidad y acceso, gestión de amenazas y vulnerabilidades, continuidad, seguridad de relaciones con proveedores, legal y cumplimiento, seguridad de la información Gestión de eventos y Garantía de la seguridad de la información;
- Dominios de seguridad: Gobierno y Ecosistema, Protección, Defensa y Resiliencia

El Anexo B de la nueva edición ilustra la correspondencia entre los controles de la nueva edición y los de la norma ISO/IEC 27002:2013; en cualquier caso la publicación de la tercera edición de ISO/IEC 27002 requerirá efectivamente una revisión de la ISO/IEC 27001. [3]

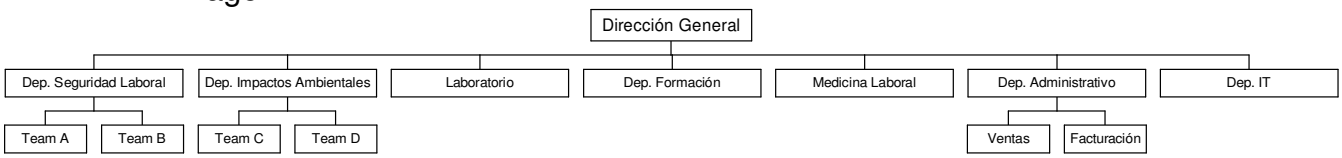
3. Contextualización

3.1 Breve descripción de la empresa

Se trata de una empresa de servicios del norte de Italia con aproximadamente 250 empleados cuya actividad es aquella de consultoría a otras empresas sobre la seguridad laboral, la prevención de riesgos laborales, la gestión de impactos ambientales, la medicina ocupacional, los cursos de formación para los empleados. Para facilitar el trabajo de sus consultores, a lo largo del tiempo la empresa ha desarrollado unos softwares para gestionar el almacenamiento, la organización, la elaboración y la recuperación de las informaciones.
El software más importante es una aplicación Windows que utiliza una base de datos SQL 2016: en un servidor ubicado en una empresa externa son almacenados aproximadamente 4.000 bases de datos, una para cada cliente (en realidad hay también un segundo servidor SQL exclusivo para un cliente que ha querido tener sus bases de datos totalmente separadas de las otras). Este programa es empleado por los consultores de la empresa y (a través de un enlace a través de la plataforma Citrix) por unos pocos clientes, y permite generar los informes necesarios para cumplir las obligaciones de ley.
En los últimos años se han también desarrollado dos aplicaciones web que utilizan dos servidores MySQL: en este caso la estructura de las aplicaciones prevé la existencia de una única base de datos que almacena las informaciones de todos los clientes. Una de estas aplicaciones gestiona la medicina laboral (y es usada solo por los médicos laborales de la empresa), mientras la otra es utilizada por los clientes para gestionar las informaciones de seguridad laboral de sus proveedores, por lo que concierne la formación de seguridad laboral según la normativa italiana (es decir que el cliente va a insertar los datos de los proveedores/consultores/elementos externos con los cuales trabaja y, entre otro, si les ha hecho formación sobre los riesgos laborales, si deben cursar unas clases, si están expuestos a peligros….). En este caso no hay intervención de los consultores de la empresa (por supuesto, puede ser necesaria la intervención del sector IT si hay problemas o errores), todavía unas de estas informaciones pueden ser útiles también para el programa “principal” visto anteriormente (por ejemplo el consultor puede no conocer todo el organigrama de una empresa o las actualizaciones, pero el médico laboral siempre tendrá la información correcta de, por ejemplo, despidos y nuevos empleos y la actualizará en su plataforma web): dado que podría ser necesario disfrutar esta información para actualizar unos datos en el otro programa, se han desarrollado unos programas batch que permiten pasar unas informaciones desde las bases de datos mySQL a las bases de datos SQL correspondientes.
Todas estas bases de datos se han migrado en 2019 a un proveedor externo, ubicado en otra ciudad, y el sector IT puede acceder a través de una VPN a los servidores.

Además de estos programas, la empresa tiene su ERP y otros programas (MS Office, programas de correo electrónico, Autocad, programas para análisis de laboratorio…) y otros servidores (Exchange y Windows Server); hay un firewall y un programa antivirus centralizado. Durante la pandemia se dio la posibilidad a consultores y empleados administrativos de conectarse a la red de la empresa a través de una VPN.

La estructura de la empresa se define según lo que aparece en la siguiente imagen:



Se trata de una estructura bastante sencilla: hay unos departamentos que se ocupan de diferentes áreas de consultoría: seguridad laboral, impactos ambientales, formación, medicina laboral, análisis de laboratorio, departamento administrativo y departamento IT. Cada departamento tiene un responsable que colabora directamente con la dirección. A su vez, unos de estos departamentos (seguridad laboral e impactos ambientales) están subdivididos en equipos de aproximadamente 15 personas, cada una con su jefe de equipo.
El sector IT está compuesto por 8 personas, pero solo el responsable del sector tiene unos conocimientos (aunque no profundizados) de la norma ISO 27001.

Como dicho anteriormente, la empresa ha desarrollado dos aplicaciones web que utilizan dos servidores MySQL; la aplicación Windows Forms utiliza un servidor MSSQL, que además está relacionado con uno de los dos servidores MySQL; hay otros servidores MSSQL utilizados por dos ERP empresariales y otros programas.
La imagen siguiente permite visualizar el diagrama de la infraestructura IT: los servidores directamente relacionados con el alcance de la certificación son aquellos que aparecen en rojo.

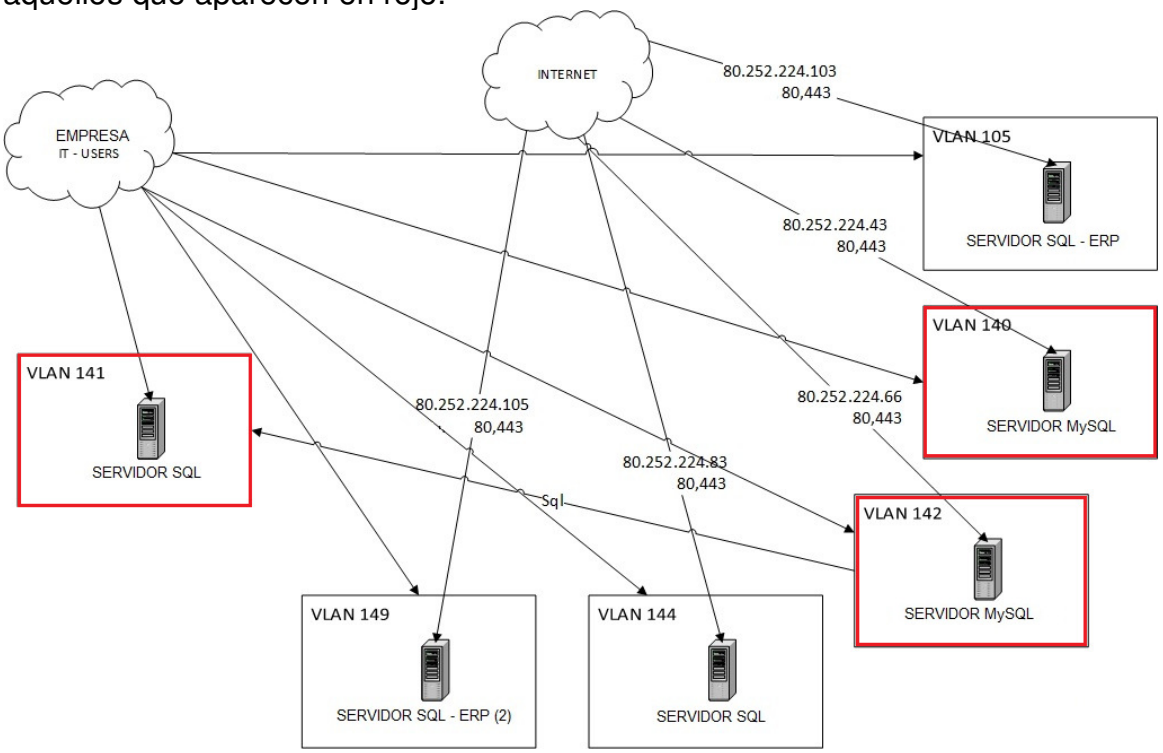


Imagen 3: Diagrama de la estructura IT de la empresa

3.2 Alcance

Aunque es claro que sería mejor hacer un análisis global e implantar un SGSI consecuente, esto significaría retrasar mucho la obtención de la certificación, siendo el número de controles e intervenciones necesarios mucho mayor, así como surgiendo la necesidad de involucrar también los proveedores y desarrolladores de los otros programas utilizados.
En realidad para satisfacer lo que requieren los clientes es suficiente que sean la aplicación Windows y las 2 aplicaciones web a obtener la certificación ISO 27001: esto permite reducir los trabajos y las correcciones necesarias y trabajar reuniendo las solicitudes de los clientes y la urgencia de la empresa.

Por esto el alcance de la certificación puede ser el "desarrollo de software para sistemas de gestión y prestación de servicios de asistencia y consultoría relacionados".

Los departamentos afectados por el SGSI son, consecuentemente: el departamento IT, aquellos de seguridad laboral y de impactos ambientales (cuyos consultores utilizan la aplicación Windows) y la medicina laboral (por su utilización de una de las dos web App). Además hay que tener en cuenta, por supuesto, la dirección (el SGSI debe estar alineado con los objetivos estratégicos y cumplir con la legislación vigente), los proveedores (deberán aplicar las medidas de protección definidas) y también los clientes (deberán cumplir las medidas de seguridad que se definirán).

4. Análisis diferencial

4.1 Análisis diferencial ISO/IEC 27002

La empresa no tiene experiencia en la implantación de un SGSI conforme al estándar ISO/IEC 27001: por eso es necesario llevar a cabo un análisis de GAP para determinar el estado de la seguridad actual y establecer el punto de partida y el esfuerzo necesario para implementar la norma. Consecuentemente, se identificarán los controles de seguridad implantados dentro de aquellos descritos en la ISO/IEC 27002, determinando el nivel de madurez para cada uno de ellos.
El modelo de madurez empleado para la valoración de los controles es aquello definido por COBIT:

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

Imagen 4: Modelo de madurez COBIT [3]

Se han utilizado la plantilla de la tabla para el análisis diferencial y, para la realización del gráfico Gral, el fichero Excel "GAP_27002_2013_corregido_v3.xlsx" puestos a disposición en la asignatura de Sistemas de Gestión de la Seguridad.

4.2 Resultado del análisis diferencial ISO/IEC 27002

El análisis diferencial completo se puede ver en el Anexo 1 al final del documento. Este es el resumen de las valoraciones, con el gráfico:

	Valor
A.5 Information security policies	**1**
A.6 Organization of information security	**1,7**
A.7 Human resource security	**0,5**
A.8 Asset management	**0,25**
A.9 Access control	**1,62**
A.10 Cryptography	**0**
A.11 Physical and environmental security	**2,42**
A.12 Operations security	**1,18**
A.13 Communications security	**0,58**
A.14 System acquisition, development and maintenance	**0,56**
A.15 Supplier relationships	**0**
A.16 Information security incident management	**0**
A.17 Information security aspects of business continuity management	**0**
A.18 Compliance	**0**

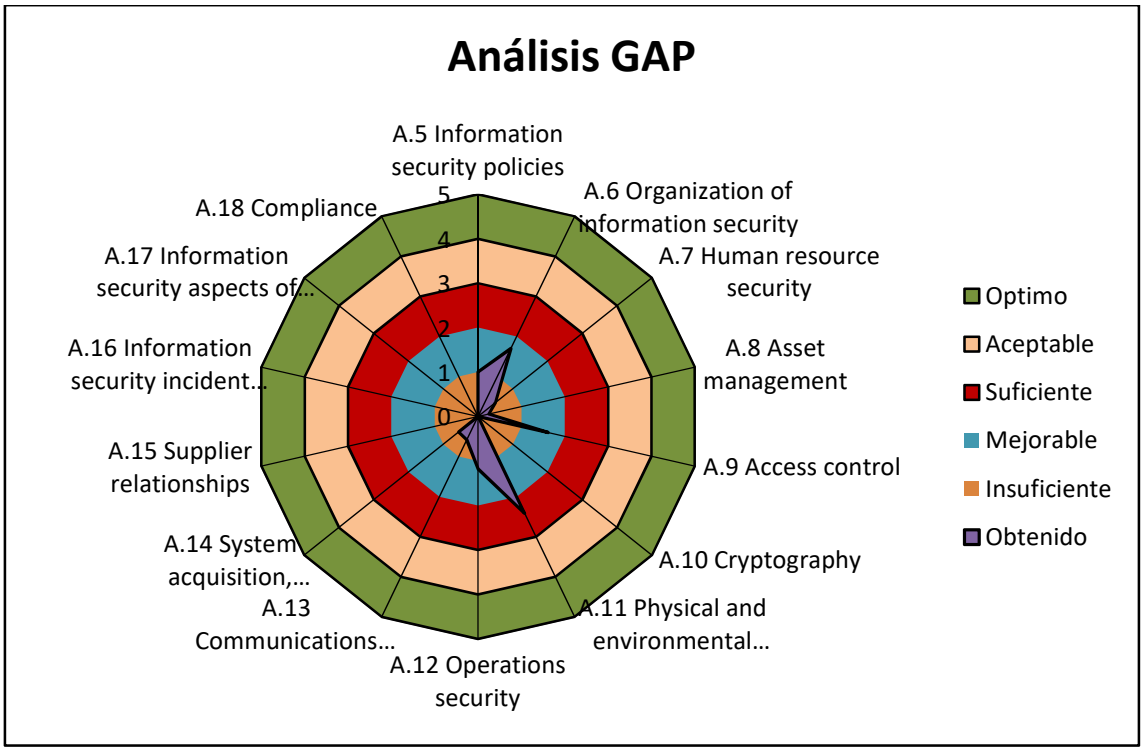


Imagen 5: Resultado del análisis GAP

4.3 Comentario al resultado del análisis diferencial

A primera vista se podría fácilmente deducir que la empresa se encuentra en un estadio inicial del proceso: los valores obtenidos son muy bajos o (en cualquier caso) incluso nulos, con la excepción de los controles de seguridad física, debido al hecho que no están gestionados directamente por la empresa, sino es el proveedor externo que gestiona los servidores de las bases de datos que se ocupa.

Todavía la situación no es tan crítica como se podría pensar: lo que falta es casi siempre la documentación, lo que no permite llegar, en el análisis, al tercer nivel de madurez. Los procesos existen, son bastante conocidos y utilizados y se aprovecha del hecho que el sector IT es pequeño y siempre es posible una confrontación directa entre sus componentes para conocer lo que se debe hacer. Y que en caso de problemas con la gestión de los datos personales (aunque en realidad nunca ha pasado) siempre hay disponibles consultores que pueden intervenir para ayudar.

Claro que esto no es posible cuando un control afecta a muchos empleados o elementos externos a la organización, pero es una consecuencia del hecho que la empresa, a pesar de tener más de 250 empleados, sigue siendo administrada como si fuera el pequeño negocio familiar que era cuando nació, un comportamiento de los empresarios que en esta parte de Italia es bastante común.

Otro punto importante a tener en cuenta es que la misma empresa a su vez ofrece asistencia a otros para la obtención de certificaciones ISO (por supuesto no de la 27001): esto significa que ya está acostumbrada a lo que se puede pedir y que tiene consultores que, por ejemplo, conocen cómo preparar y organizar la documentación necesaria.

4.4 Análisis diferencial ISO/IEC 27001

Para la evaluación de la madurez del cumplimiento de los requisitos de la norma ISO/IEC 27001, se ha utilizado la plantilla Excel buscada en https://www.pivotpointsecurity.com/iso-27001/iso-27001-resources/iso-27001-checklist/. En particular el nivel de los controles se divide en totalmente, parcialmente y no implementados, y no aplicable.
El resumen del resultado de la evaluación, visible en el Anexo 2 es:

Count	Status Code - Meaning	Status Code
9	Process is defined / documented and practiced / implemented	**Fully Implemented**
13	Process is practiced / implemented without adequate documentation; Process must be defined / documented to ensure repeatability of process and mitigate the risks.	**Partially Implemented**
78	Process is defined and not practiced	**Not Implemented**
0	Process is not applicable for the company as per the scope	**NA (Not Applicable)**

Como dicho anteriormente, la empresa no ha implantado un SGSI conforme al estándar: falta la definición (y la consecuente aplicación) de un proceso de evaluación de riesgos de seguridad, aunque se han hecho unas evaluaciones mínimas para cumplir con la legislación vigente y se ha finalmente decidido implementar un control correcto e intentar conseguir la certificación (los controles totalmente implementados son, en efecto, aquellos que ven la dirección soportar este proceso). Es por ello que se ha considerado este análisis "secundario" al anterior: se puede en efecto ver en el siguiente gráfico como la gran mayoría de los controles de la ISO/IEC 27001 ni siquiera se ha implementado parcialmente.

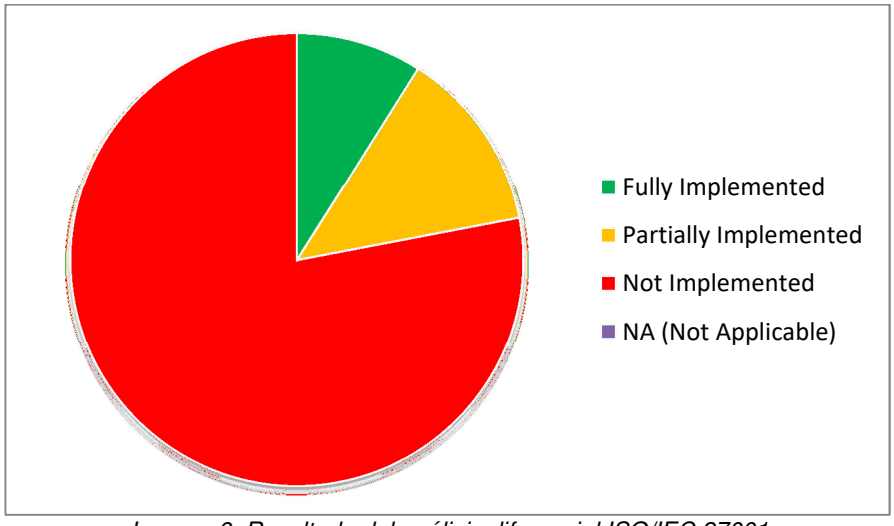


Imagen 6: Resultado del análisis diferencial ISO/IEC 27001

5. Sistema de gestión documental

Al implementar un sistema de gestión de seguridad de la información (SGSI) que cumpla con el estándar internacional ISO 27001, se debe crear y mantener documentación específica. Entre ellos, este trabajo se centrará en:

- **Política de seguridad de la información**: se trata de la normativa interna de la empresa que deben conocer todos aquellos afectados por el alcance del SGSI. Véase el Anexo 3.
- **Procedimiento de Auditorías Internas**: se proporcionan las indicaciones clásicas sobre la actividad de auditoría. La auditoría debe verificar el cumplimiento de la norma 27001 (una vez obtenida la certificación) y de las normas y procedimientos internos. Se prevén los programas, los objetivos, la elección de auditores competentes, la comunicación de los resultados a la dirección y la documentación de la actividad de auditoría. Véase el Anexo 4.
- **Gestión de Indicadores**: se detallan los indicadores que la empresa utilizará para comprobar el funcionamiento y la eficacia de las medidas de seguridad tomadas. Véase el Anexo 5.
- **Procedimiento de Revisión por la Dirección**: según la norma ISO/IEC 27001, la dirección debe revisar periódicamente el SGSI para verificar su funcionamiento y evaluar si es necesario tomar medidas correctivas. Véase el Anexo 6.
- **Gestión de Roles y Responsabilidades**: la dirección debe asignar los roles y las responsabilidades para la gestión de la seguridad de la información, y comunicarlos a toda la organización. Véase el Anexo 7.
- **Metodología de Análisis de Riesgos**: la norma ISO/IEC 27001 no establece ninguna metodología obligatoria. Pudiendo elegir, la dirección de la empresa ha decidido seguir la metodología Magerit, actualmente en la versión 3: los detalles se encuentran en el Anexo 8
- **Declaración de Aplicabilidad**: es necesario especificar cuáles de los controles de la ISO/IEC 27002:2013 se deben aplicar al SGSI de la empresa (en este caso, todos menos el 14.2.7 – Externalización del desarrollo de software). Véase el Anexo 9.

6. Análisis de riesgos

El análisis de riesgos es el proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo. Es necesario en primer lugar identificar los elementos que componen esta "ecuación" (activos, amenazas y vulnerabilidades) para luego asignarles valores objetivos y repetibles a través de una combinación de sus consecuencias y su verosimilitud/probabilidad que expresa una magnitud.
La evaluación de riesgos es una de las partes clave del proyecto de cumplimiento de ISO 27001, y es necesario tener en cuenta el contexto, el activo y su valor (del que depende el impacto), la amenaza y su posibilidad o probabilidad, y las vulnerabilidades y su gravedad (o los controles de seguridad y su robustez).
Una vez calculado el nivel de riesgo, es necesario tomar decisiones (ponderación del riesgo) para abordarlo o tratarlo asumiendo medidas para prevenir o reducir su potencial impacto: se debe comparar los resultados del análisis de riesgo con respecto a los criterios de riesgo, para determinar si el riesgo es aceptable o

tolerable o, en caso contrario, cómo intervenir. El conjunto de todas las decisiones tomadas, riesgo a riesgo, es el Plan de Tratamiento de Riesgos.

6.1 Inventario de activos

El primer paso del análisis es, como dicho, la identificación de todos los activos relacionados con el alcance del SGSI: según la guía Magerit se define un activo como "componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos." [5]

En la siguiente tabla se listan los activos de la empresa relacionados con el alcance de la certificación, teniendo en cuenta que se han excluido del análisis unos ámbitos presentes en la metodología Magerit:

Ámbito	ID	Activo
Instalaciones [L]	L01	Sala de servidores del proveedor
	L02	Sala de servidores de la empresa
	L03	*Open space* de trabajo en la empresa
	L04	Laboratorio
	L05	Oficina del jefe de la empresa
	L06	Salas de visitas (3) en el departamento médico
Hardware [HW]	HW01	Servidores SQL (4)
	HW02	Servidores MySQL (2)
	HW03	Servidor Exchange
	HW04	Servidor repositorio ficheros
	HW05	Ordenadores (50)
	HW06	Laptop (250)
	HW07	Firewall
	HW08	Móviles (150)
Aplicación [SW]	SW01	S.O. Windows Server 2016
	SW02	S.O. Ubuntu
	SW03	S.O. Windows 11
	SW04	S.O. Windows 10
	SW05	S.O. Windows 7
	SW06	MS Office 365
	SW07	MS Office 2010
	SW08	MS Visual Studio 17
	SW09	Adobe Acrobat Professional
	SW10	ERP
	SW11	Aplicación WinForm
	SW12	Web App
	SW13	Antivirus Kaspersky
	SW14	SQL Management Studio
	SW15	MySQL Management

	SW16	Programas de backup
	SW17	S.O. Móviles - IOS
	SW18	S.O. Móviles - Android
Datos [D]	D01	Datos de las empresas clientes
	D02	Datos personales sensibles
	D03	Logs
	D04	Copias de seguridad de las bases de datos
	D05	Archivos de documentación
	D06	Código fuente
Red [COM]	COM01	Cableado eléctrico
	COM02	Cableado de telecomunicaciones
	COM03	Red inalámbrica
Servicios [S]	S01	Correo electrónico
	S02	Acceso web
	S03	VPN
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización
	AUX02	Sistema de detección de incendios
	AUX03	UPS
	AUX04	Extintores
Personal [P]	P01	Jefe de la empresa
	P02	Responsable IT
	P03	Otros empleados sector IT
	P04	Consultores
	P05	Médicos laborales
	P06	Empleados administrativos

Tabla 1: Análisis de los activos

6.2 Valoración de los activos

Es necesario asignar un valor a los activos identificados anteriormente: no se trata de una valoración de su coste, sino de cuánto se puede prescindir de un activo y cuánto es necesario protegerlo. La metodología Magerit define esta valoración como "la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo". [6]

Hay que tener en cuenta diferentes factores, del coste de adquisición e instalación, al coste para recuperar la información, a las pérdidas por no disponer del activo, las sanciones (legislativas o por incumplimiento de contratos), daño a otros activos, daño a la imagen de la empresa…

Para su valoración, los activos se han clasificado utilizando la escala sugerida por Magerit (libro 3, Guía de técnicas, pág. 6):

VALOR	Criterio
MB	Muy Bajo
B	Bajo
M	Medio
A	Alto
MA	Muy Alto

Para facilitar la lectura del documento, no se propone una tabla específica para la valoración de los activos sino se pondrá el valor en la tabla resumen de valoración presente en el subcapítulo 6.4.

6.3 Dimensiones de seguridad

Es necesario, para cada activo, indicar también cuál es el aspecto de la seguridad más crítico, para poder enfocar en este la atención y las posibles salvaguardias. Hay que tener en cuenta todas las cinco dimensiones de la seguridad:

- Autenticidad [A]: permite garantizar la fuente de los datos o que una entidad sea efectivamente quien dice ser. Es una valoración típica de servicios y datos.
- Confidencialidad [C]: la información no debe ser puesta a disposición de quien no es autorizado (usuarios, entidades, procesos…)
- Integridad [I]: la información no debe alterarse sin autorización
- Disponibilidad [D]: el activo debe estar a disposición de los autorizados cuando lo necesitan
- Trazabilidad [T]: las actuaciones de una entidad deben poder ser atribuidas solo a esta.

En este caso, para la valoración del perjuicio sufrido por la empresa si cada activo se daña en cada una de estas dimensiones, se utilizará una escala de valoración de diez valores estructurada de la siguiente manera:

VALOR	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Por supuesto cada activo no debe ser considerado como una entidad totalmente independiente de las otras (y siempre “muy importante”), sino será necesario tener en cuenta la cadena de valor del servicio ofrecido.

6.4 Tabla resumen de valoración

Conformemente a las definiciones anteriores y a las escalas elegidas, se puede construir una tabla de valoración de los activos:

Ámbito	ID	Activo	Valor	Dimensiones de seguridad				
				A	C	I	D	T
Instalaciones [L]	L01	Sala de servidores del proveedor	MA	0	9	7	9	0
	L02	Sala de servidores de la	A	0	7	6	7	0
	L03	*Open space* en la empresa	B	0	3	3	2	0
	L04	Laboratorio	MB	0	3	0	1	0
	L05	Oficina del jefe de la empresa	MB	0	3	0	1	0
	L06	Salas de visitas (3) dep. médico	B	0	6	0	2	0

Hardware [HW]	HW01	Servidores SQL (4)	MA	8	9	8	8	8
	HW02	Servidores MySQL (2)	MA	8	9	8	8	8
	HW03	Servidor Exchange	M	7	8	6	4	3
	HW04	Servidor repositorio ficheros	A	7	9	8	7	5
	HW05	Ordenadores (50)	B	6	7	3	3	6
	HW06	Laptop (250)	M	6	7	3	3	6
	HW07	Firewall	M	7	7	6	8	7
	HW08	Móviles (150)	B	6	7	6	2	5
Aplicación [SW]	SW01	S.O. Windows Server 2016	MA	8	5	6	9	6
	SW02	S.O. Ubuntu	MA	8	5	6	8	6
	SW03	S.O. Windows 11	B	4	4	4	5	4
	SW04	S.O. Windows 10	B	4	4	4	5	4
	SW05	S.O. Windows 7	B	4	4	4	5	4
	SW06	MS Office 365	B	1	6	4	1	1
	SW07	MS Office 2010	MB	1	6	4	1	1
	SW08	MS Visual Studio 17	A	6	7	7	8	7
	SW09	Adobe Acrobat Professional	B	4	7	4	3	3
	SW10	ERP	M	6	9	8	7	6
	SW11	Aplicación WinForm	MA	8	9	9	7	6
	SW12	Web App	MA	8	9	8	7	6
	SW13	Antivirus Kaspersky	M	8	5	8	8	4
	SW14	SQL Management Studio	A	6	7	6	8	5
	SW15	MySQL Management	A	6	7	6	8	5
	SW16	Programas de backup	MA	8	9	8	7	5
	SW17	S.O. Móviles - IOS	B	3	4	4	3	3
	SW18	S.O. Móviles - Android	B	3	4	4	3	3
Datos [D]	D01	Datos de las empresas clientes	MA	8	9	8	7	6
	D02	Datos personales sensibles	MA	8	9	8	7	6
	D03	Logs	M	5	5	6	5	5
	D04	Copias de seguridad de las BD	MA	7	8	8	7	5
	D05	Archivos de documentación	MA	5	8	7	7	5
	D06	Código fuente	MA	8	7	8	6	7
Red [COM]	COM01	Cableado eléctrico	MA	0	0	8	9	0
	COM02	Cableado de telecomunicaciones	MA	0	0	8	9	0
	COM03	Red inalámbrica	M	0	0	7	7	0
Servicios [S]	S01	Correo electrónico	M	6	8	7	5	3
	S02	Acceso web	MA	6	9	8	8	7
	S03	VPN	MA	8	9	8	9	7
Equipamiento auxiliar [AUX]	AUX01	Sistema de climatización	MA	0	0	7	8	0
	AUX02	Sistema de detección de	MA	0	0	8	7	0
	AUX03	UPS	MA	0	0	9	8	0
	AUX04	Extintores	M	0	0	7	8	0
Personal [P]	P01	Jefe de la empresa	B	0	0	0	2	0
	P02	Responsable IT	A	0	0	0	6	0
	P03	Otros empleados sector IT	A	0	0	0	8	0

	P04	Consultores	MA	0	0	0	7	0
	P05	Médicos laborales	A	0	0	0	7	0
	P06	Empleados administrativos	MB	0	0	0	1	0

6.5 Análisis de amenazas

Es necesario identificar las amenazas a las cuales los activos identificados anteriormente están expuestos: estas, según la metodología Magerit (libro 2, capítulo 5) se pueden típicamente dividir en:

- Desastres naturales [N]: ocurren sin intervención humana (directa o indirecta), por ejemplo terremotos o inundaciones
- De origen industrial [I]: consecuencias de la actividad industrial humana, pueden ser accidentales o deliberados
- Errores y fallos no intencionados [E]: causados por las personas
- Ataques intencionados [A]: causados intencionalmente por las personas

De todas las amenazas identificadas es también necesario especificar la probabilidad de su ocurrencia: para eso se utiliza la escala de medición de la frecuencia que aparece en el libro 1 de Magerit, pág. 28:

VALOR	Probabilidad	Frecuencia	Cálculo
MA	Muy frecuente	A diario	1
A	Frecuente	Mensualmente	0,071
M	Normal	Una vez al año	0,016
B	Poco frecuente	Cada varios años	0,005
MB	Muy poco frecuente	Siglos	0,002

Y, para cada dimensión de los activos es necesario determinar el impacto que tendría la materialización de la amenaza, es decir la degradación del mismo activo:

VALOR	Impacto
100%	Muy Alto
75%	Alto
50%	Medio
20%	Bajo
5%	Muy Bajo

A continuación se muestra el resumen del impacto máximo de las amenazas sobre las dimensiones de seguridad de los ámbitos de los activos examinados:

Activos	**Dimensiones de seguridad**				
	A	**C**	**I**	**D**	**T**
[L] Instalaciones		20%	5%	100%	
[HW] Hardware		75%	100%	20%	
[SW] Aplicación	75%	100%	75%	75%	
[D] Datos	75%	100%	100%	100%	100%
[COM] Red	5%	75%	20%	75%	
[S] Servicios	75%	100%	100%	100%	75%
[AUX] Equipamiento		75%	20%	100%	
[P] Personal		75%	75%	75%	

El resultado completo de este análisis se puede encontrar en el Anexo 10.

6.6 Impacto potencial

Utilizando los resultados de los análisis anteriores, se pueden combinar las valoraciones de los activos con aquellas del impacto de las amenazas para obtener el impacto potencial de las consecuencias de la materialización de dichas amenazas sobre la empresa:

Impacto potencial = Valoración del activo * Valoración del impacto de la amenaza

En este cálculo no se tienen en cuenta las posibles contramedidas existentes: todavía su valor es relevante porque permite priorizar el plan de acción. En la tabla siguiente se puede observar el resultado obtenido:

Ámbito	ID	Activo	Impacto potencial				
			A	C	I	D	T
Instalaciones [L]	L01	Sala de servidores del proveedor	0,00	1,80	0,35	9,00	0,00
	L02	Sala de servidores de la empresa	0,00	1,40	0,30	7,00	0,00
	L03	Open space en la empresa	0,00	0,60	0,15	2,00	0,00
	L04	Laboratorio	0,00	0,60	0,00	1,00	0,00
	L05	Oficina del jefe de la empresa	0,00	0,60	0,00	1,00	0,00
	L06	Salas de visitas (3) dep. médico	0,00	1,20	0,00	2,00	0,00
Hardware [HW]	HW01	Servidores SQL (4)	0,00	6,75	1,60	8,00	0,00
	HW02	Servidores MySQL (2)	0,00	6,75	1,60	8,00	0,00
	HW03	Servidor Exchange	0,00	6,00	1,20	4,00	0,00
	HW04	Servidor repositorio ficheros	0,00	6,75	1,60	7,00	0,00
	HW05	Ordenadores (50)	0,00	5,25	0,60	3,00	0,00
	HW06	Laptop (250)	0,00	5,25	0,60	3,00	0,00
	HW07	Firewall	0,00	5,25	1,20	8,00	0,00
	HW08	Móviles (150)	0,00	5,25	1,20	2,00	0,00
Aplicación [SW]	SW01	S.O. Windows Server 2016	6,00	5,00	4,50	6,75	0,00
	SW02	S.O. Ubuntu	6,00	5,00	4,50	6,00	0,00
	SW03	S.O. Windows 11	3,00	4,00	3,00	3,75	0,00
	SW04	S.O. Windows 10	3,00	4,00	3,00	3,75	0,00
	SW05	S.O. Windows 7	3,00	4,00	3,00	3,75	0,00
	SW06	MS Office 365	0,75	6,00	3,00	0,75	0,00
	SW07	MS Office 2010	0,75	6,00	3,00	0,75	0,00
	SW08	MS Visual Studio 17	4,50	7,00	5,25	6,00	0,00
	SW09	Adobe Acrobat Professional	3,00	7,00	3,00	2,25	0,00
	SW10	ERP	4,50	9,00	6,00	5,25	0,00
	SW11	Aplicación WinForm	6,00	9,00	6,75	5,25	0,00
	SW12	Web App	6,00	9,00	6,00	5,25	0,00
	SW13	Antivirus Kaspersky	6,00	5,00	6,00	6,00	0,00
	SW14	SQL Management Studio	4,50	7,00	4,50	6,00	0,00
	SW15	MySQL Management	4,50	7,00	4,50	6,00	0,00
	SW16	Programas de backup	6,00	9,00	6,00	5,25	0,00
	SW17	S.O. Móviles - IOS	2,25	4,00	3,00	2,25	0,00
	SW18	S.O. Móviles - Android	2,25	4,00	3,00	2,25	0,00
Datos [D]	D01	Datos de las empresas clientes	6,00	9,00	8,00	7,00	6,00
	D02	Datos personales sensibles	6,00	9,00	8,00	7,00	6,00
	D03	Logs	3,75	5,00	6,00	5,00	5,00
	D04	Copias de seguridad de las BD	5,25	8,00	8,00	7,00	5,00

	D05	Archivos de documentación	3,75	8,00	7,00	7,00	5,00
	D06	Código fuente	6,00	7,00	8,00	6,00	7,00
Red [COM]	COM01	Cableado eléctrico	0,00	0,00	1,60	6,75	0,00
	COM02	Cableado de telecomunicaciones	0,00	0,00	1,60	6,75	0,00
	COM03	Red inalámbrica	0,00	0,00	1,40	5,25	0,00
Servicios [S]	S01	Correo electrónico	4,50	8,00	7,00	5,00	2,25
	S02	Acceso web	4,50	9,00	8,00	8,00	5,25
	S03	VPN	6,00	9,00	8,00	9,00	5,25
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización	0,00	0,00	1,40	8,00	0,00
	AUX02	Sistema de detección de incendios	0,00	0,00	1,60	7,00	0,00
	AUX03	UPS	0,00	0,00	1,80	8,00	0,00
	AUX04	Extintores	0,00	0,00	1,40	8,00	0,00
Personal [P]	P01	Jefe de la empresa	0,00	0,00	0,00	0,40	0,00
	P02	Responsable IT	0,00	0,00	0,00	1,20	0,00
	P03	Otros empleados sector IT	0,00	0,00	0,00	1,60	0,00
	P04	Consultores	0,00	0,00	0,00	1,40	0,00
	P05	Médicos laborales	0,00	0,00	0,00	1,40	0,00
	P06	Empleados administrativos	0,00	0,00	0,00	0,20	0,00

La tabla completa del cálculo de impacto potencial aparece el Anexo 11.

6.7 Nivel de riesgo aceptable y Riesgo residual

El último paso del análisis de riesgos es la definición de un límite de aceptación de un riesgo para cada activo: si el nivel de riesgo lo supera, será necesario intervenir para intentar reducirlo. Todavía, aunque aplicando todas las contramedidas posibles, el riesgo nunca desaparecerá sino seguirá existiendo, aunque en un nivel menor: este es el riesgo residual.
Para cada uno de los activos se calculará:

Riesgo = Impacto potencial * Frecuencia de la amenaza

Y se clasificará utilizando la ya vista escala de valores entre Muy Alto y Muy Bajo según la siguiente tabla:

Riesgo		Frecuencia				
		MB (0,002)	B (0,005)	M (0,016)	A (0,071)	MA (1)
Impacto	MA (10)	A	MA	MA	MA	MA
	A (7-9)	M	A	A	MA	MA
	M (4-6)	B	M	M	A	A
	B (2-3)	MB	B	B	M	M
	MB (1)	MB	MB	MB	B	B

El resultado completo es consultable en el Anexo 12.

La dirección ha decidido que el nivel aceptable de riesgo es Medio: esto significa que será necesario introducir controles para reducir todos los riesgos de nivel alto o muy alto. Todas las amenazas cuyo nivel sea medio o inferior para los diferentes activos no constituyen, por ahora, una amenaza a la empresa.

Consecuentemente, los activos cuyo riesgo supera el nivel considerado aceptable, y para los cuales será necesario establecer contramedidas para reducirlo, son:

Ámbito	ID	Activo	Nivel de Riesgo A	C	I	D	T
Instalaciones [L]	L01	Sala de servidores del proveedor	B	B	B	MA	B
	L02	Sala de servidores de la empresa	B	B	B	MA	B
Hardware [HW]	HW01	Servidores SQL (4)	B	A	B	MA	B
	HW02	Servidores MySQL (2)	B	A	B	MA	B
	HW04	Servidor repositorio ficheros	B	A	B	MA	B
	HW07	Firewall	MB	M	MB	A	MB
Aplicación [SW]	SW01	S.O. Windows Server 2016	A	A	A	A	B
	SW02	S.O. Ubuntu	A	A	A	A	B
	SW08	MS Visual Studio 17	A	MA	A	A	B
	SW09	Adobe Acrobat Professional	B	A	B	B	MB
	SW10	ERP	M	A	M	M	MB
	SW11	Aplicación WinForm	A	MA	A	A	B
	SW12	Web App	A	MA	A	A	B
	SW14	SQL Management Studio	A	MA	A	A	B
	SW15	MySQL Management	A	MA	A	A	B
	SW16	Programas de backup	A	MA	A	A	B
Datos [D]	D01	Datos de las empresas clientes	A	MA	MA	MA	A
	D02	Datos personales sensibles	A	MA	MA	MA	A
	D04	Copias de seguridad de las BD	A	MA	MA	MA	A
	D05	Archivos de documentación	M	MA	MA	MA	A
	D06	Código fuente	A	MA	MA	A	MA
Red [COM]	COM01	Cableado eléctrico	B	B	B	A	B
	COM02	Cableado de telecomunicaciones	B	B	B	A	B
Servicios [S]	S01	Correo electrónico	M	A	A	M	B
	S02	Acceso web	A	MA	MA	MA	A
	S03	VPN	A	MA	MA	MA	A
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización	B	B	B	MA	B
	AUX02	Sistema de detección de incendios	B	B	B	MA	B
	AUX03	UPS	B	B	B	MA	B
	AUX04	Extintores	MB	MB	MB	A	MB

Se puede observar que aparecen muchos riesgos con un nivel alto o muy alto: dado que no es posible reducirlos todos en una vez, será necesario priorizar las intervenciones empezando con aquellos activos que tienen un riesgo muy elevado en varias dimensiones, siguiendo luego con aquellos que tienen el mismo nivel pero en una sola dimensión, y finalmente, de la misma manera, considerando los activos que tienen niveles de riesgo “alto”.

7. Propuestas de proyecto

El análisis de riesgo ha permitido obtener una visión completa y exacta de la situación corriente de la empresa, con el riesgo actual de cada activo. Basándose en esto, es necesario presentar los proyectos que permitirán mejorar el estado de seguridad de la información.
Los proyectos se han dividido según su ámbito de pertenencia; en las tablas de resumen, de cada activo se indicarán el objetivo, la descripción, los riesgos relacionados y los activos cuyos riesgos serán reducidos, las dimensiones de seguridad relacionadas, el responsable, la prioridad, el plazo esperado de implementación y el coste.

7.1 Propuestas de ámbito organizativo

Proyecto 01 – Implementación de políticas de seguridad de la información	
OBJETIVO	Formalizar la política de seguridad de la información de la empresa
DESCRIPCIÓN	Es necesario formalizar y documentar todos los procedimientos actualmente informales, definiendo roles, responsabilidades, procesos, así como clasificar la información. Esto no tiene una consecuencia directa sobre la disminución de los riesgos, pero es la base para una gestión correcta. Se establecerán también las auditorías externas necesarias para la optimización de política y procedimientos. Será necesario revisar anualmente la política y su cumplimiento por parte de la dirección.
RIESGOS	-
DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Trazabilidad
ACTIVOS	Todos
CONTROLES ISO27002	A.5, A.6, A.8, A.12.7, A.18.1, A.18.2
RESPONSABLE	CEO de la empresa
PRIORIDAD	Muy Alta
PLAZO IMPLEMENTACIÓN	1 mes
COSTE	2500 € (coste del personal interno) 2000 € (coste del consultor)
INDICADORES	01 - Políticas de seguridad 02 - Roles y responsabilidades 24 - Revisiones internas

Proyecto 02 – Implementación de un plan de gestión de incidentes de seguridad	
OBJETIVO	Establecer los procedimientos de notificación y las actuaciones para resolver los incidentes de seguridad de manera rápida y eficaz.
DESCRIPCIÓN	Es necesario establecer responsabilidades y procedimientos (con su documentación) de gestión de los incidentes de seguridad: todos deben saber quién debe hacer qué, definiendo las responsabilidades de cada persona y las actuaciones que le corresponden. Es necesario también guardar todas las informaciones de los incidentes ocurridos, para que puedan ser consultadas para aprender y estudiar posibles mejorías.
RIESGOS	[E.7] Deficiencias en la organización [E.19] Fugas de información

DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Disponibilidad
ACTIVOS	Todos
CONTROLES ISO27002	A.16
RESPONSABLE	Responsable SGSI
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	1 mes
COSTE	2000 € (coste del responsable del SGSI) 2000 € (coste del consultor)
INDICADORES	20 - Eventos de seguridad 21 - Puntos débiles de seguridad

Proyecto 03 – Política de gestión de los activos	
OBJETIVO	Conocer y controlar todos los activos de la empresa
DESCRIPCIÓN	Es necesario comprobar que todos los activos sean inventariados, asignar un responsable a cada activo, documentar las normas de uso y los procedimientos para su correcta eliminación
RIESGOS	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (sw) [E.23] Errores de mantenimiento / actualización de equipos (hw) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.13] Repudio [A.22] Manipulación de programas [A.23] Manipulación de los equipos [A.25] Robo
DIM. DE SEGURIDAD	Confidencialidad, Integridad, Disponibilidad
ACTIVOS	Todos HW, SW, Datos
CONTROLES ISO27002	A.8.1, A.8.3, A.11.2.5, A.11.2.7
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	2 semanas
COSTE	1000 € (coste del personal interno)
INDICADORES	06 - Inventario de activos 07 - Propiedad de activos 08 - Devolución de activos 09 - Eliminación de soportes

Proyecto 04 – Política de gestión de las relaciones con los proveedores	
OBJETIVO	Comprobar que la relación con los proveedores sea suficientemente segura.
DESCRIPCIÓN	Es necesario comprobar los acuerdos con los proveedores, que estos tengan requisitos de seguridad suficientes, así como establecer y documentar los procedimientos para gestionar el intercambio de información y eventuales cambios en la provisión del servicio
RIESGOS	[E.3] Errores de monitorización (log) [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 (software) [E.21] Errores de mantenimiento / actualización de programas (sw) [E.23] Errores de mantenimiento / actualización de equipos (hw) [E.24] Caída del sistema por agotamiento de recursos [A.3] Manipulación de los registros de actividad (log) [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [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.29] Extorsión [A.30] Ingeniería social
DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Disponibilidad, Trazabilidad
ACTIVOS	L01 - Sala de servidores del proveedor HW01 - Servidores SQL (4) HW02 - Servidores MySQL (2) SW - Todos D01 - Datos de las empresas clientes D02 - Datos personales sensibles D03 - Logs D04 - Copias de seguridad de las BD D05 - Archivos de documentación COM01 - Cableado eléctrico COM02 - Cableado de telecomunicaciones COM03 - Red inalámbrica S01 - Correo electrónico S02 - Acceso web

	S03 - VPN AUX01 - Sistema de climatización AUX02 - Sistema de detección de incendios AUX03 - UPS AUX04 - Extintores
CONTROLES ISO27002	A.15.1, A.15.2
RESPONSABLE	Responsable Administración de la empresa
PRIORIDAD	Baja
PLAZO IMPLEMENTACIÓN	1 mes
COSTE	2000 € (coste del responsable del SGSI) 2000 € (coste del consultor)
INDICADORES	19 - Proveedores

7.2 Propuestas de ámbito tecnológico

Proyecto 05 – Implementación de un plan de gestión de usuarios y permisos	
OBJETIVO	Establecer los derechos y permisos de cada usuario del sistema (consultación y modificación de informaciones, instalación o utilización de software…)
DESCRIPCIÓN	Es necesario documentar los procesos informales que se utilizan para la gestión de usuarios y permisos, comprobar que todos tengan asignados solo los permisos mínimos que le sirven para sus tareas, que no puedan acceder a la información o instalar software sin autorización. Es consecuentemente necesario establecer en el mismo plan un procedimiento para gestionar los cambios de roles y responsabilidades de los usuarios dentro la empresa, cambios que deben reflejarse en los cambios de autorizaciones.
RIESGOS	[E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización
DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Trazabilidad
ACTIVOS	Todos HW, SW, Datos
CONTROLES ISO27002	A.9.1, A.9.2, A.9.3, A.9.4
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	1 mes
COSTE	1500 € (coste del personal interno) 1000 € (coste del consultor)
INDICADORES	10 - Accesos no autorizados 11 - Derechos de acceso

Proyecto 06 – Implementación de un plan de instalación de software	
OBJETIVO	Todos los equipos deben tener solo software autorizado y actualizado.
DESCRIPCIÓN	Se deben establecer y documentar procedimientos y mecanismos de control para que solo los administradores puedan instalar software y lo actualicen, y para que todos los equipos dispongan de programas de seguridad (por ejemplo antivirus). Además es necesario establecer mecanismos para comprobar si existen nuevas actualizaciones de software utilizado, evaluarlas y eventualmente instalarlas.

RIESGOS	[E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización [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.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [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.24] Denegación de servicio
DIM. DE SEGURIDAD	Confidencialidad, Integridad, Disponibilidad
ACTIVOS	HW – todos SW – todos D – todos P - todos
CONTROLES ISO27002	A.12.2, A.12.5, A.12.6
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	1 mes
COSTE	1500 € (coste del personal interno)
INDICADORES	15 - Protección de los sistemas 16 - Software malicioso 18 - Software no autorizado

Proyecto 07 – Implementación de protección criptográfica de los datos	
OBJETIVO	Cifrar los datos utilizados por las aplicaciones web y WinForm
DESCRIPCIÓN	Es necesario implantar controles criptográficos en los activos con información confidencial (se trata de los servidores SQL y mySQL, del servidor del archivo de ficheros y de los laptop) para protegerla. Se deberá establecer también el procedimiento para proteger los datos que deben ser transferidos. Finalmente se deberán establecer y documentar procedimientos para administrar las claves criptográficas y recuperar la información cifrada en caso de pérdida o daño de las mismas claves.
RIESGOS	[E.19] Fugas de información [E.25] Pérdida de equipos [A.11] Acceso no autorizado [A.19] Divulgación de información [A.23] Manipulación de los equipos [A.25] Robo
DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Trazabilidad
ACTIVOS	[D01] - Datos de las empresas clientes [D02] - Datos personales sensibles [D03] - Logs [D04] - Copias de seguridad de las BD [D05] - Archivos de documentación

CONTROLES ISO27002	A.10.1, A.12.2, A.13.2
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	2 meses
COSTE	4500 € (coste de los desarrolladores internos)
INDICADORES	12 - Cifrado de la información sensible

Proyecto 08 – Mejoría de los controles de seguridad	
OBJETIVO	Aunque unos controles son ya existentes, es necesario implementar nuevos después del análisis de riesgos hecho.
DESCRIPCIÓN	Se deben implementar nuevos controles relacionados con las criticidades que aparecen en el análisis de riesgos y que no eran gestionadas anteriormente, y comprobar la eficaz de aquellos ya existentes
RIESGOS	[I.5] Avería de origen físico o lógico [I.6] Corte del 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 [E.4] Errores de configuración [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [A.11] Acceso no autorizado [A.22] Manipulación de programas [A.23] Manipulación de los equipos [A.24] Denegación de servicio [A.25] Robo
DIM. DE SEGURIDAD	Autenticidad, Confidencialidad, Integridad, Disponibilidad, Trazabilidad
ACTIVOS	[L01] - Sala de servidores del proveedor [L02] - Sala de servidores de la empresa Hardware [HW] - Todos Aplicación [SW] - Todas Datos [D] - Todos Servicios [S] - Todos Equipamiento auxiliar [AUX] - Todos
CONTROLES ISO27002	A.12.2, A.12.5, A.12.6, A.13.1, A.14.1
RESPONSABLE	Responsable SGSI
PRIORIDAD	Media
PLAZO IMPLEMENTACIÓN	2 meses
COSTE	2.000 € Técnicos de la empresa 3.000 € Auditor externo
INDICADORES	10 - Accesos no autorizados 11 - Derechos de acceso 13 - Protección física 14 - Interrupciones del suministro eléctrico 15 - Protección de los sistemas 16 - Software malicioso 18 - Software no autorizado 20 - Eventos de seguridad 21 - Puntos débiles de seguridad 23 - Software licenciado

Proyecto 09 – Plan de desarrollo de código seguro	
OBJETIVO	Establecer un entorno seguro para el desarrollo de código.
DESCRIPCIÓN	Es necesario definir (y documentar, por supuesto) un procedimiento para el desarrollo de código en un entorno seguro. Una vez establecidos los requerimientos, se deberá prepararlo e implantar controles para comprobar la seguridad del entorno, su correcta utilización por los desarrolladores y la protección de los datos utilizados para las pruebas.
RIESGOS	[E.4] Errores de configuración [E.8] Difusión de software dañino [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos
DIM. DE SEGURIDAD	Confidencialidad, Integridad, Disponibilidad
ACTIVOS	[HW01] - Servidores SQL [HW02] - Servidores MySQL [HW04] - Servidor repositorio ficheros [HW05] – Ordenadores [SW01] - S.O. Windows Server 2016 [SW02] - S.O. Ubuntu [SW08] - MS Visual Studio 17 [SW11] - Aplicación WinForm [SW12] - Web App [SW14] - SQL Management Studio [SW15] - MySQL Management [D01] - Datos de las empresas clientes [D02] - Datos personales sensibles [D03] - Logs [D06] - Código fuente [P02] - Responsable IT [P03] - Otros empleados sector IT
CONTROLES ISO27002	A.12.1, A.12.2, A.12.4, A.14.2, A.14.3
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	2 meses
COSTE	1500 € (Coste de un técnico de la empresa) 5000 € (Coste de la preparación del entorno)
INDICADORES	11 - Derechos de acceso 20 - Eventos de seguridad

Proyecto 10 – Plan de continuidad de negocio	
OBJETIVO	Definir y documentar un plan de protección de activos y actividades críticas de la empresa, que permita restablecer el funcionamiento normal en un plazo aceptable en caso de la materialización de un desastre.
DESCRIPCIÓN	Se definirá un plan de actuación que, a través de la identificación de

	los procesos más críticos, y de los activos relacionados, detalle los pasos a seguir en caso de desastre para restablecer la operatividad de la empresa. Este plan deberá revisarse periódicamente (como mínimo una vez al año) para mejorarlo y adaptarlo.
RIESGOS	[N] Desastres naturales - Todos [I] De origen industrial – Todos [E.8] Difusión de software dañino [E.15] Alteración accidental de la información [E.18] Destrucción de información [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.24] Denegación de servicio [A.25] Robo [A.26] Ataque destructivo [A.27] Ocupación enemiga
DIM. DE SEGURIDAD	Disponibilidad
ACTIVOS	[HW01] Servidores SQL [HW02] Servidores MySQL [HW03] Servidor Exchange [HW04] Servidor repositorio ficheros [HW05] Ordenadores [HW07] Firewall [SW01]- S.O. Windows Server 2016 [SW02]- S.O. Ubuntu [SW03]- S.O. Windows 11 [SW04]- S.O. Windows 10 [SW05]- S.O. Windows 7 [SW08]- MS Visual Studio 17 [SW10]- ERP [SW11]- Aplicación WinForm [SW12]- Web App [SW17]- S.O. Móviles - IOS [SW18]- S.O. Móviles - Android [D01] Datos de las empresas clientes [D02] Datos personales sensibles [D03] Logs [D05] Archivos de documentación [S02] Acceso web [S03] VPN [AUX03] Todos
CONTROLES ISO27002	A.12.3, A.17
RESPONSABLE	Responsable IT
PRIORIDAD	Alta
PLAZO IMPLEMENTACIÓN	3 semanas (iniciales); seguimiento continuo.
COSTE	2.000 € (coste del responsable IT) 2.000 € (coste de otros técnicos IT)
INDICADORES	13 - Protección física 14 - Interrupciones del suministro eléctrico 17 - Backup 22 - Continuidad de negocio

Proyecto 11 – Control del estado de los UPS	
OBJETIVO	Comprobar la eficiencia de los sistemas de alimentación interrumpida
DESCRIPCIÓN	Se harán pruebas, cada 6 meses, para comprobar el correcto funcionamiento de los UPS y que los equipos sean correctamente conectados con estos.
RIESGOS	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales
DIM. DE SEGURIDAD	Disponibilidad, Integridad
ACTIVOS	[HW01] Servidores SQL [HW02] Servidores MySQL [HW03] Servidor Exchange [HW04] Servidor repositorio ficheros [HW05] Ordenadores [HW07] Firewall SW – Todos aquellos implantados en los hw mencionados [D01] Datos de las empresas clientes [D02] Datos personales sensibles [D03] Logs [D05] Archivos de documentación S02] Acceso web [S03] VPN [AUX03] UPS
CONTROLES ISO27002	-
RESPONSABLE	Responsable del equipo técnico de la empresa
PRIORIDAD	Baja (los sistemas ya existen)
PLAZO IMPLEMENTACIÓN	4 horas
COSTE	El coste de medio día laboral de un técnico de la empresa
INDICADORES	14 - Interrupciones del suministro eléctrico

7.3 Propuestas de ámbito RRHH

Proyecto 12 – Mejorar la gestión de los recursos humanos	
OBJETIVO	Mejorar la gestión de los empleados de la empresa desde la contratación hasta el despido.
DESCRIPCIÓN	Se deben definir los términos y cláusulas a incluir en los contratos de empleo, definir la política de investigación de antecedentes, lo que se debe hacer cuando un empleado termina su colaboración con la empresa, y finalmente establecer las sanciones de las violaciones de la política de seguridad (establecida anteriormente gracias al proyecto 01). La gestión de los derechos de acceso y de los permisos está ya incluida en el proyecto 05.
RIESGOS	[E.19] Fugas de información [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.11] Acceso no autorizado [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.25] Robo [A.28] Indisponibilidad del personal [A.29] Extorsión
DIM. DE SEGURIDAD	Confidencialidad
ACTIVOS	[P02] - Responsable IT [P03] - Otros empleados sector IT [P04] - Consultores [P05] - Médicos laborales [P06] - Empleados administrativos
CONTROLES ISO27002	A.7.1, A.7.2, A.7.3
RESPONSABLE	Responsable RRHH de la empresa
PRIORIDAD	Baja
PLAZO IMPLEMENTACIÓN	3 semanas
COSTE	1500 € (coste del personal interno) 800 € (coste del consultor)
INDICADORES	03 - Antecedentes de los nuevos empleados

Proyecto 13 – Plan de formación del personal	
OBJETIVO	Formar los empleados para que tengan conocimientos de seguridad, puedan entender las políticas de la empresa y conozcan los comportamientos a tener.
DESCRIPCIÓN	Se debe hacer formación al personal sobre la seguridad, los comportamientos a tener al interior y al exterior de la empresa, el mantenimiento de los activos, la transferencia de datos. Los empleados deberán también saber a quién contactar en caso de problemas. Se trata de un procedimiento continuo.
RIESGOS	[E.19] Fugas de información [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [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.25] Robo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social
DIM. DE SEGURIDAD	Confidencialidad, Disponibilidad
ACTIVOS	[P02] - Responsable IT [P03] - Otros empleados sector IT [P04] - Consultores [P05] - Médicos laborales [P06] - Empleados administrativos
CONTROLES ISO27002	A.7.2, A.11.2, A.13.2
RESPONSABLE	Responsable SGSI + Responsable del área formativa de la empresa
PRIORIDAD	Baja

PLAZO IMPLEMENTACIÓN	Continuo
COSTE	Variable, dependiendo de la formación necesaria. Aproximadamente 80 € por 4 horas de formación de cada empleado.
INDICADORES	04 - Eficacia de la formación 05 - Disciplina

7.4 Otras propuestas

Proyecto 14a – Fortalecimiento contra amenazas físicas y ambientales / Proveedor	
OBJETIVO	Mejorar la protección contra amenazas físicas, ambientales y desastres de origen industrial
DESCRIPCIÓN	Comprobar periódicamente y eventualmente sustituir los extintores, el sistema de alarma contra incendios y el sistema de aire acondicionado de la sala servidores; comprobar la protección física de los lugares.
RIESGOS	[N.1] Fuego; [N.2] Daños por agua [I.1] Fuego; [I.2] Daños por agua; [I.7] Condiciones inadecuadas de temperatura o humedad [E.18] Destrucción de información [A.18] Destrucción de información; [A.24] Denegación de servicio; [A.26] Ataque destructivo
DIM. DE SEGURIDAD	Disponibilidad
ACTIVOS	[L01] Sala de servidores del proveedor [HW01] Servidores SQL [HW02] Servidores MySQL [SW01] S.O. Windows server 2016 [SW02] S.O. Ubuntu [SW12] Web App [SW16] Programas de backup [D01] Datos de las empresas clientes [D02] Datos personales sensibles [D03] Logs [D04] Copias de seguridad de las BD [COM01] Cableado eléctrico [COM02] Cableado de telecomunicaciones [S02] Acceso web [S03] VPN [AUX01] Sistema de climatización [AUX02] Sistema de detección de incendios [AUX03] UPS [AUX04] Extintores
CONTROLES ISO27002	A.11.1
RESPONSABLE	Responsable IT y Responsable del proveedor
PRIORIDAD	Baja
PLAZO IMPLEMENTACIÓN	1 semana (se trata solo de comprobar el estado); se repetirá anualmente.
COSTE	500 €: intervención de los técnicos 50 €: eventual sustitución de extintores
INDICADORES	13 - Protección física

Proyecto 14b – Fortalecimiento contra amenazas físicas y ambientales / Empresa	
OBJETIVO	Mejorar la protección contra amenazas físicas, ambientales y desastres de origen industrial

DESCRIPCIÓN	Comprobar periódicamente y eventualmente sustituir los extintores, el sistema de alarma contra incendios de la empresa y el sistema de aire acondicionado de la sala servidores; comprobar la protección física de los lugares.
RIESGOS	[N.1] Fuego; [N.2] Daños por agua [I.1] Fuego; [I.2] Daños por agua; [I.7] Condiciones inadecuadas de temperatura o humedad [E.18] Destrucción de información [A.18] Destrucción de información; [A.24] Denegación de servicio; [A.26] Ataque destructivo
DIM. DE SEGURIDAD	Disponibilidad
ACTIVOS	[L02] Sala de servidores de la empresa [L03] Open space en la empresa [L04] Laboratorio [L05] Oficina del jefe de la empresa [L06] Salas de visitas dep. médico [HW03] Servidor Exchange [HW04] Servidor repositorio ficheros [HW05] Ordenadores [HW06] Laptop [HW07] Firewall [HW08] Móviles [SW03-18] S.O. Windows, MS Office, Visual Studio, Adobe Acrobat, ERP, Aplicación WinForm, Antivirus, S.O. Móviles [D05] Archivos de documentación [D06] Código fuente [COM01] Cableado eléctrico [COM02] Cableado de telecomunicaciones [COM03] Red inalámbrica [S01] Correo electrónico [S02] Acceso web [S03] VPN [AUX01] Sistema de climatización [AUX02] Sistema de detección de incendios [AUX03] UPS [AUX04] Extintores
CONTROLES ISO27002	A.11.1
RESPONSABLE	Responsable IT
PRIORIDAD	Media
PLAZO IMPLEMENTACIÓN	2 semanas; se repetirá anualmente
COSTE	800 €: intervención de los técnicos 150 €: eventual sustitución de extintores
INDICADORES	13 - Protección física

7.5 Planificación

No todos los proyectos son secuenciales entre sí, y consecuentemente unos se pueden actuar contemporáneamente, dependiendo de la disponibilidad de los recursos (en particular aquellos internos).
El único proyecto realmente necesario para la implementación de todos los otros es el primero, la definición de la política de seguridad de la empresa: es decir que sin esta definición no tendría sentido implementar los otros proyectos y que, consecuentemente, es el primero que debe necesariamente realizarse. Otros proyectos, debido a sus características y a la amplia implicación de usuarios / empleados, no tienen una duración limitada, sino son continuativos. Un ejemplo de estos es la formación del personal: es necesario, por ejemplo, repetir periódicamente la formación sobre unos argumentos, y también es necesario dividir los empleados en pequeños grupos para asistir a los cursos, así que podría ser necesario planificar la misma formación durante unos meses para que todos puedan ser formados.
Se ha estudiado una planificación que pueda, en aproximadamente 10 meses, permitir a la empresa ejecutar los proyectos: se encuentra en el Anexo 12.

7.6 Resultados

La comparación completa de la situación antes y después de la ejecución de las propuestas se puede ver en el Anexo 13. Aquí aparece la comparación de los resúmenes de las valoraciones, con sus gráficos:

	Antes	Después
A.5 Information security policies	1	4
A.6 Organization of information security	1,7	4
A.7 Human resource security	0,5	4,5
A.8 Asset management	0,25	4,17
A.9 Access control	1,62	4,18
A.10 Cryptography	0	4
A.11 Physical and environmental security	2,42	3,64
A.12 Operations security	1,18	4,57
A.13 Communications security	0,58	4
A.14 System acquisition, development and maintenance	0,56	3,85
A.15 Supplier relationships	0	3,75
A.16 Information security incident management	0	4
A.17 Information security aspects of business continuity management	0	4
A.18 Compliance	0	4,43

Hay que destacar que, siendo muchos de los controles y procedimientos implementados correctamente por la primera vez, en los resultados se ha preferido asignar el valor “4- Gestionado” en vez que “5-Optimizado”: en efecto el autor cree que la optimización se podrá conseguir, en general, después de un

periodo de “rodaje” que permita a la empresa comprobar e implementar los ajustes necesarios que se requieren para adaptar la teoría a la práctica.
En cualquier caso el progreso es evidente, como se puede ver comparando los gráficos:

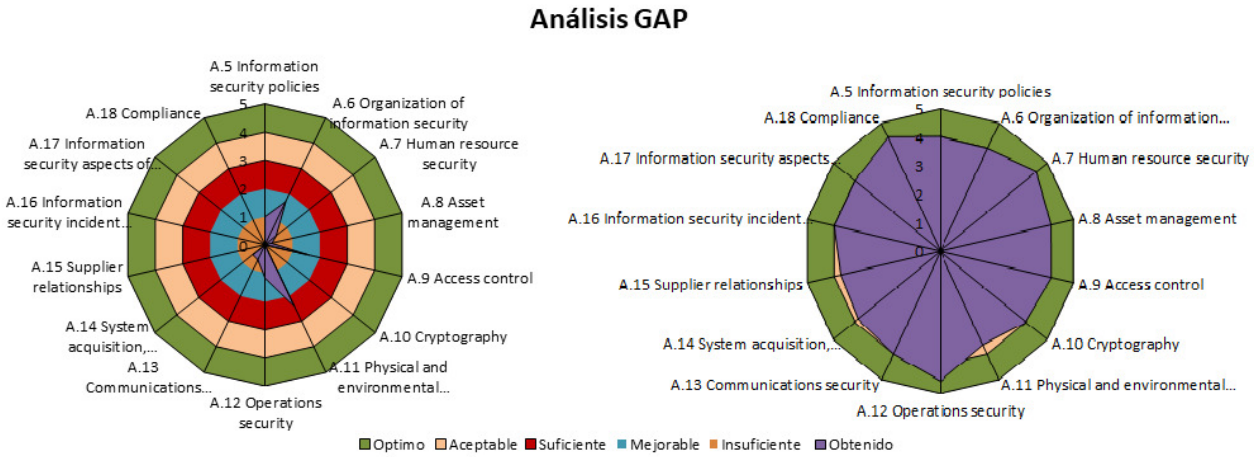


Imagen 7: Comparación del resultado del análisis GAP antes (a la izquierda) y después (a la derecha) de la ejecución de las propuestas de proyecto

8. Auditoría de cumplimiento

El objetivo de la auditoría es la evaluación del estado de la seguridad de la información de la empresa de servicios después de la realización de los proyectos propuestos: esto se hace evaluando los controles de la ISO/IEC 27002:2013.
Se evaluarán los 114 controles según la escala del modelo de madurez de la capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.

90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
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, se tienen 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.

8.1 Evaluación de la madurez ISO 27002

El resultado completo de la auditoría se puede ver en el Anexo 14. A continuación se muestra un resumen de las valoraciones obtenido atribuyendo a los diferentes niveles de los 114 controles el correspondiente valor en porcentaje de la tabla anterior:

CONTROL	VALOR CMM
A.5. Políticas de seguridad de la información	**100,00%**
A.5.1. Directrices de la dirección en seguridad de la información	100,00%
A.6. Organización de la seguridad de la información	**89,25%**
A.6.1. Organización interna	86,00%
A.6.2. Los dispositivos móviles y el teletrabajo	92,50%
A.7. Seguridad ligada a los recursos humanos	**96,11%**
A.7.1. Antes del empleo	95,00%
A.7.2. Durante el empleo	98,33%
A.7.3. Finalización del empleo o cambio en el puesto de trabajo	95,00%
A.8. Gestión de activos	**84,58%**
A.8.1. Responsabilidad sobre los activos	93,75%
A.8.2. Clasificación de la información	78,33%
A.8.3. Manejo de soportes de almacenamiento	81,67%
A.9. Control de acceso	**95,00%**
A.9.1. Requisitos de negocio para el control de acceso	97,50%
A.9.2. Gestión de acceso de usuario	87,50%
A.9.3. Responsabilidades de usuario	100,00%
A.9.4. Control de acceso a sistemas y aplicaciones	95,00%
A.10. Cifrado	**95,00%**
A.10.1. Controles criptográficos	95,00%
A.11. Seguridad física y ambiental	**71,94%**
A.11.1. Áreas seguras	78,33%
A.11.2. Seguridad de los equipos	65,56%
A.12. Seguridad en las operaciones	**88,39%**
A.12.1. Responsabilidades y procedimientos de operación	73,75%
A.12.2. Protección contra código malicioso	100,00%
A.12.3. Copias de seguridad	100,00%

A.12.4. Registro de actividad y supervisión	92,50%
A.12.5 control del software en explotación	100,00%
A.12.6 gestión de la vulnerabilidad técnica	52,50%
A.12.7. Consideraciones sobre las auditorías de los sistemas de información	100,00%
A.13. Seguridad de las comunicaciones	**68,96%**
A.13.1. Gestión de la seguridad en redes	66,67%
A.13.2. Intercambio de información con partes externas	71,25%
A.14. Adquisición, desarrollo y mantenimiento de sistemas	**91,81%**
A.14.1. Requisitos de seguridad de los sistemas de información	91,67%
A.14.2. Seguridad en los procesos de desarrollo y soporte	83,75%
A.14.3. Datos de prueba	100,00%
A.15. Relaciones con los proveedores	**71,25%**
A.15.1. Seguridad de la información en las relaciones con los proveedores	90,00%
A.15.2. Gestión de la prestación del servicio de los proveedores	52,50%
A.16. Gestión de incidentes de seguridad de la información	**91,43%**
A.16.1. Gestión de incidentes de seguridad de la información y mejoras	91,43%
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	**95,00%**
A.17.1. Continuidad de la seguridad de la información	100,00%
A.17.2. Redundancias	90,00%
A.18. Cumplimiento	**97,50%**
A.18.1. Cumplimiento de los requisitos legales y contractuales	95,00%
A.18.2. Revisiones de la seguridad de la información	100,00%

8.2 Evaluación de la madurez ISO 27001

El resultado completo de la auditoría se puede ver en el Anexo 15. A continuación se muestra un resumen de las valoraciones obtenido atribuyendo a los diferentes niveles de los controles el correspondiente valor en porcentaje de la tabla anterior:

	COONTROL ISO 27001	VALOR CMM
4	**Contexto de la organización**	**100,00%**
4,1	Comprensión de la organización y de su contexto	100,00%
4,2	Comprensión de las necesidades y expectativas de las partes interesadas	100,00%
4,3	Determinación del alcance del SGS	100,00%
4,4	SGSI	100,00%
5	**Liderazgo**	**100,00%**
5,1	Liderazgo y compromiso	100,00%
5,2	Política	100,00%
5,3	Roles, responsabilidades y autoridades en la organización	100,00%
6	**Planificación**	**95,42%**
6,1	Acciones para hacer frente a los riesgos y oportunidades	97,50%
6,2	Objetivos de seguridad de la información y planificación para conseguirlos	93,33%
7	**Soporte**	**90,30%**
7,1	Recursos	100,00%
7,2	Competencia	61,25%
7,3	Concienciación	100,00%
7,4	Comunicación	100,00%
7,5	Información documentada	90,24%

8	**Operación**	**97,92%**
8,1	Planificación y control	96,25%
8,2	Valoración de los riesgos de la seguridad de la información	100,00%
8,3	Tratamiento de los riesgos de la seguridad de la información	97,50%
9	**Evaluación**	**98,45%**
9,1	Seguimiento, medición, análisis y evaluación	97,50%
9,2	Auditoría interna	100,00%
9,3	Revisión por la dirección	97,86%
10	**Mejora**	**96,07%**
10,1	No conformidad y acciones correctivas	97,14%
10,2	Mejora continua	95,00%

8.3 Resultados

La auditoría ha entonces permitido evidenciar la ejecución del análisis de riesgo y el seguimiento de un plan de tratamiento correspondiente: el resultado está reflejado en el avance de implementación de los controles de seguridad.
En este subcapítulo se muestran las gráficas de los resultados de las evaluaciones anteriores:

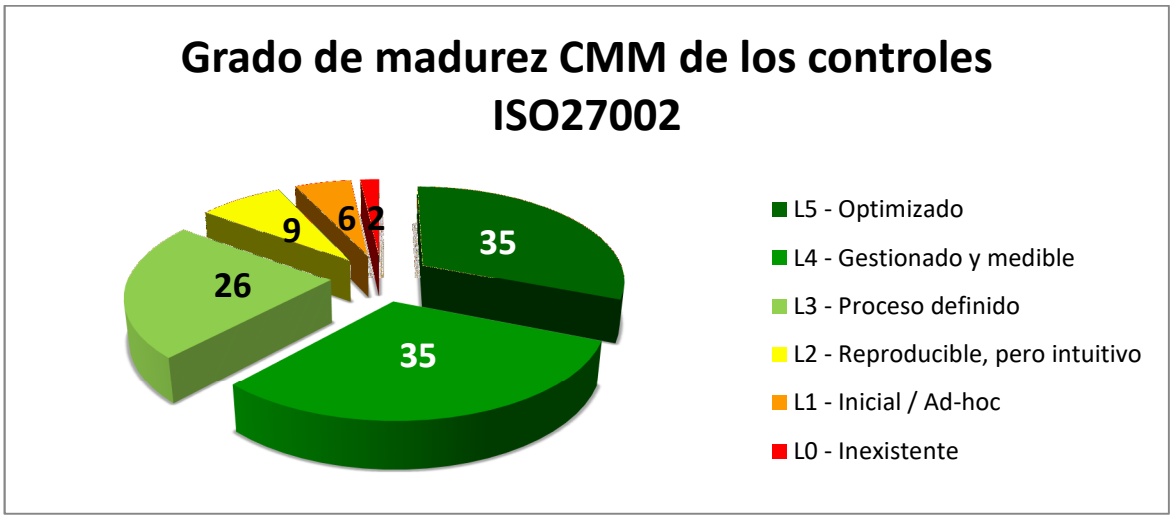


Imagen 8: Grado de madurez CMM de los controles ISO27002

Los dos controles que obtiene un nivel inexistente se refieren al hecho que no se implementaron procedimientos para trabajar en áreas seguras y para asegurar el cableado eléctrico y de telecomunicaciones.
Considerando que con un nivel de madurez 3, 4 o 5 la organización cumple con los requisitos del estándar, y que el nivel 2 identifica las observaciones (es decir aquellos aspectos que no son incumplimientos, pero podrían llegar a serlo si en el futuro no se trabajan), las no conformidades son en total 8 (correspondientes a los controles con nivel inexistente o inicial).

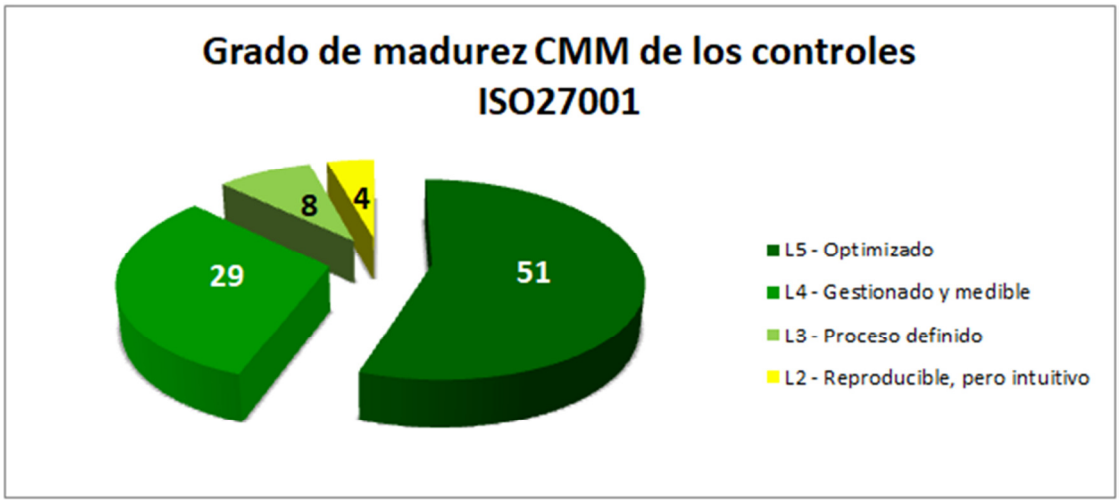


Imagen 9: Grado de madurez CMM de los controles ISO27001

De la misma manera, aplicando las mismas consideraciones de cumplimiento o incumplimiento a los controles de la norma ISO27001, se puede ver que esta vez no aparecen no conformidades, sino solo 4 observaciones.

Se puede también observar que, por lo que concierne los controles ISO27002, el resultado se acerca bastante al objetivo de un nivel optimizado: los que más se adelantan (aunque con resultados positivos) son la seguridad física y ambiental, aquella de las comunicaciones y las relaciones con los proveedores:

Imagen 10: ISO27002 – Nivel de cumplimiento

El mismo gráfico relativo a los controles ISO27001 permite ver que esta vez la empresa se acerca mucho al valor objetivo:

Imagen 11: ISO27001 – Nivel de cumplimiento

Los objetivos en realidad pueden parecer bastante ambiciosos; todavía cae recordar que la empresa dispone de trabajadores que son consultores a otras empresas en procesos de certificación de otros estándares y que ya tiene otras certificaciones (ISO 9001, ISO 21001, UNI CEI EN ISO 50001, UNI ISO 45001, UNI EN ISO 14001) así que está acostumbrada a estos tipos de procesos. Por esto los resultados obtenidos en pocos meses son de nivel alto: pero es claro que se trata de un proceso continuo y que siempre es necesario enfrentarse a nuevos desafíos.

9. Conclusiones

Habiendo realizado con éxito todas las fases anteriores, se ha realizado el objetivo planificado al inicio del proyecto, es decir que la empresa esté lista para obtener la certificación ISO 27001.

En particular, se ha definido un alcance suficientemente amplio, pero al mismo tiempo no inclusivo de toda la organización, para poder circunscribir los análisis y las intervenciones necesarias, reduciendo así el tiempo necesario para cumplir con ellas. Se ha definido y documentado el esquema documental, realizado un análisis de riesgos inicial que ha permitido identificar los activos prioritarios, valorar las amenazas y su impacto, definir el nivel de riesgo aceptable y, en resumen, conocer la situación de partida.

Gracias a esto se han podido establecer propuestas de proyecto a llevar a cabo en un plazo de 10 meses: un periodo corto, viendo los niveles iniciales aparentemente bajos, pero hay que tener en cuenta que muchos de los procedimientos existían informalmente y solo era necesario codificarlos, documentarlos y establecer controles.

El resultado fue en primer lugar aquello de satisfacer los requisitos para la obtención de la certificación, necesaria para poder trabajar con bancos y administraciones públicas, pero también aquello de mitigar los riesgos y mejorar sensiblemente el estado de seguridad de la empresa.

El objetivo siguiente a este trabajo será aquello de la obtención efectiva de la certificación ISO 27001, sin olvidar que será necesario plantear nuevos proyectos para mejorar los controles menos maduros, efectuar revisiones y auditorías periódicas al sistema de seguridad de la información de la empresa, y siempre buscar mejorías y ajustamientos contra nuevas amenazas.

Finalmente hay que considerar que, dado que se han excluido partes de la organización del proceso de certificación y, consecuentemente, del análisis de riesgos, sería oportuno (teniendo a disposición más tiempo), ampliar el alcance de la certificación para incluirlos, así como gradualmente aumentar el nivel de seguridad requerido (por ejemplo modificando el nivel de riesgo aceptable).

10. Glosario

Activo: cualquier elemento que tenga valor para la organización, relacionado con el tratamiento de la información, y que consecuentemente necesita ser protegido

Alcance: ámbito de la organización sometido al SGSI

Amenaza: cualquier potencial ocurrencia que puede causar daños al sistema de información o a la organización

Autenticidad: propiedad que permite garantizar la fuente de los datos o que una entidad sea lo que dice ser

Confidencialidad: propiedad según la cual la información no debe ponerse a disposición de quien no está autorizado

Disponibilidad: propiedad según la cual la información debe estar a disposición de los autorizados cuando la necesitan

Impacto: coste (no necesariamente financiero) de un incidente para la empresa

Incidente: evento que puede comprometer la seguridad de la información y/o la operatividad del negocio. Es la materialización de una amenaza

Integridad: propiedad que garantiza que la información no ha sido modificada sin autorización

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborada por el Ministerio de Administraciones Públicas

Riesgo: probabilidad que una amenaza se materialice causando un impacto sobre un activo

Riesgo residual: aquello que permanece tras el tratamiento del riesgo

Salvaguarda: procedimiento que permite reducir el riesgo

SGSI: Sistema de Gestión de Seguridad de la Información

Trazabilidad: propiedad que permite asociar las acciones relacionadas con la información a una entidad o a un individuo preciso

Vulnerabilidad: debilidad que presentan los activos y que facilita la materialización de las amenazas.

11. Bibliografía

[1] Wikipedia - *ISO/IEC 27001*, https://it.wikipedia.org/wiki/ISO/IEC_27001, fecha de consultación: 23/02/2022

[2] Garre Gui S., Segovia Henares A.J., Tortajada Gallego A. (2020), *Implantación de un sistema de gestión de la seguridad de la información (SGSI)*, pág. 17

[3] Archiva (2/3/2022), *Introduzione alla nuova ISO/IEC 27002 e le conseguenze per le aziende certificate ISO/IEC 27001,* https://www.archivagroup.it/2022/03/02/nuova-iso-iec-27002/, fecha de consultación: 07/03/2022

[4] UOC – Xwiki - *Análisis diferencial*, https://xwiki.recursos.uoc.edu/wiki/matm1709/view/Main/An%C3%A1lisis%20diferencial#Attachments, fecha de consultación: 25/02/2022

[5] Ministerio de Hacienda y Administraciones Públicas (10/2012), *MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I: Método*, pág. 22

[6] Ministerio de Hacienda y Administraciones Públicas (10/2012), *MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I: Método*, pág. 25

Anexo 1 - Tabla del análisis diferencial ISO 27002

CONTROL	VALOR CMM	JUSTIFICACIÓN DE LA VALORACIÓN / EVIDENCIAS
A.5. Políticas de seguridad de la información **A.5.1. Directrices de la dirección en seguridad de la información**		
5.1.1. Políticas para la seguridad de la información	**2**	Aunque no existen reglas definidas y documentadas, hay procedimientos conocidos por todo el personal sobre el análisis de riesgo y la gestión de autorizaciones a la información. Además el código de conducta informático establece unas restricciones de las funciones y operaciones que las diferentes categorías de empleados pueden tener.
5.1.2. Revisión de las políticas para la seguridad de la información	**0**	Las reglas definidas son informales, así que no hay una revisión planificada, sino una adaptación ocasional del comportamiento a las nuevas situaciones que pueden ocurrir.
A.6. Organización de la seguridad de la información **A.6.1. Organización interna**		
6.1.1. Roles y responsabilidades en la seguridad de la información.	**1**	El departamento IT es informalmente responsable de la seguridad de la información, aunque no hay una división de los roles clara y definida. Esto significa que la empresa reconoce que es necesario gestionar la seguridad, pero roles y responsabilidades se establecen (informalmente) dentro del departamento cada vez que es necesario.
6.1.2. Segregación de tareas.	**2**	Hay una parcial segregación de funciones (los usuarios no pueden instalar programas o aplicaciones en ordenadores o móviles, sino deben preguntar al departamento IT) y una limitación sobre los sitios que se pueden visitar en la oficina, pero no hay control sobre el uso indebido de los activos fuera de la empresa.
6.1.3. Contacto con las autoridades.	**0**	Dado que no hay un responsable o reglas formales de la seguridad, tampoco hay alguien encargado (o un procedimiento claro) de contactar las autoridades en caso de sospecha, o cierta, violación de la ley.
6.1.4. Contacto con grupos de interés especial.	**2**	Unos de los empleados del proveedor que gestiona los servidores tienen conocimientos especializados en seguridad.
6.1.5. Seguridad de la información en la gestión de proyectos.	**2**	El procedimiento de análisis de riesgos de seguridad prevé unos requisitos de seguridad, aunque solo en los proyectos de desarrollo de aplicaciones que requieren acceso a las bases de datos de la empresa.
A.6. Organización de la seguridad de la información **A.6.2. Los dispositivos móviles y el teletrabajo**		
6.2.1. Política de dispositivos móviles	**2**	Los usuarios saben que no pueden instalar apps sin pedir permiso al departamento IT, todavía no hay restricciones prácticas (se confía en los usuarios).
6.2.2. Teletrabajo	**2**	Hay un procedimiento de gestión segura de las conexiones desde el exterior (VPN) que permite a la empresa tener unas medidas de seguridad y de protección de los accesos. Se aplican, en el acceso desde el exterior, las mismas restricciones establecidas por la política de seguridad de la información.

A.7. Seguridad ligada a los recursos humanos **A.7.1. Antes del empleo**		
7.1.1. Investigación de antecedentes	**0**	No se comprueban los currículos vitae de los candidatos al puesto de trabajo ni las competencias de manejo de información sensible en caso de promoción interna.
7.1.2. Términos y condiciones del empleo	**1**	Los acuerdos de empleo incluyen generalmente cláusulas de confidencialidad, de protección de datos y de derechos de propiedad intelectual. Todavía estas se aplican a discreción de la dirección, y no aparecen en los acuerdos estipulados hace unos años.
A.7. Seguridad ligada a los recursos humanos **A.7.2. Durante el empleo**		
7.2.1. Responsabilidades de gestión	**0**	Dado que no hay un proceso formal de gestión, no hay responsables y los empleados son acostumbrados a unas reglas informales, pero sin un real nivel de concienciación en seguridad de la información. La dirección considera suficientes las medidas adoptadas y no se ha mostrado, en el pasado, interesada a adoptar un modelo a seguir.
7.2.2. Concienciación, educación y capacitación en Seguridad de la Información	**0**	No hay educación ni actualizaciones periódicas sobre procedimientos de la organización, dado que no están formalizados. De vez en cuando se envía un correo electrónico para recordar a los usuarios los peligros del uso descuidado del correo electrónico, pero no es suficiente para reconocer un nivel inicial del asunto.
7.2.3. Proceso disciplinario	**0**	No se ha definido el alcance de las violaciones ni, consecuentemente, se han definido sanciones para los empleados que producen una violación de la seguridad.
A.7. Seguridad ligada a los recursos humanos **A.7.3. Finalización del empleo o cambio en el puesto de trabajo**		
7.3.1. Responsabilidades ante la finalización o cambio	**1**	Cuando hay clausulas en los contratos, se definen también responsabilidades y funciones válidas también después de la finalización del empleo, pero (como visto anteriormente) estas no siempre existen. No se gestionan de manera automática los cambios de responsabilidad debidos a cambios internos.
A.8. Gestión de activos **A.8.1. Responsabilidad sobre los activos**		
8.1.1. Inventario de activos	**0**	No hay un inventario preciso de los activos: se sabe que, por ejemplo, cada empleado tiene un ordenador y un móvil, pero no se almacenaron los datos (número serial o nombre del ordenador) y solo hay un software de escaneo de la red de la empresa que permite conocer unos datos de los ordenadores (cuándo se conectaron la última vez, con cuál usuario, qué software tienen…) pero no se gestiona el inventario de todos los activos ni se registran las devoluciones y los cambios.
8.1.2. Propiedad de los activos	**0**	No existiendo un inventario de los activos, no hay un responsable ni se puede conocer el propietario exacto de cada elemento.
8.1.3. Uso aceptable de los activos	**2**	El código de conducta, conocido por toda la organización, establece unas normas de comportamiento (por ejemplo el hecho que no se permite instalar software sin autorización, y está prohibido conectarse a sitios web que no sirven para el trabajo, o utilizar social media…)

8.1.4. Devolución de activos	**1**	El departamento IT está informalmente encargado de recoger los activos de los empleados que terminan su relación laboral, pero se limita a ordenadores y móviles dado que no se registró si, por ejemplo, a un empleado fue entregado un disco duro externo o un pendrive usb. A veces no es el departamento IT que se ocupa de la devolución de los activos, sino la secretaria del empleado. Tampoco se puede conocer si alguien copió ficheros guardados en la red empresarial.
A.8. Gestión de activos **A.8.2. Clasificación de la información**		
8.2.1. Clasificación de la información	**0**	No se clasifica la información en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
8.2.2. Etiquetado de la Información	**0**	No existiendo clasificación de la información, tampoco existe un procedimiento para etiquetarla en conformidad con esta.
8.2.3. Manipulación de la información	**0**	Sin esquema de clasificación no puede existir un conjunto de procedimientos para la manipulación de la información.
A.8. Gestión de activos **A.8.3. Manejo de soportes de almacenamiento**		
8.3.1. Gestión de soportes extraíbles	**0**	No hay un registro de los soportes extraíbles y, no existiendo una clasificación de la información, no se controla la transferencia de información a medios extraíbles.
8.3.2. Eliminación de soportes.	**0**	Los soportes no se destruyen de forma segura, y no se distinguen aquellos que almacenan información confidencial o sensible de los demás.
8.3.3. Soportes físicos en tránsito	**0**	No hay protección de los soportes durante su transporte, ni registros de los mismos transportes; solo se aplican protecciones para protegerlos de los daños físicos.
A.9. Control de acceso **A.9.1. Requisitos de negocio para el control de acceso**		
9.1.1. Política de control de acceso	**0**	No existe una política de control de acceso basada en los requisitos de negocio y de seguridad de la información, no gestionándose los riesgos de seguridad de la información. Tampoco hay diferenciación.
9.1.2. Acceso a redes y a los servicios en red	**2**	El código de conducta informático define el comportamiento para acceder y utilizar redes y servicios. Se aplican también unos (limitados) filtros, pero no hay monitorización ni control constante del uso.
A.9. Control de acceso **A.9.2. Gestión de acceso de usuario**		
9.2.1. Registro y baja de usuario	**2**	Los identificadores de usuario son dados por el departamento IT a todos los empleados cuando empiezan a trabajar en la organización y cuando la dejan se inhabilitan, pero no hay un control periódico establecido.
9.2.2. Provisión de acceso de usuario	**2**	Existe un procedimiento conocido para la definición y asignación de los derechos de acceso, dividiéndose los usuarios en administradores y no-administradores.
9.2.3. Gestión de privilegios de acceso	**1**	Dado que no existe un procedimiento documentado de provisión de acceso, los privilegios están informalmente gestionados por el departamento IT, pero no se controlan periódicamente.

9.2.4. Gestión de la información secreta de autenticación de los usuarios	**2**	La asignación de la información secreta de autenticación no se proporciona de manera segura (los nuevos usuarios tienen siempre la misma contraseña inicial, que se comunica oralmente). Todavía los usuarios deben cambiarla obligatoriamente en el primer uso.
9.2.5. Revisión de los derechos de acceso de usuario	**1**	No se revisan los derechos de acceso de usuario periódicamente o después de cambios, sino de una manera casual.
9.2.6. Retirada o reasignación de los derechos de acceso	**2**	Tras la finalización del empleo se bloquea el usuario y consecuentemente sus derechos de acceso se eliminan. Todavía no existe un procedimiento automático, sino es necesario esperar la intervención del departamento IT.
A.9. Control de acceso **A.9.3. Responsabilidades de usuario**		
9.3.1. Uso de información secreta de autenticación	**2**	No se advierten los usuarios de mantener confidencial la información; existen requisitos (longitud mínima, caracteres especiales…) en la selección de contraseñas.
A.9. Control de acceso **A.9.4. Control de acceso a sistemas y aplicaciones**		
9.4.1. Restricción del acceso a la información.	**1**	Se restringe el acceso a la información de los usuarios, pero no hay un control sobre el acceso de las aplicaciones.
9.4.2. Procedimientos seguros de inicio de sesión	**2**	Se terminan las sesiones inactivas después de 10 minutos de inactividad, se esconde la contraseña y se transmite cifrada por red; existe una protección contra los ataques de fuerza bruta (imposibilidad de reintentar durante 20 minutos después de 3 tentativos errados).
9.4.3. Sistema de gestión de contraseñas.	**2**	El procedimiento no está documentado, pero es bien conocido. Es necesario cambiar las contraseñas tras el primer inicio de sesión y periódicamente, se imponen unos requisitos de las contraseñas y se mantiene un registro de las contraseñas para evitar su reutilización.
9.4.4. Uso de utilidades con privilegios del sistema	**2**	El uso de utilidades con privilegios del sistema está restringido (es posible solo para los administradores) y bien conocido, aunque no documentado.
9.4.5. Control de acceso al código fuente de los programas	**2**	El código fuente de los programas está accesible solo para los desarrolladores y administradores del sistema. Falta la documentación del procedimiento.
A.10. Cifrado **A.10.1. Controles criptográficos**		
10.1.1. Política de uso de los controles criptográficos	**0**	No existe una política sobre el uso de los controles criptográficos para proteger la información.
10.1.2. Gestión de claves	**0**	No existe una política sobre el uso, la protección y la duración de las claves de cifrado.
A.11. Seguridad física y ambiental **A.11.1. Áreas seguras**		
11.1.1. Perímetro de seguridad física	**5**	El proveedor que gestiona los servidores asegura que están protegidos físicamente con controles de acceso automático, y que el proceso está documentado.
11.1.2. Controles físicos de entrada	**5**	El proveedor que gestiona los servidores autoriza los accesos, registrando las horas de entrada y salida de los visitadores.
11.1.3. Seguridad de oficinas, despachos y recursos	**3**	Existen señales que identifiquen la existencia de actividades de tratamiento de la información; todavía no se han considerado los campos electromagnéticos.

11.1.4. Protección contra las amenazas externas y ambientales	**3**	Existe solo un plan de protección de la sala de servidores contra el fuego, no se evaluaron otros desastres ambientales ni daños causados por el hombre.
11.1.5. El trabajo en áreas seguras	**0**	No se implementaron procedimientos para trabajar en áreas seguras.
11.1.6. Áreas de carga y descarga	**3**	Las áreas de carga y descarga están al exterior del edificio y no es necesario que el personal externo encargado de las operaciones acceda a otras zonas del edificio.
A.11. Seguridad física y ambiental **A.11.2. Seguridad de los equipos**		
11.2.1. Emplazamiento y protección de equipos	**5**	Los servidores están en una sala con mecanismos de control de temperatura y humedad y un extintor de incendios.
11.2.2. Instalaciones de suministro	**5**	Los servidores están conectados a UPS para protegerlos de fallos de alimentación u otras alteraciones. Los UPS son conformes a los requisitos legales. Se hacen pruebas periódicas.
11.2.3. Seguridad del cableado	**0**	El cableado eléctrico y de telecomunicaciones no está protegido frente a interceptaciones, interferencias o daños.
11.2.4. Mantenimiento de los equipos	**2**	Los servidores se mantienen regularmente, de acuerdo con las necesidades del cliente. Los ordenadores de los empleados de la empresa se gestionan sin regularidad.
11.2.5. Retirada de materiales propiedad de la empresa	**1**	Los empleados pueden sacar los activos fuera de las instalaciones. Los usuarios de tercera parte pueden hacerlo si son claramente identificados, pero no existe un registro de las retiradas ni se ha establecido una limitación al tiempo.
11.2.6. Seguridad de los equipos fuera de las instalaciones	**0**	No se aplican medidas de seguridad a los equipos fuera de las instalaciones, solo se recomienda a los usuarios de no dejarlos visibles y sin control en los coches.
11.2.7. Reutilización o eliminación segura de equipos	**0**	No existe eliminación segura de equipos, no se comprueba si tienen información sensible ni si se eliminó el sw bajo licencia.
11.2.8. Equipo de usuario desatendido	**2**	El código de conducta informático impone a los usuarios de activar el protector de pantalla con contraseña después de 10 minutos de inactividad.
11.2.9. Política de puesto de trabajo despejado y pantalla limpia	**0**	No existen procedimientos sobre cómo guardar la información sensible (electrónica o en papel) ni sobre el retiro de soportes con información sensible de las impresoras.
A.12. Seguridad en las operaciones **A.12.1. Responsabilidades y procedimientos de operación**		
12.1.1. Documentación de procedimientos de operación	**0**	Las operaciones no son documentadas y no existe nada a disposición de los usuarios que lo necesiten.
12.1.2. Gestión de cambios	**0**	No existen registros, pruebas o planificaciones de los cambios.
12.1.3. Gestión de capacidades	**0**	No se han identificado formalmente los requisitos de capacidad de los recursos, y a veces hay problemas (en general pequeños) de rendimiento.
12.1.4. Separación de recursos de desarrollo, prueba y operación	**0**	No se separan los recursos de desarrollo, prueba y operación, y las pruebas se hacen en el sistema en producción.
A.12. Seguridad en las operaciones **A.12.2. Protección contra código malicioso**		

12.2.1. Controles contra el código malicioso	**2**	Todos los ordenadores tienen instalado un software antivirus centralizado que se actualiza periódicamente. No existen procedimientos de concienciación a los usuarios.
A.12. Seguridad en las operaciones **A.12.3. Copias de seguridad**		
12.3.1. Copias de seguridad de la información	**5**	Se hace una copia de seguridad de las bases de datos cada noche; se guardan las copias diarias durante una semana, luego se guarda una copia de seguridad por semana durante un mes, y una copia de seguridad mensual durante un año. La política de copias de seguridad está documentada en los acuerdos entre la empresa y el proveedor que gestiona los servidores.
A.12. Seguridad en las operaciones **A.12.4. Registro de actividad y supervisión**		
12.4.1. Registro de eventos	**0**	No se registran las actividades de los usuarios, las excepciones, los fallos y los eventos de seguridad de la información.
12.4.2. Protección de la información de registro	**0**	No existiendo el registro de eventos, no se puede proteger.
12.4.3. Registros de administración y operación	**0**	No se registran las actividades de los administradores y operadores de sistemas.
12.4.4. Sincronización del reloj	**1**	Los relojes de todos los sistemas de tratamiento de la información de la organización están sincronizados con la hora del servidor principal, aunque un usuario podría modificar manualmente la impostación de su ordenador.
A.12 seguridad en las operaciones **A.12.5 control del software en explotación**		
12.5.1. Instalación del software en explotación	**0**	No existen procedimientos para controlar el software en explotación; no hay un control periódico de las actualizaciones del software; no existiendo una separación de recursos de desarrollo, prueba y operación, puede ocurrir que los sistemas operativos manejen códigos en desarrollo.
A.12 seguridad en las operaciones **A.12.6 gestión de la vulnerabilidad técnica**		
12.6.1. Gestión de las vulnerabilidades técnicas	**0**	No existiendo un inventario de los activos, no existen informaciones exactas acerca de las vulnerabilidades técnicas.
12.6.2. Restricciones en la instalación de software	**2**	Los usuarios no tienen permisos de instalación de software en sus ordenadores; se trata de un procedimiento no documentado pero conocido a través del código de conducta informático.
A.12. Seguridad en las operaciones **A.12.7. Consideraciones sobre las auditorías de los sistemas de información**		
12.7.1. Controles de auditoría de sistema de información	**0**	No se hacen actividades de auditoría a sistemas y datos.
A.13. Seguridad de las comunicaciones **A.13.1. Gestión de la seguridad en redes**		
13.1.1. Controles de red	**1**	Hay un firewall que permite registrar y monitorizar los eventos; todavía no se han establecido con claridad roles, responsabilidades y procedimientos para la gestión y el control.

13.1.2. Seguridad en los servicios de red	**1**	Hay un firewall para proporcionar seguridad a la red, pero no existen procedimientos para restringir el acceso a los servicios de red o a las aplicaciones.
13.1.3. Segregación en redes.	**0**	No existe segregación en redes distintas.
A.13. Seguridad de las comunicaciones **A.13.2. Intercambio de información con partes externas**		
13.2.1. Políticas y procedimientos de intercambio de información	**0**	Excepto por el antivirus que protege contra el malware transmitido a través de comunicaciones electrónicas, no existen procedimientos o controles para proteger el intercambio de información.
13.2.2. Acuerdos de intercambio de información	**0**	No se han establecido acuerdos para el intercambio seguro de información entre la organización y terceros.
13.2.3. Mensajería electrónica	**0**	No se implantaron medidas de protección de la mensajería electrónica.
13.2.4. Acuerdos de confidencialidad o no revelación	**2**	Existen acuerdos de confidencialidad entre la organización y la mayoría de sus empleados, y entre la organización y sus proveedores, pero no hay un procedimiento documentado.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.1. Requisitos de seguridad de los sistemas de información**		
14.1.1. Análisis de requisitos y especificaciones de seguridad de la información	**0**	Los requisitos relacionados con la seguridad de la información no se incluyen en los requisitos para los nuevos sistemas de información o para mejoras a aquellos existentes.
14.1.2. Asegurar los servicios de aplicaciones en redes públicas	**0**	No se protege la información involucrada en aplicaciones que pasan a través de redes públicas.
14.1.3. Protección de las transacciones de servicios de aplicaciones	**0**	No se aplican medidas de protección contra transmisión incompleta, errores de enrutamiento, alteración, revelación, duplicación o reproducción no autorizada.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.2. Seguridad en los procesos de desarrollo y soporte**		
14.2.1. Política de desarrollo seguro	**2**	Existe un procedimiento de desarrollo seguro de software, ampliamente conocido por el personal aunque no documentado.
14.2.2. Procedimiento de control de cambios en sistemas	**1**	El procedimiento de desarrollo seguro permite también controlar los cambios a lo largo del ciclo de vida del desarrollo y, consecuentemente, tener una protección adicional. Todavía no existe siempre un entorno de desarrollo separado de aquello de explotación.
14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios el sistema operativo	**2**	El procedimiento de desarrollo seguro hace que cuando se modifican los sistemas operativos se revisan y prueban las aplicaciones críticas de negocio.
14.2.4. Restricciones a los cambios en los paquetes de software	**2**	Según el procedimiento de desarrollo seguro (no documentado pero conocido por el personal), los cambios en los paquetes de software se limitan a aquellos necesarios y se hace un control riguroso.
14.2.5. Principios de ingeniería de sistemas seguros	**2**	Los procedimientos de ingeniería de sistemas de información seguros se aplican, gracias al procedimiento de desarrollo seguro, a las implantaciones de sistemas de información. Todavía no están documentados, siendo no documentado el procedimiento de desarrollo seguro.
14.2.6. Entorno de desarrollo seguro	**2**	El procedimiento de desarrollo seguro establece y protege adecuadamente el entorno; falta la documentación.
14.2.7. Externalización del desarrollo de software	**-**	No hay software desarrollado externamente

14.2.8. Pruebas funcionales de seguridad de sistemas	**2**	Las prácticas de desarrollo seguro incluyen pruebas de la seguridad funcional durante el desarrollo.
14.2.9. Pruebas de aceptación de sistemas	**2**	El procedimiento de desarrollo seguro establece programas de prueba de aceptación y criterios relacionados para nuevos sistemas o actualizaciones. Falta la documentación.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.3. Datos de prueba**		
14.3.1. Protección de los datos de prueba	**0**	No siempre se evita el uso de datos reales personales o confidenciales.
A.15. Relaciones con los proveedores **A.15.1. Seguridad de la información en las relaciones con los proveedores**		
15.1.1. Política de seguridad de la información en las relaciones con los proveedores	**0**	No existen requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso de los proveedores a los activos de la organización. No existen procedimientos para definir los tipos de acceso, la supervisión y el control.
15.1.2. Requisitos de seguridad en contratos con terceros	**0**	Si existen acuerdos, son verbales. En general no existe en los contratos con terceros una descripción de la información facilitada (que tampoco está clasificada) ni se establecen un conjunto acordado de controles, la gestión de incidentes, el derecho de auditar los procesos de los proveedores u otros elementos.
15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones	**0**	No existe un procedimiento de gestión de riesgos de la cadena de suministro TIC.
A.15. Relaciones con los proveedores **A.15.2. Gestión de la prestación del servicio de los proveedores**		
15.2.1. Control y revisión de la provisión de servicios del proveedor	**0**	La provisión de servicios de los proveedores no se controla, revisa ni audita.
15.2.2. Gestión de cambios en la provisión del servicio del proveedor	**0**	No existen procedimientos para gestionar los cambios en la provisión del servicio.
A.16. Gestión de incidentes de seguridad de la información **A.16.1. Gestión de incidentes de seguridad de la información y mejoras**		
16.1.1. Responsabilidades y procedimientos	**0**	No se han establecido ni las responsabilidades ni los procedimientos de gestión de los incidentes de seguridad, y consecuentemente no se garantiza una respuesta rápida, efectiva y adecuada.
16.1.2. Notificación de los eventos de seguridad de la información.	**0**	Trabajadores, contratistas y terceros no están adecuadamente formados y no es seguro que conocen su responsabilidad de comunicar cualquier evento de seguridad de la información.
16.1.3. Notificación de puntos débiles de la seguridad	**0**	No existen obligaciones de los usuarios anotar y notificar los puntos débiles observados o sospechados de existir.
16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información	**1**	Se evalúan los eventos de seguridad de la información, pero no existe un procedimiento exacto para decidir si clasificarlos como incidentes de seguridad de información.
16.1.5. Respuesta a incidentes de seguridad de la información.	**0**	No hay procedimientos documentados para responder a los incidentes de seguridad de la información.

16.1.6. Aprendizaje de los incidentes de seguridad de la información.	**1**	A veces se utiliza el conocimiento obtenido de la resolución de incidentes de seguridad para reducir la probabilidad o el impacto de los incidentes futuros, pero no siempre.
16.1.7. Recopilación de evidencias	**0**	No existen procedimientos de recogida de evidencias.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.1. Continuidad de la seguridad de la información**		
17.1.1. Planificación de la continuidad de la seguridad de la información	**1**	Se han analizado las necesidades de continuidad de unos procesos críticos, pero no existe documentación ni se ha desarrollado un análisis completo.
17.1.2. Implementar la continuidad de la seguridad de la información	**1**	Se han establecido planes correspondientes a los análisis del control A.17.1.1 bien conocidos por los administradores del departamento IT, pero no existe documentación.
17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**0**	No existiendo documentación, no se revisan ni se verifican los planes de continuidad.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.2. Redundancias**		
17.2.1. Disponibilidad de los recursos de tratamiento de la información	**0**	No hay redundancia de recursos de tratamiento de la información.
A.18. Cumplimiento **A.18.1. Cumplimiento de los requisitos legales y contractuales**		
18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	**0**	No existe documentación explícita de los requisitos pertinentes para ningún sistema de información de la organización.
18.1.2. Derechos de propiedad intelectual (DPI)	**1**	Se han implementado unos controles sobre el uso de productos de software patentados, pero no sobre el uso de materiales con respecto a los cuales pueden existir derechos de propiedad intelectual.
18.1.3. Protección de los registros de la organización	**0**	No existe protección de los registros contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado.
18.1.4. Protección y privacidad de la información de carácter personal	**0**	No existe un procedimiento para garantizar la protección y la privacidad de los datos.
18.1.5. Regulación de los controles criptográficos	**0**	No se utilizan controles criptográficos.
A.18. Cumplimiento **A.18.2. Revisiones de la seguridad de la información**		
18.2.1. Revisión independiente de la seguridad de la información	**0**	No existe revisión independiente de la gestión de la seguridad de la información ni a intervalos planificados ni cuando se producen cambios significativos.
18.2.2. Cumplimiento de las políticas y normas de seguridad	**0**	Los directivos no revisan el cumplimiento de políticas y normas de seguridad.
18.2.3. Comprobación del cumplimiento técnico	**0**	No existe comprobación periódica del cumplimiento técnico de los sistemas de la seguridad de la información.

Anexo 2 - Tabla del análisis diferencial ISO 27001

ISO 27001 clause	Mandatory requirement for the ISMS	Status	Do You Have Documents / Records to Reference to Prove Compliance?	Notes
4				
4,1				
4,1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	**Not Implemented**	No	Es necesario implementar el SGSI
4,2				
4,2	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security	**Partially Implemented**	No	Se han individuado el objetivo, los sectores y los procesos involucrados, aunque falta una documentación formal.
4,3				
4,3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	**Partially Implemented**	No	Se han individuado el objetivo, los sectores y los procesos involucrados, aunque falta una documentación formal.
4,4				
4,4	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	**Not Implemented**	No	Es necesario implementar el SGSI
5	**Leadership**			
5,1				
5,1	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:			

5.1 (a)	ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (b)	ensuring the integration of the information security management system requirements into the organization's processes;	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (c)	ensuring that the resources needed for the information security management system are available;	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (d)	communicating the importance of effective information security management and of conforming to the information security management system requirements;	**Partially Implemented**	Yes	Se ha comunicado la importancia del objetivo a los sectores interesados pero no a toda la organización.
5.1 (e)	ensuring that the information security management system achieves its intended outcome(s);	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (f)	directing and supporting persons to contribute to the effectiveness of the information security management system;	**Fully Implemented**	Yes	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (g)	promoting continual improvement; and	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (h)	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5,2				
5,2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security	**Partially Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte. Falta la documentación

	management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate			
5,3				
5,3	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	**Partially Implemented**	No	Se han individuado los roles y responsabilidades pero es necesario revisarlos atentamente; falta la comunicación oficial.
6				
6,1				
6.1.1	**General**			
6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement	**Partially Implemented**	No	Hay unos procedimientos, pero no exhaustivos y falta la documentación.
6.1.1 (d)	The organization shall plan actions to address these risks and opportunities; and	**Partially Implemented**	No	Hay unos procedimientos, pero no exhaustivos y falta la documentación.
6.1.1 (e)	The organization shall plan how to: 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	**Not Implemented**	No	Falta la integración y la evaluación de la eficacia
6.1.2				
6.1.2	The organization shall define and apply an information security risk assessment process that:			

6.1.2 (a)	establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.2 (b)	ensures that repeated information security risk assessments produce consistent, valid and comparable results;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.2 (c)	identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.2 (d)	analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.2 (e)	evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analyzed risks for risk treatment.	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.3				
6.1.3	The organization shall define and apply an information security risk treatment process to:			
6.1.3 (a)	select appropriate information security risk treatment options, taking account of the risk assessment results;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.3 (b)	determine all controls that are necessary to implement the information security risk treatment option(s) chosen;	**Not Implemented**	No	Es necesario implementar el SGSI

6.1.3 (c)	compare the controls determined in 6.1.3 (b) above with those in Annex A and verify that no necessary controls have been omitted;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.3 (d)	produce a Statement of Applicability that contains the necessary controls (see 6.1.3.b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.3 (e)	formulate an information security risk treatment plan; and	**Not Implemented**	No	Es necesario implementar el SGSI
6.1.3 (f)	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	**Not Implemented**	No	Es necesario implementar el SGSI
6,2				
6,2	The organization shall establish information security objectives at relevant functions and levels.	**Not Implemented**	No	Es necesario implementar el SGSI
6,2	The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.	**Not Implemented**	No	Es necesario implementar el SGSI
6,2	When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated.	**Not Implemented**	No	Es necesario implementar el SGSI

7				
7,1				
7,1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	**Fully Implemented**	No	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura los recursos necesarios.
7,2				
7,2	The organization shall:			
7.2 (a)	determine the necessary competence of person(s) doing work under its control that affects its information security performance;	**Not Implemented**	No	No se ha determinado
7.2 (b)	ensure that these persons are competent on the basis of appropriate education, training, or experience;	**Partially Implemented**	No	Se ocuparán del SGSI empleados con conocimiento del sector IT
7.2 (c)	where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and	**Partially Implemented**	No	Se han planificado cursos de formación y se ha contratado una consultoría especializada.
7.2 (d)	retain appropriate documented information as evidence of competence.	**Not Implemented**	No	Es necesario implementar el SGSI
7,3				
7,3	Persons doing work under the organization's control shall be aware of:			
7.3 (a)	the information security policy;	**Partially Implemented**	Yes	La conocen solo los empleados involucrados con el SGSI.
7.3 (b)	their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and	**Partially Implemented**	No	La conocen solo los empleados involucrados con el SGSI.
7.3 (c)	the implications of not conforming with the information security management system requirements.	**Partially Implemented**	No	La conocen solo los empleados involucrados con el SGSI.
7,4				
7,4	The organization shall determine the need for internal and external communications relevant to the information security management system including:			
7.4 (a)	on what to communicate;	**Not Implemented**	No	Es necesario implementarlo con el SGSI

7.4 (b)	when to communicate;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.4 (c)	with whom to communicate;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.4 (d)	who shall communicate; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.4 (e)	the processes by which communication shall be effected.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7,5				
7.5.1				
7.5.1	The organization's information security management system shall include:			
7.5.1 (a)	documented information required by this International Standard; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.1 (b)	documented information determined by the organization as being necessary for the effectiveness of the information security management system.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.2				
7.5.2	When creating and updating documented information the organization shall ensure appropriate:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.2 (a)	identification and description (e.g. a title, date, author, or reference number);	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.2 (b)	format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.2 (c)	review and approval for suitability and adequacy.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3				
7.5.3	Documented information required by the information security management system and by this International Standard shall be controlled to ensure:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3 (a)	it is available and suitable for use, where and when it is needed; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3 (b)	it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3	For the control of documented information, the organization shall address the following activities, as applicable:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3 (c)	distribution, access, retrieval	**Partially**	No	Hay una parcial restricción de

	and use;	**Implemented**		acceso a los ficheros de documentación.
7.5.3 (d)	storage and preservation, including the preservation of legibility;	**Fully Implemented**	No	Hay un procedimiento correcto de copias de seguridad
7.5.3 (e)	control of changes (e.g. version control); and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3 (f)	retention and disposition.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
7.5.3	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8				
8,1				
8,1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,1	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,1	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,1	The organization shall ensure that outsourced processes are determined and controlled.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,2				
8,2	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.a.	**Not Implemented**	No	Es necesario implementarlo con el SGSI

8,2	The organization shall retain documented information of the results of the information security risk assessments.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,3				
8,3	The organization shall implement the information security risk treatment plan.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
8,3	The organization shall retain documented information of the results of the information security risk treatment.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9				
9,1				
9,1	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (a)	what needs to be monitored and measured, including information security processes and controls;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (b)	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (c)	when the monitoring and measuring shall be performed;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (d)	who shall monitor and measure;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (e)	when the results from monitoring and measurement shall be analyzed and evaluated; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.1 (f)	who shall analyze and evaluate these results.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9,2				
9,2	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (a)	conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (b)	is effectively implemented	**Not**	No	Es necesario implementarlo con

	and maintained.	**Implemented**		el SGSI
9,2	The organization shall:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (c)	plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (d)	define the audit criteria and scope for each audit;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (e)	select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (f)	ensure that the results of the audits are reported to relevant management; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.2 (g)	retain documented information as evidence of the audit programme(s) and the audit results.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9,3				
9,3	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.3 (a)	the status of actions from previous management reviews;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.3 (b)	changes in external and internal issues that are relevant to the information security management system;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.3 (c)	feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.3 (d)	feedback from interested parties;	**Not Implemented**	No	Es necesario implementarlo con el SGSI

9.3 (e)	results of risk assessment and status of risk treatment plan; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9.3 (f)	opportunities for continual improvement.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
9,3	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10				
10,1				
10,1	When a nonconformity occurs, the organization shall:			Es necesario implementarlo con el SGSI
10.1 (a)	react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10.1 (b)	evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10.1 (c)	implement any action needed;	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10.1 (d)	review the effectiveness of any corrective action taken; and	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10.1 (e)	make changes to the information security management system, if necessary.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10,1	Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10.1 (f)	the nature of the nonconformities and any subsequent actions taken, and	**Not Implemented**	No	Es necesario implementarlo con el SGSI

10.1 (g)	the results of any corrective action.	**Not Implemented**	No	Es necesario implementarlo con el SGSI
10,2				
10,2	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	**Not Implemented**	No	Es necesario implementarlo con el SGSI

Anexo 3 - Política de seguridad de las informaciones

1 - PROPÓSITO

El presente documento tiene por objeto describir los principios generales de seguridad de la información definidos por la empresa para desarrollar un Sistema de Gestión de Seguridad de la Información eficiente y seguro.

2 - DESCRIPCIÓN

Para la empresa, la seguridad de la información tiene como objetivo primordial la protección de los datos y la información, de la estructura tecnológica, física, lógica y organizativa responsable de su gestión. Esto significa obtener y mantener un sistema de gestión de la información seguro, dentro del alcance definido para el SGSI, respetando las siguientes propiedades:

1. **Confidencialidad**: garantizar que la información sea accesible solo para personas y/o procesos debidamente autorizados.
2. **Integridad**: salvaguardar la consistencia de la información de cambios no autorizados.
3. **Disponibilidad**: garantizar que los usuarios autorizados tengan acceso a la información y elementos arquitectónicos asociados cuando lo soliciten.
4. **Control**: asegurarse de que la gestión de datos siempre se realice a través de procesos y herramientas seguros y probados.
5. **Autenticidad**: garantizar una fuente de información confiable.
6. **Privacidad**: garantizar la protección y control de los datos personales.

Como parte de la gestión de los servicios ofrecidos por la empresa, a través de su infraestructura tecnológica, el cumplimiento de los niveles de seguridad establecidos a través de la implementación del SGSI asegura:

- la garantía de haber designado un socio confiable para procesar sus activos de información;
- una alta imagen corporativa;
- pleno cumplimiento de los Acuerdos de Nivel de Servicio establecidos con los clientes;
- la satisfacción del cliente;
- cumplimiento de la normativa vigente y de las normas internacionales de seguridad

Por ello, la empresa intenta desarrollar un sistema seguro de gestión de la información siguiendo los requisitos especificados por la norma ISO 27001:2013 y las leyes de obligado cumplimiento como medio de gestionar la seguridad de la información como parte de su negocio.

3 - ÁMBITO DE APLICACIÓN

La política de seguridad de la información de la empresa se aplica a todo el personal interno y de terceros que colaboran en la gestión de la información ya todos los procesos y recursos que intervienen en el diseño, implementación, puesta en marcha y prestación continuada de los servicios.

4 - POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la empresa representa el compromiso de la organización con los clientes y terceros para garantizar la seguridad de la información, herramientas

físicas, lógicas y organizativas adecuadas para el tratamiento de la información en todas las actividades.
La política de seguridad de la información de la empresa se inspira en los siguientes principios:

1. Garantizar a la organización el pleno conocimiento de la información gestionada y la valoración de su criticidad, con el fin de facilitar la implantación de niveles adecuados de protección.
2. Garantizar el acceso seguro a la información, a fin de evitar el tratamiento no autorizado o sin los derechos necesarios.
3. Asegurar que la organización y terceros colaboren en el tratamiento de la información mediante la adopción de procedimientos encaminados a cumplir con niveles de seguridad adecuados.
4. Asegurar que la organización y los terceros que colaboran en el tratamiento de la información son plenamente conscientes de los problemas de seguridad.
5. Asegurar que las anomalías y accidentes que afecten el sistema de información y los niveles de seguridad corporativa sean reconocidos oportunamente y correctamente gestionados a través de sistemas eficientes de prevención, comunicación y reacción con el fin de minimizar el impacto en el negocio.
6. Asegurar que el acceso a las oficinas y locales individuales de la empresa sea realizado exclusivamente por personal autorizado, para garantizar la seguridad de las áreas y bienes presentes.
7. Velar por el cumplimiento de los requisitos legales y el cumplimiento de los compromisos de seguridad establecidos en los contratos con terceros.
8. Garantizar la detección de eventos anómalos, accidentes y vulnerabilidades de los sistemas de información para respetar la seguridad y disponibilidad de los servicios y la información.
9. Asegurar la continuidad del negocio corporativo y la recuperación ante desastres, mediante la aplicación de los procedimientos de seguridad establecidos.

La política de seguridad de la información está formalizada en el SGSI, se actualiza constantemente para asegurar su mejora continua y se comparte con la organización, terceros y clientes, a través de un sistema de intranet y canales de comunicación específicos.

5 - RESPONSABILIDAD DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección es responsable del sistema de gestión segura de la información, acorde con la evolución del contexto empresarial y de mercado, evaluando las acciones a tomar ante eventos como:

- desarrollos comerciales significativos
- nuevas amenazas en comparación con las consideradas en la actividad de análisis de riesgos
- incidentes de seguridad significativos
- evolución del contexto normativo o legislativo en relación con el tratamiento seguro de la información

Anexo 4 – Procedimiento de auditorías internas

1 - PROPÓSITO

A través de este procedimiento se quiere:

- definir los procedimientos para la realización de auditorías internas, entendidas como momentos de colaboración e intercambio de información entre los distintos sectores de la organización y dirigidas a:
  - verificar cualitativamente la organización;
  - evaluar la configuración y gestión de los diversos procesos;
  - detectar fortalezas y "buenas prácticas";
  - identificar áreas y oportunidades de mejora;
  - emprender las estrategias de mejora apropiadas
- garantizar que las auditorías internas se planifiquen cuidadosamente y que sus resultados se documenten y se publiquen.

2 - CAMPO DE APLICACIÓN

El procedimiento es aplicable a todas las auditorías internas relacionadas con la implantación de la certificación ISO 27001. Por Auditoría entendemos un proceso sistemático, independiente y documentado para verificar las actividades inherentes al Sistema de Gestión, los resultados obtenidos y si lo elaborado se implementa efectivamente y es adecuado para lograr los objetivos. En particular, se considera esencial un adecuado equilibrio entre la atención a los aspectos procesales (documentación) y la observación de hechos concretos y sustanciales.

3 – COMPOSICION DE LOS EQUIPOS DE AUDITORIA

Se requiere que el jefe del equipo tenga como mínimo 2 años de experiencia en la participación a auditorias.
El responsable del sector IT deberá participar a cada auditoría; los otros componentes del equipo deberán tener conocimientos técnicos del área interesada por la auditoría.
Se requiere que, con la excepción del responsable IT, los otros componentes sean independientes de la organización, que tengan conocimientos de la norma ISO27001, capacidad de trabajar en equipo, de comunicar y de preparar informes.

4 – RESPONSABILIDADES

El Responsable del SGSI tiene la responsabilidad de:

- definir el plan anual de auditoría interna;
- definir los objetivos específicos de cada auditoría;
- asegurar la formación de los auditores internos;
- establecer equipos de auditoría;
- gestionar las relaciones con los responsables y grupos sectoriales.

Los equipos de auditoría tienen la responsabilidad de:

- realizar los planes de auditoria;
- realizar las auditorías;
- tomar nota de todas las observaciones relativas a las verificaciones realizadas;
- redactar los informes finales

5 – PLANIFICACIÓN

Las auditorías son planificadas anualmente por el Responsable del SGSI que indica brevemente los objetivos y alcances de las auditorías y los departamentos/unidades sujetos. La aprobación es por el gerente de departamento.

Después de la aprobación del plan anual de auditoría, el Responsable del SGSI compila el programa de auditoría, donde se detalla lo siguiente para cada auditoría a realizar:

- los elementos del sistema de gestión, objetos de auditoría
- la identificación de los documentos de referencia
- las previsiones de tiempos y duración de las principales actividades de auditoría
- la identidad de los miembros del equipo de auditoría

En general, teniendo en cuenta las necesidades organizativas de la empresa, se requiere que se revisen los aspectos con la situación más crítica una vez al año, y los otros críticos una vez cada año y medio. En cualquier caso, es obligatorio que se planifique la revisión de todos los controles del Anexo A como mínimo una vez durante los 3 años del proceso de certificación.
De manera excepcional se establece una primera revisión (adicional) completa del sistema 6 meses después del completamiento de la implantación del SGSI.

Este es el calendario de las revisiones planificadas durante el primer trienio:

Ámbito	ID	Activo	Año 1			Año 2				Año 3			
			M6	M9	M12	M3	M6	M9	M12	M2	M4	M6	M8
Instalaciones [L]	L01	Sala de servidores del proveedor	X				X					X	
	L02	Sala de servidores de la empresa	X				X					X	
	L03	Open space en la empresa	X										
	L04	Laboratorio	X										
	L05	Oficina del jefe de la empresa	X										
	L06	Salas de visitas (3) dep. médico	X										
Hardware [HW]	HW01	Servidores SQL (4)	X				X			X			
	HW02	Servidores MySQL (2)	X				X			X			
	HW03	Servidor Exchange	X						X				
	HW04	Servidor repositorio ficheros	X				X			X			
	HW05	Ordenadores (50)	X								X		
	HW06	Laptop (250)	X								X		
	HW07	Firewall	X						X				
	HW08	Móviles (150)	X								X		
Aplicación [SW]	SW01	S.O. Windows Server 2016	X				X			X			
	SW02	S.O. Ubuntu	X				X			X			
	SW03	S.O. Windows 11	X								X		
	SW04	S.O. Windows 10	X								X		
	SW05	S.O. Windows 7	X								X		
	SW06	MS Office 365	X								X		
	SW07	MS Office 2010	X										
	SW08	MS Visual Studio 17	X					X					
	SW09	Adobe Acrobat Professional	X								X		
	SW10	ERP	X				X			X			
	SW11	Aplicación WinForm	X					X					
	SW12	Web App	X					X					
	SW13	Antivirus Kaspersky	X								X		
	SW14	SQL Management Studio	X				X			X			
	SW15	MySQL Management	X				X			X			
	SW16	Programas de backup	X				X			X			
	SW17	S.O. Móviles - IOS	X								X		
	SW18	S.O. Móviles - Android	X								X		

Ámbito	ID	Activo	Año 1			Año 2				Año 3			
			M6	M9	M12	M3	M6	M9	M12	M2	M4	M6	M8
Datos [D]	D01	Datos de las empresas clientes	X			X							X
	D02	Datos personales sensibles	X			X							X
	D03	Logs	X										X
	D04	Copias de seguridad de las BD	X			X							X
	D05	Archivos de documentación	X				X						X
	D06	Código fuente	X					X		X			
Red [COM]	COM01	Cableado eléctrico	X									X	
	COM02	Cableado de telecomunicaciones	X									X	
	COM03	Red inalámbrica	X									X	
Servicios [S]	S01	Correo electrónico	X						X				
	S02	Acceso web	X			X							X
	S03	VPN	X			X							X
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización	X				X					X	
	AUX02	Sistema de detección de incendios	X				X					X	
	AUX03	UPS	X				X					X	
	AUX04	Extintores	X				X					X	
Personal [P]	P01	Jefe de la empresa	X										
	P02	Responsable IT	X										
	P03	Otros empleados sector IT	X										
	P04	Consultores	X										
	P05	Médicos laborales	X										
	P06	Empleados administrativos	X										

Es posible que también se realicen auditorías en periodos no planificados, en el caso que se cumple alguna de las siguientes condiciones:

- Detección de una anomalía grave en uno de los elementos del sistema de gestión
- Cambios de proceso o reorganizaciones internas de departamentos/unidades ya inspeccionadas
- Control de las medidas correctoras implantadas
- Cambios legislativos

6 - REALIZACIÓN DE LA AUDITORÍA

El equipo de auditoría procede según lo establecido en el programa de auditoría, a través de entrevistas, examen de documentación y registros y observaciones sobre la utilidad y condiciones de funcionamiento. Debe recabar un número suficiente de evidencias objetivas para determinar el cumplimiento del departamento/unidad auditado con los requisitos preestablecidos.

7 - INFORME DE AUDITORÍA

El equipo de auditoría luego elabora un informe que incluye:

- Objetivos y alcance de la auditoría
- La lista de personas contactadas e involucradas.
- Un resumen de los resultados y una evaluación crítica de la eficacia de los elementos examinados en el sistema de gestión
- La descripción de las no conformidades.

Este informe se distribuye al Responsable del SGSI y al gerente del departamento / unidad inspeccionado.

8 - ARCHIVO

La documentación producida es archivada por el Responsable del SGSI.

Anexo 5 – Gestión de indicadores

1 - PROPÓSITO

Se detallan los indicadores que utiliza la empresa para controlar el funcionamiento de las medidas de seguridad de la información que se van a implantar, así como su eficacia y eficiencia: se indican también los mecanismos y la periodicidad de medida de cada uno.

2 – TABLA DE INDICADORES

N.	Nombre	Control	Objetivo	Formula	Period.	Valor objetivo	Valor umbral	Responsable
01	Políticas de seguridad	5.1.2	Verificar que la dirección revisa el documento	Revisiones / Año	Anual	2	1	Responsable SGSI
02	Roles y responsabilidades	6.1.1	Verificar si se han asignado todos los roles y responsabilidades en seguridad de la información	(Tareas de seguridad con responsable / Tareas de seguridad)	Anual	100%	80%	Responsable IT
03	Antecedentes de los nuevos empleados	7.1.1	Verificar si se han comprobado los antecedentes de los nuevos trabajadores	(N° revisados / nuevos empleados)	Anual	100%	80%	Responsable HR
04	Eficacia de la formación	7.2.2	Comprobar la eficacia de los cursos de formación relativos a la seguridad	Medida de encuestas de valoración	Anual	9	7.5	Responsable sector formación
05	Disciplina	7.2.3	Verificar cuántas acciones de los trabajadores han provocado brechas de seguridad	Sanciones / Año	Anual	0	3	Responsable IT
06	Inventario de activos	8.1.1	Verificar si se han identificado los activos relevantes	Activos inventariados / Activos totales	Trimestral	100%	80%	Responsable SGSI
07	Propiedad de activos	8.1.2	Verificar si todos los activos tienen un propietario	Activos con propietario / Activos totales	Trimestral	100%	80%	Responsable IT
08	Devolución de activos	8.1.4	Verificar si todos los activos que deberían ser devueltos lo han sido	Activos devueltos / Activos que deberían ser devueltos	Trimestral	100%	90%	Responsable IT
09	Eliminación de soportes	8.3.2 11.2.7	Medida del porcentaje de eliminación segura de los soportes eliminados	Soportes eliminados de forma segura / Soportes eliminados	Trimestral	100%	90%	Responsable IT

10	Accesos no autorizados	9.1.2	Medida de la cantidad de accesos no autorizados a la organización	Accesos no autorizados / Accesos totales	Trimestral	0%	1%	Responsable IT
11	Derechos de acceso	9.2.1 9.2.2 9.2.3 9.2.5 9.2.6	Medida de la eficaz de la gestión de la asignación, modificación y eliminación de los derechos de acceso	Trabajadores con derecho de acceso / Total trabajadores	Trimestral	100%	95%	Responsable IT
12	Cifrado de la información sensible	10.1.1	Medida de la encriptación de los datos sensibles	Columnas de tablas con datos sensibles cifrados / Columnas de tablas con datos sensibles	Anual	100%	90%	Responsable IT
13	Protección física	11.1.1 11.1.2 11.1.3	Medida de la eficaz de la protección física de los locales	Intrusiones / (Intrusiones + intentos sin éxito)	Anual	0%	1%	Administrador de la empresa
14	Interrupciones del suministro eléctrico	11.2.2	Medida de la capacidad de los UPS de garantizar la continuidad de equipos y servidores	Equipos caídos por falta de alimentación / (N° interrupciones suministro * Equipos que han sufrido interrupción)	Anual	0	1%	Responsable equipo técnico
15	Protección de los sistemas	12.2.1	Verificar cuántos sistemas no están protegidos y constituyen un peligro	Equipos sin software de protección / Equipos totales	Mensual	0%	0%	Técnico 1 IT
16	Software malicioso	12.2.1	Medida del número de ataques potenciales	Software malicioso detectado / Mes	Mensual	0	10	Técnico 1 IT
17	Backup	12.3.1	Medida de la ejecución correcta de las copias de seguridad	Backup con éxito / Backup	Semestral	100%	98%	Técnico 2 IT
18	Software no autorizado	12.6.2	Verificar cuánto software no autorizado (y potencialmente peligroso) se ha instalado	Software no autorizado / Software instalado	Anual	0%	5%	Técnico 2 IT
19	Proveedores	15.2.1	Verificar la fiabilidad de los proveedores	N° incumplimientos de proveedores / Semestre	Semestral	0	1	Responsable IT
20	Eventos de seguridad	16.1.2	Medida de los problemas de seguridad detectados	N° de notificaciones / Trimestre	Trimestral	0	2	Responsable IT
21	Puntos débiles de seguridad	16.1.3	Medida de los problemas de seguridad detectados	N° de notificaciones / Trimestre	Semestral	0	1	Responsable IT

22	Continuidad de negocio	17.1.2	Verificar la fiabilidad de los sistemas	N° procesos interrumpidos / N° procesos	Trimestral	0%	5%	Responsable IT
23	Software licenciado	18.1.2	Medida del cumplimiento de los derechos de copyright	N° licencias / N° software instalado	Semestral	100%	98%	Técnico 2 IT

Anexo 6 - Procedimiento de Revisión por la Dirección

La dirección de la empresa deberá revisar periódicamente el Sistema de Gestión de Seguridad de la Información, según lo que el mismo SGSI implantado establece. Esto permitirá evaluar si el sistema está funcionando correctamente o si es necesario cambiar o mejorar unos controles.

Los objetivos del procedimiento son:
- Revisar la política de seguridad de la información
- Revisar los objetivos y analizar su cumplimiento
- Identificar cambios en la organización
- Identificar nuevas amenazas y cambios en los niveles de riesgo
- Identificar cambios legislativos
- Analizar la eficacia de las medidas tomadas y la necesidad de cambios o mejorías
- Documentar los resultados de la revisión

1 - PLANIFICACIÓN

El sistema será comprobado según el calendario establecido para los procedimientos de auditorías internas. La revisión deberá completarse dentro de 2 semanas de la entrega a la dirección de los resultados de las auditorías internas.

2 - REVISIÓN

La dirección, siguiendo los informes recibidos y coadyuvada por el responsable del SGSI, deberá:

a) Revisar el estado de las acciones definidas en las revisiones anteriores (si existen): se verificará si las acciones propuestas han sido realizadas, y qué resultados aportaron.
b) Examinar los cambios (internos o externos a la empresa) que pueden afectar el SGSI: el responsable del SGSI deberá comunicar a la dirección, anteriormente a la revisión, los cambios que pueden ser relevantes, para que esta los pueda revisar.
c) Revisar las informaciones de retroalimentación de rendimiento: no conformidades, acciones correctivas, auditorias precedentes, resultados esperados y obtenidos según lo establecido en la gestión de indicadores.
d) Analizar los comentarios de las áreas interesadas (técnicos de la empresa, usuarios, proveedores), que deberán ser recogidas anteriormente a la revisión por el responsable del SGSI.
e) Revisar el informe de riesgos y la situación de las acciones tomadas, comprobando si son conformes al plan de actuación.
f) Revisar las oportunidades de mejoría: se comprobará si las recomendaciones recibidas en las últimas auditorías (externas o internas) revisadas han sido aplicadas y se evaluarán otras eventuales sugerencias recibidas.

3 - ENTRADAS

Se tomarán consecuentemente en cuenta:
- Resultados de revisiones antecedentes
- Resultados de los indicadores establecidos
- Resultados de auditorías internas
- Non conformidades recibidas

- Cambios en la organización
- Sugerencias recibidas
- Legislación vigente

4 - SALIDAS

Se producirá un informe de revisión, documento en el cual deberán aparecer:
- Actualización de la evaluación de los riesgos
- Eventuales mejorías de controles y procedimientos existentes
- Eventual introducción de nuevos controles y procedimientos

Anexo 7 – Gestión de Roles y Responsabilidades

A continuación se van a detallar roles y responsabilidades establecidos por la dirección para el Sistema de Gestión de la Seguridad de la Información.

1 - Comité de Seguridad

El comité de seguridad de la empresa está formado por:

- Director de la empresa;
- Gerente del sector IT
- Consultor externo, experto de la norma ISO/IEC 27001
- Responsable del proveedor

Sus funciones y responsabilidades son:

- Establecer los objetivos y las políticas de seguridad
- Asignar roles y responsabilidades a los involucrados con el SGSI
- Validar el análisis de los riesgos y las medidas tomadas
- Aprobar y supervisar la aplicación del plan de seguridad
- Supervisar el plan de continuidad
- Comprobar la legislación vigente
- Revisar periódicamente la evolución y la eficacia del SGSI
- Analizar los resultados de los indicadores elegidos
- Favorecer la concienciación y la formación de los empleados

2 - Responsable de la seguridad

Es el gerente del sector IT. Deberá:

- Elaborar, desarrollar y gestionar la política de seguridad
- Ser responsable de la implantación del SGSI
- Supervisar la aplicación de las medidas elegidas
- Supervisar el seguimiento de los incidentes de seguridad
- Comprobar el funcionamiento de los indicadores y aprobar nuevos, si necesario
- Informar al Comité de Seguridad
- Proponer nuevos objetivos
- Coordinar las actividades de los equipos
- Coordinar las auditorías internas

3 - Técnicos del sector IT

Dependiendo de sus conocimientos, experiencia y ámbito laboral, deberán:

- Implantar y comprobar las medidas correctivas
- Gestionar los informes de los indicadores
- Revisar la seguridad de su área de competencia
- Colaborar con los otros para la gestión de la seguridad
- Sugerir nuevas necesidades
- Gestionar los permisos de acceso de los usuarios
- Gestionar las copias de seguridad
- Gestionar los programas, la criptografía, la red…
- Informar al responsable sobre eventuales problemas
- Sugerir posibles mejorías

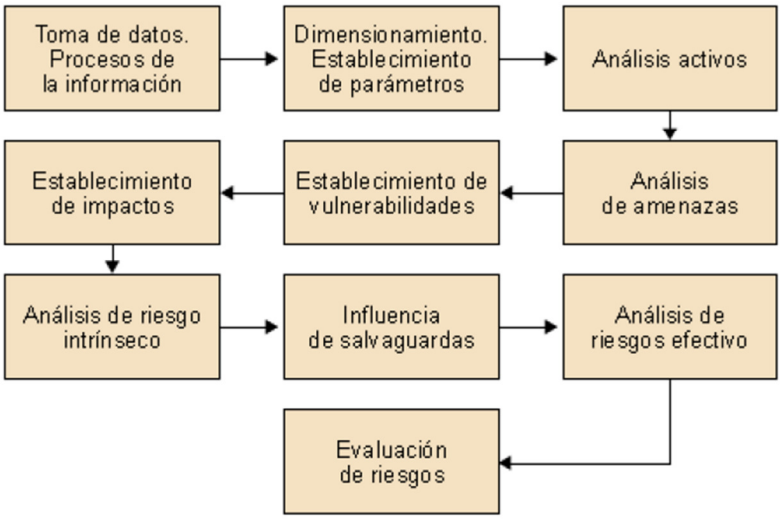
4 - Otros trabajadores

Deberán:

- Utilizar de manera adecuada los activos de la organización
- Evitar comportamientos que puedan poner en peligro la organización
- Respetar la política de seguridad de la empresa
- Informar sobre posibles problemas de seguridad encontrados
- Mantener la confidencialidad de la información
- Respetar la legislación vigente

Anexo 8 – Metodología de Análisis de Riesgos

La metodología elegida por la empresa para la implantación del SGSI es Magerit, elaborada por el español MAP (Ministerio de Administraciones Públicas), actualmente en la versión 3 y estructurada en 3 libros (Método, Catálogo de elementos y Guía de técnicas).
Se trata de un proceso compuesto por diferentes fases, que aparecen en la imagen siguiente y que se van a resumir a continuación:



Fuente: Cruz Allende D., Tortajada Gallego A., Segovia Henares A.J. (2020), *Análisis de riesgos*, pág. 18

En primer lugar será necesario elegir el alcance, definir el nivel de detalle deseado y, consecuentemente a esto, inventariar los activos que se tomarán en cuenta y analizar los procesos de la empresa.
Durante la segunda fase, fundamental, se deben individuar los parámetros que serán utilizados durante todo el análisis:

- Valoración económica de los activos: debe tener en cuenta el valor de reposición (si se pierde o no es utilizable), de configuración (tiempo de la adquisición a cuando se ha configurado y se puede utilizar), el valor que se pierde mientras no se puede utilizar para su función, y el valor de pérdida de oportunidad
- Valoración de las vulnerabilidades según su ocurrencia temporal
- Valoración del impacto, es decir el porcentaje del valor del activo perdido al materializarse un riesgo sobre el
- Efectividad del control de seguridad, es decir cuánto, en porcentaje, una medida puede reducir el riesgo inicial.

Todos estos parámetros se clasifican, según su valoración, en una escalera con grados "Muy Alto, Alto, Medio, Bajo, Muy Bajo".
Luego se analizarán los activos que son relacionados con el alcance de la certificación, clasificándolos según su valoración económica.
La cuarta fase es el análisis de las amenazas, es decir de aquellas situaciones que podrían verificarse llegando a un problema de seguridad: pueden ser accidentes, consecuencias de errores o de comportamientos intencionales.
Se establecen las vulnerabilidades estimando su frecuencia de ocurrencia.
De la misma manera se evalúan cuáles pueden ser las posibles consecuencias de la materialización de las amenazas sobre los activos.

El riesgo intrínseco se define como el valor del activo multiplicado por su vulnerabilidad y el impacto: no se tienen en cuenta las medidas de seguridad que pueden existir en la organización. Además cabe destacar que, aunque la metodología Magerit no lo prevé, la norma ISO27001 requiere la asignación de un propietario a cada riesgo.
Consecuente al análisis anterior se deben escoger las mejores soluciones posibles para reducir el riesgo: las medidas de seguridad pueden ser preventivas (reducen la ocurrencia de las vulnerabilidades) o correctivas (reducen el impacto de las amenazas).
Eso permite evaluar el riesgo efectivo, que se calcula multiplicando el valor activo por la vulnerabilidad y su porcentaje de disminución, y por el impacto y su porcentaje de disminución.

En resumen:
Riesgo intrínseco = Valor del activo * Vulnerabilidad * Impacto
Riesgo efectivo = Valor activo * (Vulnerabilidad * Porcentaje de disminución) * (Impacto * Porcentaje de disminución) = Riesgo intrínseco * Porcentaje de disminución de vulnerabilidad * Porcentaje de disminución de impacto

La última fase consiste en la decisión de cómo gestionar los riesgos: se pueden reducir eligiendo las medidas de seguridad que se implementarán, entre todas aquellas disponibles), transferir o aceptarlos. Es necesario elaborar un plan de acción que contenga las prioridades de gestión (no se pueden gestionar todos los riesgos contemporáneamente, así que es necesario establecer cuáles son más importantes), el análisis de costes y beneficios para cada medida posible, la selección final de aquellas a implantar, su asignación a responsables y la implantación de controles.

Anexo 9 - Declaración de Aplicabilidad

En la siguiente tabla, por cada uno de los controles de la ISO/IEC 27002:2013 se especifica si deben ser aplicados al SGSI de la empresa.

CONTROL	APLICA	JUSTIFICACIÓN DE LA VALORACIÓN / EVIDENCIAS
A.5. Políticas de seguridad de la información **A.5.1. Directrices de la dirección en seguridad de la información**		
5.1.1. Políticas para la seguridad de la información	**SI**	Las políticas de seguridad de la información son necesarias para establecer las normas de seguridad de la empresa. Deben ser aprobadas por la dirección y comunicadas a los trabajadores.
5.1.2. Revisión de las políticas para la seguridad de la información	**SI**	Es necesario revisarlas periódicamente o cuando ocurren cambios significativos.
A.6. Organización de la seguridad de la información **A.6.1. Organización interna**		
6.1.1. Roles y responsabilidades en la seguridad de la información.	**SI**	La norma requiere la asignación de roles y responsabilidades.
6.1.2. Segregación de tareas.	**SI**	Requerida por la norma, es necesaria para reducir el riesgo de accesos y modificaciones no autorizadas.
6.1.3. Contacto con las autoridades.	**SI**	Necesario.
6.1.4. Contacto con grupos de interés especial.	**SI**	Necesario.
6.1.5. Seguridad de la información en la gestión de proyectos.	**SI**	En los proyectos se deben tener en cuentas los aspectos de la seguridad de la información.
A.6. Organización de la seguridad de la información **A.6.2. Los dispositivos móviles y el teletrabajo**		
6.2.1. Política de dispositivos móviles	**SI**	Es necesario gestionar los riesgos del uso de dispositivos móviles.
6.2.2. Teletrabajo	**SI**	Es necesario gestionar los riesgos del teletrabajo
A.7. Seguridad ligada a los recursos humanos **A.7.1. Antes del empleo**		
7.1.1. Investigación de antecedentes	**SI**	Necesario. La investigación se hará de acuerdo con la legislación vigente.
7.1.2. Términos y condiciones del empleo	**SI**	Los acuerdos de empleo deben incluir cláusulas de confidencialidad, de protección de datos y de derechos de propiedad intelectual.
A.7. Seguridad ligada a los recursos humanos **A.7.2. Durante el empleo**		
7.2.1. Responsabilidades de gestión	**SI**	Empleados y contratistas deben aplicar la seguridad de la información según las políticas y procedimientos establecidos en la empresa
7.2.2. Concienciación, educación y capacitación en Seguridad de la Información	**SI**	Es necesario para la mejoría y para que todos reciban una adecuada educación y concienciación sobre las políticas y procedimientos.
7.2.3. Proceso disciplinario	**SI**	Es necesario establecer las acciones a tomar ante los empleados que provocan brechas de seguridad.

A.7. Seguridad ligada a los recursos humanos **A.7.3. Finalización del empleo o cambio en el puesto de trabajo**		
7.3.1. Responsabilidades ante la finalización o cambio	**SI**	Es necesario definir y comunicar a los empleados las responsabilidades y obligaciones que deben cumplir.
A.8. Gestión de activos **A.8.1. Responsabilidad sobre los activos**		
8.1.1. Inventario de activos	**SI**	Necesario para una correcta evaluación de los riesgos.
8.1.2. Propiedad de los activos	**SI**	Es necesario que cada activo tenga un responsable de su adecuada gestión.
8.1.3. Uso aceptable de los activos	**SI**	Los usuarios deben ser responsables del uso que hacen de los recursos de tratamiento de información.
8.1.4. Devolución de activos	**SI**	Es necesario formalizar un proceso de devolución de los activos físicos y electrónicos de propiedad de la empresa.
A.8. Gestión de activos **A.8.2. Clasificación de la información**		
8.2.1. Clasificación de la información	**SI**	Es necesario conocer la importancia de la revelación o modificación de la información, frente a requisitos legales, criticidad, sensibilidad y valor.
8.2.2. Etiquetado de la Información	**SI**	La información debe ser etiquetada según su clasificación.
8.2.3. Manipulación de la información	**SI**	Es necesario establecer procedimientos para la manipulación de la información, dependientes de su clasificación.
A.8. Gestión de activos **A.8.3. Manejo de soportes de almacenamiento**		
8.3.1. Gestión de soportes extraíbles	**SI**	Es necesario implementar procedimientos para la gestión de soportes extraíbles.
8.3.2. Eliminación de soportes.	**SI**	Los soportes deben ser destruidos de forma segura, para minimizar el riesgo de filtraciones de información confidencial o sensible a personas no autorizadas.
8.3.3. Soportes físicos en tránsito	**SI**	Es necesario proteger los soportes durante su transporte fuera de la organización.
A.9. Control de acceso **A.9.1. Requisitos de negocio para el control de acceso**		
9.1.1. Política de control de acceso	**SI**	Se debe establecer una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
9.1.2. Acceso a redes y a los servicios en red	**SI**	Es necesario autorizar específicamente los usuarios al uso de redes y servicios.
A.9. Control de acceso **A.9.2. Gestión de acceso de usuario**		
9.2.1. Registro y baja de usuario	**SI**	Es necesario gestionar los derechos de acceso de todos los usuarios.
9.2.2. Provisión de acceso de usuario	**SI**	Es necesario gestionar los derechos de acceso de todos los usuarios.
9.2.3. Gestión de privilegios de acceso	**SI**	Es necesario gestionar los derechos de acceso de todos los usuarios.
9.2.4. Gestión de la información secreta de autenticación de los usuarios	**SI**	La información de autenticación de cada usuario debe mantenerse secreta.
9.2.5. Revisión de los derechos de acceso de usuario	**SI**	Es necesario gestionar los derechos de acceso de todos los usuarios.

9.2.6. Retirada o reasignación de los derechos de acceso	**SI**	Es necesario gestionar los derechos de acceso de todos los usuarios.
A.9. Control de acceso **A.9.3. Responsabilidades de usuario**		
9.3.1. Uso de información secreta de autenticación	**SI**	La información de autenticación de cada usuario debe mantenerse secreta.
A.9. Control de acceso **A.9.4. Control de acceso a sistemas y aplicaciones**		
9.4.1. Restricción del acceso a la información.	**SI**	Se debe restringir el acceso a la información según la política de control de acceso
9.4.2. Procedimientos seguros de inicio de sesión	**SI**	Es necesario establecer un procedimiento seguro de inicio de sesión.
9.4.3. Sistema de gestión de contraseñas.	**SI**	Es fundamental utilizar contraseñas seguras y robustas.
9.4.4. Uso de utilidades con privilegios del sistema	**SI**	El uso de utilidades con privilegios del sistema debe ser restringido.
9.4.5. Control de acceso al código fuente de los programas	**SI**	Es necesario controlar y restringir el acceso al código fuente de los programas.
A.10. Cifrado **A.10.1. Controles criptográficos**		
10.1.1. Política de uso de los controles criptográficos	**SI**	Es necesario implementar una política sobre el uso de los controles criptográficos para proteger la información.
10.1.2. Gestión de claves	**SI**	Las claves de cifrado deben ser protegidas.
A.11. Seguridad física y ambiental **A.11.1. Áreas seguras**		
11.1.1. Perímetro de seguridad física	**SI**	Las áreas que contienen información sensible deben estar protegidas físicamente.
11.1.2. Controles físicos de entrada	**SI**	Las áreas seguras deben estar protegidas físicamente y permitir el acceso solo a los autorizados.
11.1.3. Seguridad de oficinas, despachos y recursos	**SI**	Deben estar protegidos físicamente.
11.1.4. Protección contra las amenazas externas y ambientales	**SI**	Es necesario establecer una protección física contra desastres naturales y daños causados por el hombre.
11.1.5. El trabajo en áreas seguras	**SI**	Deben implementarse procedimientos para trabajar en áreas seguras.
11.1.6. Áreas de carga y descarga	**SI**	Es necesario evitar accesos no autorizados a las instalaciones.
A.11. Seguridad física y ambiental **A.11.2. Seguridad de los equipos**		
11.2.1. Emplazamiento y protección de equipos	**SI**	Los equipos deben estar protegidos.
11.2.2. Instalaciones de suministro	**SI**	Hay que evitar alteraciones causadas por fallos en las instalaciones de suministro.
11.2.3. Seguridad del cableado	**SI**	El cableado eléctrico y de telecomunicaciones debe estar protegido frente a interceptaciones, interferencias o daños.
11.2.4. Mantenimiento de los equipos	**SI**	Es necesario garantizar disponibilidad e integridad de los equipos.
11.2.5. Retirada de materiales propiedad de la empresa	**SI**	Es necesario establecer un procedimiento para sacar los activos fuera de la empresa.
11.2.6. Seguridad de los equipos fuera de las instalaciones	**SI**	Deben aplicarse medidas de seguridad a los equipos fuera de las instalaciones.

11.2.7. Reutilización o eliminación segura de equipos	**SI**	Se debe comprobar la eliminación segura de datos sensibles y software bajo licencia antes de eliminar o reutilizar los equipos.
11.2.8. Equipo de usuario desatendido	**SI**	El equipo desatendido debe estar protegido.
11.2.9. Política de puesto de trabajo despejado y pantalla limpia	**SI**	Pantalla y puestos de trabajo no deben tener información confidencial.
A.12. Seguridad en las operaciones **A.12.1. Responsabilidades y procedimientos de operación**		
12.1.1. Documentación de procedimientos de operación	**SI**	Los procedimientos de operación deben documentarse y estar a disposición de aquellos que los necesitan.
12.1.2. Gestión de cambios	**SI**	Deben controlarse todos los cambios que afectan a la seguridad de la información.
12.1.3. Gestión de capacidades	**SI**	Es necesario supervisar la utilización de los recursos y ajustarla para garantizar el rendimiento requerido.
12.1.4. Separación de recursos de desarrollo, prueba y operación	**SI**	Los recursos de desarrollo, prueba y operación deben separarse.
A.12. Seguridad en las operaciones **A.12.2. Protección contra código malicioso**		
12.2.1. Controles contra el código malicioso	**SI**	Es necesario proteger los equipos del código malicioso y concienciar a los usuarios.
A.12. Seguridad en las operaciones **A.12.3. Copias de seguridad**		
12.3.1. Copias de seguridad de la información	**SI**	Se deben hacer copias de seguridad y verificarlas periódicamente.
A.12. Seguridad en las operaciones **A.12.4. Registro de actividad y supervisión**		
12.4.1. Registro de eventos	**SI**	Es necesario registrar actividades de los usuarios, fallos, excepciones y eventos de seguridad.
12.4.2. Protección de la información de registro	**SI**	Deben protegerse las informaciones del registro contra accesos no autorizados y modificaciones.
12.4.3. Registros de administración y operación	**SI**	Es necesario registrar actividades de los administradores y operadores de sistemas.
12.4.4. Sincronización del reloj	**SI**	Los relojes de todos los sistemas de tratamiento de la información de la organización deben estar sincronizados.
A.12 seguridad en las operaciones **A.12.5 control del software en explotación**		
12.5.1. Instalación del software en explotación	**SI**	Debe controlarse el software en explotación así como sus actualizaciones.
A.12 seguridad en las operaciones **A.12.6 gestión de la vulnerabilidad técnica**		
12.6.1. Gestión de las vulnerabilidades técnicas	**SI**	Es necesario disponer de las informaciones de las vulnerabilidades técnicas de los activos.
12.6.2. Restricciones en la instalación de software	**SI**	Los usuarios no deben tener permisos de instalación de software.
A.12. Seguridad en las operaciones **A.12.7. Consideraciones sobre las auditorías de los sistemas de información**		
12.7.1. Controles de auditoría de sistema de información	**SI**	Es necesario planificar las actividades de auditorías.

A.13. Seguridad de las comunicaciones **A.13.1. Gestión de la seguridad en redes**		
13.1.1. Controles de red	**SI**	Es necesario gestionar y proteger la red.
13.1.2. Seguridad en los servicios de red	**SI**	Es necesario gestionar y proteger los servicios de red
13.1.3. Segregación en redes.	**SI**	Los distintos grupos deben estar segregados en redes distintas.
A.13. Seguridad de las comunicaciones **A.13.2. Intercambio de información con partes externas**		
13.2.1. Políticas y procedimientos de intercambio de información	**SI**	Deben establecerse procedimientos o controles para proteger el intercambio de información.
13.2.2. Acuerdos de intercambio de información	**SI**	La empresa y los terceros deben acordarse para el intercambio seguro de información y software.
13.2.3. Mensajería electrónica	**SI**	Debe protegerse la información objeto de mensajería electrónica.
13.2.4. Acuerdos de confidencialidad o no revelación	**SI**	La empresa debe establecer acuerdos de confidencialidad con empleados y proveedores.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.1. Requisitos de seguridad de los sistemas de información**		
14.1.1. Análisis de requisitos y especificaciones de seguridad de la información	**SI**	Se requiere la inclusión de los requisitos relacionados con la seguridad de la información en los requisitos para los nuevos sistemas de información o para las mejoras de los sistemas existentes.
14.1.2. Asegurar los servicios de aplicaciones en redes públicas	**SI**	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida.
14.1.3. Protección de las transacciones de servicios de aplicaciones	**SI**	La información involucrada en transacciones de servicios debe ser protegida contra transmisión incompleta, errores de enrutamiento, alteración, revelación, duplicación o reproducción no autorizada.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.2. Seguridad en los procesos de desarrollo y soporte**		
14.2.1. Política de desarrollo seguro	**SI**	Deben existir reglas para el desarrollo seguro de software.
14.2.2. Procedimiento de control de cambios en sistemas	**SI**	Los cambios deben controlarse a través de procedimientos formales.
14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios el sistema operativo	**SI**	Cuando se modifican los sistemas operativos deben revisarse y probar las aplicaciones críticas de negocio.
14.2.4. Restricciones a los cambios en los paquetes de software	**SI**	Los cambios en los paquetes de software deben limitarse a aquellos necesarios y deben ser controlados rigurosamente.
14.2.5. Principios de ingeniería de sistemas seguros	**SI**	Los procedimientos de ingeniería de sistemas de información seguros deben aplicarse a las implantaciones de sistemas de información.
14.2.6. Entorno de desarrollo seguro	**SI**	Es necesario utilizar un procedimiento de desarrollo seguro para proteger adecuadamente el entorno.
14.2.7. Externalización del desarrollo de software	**NO**	No hay software desarrollado externamente
14.2.8. Pruebas funcionales de seguridad de sistemas	**SI**	Las prácticas de desarrollo seguro deben incluir pruebas de la seguridad funcional durante el desarrollo.
14.2.9. Pruebas de aceptación	**SI**	El procedimiento de desarrollo seguro establece

de sistemas		programas de prueba de aceptación y criterios relacionados para nuevos sistemas o actualizaciones.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.3. Datos de prueba**		
14.3.1. Protección de los datos de prueba	**SI**	Debe evitarse el uso de datos reales personales o confidenciales para las pruebas.
A.15. Relaciones con los proveedores **A.15.1. Seguridad de la información en las relaciones con los proveedores**		
15.1.1. Política de seguridad de la información en las relaciones con los proveedores	**SI**	Es necesario acordarse con los proveedores para mitigar los riesgos asociados con sus accesos a los activos de la organización.
15.1.2. Requisitos de seguridad en contratos con terceros	**SI**	Deben documentarse los acuerdos con los proveedores y las obligaciones de ambas partes.
15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones	**SI**	Se deben gestionar los riesgos de la cadena de suministro TIC.
A.15. Relaciones con los proveedores **A.15.2. Gestión de la prestación del servicio de los proveedores**		
15.2.1. Control y revisión de la provisión de servicios del proveedor	**SI**	Se debe controlar, revisar y auditar la provisión de servicios de los proveedores.
15.2.2. Gestión de cambios en la provisión del servicio del proveedor	**SI**	Debe establecerse un procedimiento para gestionar los cambios en la provisión del servicio.
A.16. Gestión de incidentes de seguridad de la información **A.16.1. Gestión de incidentes de seguridad de la información y mejoras**		
16.1.1. Responsabilidades y procedimientos	**SI**	Responsabilidades y procedimientos de gestión de los incidentes de seguridad son fundamentales para garantizar una respuesta rápida, efectiva y adecuada.
16.1.2. Notificación de los eventos de seguridad de la información.	**SI**	Es necesario que trabajadores, contratistas y terceros sean adecuadamente formados y comuniquen cualquier evento de seguridad de la información.
16.1.3. Notificación de puntos débiles de la seguridad	**SI**	Los usuarios deben anotar y notificar los puntos débiles observados o sospechados de existir.
16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información	**SI**	Debe evaluarse los eventos de seguridad de la información, y seguir un riguroso procedimiento para poderlos clasificar como incidentes de seguridad de información.
16.1.5. Respuesta a incidentes de seguridad de la información.	**SI**	Deben existir procedimientos documentados para responder a los incidentes de seguridad de la información.
16.1.6. Aprendizaje de los incidentes de seguridad de la información.	**SI**	Es necesario disfrutar del conocimiento obtenido de la resolución de incidentes de seguridad para reducir la probabilidad o el impacto de los incidentes futuros, pero no siempre.
16.1.7. Recopilación de evidencias	**SI**	Es necesario definir procedimientos de recogida de evidencias.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.1. Continuidad de la seguridad de la información**		
17.1.1. Planificación de la continuidad de la seguridad de la información	**SI**	La continuidad de los procesos debe formar parte de los sistemas de gestión de continuidad del negocio.

17.1.2. Implementar la continuidad de la seguridad de la información	**SI**	Consecuentemente deben establecerse planes correspondientes a los análisis del control A.17.1.1.
17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**SI**	Deben verificarse y revisar los planes de continuidad.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.2. Redundancias**		
17.2.1. Disponibilidad de los recursos de tratamiento de la información	**SI**	Es necesario evaluar e implementar la redundancia de recursos de tratamiento de la información necesaria.
A.18. Cumplimiento **A.18.1. Cumplimiento de los requisitos legales y contractuales**		
18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	**SI**	Deben documentarse todos los requisitos pertinentes al sistema de información de la organización.
18.1.2. Derechos de propiedad intelectual (DPI)	**SI**	Deben implementarse controles sobre el uso de productos de software patentados.
18.1.3. Protección de los registros de la organización	**SI**	Los registros de la organización deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado.
18.1.4. Protección y privacidad de la información de carácter personal	**SI**	Debe establecerse un procedimiento para garantizar la protección y la privacidad de los datos.
18.1.5. Regulación de los controles criptográficos	**SI**	Los controles criptográficos deben cumplir con la legislación vigente.
A.18. Cumplimiento **A.18.2. Revisiones de la seguridad de la información**		
18.2.1. Revisión independiente de la seguridad de la información	**SI**	Es necesaria una revisión independiente de la gestión de la seguridad de la información, periódica y cuando se producen cambios significativos.
18.2.2. Cumplimiento de las políticas y normas de seguridad	**SI**	Los directivos deben revisar el cumplimiento de políticas y normas de seguridad.
18.2.3. Comprobación del cumplimiento técnico	**SI**	El cumplimiento técnico de los sistemas de la seguridad de la información debe comprobarse periodicamente.

Anexo 10 – Tabla del análisis de amenazas

	Amenaza	Frecuencia	Activos	A	C	I	D	T
[N] Desastres nat.	[N.1] Fuego	MB	HW				100%	
		MB	AUX				100%	
		MB	L				100%	
	[N.2] Daños por agua	MB	HW				75%	
		MB	AUX				75%	
		MB	L				50%	
[I] De origen industrial	[I.1] Fuego	MB	HW				100%	
		MB	AUX				100%	
		MB	L				100%	
	[I.2] Daños por agua	MB	HW				75%	
		MB	AUX				75%	
		MB	L				50%	
	[I.*] Desastres industriales	MB	HW				75%	
		MB	AUX				50%	
		MB	L				20%	
	[I.3] Contaminación mecánica	B	HW				50%	
		B	AUX				20%	
	[I.4] Contaminación electromagnética	B	HW				75%	
		B	AUX				50%	
	[I.5] Avería de origen físico o lógico	M	SW				20%	
		M	HW				20%	
		M	AUX				20%	
	[I.6] Corte del suministro eléctrico	M	HW				20%	
		M	AUX				75%	
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	HW				50%	
		M	AUX				20%	
	[I.8] Fallo de servicios de comunicaciones	M	COM				75%	
	[I.9] Interrupción de otros servicios y suministros esenciales	A	AUX				20%	
	[I.11] Emanaciones electromagnéticas	MB	HW		50%			
		MB	AUX		75%			
		MB	L		5%			
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	MA	D		75%	75%	5%	
		A	S		50%	20%	5%	
		A	SW		5%	5%	5%	
	[E.2] Errores del administrador	M	D		20%	75%	20%	
		M	S		5%	20%	20%	
		M	SW		5%	5%	5%	
		M	HW		20%	5%	20%	
		M	COM		5%	5%	5%	

	[E.3] Errores de monitorización (log)	M	D			20%		75%
	[E.4] Errores de configuración	M	D			50%		
	[E.7] Deficiencias en la organización	A	P				20%	
	[E.8] Difusión de software dañino	M	SW		75%	75%	75%	
	[E.9] Errores de [re-]encaminamiento	M	S		50%			
		M	SW		50%			
		M	COM		20%			
	[E.10] Errores de secuencia	B	S			5%		
		B	SW			5%		
		B	COM			5%		
	[E.15] Alteración accidental de la información	B	D			20%		
		B	S			5%		
		B	SW			5%		
		B	COM			5%		
		B	L			5%		
	[E.18] Destrucción de información	M	D				20%	
		B	S				20%	
		B	SW				5%	
		B	COM				5%	
		MB	L				5%	
	[E.19] Fugas de información	M	D		75%			
		M	S		50%			
		B	SW		50%			
		B	COM		50%			
		B	L		20%			
		A	P		75%			
	[E.20] Vulnerabilidades de los programas (software)	M	SW		75%	75%	20%	
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	SW			20%	5%	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	HW				20%	
		M	AUX				5%	
	[E.24] Caída del sistema por agotamiento de recursos	M	S				75%	
		M	HW				75%	
		B	COM				75%	
	[E.25] Pérdida de equipos	A	HW		75%		5%	
		B	AUX		20%		20%	
	[E.28] Indisponibilidad del personal	MA	P				5%	
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	B	D			100%		100%
	[A.4] Manipulación de la configuración	B	D	50%	100%	75%		
	[A.5] Suplantación de la identidad del usuario	B	D	75%	100%	75%		
		B	S	75%	100%	75%		
		B	SW	75%	75%	75%		
		B	COM	5%	5%	5%		

[A.6] Abuso de privilegios de acceso	B	D		50%	75%	5%	
	B	S		50%	75%	5%	
	B	SW		50%	75%	5%	
	B	HW		20%	5%	5%	
	B	COM		5%	5%	5%	
[A.7] Uso no previsto	B	S		50%	50%	20%	
	B	SW		20%	20%	20%	
	B	HW		5%	20%	20%	
	B	COM		5%	5%	5%	
	B	AUX		5%	5%	5%	
	B	L		5%	5%	5%	
[A.9] [Re-]encaminamiento de mensajes	MB	S		100%			
	MB	SW		100%			
	MB	COM		75%			
[A.10] Alteración de secuencia	MB	S			5%		
	MB	SW			5%		
	MB	COM			5%		
[A.11] Acceso no autorizado	B	D		100%	100%		
	B	S		100%	100%		
	B	SW		75%	75%		
	B	HW		20%	20%		
	B	COM		20%	20%		
	B	AUX		20%	20%		
	B	L		5%	5%		
[A.12] Análisis de tráfico	MB	COM		5%			
[A.13] Repudio	B	S			5%		75%
	B	D			5%		75%
[A.14] Interceptación de información (escucha)	MB	COM		75%			
[A.15] Modificación deliberada de la información	B	D			100%		
	B	S			75%		
	B	SW			75%		
	B	COM			20%		
	B	L			5%		
[A.18] Destrucción de información	B	D				100%	
	B	S				75%	
	B	SW				75%	
	B	L				100%	
[A.19] Divulgación de información	B	D		100%			
	B	S		75%			
	B	SW		75%			
	B	COM		20%			
	B	L		20%			
[A.22] Manipulación de programas	B	SW		100%	50%	50%	

[A.23] Manipulación de los equipos	B	HW		50%		20%	
	B	AUX		5%		5%	
[A.24] Denegación de servicio	B	S				100%	
	B	HW				50%	
	B	COM				20%	
[A.25] Robo	A	HW		75%		5%	
	B	AUX		5%		5%	
[A.26] Ataque destructivo	MB	HW				100%	
	MB	AUX				100%	
	MB	L				20%	
[A.27] Ocupación enemiga	MB	L		20%		100%	
[A.28] Indisponibilidad del personal	M	P				20%	
[A.29] Extorsión	B	P		50%	50%	5%	
[A.30] Ingeniería social	B	p		75%	75%	5%	

Anexo 11 – Tabla de impacto potencial

Ámbito	ID	Activo	Valor	Dimensiones de seguridad					Impacto					Impacto potencial				
				A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Instalaciones [L]	L01	Sala de servidores del proveedor	MA	0	9	7	9	0	0%	20%	5%	100%	0%	0,00	1,80	0,35	9,00	0,00
	L02	Sala de servidores de la empresa	A	0	7	6	7	0	0%	20%	5%	100%	0%	0,00	1,40	0,30	7,00	0,00
	L03	Open space en la empresa	B	0	3	3	2	0	0%	20%	5%	100%	0%	0,00	0,60	0,15	2,00	0,00
	L04	Laboratorio	MB	0	3	0	1	0	0%	20%	5%	100%	0%	0,00	0,60	0,00	1,00	0,00
	L05	Oficina del jefe de la empresa	MB	0	3	0	1	0	0%	20%	5%	100%	0%	0,00	0,60	0,00	1,00	0,00
	L06	Salas de visitas (3) dep. médico	B	0	6	0	2	0	0%	20%	5%	100%	0%	0,00	1,20	0,00	2,00	0,00
Hardware [HW]	HW01	Servidores SQL (4)	MA	8	9	8	8	8	0%	75%	20%	100%	0%	0,00	6,75	1,60	8,00	0,00
	HW02	Servidores MySQL (2)	MA	8	9	8	8	8	0%	75%	20%	100%	0%	0,00	6,75	1,60	8,00	0,00
	HW03	Servidor Exchange	M	7	8	6	4	3	0%	75%	20%	100%	0%	0,00	6,00	1,20	4,00	0,00
	HW04	Servidor repositorio ficheros	A	7	9	8	7	5	0%	75%	20%	100%	0%	0,00	6,75	1,60	7,00	0,00
	HW05	Ordenadores (50)	B	6	7	3	3	6	0%	75%	20%	100%	0%	0,00	5,25	0,60	3,00	0,00
	HW06	Laptop (250)	M	6	7	3	3	6	0%	75%	20%	100%	0%	0,00	5,25	0,60	3,00	0,00
	HW07	Firewall	M	7	7	6	8	7	0%	75%	20%	100%	0%	0,00	5,25	1,20	8,00	0,00
	HW08	Móviles (150)	B	6	7	6	2	5	0%	75%	20%	100%	0%	0,00	5,25	1,20	2,00	0,00
Aplicación [SW]	SW01	S.O. Windows Server 2016	MA	8	5	6	9	6	75%	100%	75%	75%	0%	6,00	5,00	4,50	6,75	0,00
	SW02	S.O. Ubuntu	MA	8	5	6	8	6	75%	100%	75%	75%	0%	6,00	5,00	4,50	6,00	0,00
	SW03	S.O. Windows 11	B	4	4	4	5	4	75%	100%	75%	75%	0%	3,00	4,00	3,00	3,75	0,00
	SW04	S.O. Windows 10	B	4	4	4	5	4	75%	100%	75%	75%	0%	3,00	4,00	3,00	3,75	0,00
	SW05	S.O. Windows 7	B	4	4	4	5	4	75%	100%	75%	75%	0%	3,00	4,00	3,00	3,75	0,00
	SW06	MS Office 365	B	1	6	4	1	1	75%	100%	75%	75%	0%	0,75	6,00	3,00	0,75	0,00
	SW07	MS Office 2010	MB	1	6	4	1	1	75%	100%	75%	75%	0%	0,75	6,00	3,00	0,75	0,00
	SW08	MS Visual Studio 17	A	6	7	7	8	7	75%	100%	75%	75%	0%	4,50	7,00	5,25	6,00	0,00
	SW09	Adobe Acrobat Professional	B	4	7	4	3	3	75%	100%	75%	75%	0%	3,00	7,00	3,00	2,25	0,00
	SW10	ERP	M	6	9	8	7	6	75%	100%	75%	75%	0%	4,50	9,00	6,00	5,25	0,00
	SW11	Aplicación WinForm	MA	8	9	9	7	6	75%	100%	75%	75%	0%	6,00	9,00	6,75	5,25	0,00
	SW12	Web App	MA	8	9	8	7	6	75%	100%	75%	75%	0%	6,00	9,00	6,00	5,25	0,00
	SW13	Antivirus Kaspersky	M	8	5	8	8	4	75%	100%	75%	75%	0%	6,00	5,00	6,00	6,00	0,00
	SW14	SQL Management Studio	A	6	7	6	8	5	75%	100%	75%	75%	0%	4,50	7,00	4,50	6,00	0,00
	SW15	MySQL Management	A	6	7	6	8	5	75%	100%	75%	75%	0%	4,50	7,00	4,50	6,00	0,00

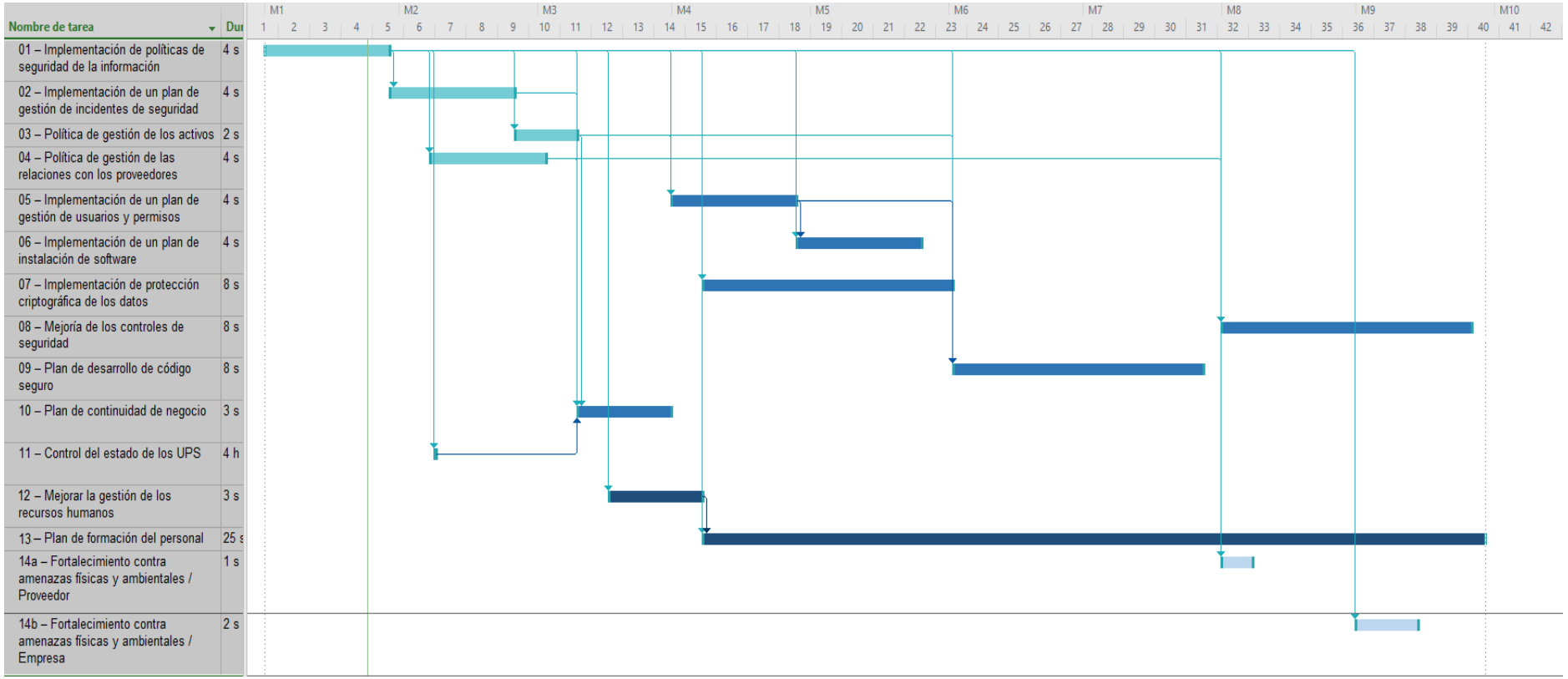
	SW16	Programas de backup	MA	8	9	8	7	5	75%	100%	75%	75%	0%	6,00	9,00	6,00	5,25	0,00
	SW17	S.O. Móviles - IOS	B	3	4	4	3	3	75%	100%	75%	75%	0%	2,25	4,00	3,00	2,25	0,00
	SW18	S.O. Móviles - Android	B	3	4	4	3	3	75%	100%	75%	75%	0%	2,25	4,00	3,00	2,25	0,00
Datos [D]	D01	Datos de las empresas clientes	MA	8	9	8	7	6	75%	100%	100%	100%	100%	6,00	9,00	8,00	7,00	6,00
	D02	Datos personales sensibles	MA	8	9	8	7	6	75%	100%	100%	100%	100%	6,00	9,00	8,00	7,00	6,00
	D03	Logs	M	5	5	6	5	5	75%	100%	100%	100%	100%	3,75	5,00	6,00	5,00	5,00
	D04	Copias de seguridad de las BD	MA	7	8	8	7	5	75%	100%	100%	100%	100%	5,25	8,00	8,00	7,00	5,00
	D05	Archivos de documentación	MA	5	8	7	7	5	75%	100%	100%	100%	100%	3,75	8,00	7,00	7,00	5,00
	D06	Código fuente	MA	8	7	8	6	7	75%	100%	100%	100%	100%	6,00	7,00	8,00	6,00	7,00
Red [COM]	COM01	Cableado eléctrico	MA	0	0	8	9	0	5%	75%	20%	75%	0%	0,00	0,00	1,60	6,75	0,00
	COM02	Cableado de telecomunicaciones	MA	0	0	8	9	0	5%	75%	20%	75%	0%	0,00	0,00	1,60	6,75	0,00
	COM03	Red inalámbrica	M	0	0	7	7	0	5%	75%	20%	75%	0%	0,00	0,00	1,40	5,25	0,00
Servicios [S]	S01	Correo electrónico	M	6	8	7	5	3	75%	100%	100%	100%	75%	4,50	8,00	7,00	5,00	2,25
	S02	Acceso web	MA	6	9	8	8	7	75%	100%	100%	100%	75%	4,50	9,00	8,00	8,00	5,25
	S03	VPN	MA	8	9	8	9	7	75%	100%	100%	100%	75%	6,00	9,00	8,00	9,00	5,25
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización	MA	0	0	7	8	0	0%	75%	20%	100%	0%	0,00	0,00	1,40	8,00	0,00
	AUX02	Sistema de detección de incendios	MA	0	0	8	7	0	0%	75%	20%	100%	0%	0,00	0,00	1,60	7,00	0,00
	AUX03	UPS	MA	0	0	9	8	0	0%	75%	20%	100%	0%	0,00	0,00	1,80	8,00	0,00
	AUX04	Extintores	M	0	0	7	8	0	0%	75%	20%	100%	0%	0,00	0,00	1,40	8,00	0,00
Personal [P]	P01	Jefe de la empresa	B	0	0	0	2	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	0,40	0,00
	P02	Responsable IT	A	0	0	0	6	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	1,20	0,00
	P03	Otros empleados sector IT	A	0	0	0	8	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	1,60	0,00
	P04	Consultores	MA	0	0	0	7	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	1,40	0,00
	P05	Médicos laborales	A	0	0	0	7	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	1,40	0,00
	P06	Empleados administrativos	MB	0	0	0	1	0	0%	75%	75%	20%	0%	0,00	0,00	0,00	0,20	0,00

Anexo 12 – Nivel de riesgo

Ámbito	ID	Activo	Frecuencia	Impacto potencial					Nivel de Riesgo				
				A	C	I	D	T	A	C	I	D	T
Instalaciones [L]	L01	Sala de servidores del proveedor	MA	0,00	1,80	0,35	9,00	0,00	B	B	B	MA	B
	L02	Sala de servidores de la empresa	A	0,00	1,40	0,30	7,00	0,00	B	B	B	MA	B
	L03	Open space en la empresa	B	0,00	0,60	0,15	2,00	0,00	MB	MB	MB	B	MB
	L04	Laboratorio	MB	0,00	0,60	0,00	1,00	0,00	MB	MB	MB	MB	MB
	L05	Oficina del jefe de la empresa	MB	0,00	0,60	0,00	1,00	0,00	MB	MB	MB	MB	MB
	L06	Salas de visitas (3) dep. médico	B	0,00	1,20	0,00	2,00	0,00	MB	MB	MB	B	MB
Hardware [HW]	HW01	Servidores SQL (4)	MA	0,00	6,75	1,60	8,00	0,00	B	A	B	MA	B
	HW02	Servidores MySQL (2)	MA	0,00	6,75	1,60	8,00	0,00	B	A	B	MA	B
	HW03	Servidor Exchange	M	0,00	6,00	1,20	4,00	0,00	MB	M	MB	M	MB
	HW04	Servidor repositorio ficheros	A	0,00	6,75	1,60	7,00	0,00	B	A	B	MA	B
	HW05	Ordenadores (50)	B	0,00	5,25	0,60	3,00	0,00	MB	M	MB	B	MB
	HW06	Laptop (250)	M	0,00	5,25	0,60	3,00	0,00	MB	M	MB	B	MB
	HW07	Firewall	M	0,00	5,25	1,20	8,00	0,00	MB	M	MB	A	MB
	HW08	Móviles (150)	B	0,00	5,25	1,20	2,00	0,00	MB	M	MB	B	MB
Aplicación [SW]	SW01	S.O. Windows Server 2016	MA	6,00	5,00	4,50	6,75	0,00	A	A	A	A	B
	SW02	S.O. Ubuntu	MA	6,00	5,00	4,50	6,00	0,00	A	A	A	A	B
	SW03	S.O. Windows 11	B	3,00	4,00	3,00	3,75	0,00	B	M	B	B	MB
	SW04	S.O. Windows 10	B	3,00	4,00	3,00	3,75	0,00	B	M	B	B	MB
	SW05	S.O. Windows 7	B	3,00	4,00	3,00	3,75	0,00	B	M	B	B	MB
	SW06	MS Office 365	B	0,75	6,00	3,00	0,75	0,00	MB	M	B	MB	MB
	SW07	MS Office 2010	MB	0,75	6,00	3,00	0,75	0,00	MB	B	MB	MB	MB
	SW08	MS Visual Studio 17	A	4,50	7,00	5,25	6,00	0,00	A	MA	A	A	B
	SW09	Adobe Acrobat Professional	B	3,00	7,00	3,00	2,25	0,00	B	A	B	B	MB
	SW10	ERP	M	4,50	9,00	6,00	5,25	0,00	M	A	M	M	MB
	SW11	Aplicación WinForm	MA	6,00	9,00	6,75	5,25	0,00	A	MA	A	A	B
	SW12	Web App	MA	6,00	9,00	6,00	5,25	0,00	A	MA	A	A	B
	SW13	Antivirus Kaspersky	M	6,00	5,00	6,00	6,00	0,00	M	M	M	M	MB
	SW14	SQL Management Studio	A	4,50	7,00	4,50	6,00	0,00	A	MA	A	A	B
	SW15	MySQL Management	A	4,50	7,00	4,50	6,00	0,00	A	MA	A	A	B
	SW16	Programas de backup	MA	6,00	9,00	6,00	5,25	0,00	A	MA	A	A	B
	SW17	S.O. Móviles - IOS	B	2,25	4,00	3,00	2,25	0,00	B	M	B	B	MB
	SW18	S.O. Móviles - Android	B	2,25	4,00	3,00	2,25	0,00	B	M	B	B	MB
Datos [D]	D01	Datos de las empresas clientes	MA	6,00	9,00	8,00	7,00	6,00	A	MA	MA	MA	A
	D02	Datos personales sensibles	MA	6,00	9,00	8,00	7,00	6,00	A	MA	MA	MA	A
	D03	Logs	M	3,75	5,00	6,00	5,00	5,00	M	M	M	M	M
	D04	Copias de seguridad de las BD	MA	5,25	8,00	8,00	7,00	5,00	A	MA	MA	MA	A
	D05	Archivos de documentación	MA	3,75	8,00	7,00	7,00	5,00	M	MA	MA	MA	A
	D06	Código fuente	MA	6,00	7,00	8,00	6,00	7,00	A	MA	MA	A	MA
Red [COM]	COM01	Cableado eléctrico	MA	0,00	0,00	1,60	6,75	0,00	B	B	B	A	B
	COM02	Cableado de telecomunicaciones	MA	0,00	0,00	1,60	6,75	0,00	B	B	B	A	B
	COM03	Red inalámbrica	M	0,00	0,00	1,40	5,25	0,00	MB	MB	MB	M	MB
Servicios [S]	S01	Correo electrónico	M	4,50	8,00	7,00	5,00	2,25	M	A	A	M	B
	S02	Acceso web	MA	4,50	9,00	8,00	8,00	5,25	A	MA	MA	MA	A
	S03	VPN	MA	6,00	9,00	8,00	9,00	5,25	A	MA	MA	MA	A
Equipamiento auxiliar [AUX]	AUX 01	Sistema de climatización	MA	0,00	0,00	1,40	8,00	0,00	B	B	B	MA	B
	AUX02	Sistema de detección de incendios	MA	0,00	0,00	1,60	7,00	0,00	B	B	B	MA	B

	AUX03	UPS	MA	0,00	0,00	1,80	8,00	0,00	B	B	B	MA	B
	AUX04	Extintores	M	0,00	0,00	1,40	8,00	0,00	MB	MB	MB	A	MB
Personal [P]	P01	Jefe de la empresa	B	0,00	0,00	0,00	0,40	0,00	MB	MB	MB	MB	MB
	P02	Responsable IT	A	0,00	0,00	0,00	1,20	0,00	B	B	B	B	B
	P03	Otros empleados sector IT	A	0,00	0,00	0,00	1,60	0,00	B	B	B	B	B
	P04	Consultores	MA	0,00	0,00	0,00	1,40	0,00	B	B	B	B	B
	P05	Médicos laborales	A	0,00	0,00	0,00	1,40	0,00	B	B	B	B	B
	P06	Empleados administrativos	MB	0,00	0,00	0,00	0,20	0,00	MB	MB	MB	MB	MB

Anexo 12 – Planificación de los proyectos



Anexo 13 – Análisis diferencial ISO 27002 antes y después de la realización de los proyectos

				Antes	Después
CONTROL				Evaluación	Evaluación
A.5 Information security policies					
	A.5.1 Management direction for information security				
		A.5.1.1	Policies for information security	2 - Repetible	4 - Gestionado
		A.5.1.2	Review of the policies for information security	0 - No existente	4 - Gestionado
A.6 Organization of information security					
	A.6.1 Internal organization				
		A.6.1.1	Information security roles and responsibilities	1 - Inicial	4 - Gestionado
		A.6.1.2	Segregation of duties	2 - Repetible	4 - Gestionado
		A.6.1.3	Contact with authorities	0 - No existente	5 - Optimizado
		A.6.1.4	Contact with special interest groups	2 - Repetible	3 - Definido
		A.6.1.5	Information security in project management	2 - Repetible	4 - Gestionado
	A.6.2 Mobile devices and teleworking				
		A.6.2.1	Mobile device policy	2 - Repetible	4 - Gestionado
		A.6.2.2	Teleworking	2 - Repetible	4 - Gestionado
A.7 Human resource security					
	A.7.1 Prior to employment				
		A.7.1.1	Screening	0 - No existente	4 - Gestionado
		A.7.1.2	Terms and conditions of employment	1 - Inicial	5 - Optimizado
	A.7.2 During employment				
		A.7.2.1	Management responsibilities	0 - No existente	4 - Gestionado
		A.7.2.2	Information security awareness, education and training	0 - No existente	4 - Gestionado
		A.7.2.3	Disciplinary process	0 - No existente	4 - Gestionado
	A.7.3 Termination and change of employment				
		A.7.3.1	Termination or change of employment responsibilities	1 - Inicial	5 - Optimizado
A.8 Asset management					
	A.8.1 Responsibility for asset				
		A.8.1.1	Inventory of assets	0 - No existente	5 - Optimizado
		A.8.1.2	Ownership of assets	0 - No existente	5 - Optimizado
		A.8.1.3	Acceptable use of assets	2 - Repetible	4 - Gestionado
		A.8.1.4	Return of assets	1 - Inicial	4 - Gestionado
	A.8.2 Information classification				
		A.8.2.1	Classification of information	0 - No existente	4 - Gestionado
		A.8.2.2	Labelling of informa tion	0 - No existente	4 - Gestionado
		A.8.2.3	Handling of assets	0 - No existente	4 - Gestionado
	A.8.3 Media handling				
		A.8.3.1	Management of removable media	0 - No existente	4 - Gestionado
		A.8.3.2	Disposal of media	0 - No existente	4 - Gestionado
		A.8.3.3	Physical media transfer	0 - No existente	4 - Gestionado
A.9 Access control					
	A.9.1 Business requirements of access control				

		A.9.1.1	Access control policy	0 - No existente	4 - Gestionado
		A.9.1.2	Access to networks and network services	2 - Repetible	4 - Gestionado
	A.9.2 User access management				
		A.9.2.1	User registration and de-registration	2 - Repetible	5 - Optimizado
		A.9.2.2	User access provisioning	2 - Repetible	4 - Gestionado
		A.9.2.3	Management of privileged access rights	1 - Inicial	5 - Optimizado
		A.9.2.4	Management of secret authentication information of users	2 - Repetible	4 - Gestionado
		A.9.2.5	Review of user access rights	1 - Inicial	4 - Gestionado
		A.9.2.6	Removal or adjustment of access rights	2 - Repetible	5 - Optimizado
	A.9.3 User responsibilities				
		A.9.3.1	Use of secret authentication information	2 - Repetible	4 - Gestionado
	A.9.4 System and application access control				
		A.9.4.1	Information access restriction	1 - Inicial	4 - Gestionado
		A.9.4.2	Secure log-on procedures	2 - Repetible	4 - Gestionado
		A.9.4.3	Password managment system	2 - Repetible	5 - Optimizado
		A.9.4.4	Use of privileged utility programs	2 - Repetible	4 - Gestionado
		A.9.4.5	Access control to program source code	2 - Repetible	4 - Gestionado
A.10 Cryptography					
	A.10.1 Cryptographic controls				
		A.10.1.1	Policy on the use of cryptographic controls	0 - No existente	4 - Gestionado
		A.10.1.2	Key management	0 - No existente	4 - Gestionado
A.11 Physical and environmental security					
	A.11.1 Secure areas				
		A.11.1.1	Physical security perimeter	5 - Optimizado	5 - Optimizado
		A.11.1.2	Physical entry controls	5 - Optimizado	5 - Optimizado
		A.11.1.3	Securing offices, rooms and facilities	3 - Definido	3 - Definido
		A.11.1.4	Protecting against external and environmental threats	3 - Definido	3 - Definido
		A.11.1.5	Working in secure areas	0 - No existente	0 - No existente
		A.11.1.6	Delivery and loading areas	3 - Definido	3 - Definido
	A.11.2 Equipment				
		A.11.2.1	Equipment siting and protection	5 - Optimizado	5 - Optimizado
		A.11.2.2	Supporting utilities	5 - Optimizado	5 - Optimizado
		A.11.2.3	Cabling security	0 - No existente	3 - Definido
		A.11.2.4	Equipment maintenance	2 - Repetible	4 - Gestionado
		A.11.2.5	Removal of assets	1 - Inicial	4 - Gestionado
		A.11.2.6	Security of equipment and assets off-premises	0 - No existente	4 - Gestionado
		A.11.2.7	Secure disposal or reuse of equipment	0 - No existente	4 - Gestionado
		A.11.2.8	Unattended user equipment	2 - Repetible	4 - Gestionado
		A.11.2.9	Clear desk and clear screen policy	0 - No existente	4 - Gestionado
A.12 Operations security					
	A.12.1 Operational procedures and responsibilities				
		A.12.1.1	Documented operating procedures	0 - No existente	4 - Gestionado
		A.12.1.2	Change management	0 - No existente	4 - Gestionado
		A.12.1.3	Capacity management	0 - No existente	4 - Gestionado
		A.12.1.4	Separation of development, testing and operational	0 - No existente	4 - Gestionado

			environments	
	A.12.2 Protection from malware			
		A.12.2.1	Controls against malware	2 - Repetible	5 - Optimizado
	A.12.3 Backup			
		A.12.3.1	Information backup	5 - Optimizado	5 - Optimizado
	A.12.4 Logging and monitoring			
		A.12.4.1	Event logging	0 - No existente	4 - Gestionado
		A.12.4.2	Protection of log information	0 - No existente	4 - Gestionado
		A.12.4.3	Administrator and operator logs	0 - No existente	4 - Gestionado
		A.12.4.4	Clock synchronisation	1 - Inicial	4 - Gestionado
	A.12.5 Control of operational software			
		A.12.5.1	Installation of software on operational systems	0 - No existente	5 - Optimizado
	A.12.6 Technical vulnerability management			
		A.12.6.1	Management of technical vulnerabilities	0 - No existente	5 - Optimizado
		A.12.6.2	Restrictions on software installation	2 - Repetible	5 - Optimizado
	A.12.7 Information systems audit considerations			
		A.12.7.1	Information systems audit controls		4 - Gestionado
A.13 Communications security					
	A.13.1 Network security management			
		A.13.1.1	Network controls	1 - Inicial	4 - Gestionado
		A.13.1.2	Security of network services	1 - Inicial	4 - Gestionado
		A.13.1.3	Segregation in networks	0 - No existente	4 - Gestionado
	A.13.2 Information transfer			
		A.13.2.1	Information transfer policies and procedures	0 - No existente	4 - Gestionado
		A.13.2.2	Agreements on information transfer	0 - No existente	4 - Gestionado
		A.13.2.3	Electronic messaging	0 - No existente	4 - Gestionado
		A.13.2.4	Confidentiality or nondisclosure agreements	2 - Repetible	4 - Gestionado
A.14 System acquisition, development and maintenance					
	A.14.1 Security requirements of information systems			
		A.14.1.1	Information security requirements analysis and specification	0 - No existente	4 - Gestionado
		A.14.1.2	Securing application services on public networks	0 - No existente	4 - Gestionado
		A.14.1.3	Protecting application services transactions	0 - No existente	4 - Gestionado
	A.14.2 Security in development and support processes			
		A.14.2.1	Secure development policy	2 - Repetible	4 - Gestionado
		A.14.2.2	System change control procedures.	1 - Inicial	4 - Gestionado
		A.14.2.3	Technical review of applications after operating platform	2 - Repetible	4 - Gestionado
		A.14.2.4	Restrictions on changes to software packages	2 - Repetible	4 - Gestionado
		A.14.2.5	Secure system engi neering principles	2 - Repetible	4 - Gestionado
		A.14.2.6	Secure development environment	2 - Repetible	4 - Gestionado
		A.14.2.7	Outsourced development		
		A.14.2.8	System security testing	2 - Repetible	4 - Gestionado
		A.14.2.9	System acceptance testing	2 - Repetible	4 - Gestionado
	A.14.3 Test data			
		A.14.3.1	Protection of test data	0 - No existente	4 - Gestionado
A.15 Supplier relationships					

	A.15.1 Information security in supplier relationships				
		A.15.1.1	Information security policy for supplier relationships	0 - No existente	4 - Gestionado
		A.15.1.2	Addressing security within supplier agreements	0 - No existente	4 - Gestionado
		A.15.1.3	Information and communication technology supply chain	0 - No existente	4 - Gestionado
	A.15.2 Supplier service delivery management				
		A.15.2.1	Monitoring and review of supplier services	0 - No existente	3 - Definido
		A.15.2.2	Managing changes to supplier services	0 - No existente	3 - Definido
A.16 Information security incident management					
	A.16.1 Management of information security incidents and improvements				
		A.16.1.1	Responsibilities and procedures	0 - No existente	4 - Gestionado
		A.16.1.2	Reporting information security events	0 - No existente	4 - Gestionado
		A.16.1.3	Reporting information security weaknesses	0 - No existente	4 - Gestionado
		A.16.1.4	Assessment of and decision on information security events	1 - Inicial	4 - Gestionado
		A.16.1.5	Response to information security incidents	1 - Inicial	4 - Gestionado
		A.16.1.6	Learning from information security incidents	0 - No existente	4 - Gestionado
		A.16.1.7	Collection of evidence	0 - No existente	4 - Gestionado
A.17 Information security aspects of business continuity management					
	A.17.1 Information security continuity				
		A.17.1.1	Planning information security continuity	0 - No existente	4 - Gestionado
		A.17.1.2	Implementing information security continuity	0 - No existente	4 - Gestionado
		A.17.1.3	Verify, review and evaluate information security continuity	0 - No existente	4 - Gestionado
	A.17.2 Redundancies				
		A.17.2.1	Availability of information processing facilities	0 - No existente	4 - Gestionado
A.18 Compliance					
	A.18.1 Compliance with legal and contractual requirements				
		A.18.1.1	Identification of applicable legislation and contractual requirements	0 - No existente	5 - Optimizado
		A.18.1.2	Intellectual property rights	0 - No existente	4 - Gestionado
		A.18.1.3	Protection of records	0 - No existente	4 - Gestionado
		A.18.1.4	Privacy and protection of personally identifiable information	0 - No existente	4 - Gestionado
		A.18.1.5	Regulation of cryptographic controls	0 - No existente	4 - Gestionado
	A.18.2 Information security reviews				
		A.18.2.1	Independent review of information security	0 - No existente	5 - Optimizado
		A.18.2.2	Compliance with security policies and standards	0 - No existente	5 - Optimizado
		A.18.2.3	Technical compliance review	0 - No existente	4 - Gestionado

Anexo 14 – Evaluación de la madurez ISO27002

CONTROL	VALOR CMM	Cumplimiento	JUSTIFICACIÓN DE LA VALORACIÓN / EVIDENCIAS
A.5. Políticas de seguridad de la información **A.5.1. Directrices de la dirección en seguridad de la información**			
5.1.1. Políticas para la seguridad de la información	**5**	**Cumple**	Se ha definido una política de seguridad que está documentada y la cual se aplican mejorías.
5.1.2. Revisión de las políticas para la seguridad de la información	**5**	**Cumple**	La política de seguridad ya se ha revisado una vez, se revisará al menos una vez por año y hay un proyecto de mejorías
A.6. Organización de la seguridad de la información **A.6.1. Organización interna**			
6.1.1. Roles y responsabilidades en la seguridad de la información.	**5**	**Cumple**	El responsable IT ha recibido formalmente el rol de responsable de la seguridad de la información; se han definido roles y responsabilidades y se puede medir la ejecución de la tarea.
6.1.2. Segregación de tareas.	**4**	**Cumple**	Hay una segregación de funciones de los empleados y existen indicadores para comprobar la eficaz.
6.1.3. Contacto con las autoridades.	**3**	**Cumple**	Se ha documentado el procedimiento a tener y se han establecido los roles. No hay indicadores para medir la eficaz que puedan ayudar a mejorar.
6.1.4. Contacto con grupos de interés especial.	**2**	**Observación**	No existe documentación sobre los contactos con grupos de interés especial.
6.1.5. Seguridad de la información en la gestión de proyectos.	**4**	**Cumple**	Se han estudiado y documentado los requisitos de seguridad para los proyectos que requieren acceso a la información. Faltan indicadores para evaluar la seguridad de la información.
A.6. Organización de la seguridad de la información **A.6.2. Los dispositivos móviles y el teletrabajo**			
6.2.1. Política de dispositivos móviles	**3**	**Cumple**	Se estableció un procedimiento de gestión de los dispositivos móviles, todavía no existen indicadores específicos para comprobar su eficaz.
6.2.2. Teletrabajo	**4**	**Cumple**	Hay un procedimiento de gestión segura de las conexiones desde el exterior (VPN) que permite a la empresa tener unas medidas de seguridad y de protección de los accesos. Se aplican, en el acceso desde el exterior, las mismas restricciones establecidas por la política de seguridad de la información.
A.7. Seguridad ligada a los recursos humanos **A.7.1. Antes del empleo**			
7.1.1. Investigación de antecedentes	**4**	**Cumple**	Se han establecido los procedimientos de investigación de antecedentes y se ha establecido un indicador para comprobar la efectuación. Todavía no hay evidencias de revisiones y mejorías del proceso.

7.1.2. Términos y condiciones del empleo	**4**	**Cumple**	Se definen correctamente los acuerdos de empleo, con cláusulas de confidencialidad, de protección de datos y de derechos de propiedad intelectual: se aplican a todos los nuevos acuerdos estipulados.
A.7. Seguridad ligada a los recursos humanos **A.7.2. Durante el empleo**			
7.2.1. Responsabilidades de gestión	**5**	**Cumple**	Se han definido los roles y las responsabilidades de gestión, y se ha revisado el modelo una vez.
7.2.2. Concienciación, educación y capacitación en Seguridad de la Información	**5**	**Cumple**	Se ha establecido un plan de educación y formación para educar y concienciar todos los empleados. Se tienen en cuenta sus sugerencias a través encuestas de valoración de los cursos, que permiten mejorar el asunto.
7.2.3. Proceso disciplinario	**4**	**Cumple**	Se han codificado las posibles violaciones y las consecuencias disciplinarias que pueden tener; se mide el número de violaciones ocurridas.
A.7. Seguridad ligada a los recursos humanos **A.7.3. Finalización del empleo o cambio en el puesto de trabajo**			
7.3.1. Responsabilidades ante la finalización o cambio	**4**	**Cumple**	Gracias a las cláusulas en los contratos, se han definido también responsabilidades y funciones válidas también después de la finalización del empleo. Se ha establecido un procedimiento para gestionar los cambios de responsabilidad debidos a cambios internos.
A.8. Gestión de activos **A.8.1. Responsabilidad sobre los activos**			
8.1.1. Inventario de activos	**4**	**Cumple**	Se ha empezado a inventariar los activos y se dispone de un indicador que permite evaluar el progreso de la tarea. Todavía ,debido al elevado número de activos totales y a su dispersión, aún es necesario mejorar el nivel.
8.1.2. Propiedad de los activos	**4**	**Cumple**	Valen las mismas consideraciones del punto anterior: se ha empezado el proceso y todos los activos inventariados tienen un propietario.
8.1.3. Uso aceptable de los activos	**3**	**Cumple**	El código de conducta, documentado y conocido por toda la organización, establece unas normas de comportamiento (por ejemplo el hecho que no se permite instalar software sin autorización, y está prohibido conectarse a sitios web que no sirven para el trabajo, o utilizar social media…)
8.1.4. Devolución de activos	**4**	**Cumple**	El departamento IT está formalmente encargado de recoger los activos de los empleados que terminan su relación laboral. Faltan, por deficiencias anteriores, las registraciones de, por ejemplo, discos duros externos o pendrive usb entregados a los usuarios.

A.8. Gestión de activos **A.8.2. Clasificación de la información**			
8.2.1. Clasificación de la información	**4**	**Cumple**	La información se ha clasificado en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
8.2.2. Etiquetado de la Información	**2**	**Observación**	La información está solo parcialmente etiquetada y no existe un documento para las directrices de etiquetado.
8.2.3. Manipulación de la información	**3**	**Cumple**	Se han definido los procedimientos para la manipulación de la información y hay trazabilidad de las manipulaciones de la información crítica.
A.8. Gestión de activos **A.8.3. Manejo de soportes de almacenamiento**			
8.3.1. Gestión de soportes extraíbles	**2**	**Observación**	Se ha creado un registro de los soportes extraíbles entregados en el último periodo; todavía faltan aquellos entregados anteriormente, no hay limitaciones a la utilización de soportes personales y no existe un indicador.
8.3.2. Eliminación de soportes.	**5**	**Cumple**	Se ha establecido la manera de destruir los soportes de forma segura, y se mide su actuación.
8.3.3. Soportes físicos en tránsito	**4**	**Cumple**	Existe un procedimiento documentado para su gestión.
A.9. Control de acceso **A.9.1. Requisitos de negocio para el control de acceso**			
9.1.1. Política de control de acceso	**5**	**Cumple**	Existe una política de control de accesos definida y conocida por todos los trabajadores; se revisa periódicamente.
9.1.2. Acceso a redes y a los servicios en red	**4**	**Cumple**	Se ha definido formalmente el comportamiento para acceder y utilizar redes y servicios. Hay monitorización de los abusos.
A.9. Control de acceso **A.9.2. Gestión de acceso de usuario**			
9.2.1. Registro y baja de usuario	**4**	**Cumple**	Los identificadores de usuario son dados por el departamento IT a todos los empleados cuando empiezan a trabajar en la organización y cuando la dejan se inhabilitan, según un procedimiento bien definido. Se controlan periódicamente.
9.2.2. Provisión de acceso de usuario	**4**	**Cumple**	Se ha definido el procedimiento para la definición y asignación de los derechos de acceso, dividiéndose los usuarios en administradores y no-administradores.
9.2.3. Gestión de privilegios de acceso	**4**	**Cumple**	Los privilegios están gestionados por el departamento IT, y revisados periódicamente.
9.2.4. Gestión de la información secreta de autenticación de los usuarios	**2**	**Observación**	La asignación de la información secreta de autenticación no se proporciona de manera segura (los nuevos usuarios tienen siempre la misma contraseña inicial, que se comunica oralmente). Todavía los usuarios deben cambiarla obligatoriamente en el primer uso.

9.2.5. Revisión de los derechos de acceso de usuario	**4**	**Cumple**	Los derechos de acceso de usuario se revisan periódicamente o después de cambios de roles.
9.2.6. Retirada o reasignación de los derechos de acceso	**4**	**Cumple**	Tras la finalización del empleo se bloquea el usuario y consecuentemente sus derechos de acceso se eliminan. Se ha definido el procedimiento para informar el departamento IT que es necesaria su intervención.
A.9. Control de acceso **A.9.3. Responsabilidades de usuario**			
9.3.1. Uso de información secreta de autenticación	**5**	**Cumple**	Hay un procedimiento definido y documentado, y formación al personal. Los usuarios saben que deben mantener confidencial la información; existen requisitos (longitud mínima, caracteres especiales…) en la selección de contraseñas.
A.9. Control de acceso **A.9.4. Control de acceso a sistemas y aplicaciones**			
9.4.1. Restricción del acceso a la información.	**4**	**Cumple**	Se restringe el acceso a la información de los usuarios, y un se ha identificado el responsable que además controla el acceso de las aplicaciones.
9.4.2. Procedimientos seguros de inicio de sesión	**3**	**Cumple**	Se terminan las sesiones inactivas después de 10 minutos de inactividad, se esconde la contraseña y se transmite cifrada por red; existe una protección contra los ataques de fuerza bruta (imposibilidad de reintentar durante 20 minutos después de 3 tentativos errados). Faltan indicadores
9.4.3. Sistema de gestión de contraseñas.	**5**	**Cumple**	El procedimiento está documentado y bien conocido. Es necesario cambiar las contraseñas tras el primer inicio de sesión y periódicamente, se imponen unos requisitos de las contraseñas y se mantiene un registro de las contraseñas para evitar su reutilización.
9.4.4. Uso de utilidades con privilegios del sistema	**4**	**Cumple**	El uso de utilidades con privilegios del sistema está restringido (es posible solo para los administradores), bien conocido y documentado.
9.4.5. Control de acceso al código fuente de los programas	**4**	**Cumple**	El código fuente de los programas está accesible solo para los desarrolladores y administradores del sistema. El procedimiento prevé también controles periódicos, aunque faltan indicadores.
A.10. Cifrado **A.10.1. Controles criptográficos**			
10.1.1. Política de uso de los controles criptográficos	**4**	**Cumple**	La información sensible almacenada se protege a través de controles criptográficos; se ha establecido también una medida del nivel de protección.
10.1.2. Gestión de claves	**4**	**Cumple**	Se ha establecido un procedimiento para la política de controles criptográficos que incluye la protección y la duración de las claves de cifrado.

A.11. Seguridad física y ambiental **A.11.1. Áreas seguras**			
11.1.1. Perímetro de seguridad física	**5**	**Cumple**	El proveedor que gestiona los servidores asegura que están protegidos físicamente con controles de acceso automático, y que el proceso está documentado. Se ha añadido también un control para medir los resultados de la protección.
11.1.2. Controles físicos de entrada	**5**	**Cumple**	El proveedor que gestiona los servidores autoriza los accesos, registrando las horas de entrada y salida de los visitadores. Se ha añadido también un control para medir los resultados de la protección.
11.1.3. Seguridad de oficinas, despachos y recursos	**3**	**Cumple**	Existen señales que identifiquen la existencia de actividades de tratamiento de la información; todavía aún no se han considerado los campos electromagnéticos. Se ha añadido también un control para medir los resultados de la protección.
11.1.4. Protección contra las amenazas externas y ambientales	**3**	**Cumple**	Existe solo un plan de protección de la sala de servidores contra el fuego, no se evaluaron otros desastres ambientales ni daños causados por el hombre.
11.1.5. El trabajo en áreas seguras	**0**	**No cumple**	No se implementaron procedimientos para trabajar en áreas seguras.
11.1.6. Áreas de carga y descarga	**3**	**Cumple**	Las áreas de carga y descarga están al exterior del edificio y no es necesario que el personal externo encargado de las operaciones acceda a otras zonas del edificio.
A.11. Seguridad física y ambiental **A.11.2. Seguridad de los equipos**			
11.2.1. Emplazamiento y protección de equipos	**5**	**Cumple**	Los servidores están en una sala con mecanismos de control de temperatura y humedad y un extintor de incendios.
11.2.2. Instalaciones de suministro	**5**	**Cumple**	Los servidores están conectados a UPS para protegerlos de fallos de alimentación u otras alteraciones. Los UPS son conformes a los requisitos legales. Se hacen pruebas periódicas.
11.2.3. Seguridad del cableado	**0**	**No cumple**	El cableado eléctrico y de telecomunicaciones no está protegido frente a interceptaciones, interferencias o daños.
11.2.4. Mantenimiento de los equipos	**3**	**Cumple**	Los servidores se mantienen regularmente, de acuerdo con las necesidades del cliente. Los ordenadores de los empleados de la empresa se gestionan sin regularidad, aunque el procedimiento está documentado, por la dificultad de tener los ordenadores disponibles (a menudo los consultores trabajan externamente).
11.2.5. Retirada de materiales propiedad de la empresa	**2**	**Observación**	Los empleados pueden sacar los activos fuera de las instalaciones. Hay un procedimiento definido para los usuarios de tercera parte, para los cuales se ha establecido un registro de las retiradas. No se ha establecido una limitación al tiempo.

11.2.6. Seguridad de los equipos fuera de las instalaciones	**2**	**Observación**	No se aplican medidas de seguridad a los equipos fuera de las instalaciones, aunque los trabajadores están formados; no existen controles.
11.2.7. Reutilización o eliminación segura de equipos	**5**	**Cumple**	Se ha establecido un procedimiento para la eliminación de la información de los equipos que deben ser reutilizados. Se ha establecido la manera de destruir los soportes de forma segura, y se mide su actuación.
11.2.8. Equipo de usuario desatendido	**3**	**Cumple**	El procedimiento impone a los usuarios de activar el protector de pantalla con contraseña después de 10 minutos de inactividad. Faltan todavía los controles.
11.2.9. Política de puesto de trabajo despejado y pantalla limpia	**1**	**No cumple**	No existen procedimientos sobre cómo guardar la información sensible en papel ni sobre la pantalla, solo se confía en la formación hecha a los trabajadores.
A.12. Seguridad en las operaciones **A.12.1. Responsabilidades y procedimientos de operación**			
12.1.1. Documentación de procedimientos de operación	**5**	**Cumple**	Se han documentado todas las operaciones que se deben hacer relacionadas con el manejo de la información.
12.1.2. Gestión de cambios	**4**	**Cumple**	Se han establecido registros y procedimientos para los cambios, falta su planificación.
12.1.3. Gestión de capacidades	**3**	**Cumple**	Se han identificado formalmente los requisitos de capacidad de los recursos; todavía falta una medición para comprobar están adecuados o si sería necesario modificarlos.
12.1.4. Separación de recursos de desarrollo, prueba y operación	**1**	**No cumple**	Se ha reconocido que es necesario separar los recursos de desarrollo, prueba y operación.
A.12. Seguridad en las operaciones **A.12.2. Protección contra código malicioso**			
12.2.1. Controles contra el código malicioso	**5**	**Cumple**	Todos los ordenadores tienen instalado un software antivirus centralizado que se actualiza periódicamente. Se controla periódicamente que no se haya olvidado ninguno.
A.12. Seguridad en las operaciones **A.12.3. Copias de seguridad**			
12.3.1. Copias de seguridad de la información	**5**	**Cumple**	Se hace una copia de seguridad de las bases de datos cada noche; se guardan las copias diarias durante una semana, luego se guarda una copia de seguridad por semana durante un mes, y una copia de seguridad mensual durante un año. La política de copias de seguridad está documentada en los acuerdos entre la empresa y el proveedor que gestiona los servidores. Se ha añadido un indicador.
A.12. Seguridad en las operaciones **A.12.4. Registro de actividad y supervisión**			
12.4.1. Registro de eventos	**3**	**Cumple**	Se registran actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información, todavía no se puede evaluar su revisión ni existen planes de mejoría.

12.4.2. Protección de la información de registro	**3**	**Cumple**	Los registros de eventos se protegen; todavía no existe un control de la eficaz de esta protección.
12.4.3. Registros de administración y operación	**3**	**Cumple**	Se registran las actividades de los administradores y operadores de sistemas. Como en el punto 12.4.1 no se puede evaluar su revisión y consecuentemente no se puede mejorar
12.4.4. Sincronización del reloj	**5**	**Cumple**	Los relojes de todos los sistemas de tratamiento de la información de la organización están sincronizados con la hora del servidor principal.
A.12 seguridad en las operaciones **A.12.5 control del software en explotación**			
12.5.1. Instalación del software en explotación	**5**	**Cumple**	Hay procedimientos para instalar y controlar el software en explotación; hay un control periódico de las actualizaciones del software.
A.12 seguridad en las operaciones **A.12.6 gestión de la vulnerabilidad técnica**			
12.6.1. Gestión de las vulnerabilidades técnicas	**1**	**No cumple**	No se ha establecido un procedimiento para la obtención de informaciones acerca de las vulnerabilidades; los administradores solo saben que deben comprobarlas periódicamente.
12.6.2. Restricciones en la instalación de software	**4**	**Cumple**	Los usuarios no tienen permisos de instalación de software en sus ordenadores; se controlan periódicamente los equipos y los programas que tienen instalados.
A.12. Seguridad en las operaciones **A.12.7. Consideraciones sobre las auditorías de los sistemas de información**			
12.7.1. Controles de auditoría de sistema de información	**5**	**Cumple**	Existe un plan de auditoría a sistemas y datos.
A.13. Seguridad de las comunicaciones **A.13.1. Gestión de la seguridad en redes**			
13.1.1. Controles de red	**4**	**Cumple**	Hay un firewall que permite registrar y monitorizar los eventos; se han establecido con claridad roles, responsabilidades y procedimientos para la gestión y el control. Faltan indicadores
13.1.2. Seguridad en los servicios de red	**4**	**Cumple**	Hay un firewall para proporcionar seguridad a la red, y se han establecidos procedimientos para restringir el acceso a los servicios de red o a las aplicaciones. Faltan indicadores
13.1.3. Segregación en redes.	**1**	**No cumple**	No existe segregación en redes distintas. La dirección ha reconocido que es necesario dividir las redes.
A.13. Seguridad de las comunicaciones **A.13.2. Intercambio de información con partes externas**			
13.2.1. Políticas y procedimientos de intercambio de información	**3**	**Cumple**	Existe un procedimiento para proteger el intercambio de información; no se revisa y no se controla.
13.2.2. Acuerdos de intercambio de información	**1**	**No cumple**	No se han establecido acuerdos para el intercambio seguro de información entre la organización y terceros. Se sabe que es necesario hacerlo.

13.2.3. Mensajería electrónica	**3**	**Cumple**	La mensajería electrónica está protegida, todavía no hay indicadores y no se revisa.
13.2.4. Acuerdos de confidencialidad o no revelación	**4**	**Cumple**	Existen acuerdos de confidencialidad entre la organización y la mayoría de sus empleados, y entre la organización y sus proveedores, y se ha documentado el procedimiento.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.1. Requisitos de seguridad de los sistemas de información**			
14.1.1. Análisis de requisitos y especificaciones de seguridad de la información	**4**	**Cumple**	Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas de información y para mejoras a aquellos existentes. Faltan indicadores para revisarlos.
14.1.2. Asegurar los servicios de aplicaciones en redes públicas	**3**	**Cumple**	Se han implantado medidas para proteger la información involucrada en aplicaciones que pasan a través de redes públicas. Todavía no se revisan ni se controlan.
14.1.3. Protección de las transacciones de servicios de aplicaciones	**3**	**Cumple**	Se aplican medidas de protección contra transmisión incompleta, errores de enrutamiento, alteración, revelación, duplicación o reproducción no autorizada. Todavía no se revisan ni se controlan.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.2. Seguridad en los procesos de desarrollo y soporte**			
14.2.1. Política de desarrollo seguro	**4**	**Cumple**	Existe un procedimiento documentado de desarrollo seguro de software, ampliamente conocido por el personal.
14.2.2. Procedimiento de control de cambios en sistemas	**3**	**Cumple**	El procedimiento de desarrollo seguro permite también controlar los cambios a lo largo del ciclo de vida del desarrollo y, consecuentemente, tener una protección adicional. Todavía no existe siempre un entorno de desarrollo separado de aquello de explotación.
14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios el sistema operativo	**4**	**Cumple**	El procedimiento de desarrollo seguro hace que cuando se modifican los sistemas operativos se revisan y prueban las aplicaciones críticas de negocio.
14.2.4. Restricciones a los cambios en los paquetes de software	**5**	**Cumple**	Según el procedimiento de desarrollo seguro, los cambios en los paquetes de software se limitan a aquellos necesarios y se hace un control riguroso.
14.2.5. Principios de ingeniería de sistemas seguros	**2**	**Observación**	Los procedimientos de ingeniería de sistemas de información seguros se aplican, gracias al procedimiento de desarrollo seguro, a las implantaciones de sistemas de información. Todavía no están documentados.
14.2.6. Entorno de desarrollo seguro	**2**	**Observación**	El procedimiento de desarrollo seguro establece y protege adecuadamente el entorno. Falta todavía la separación de los recursos de desarrollo, prueba y operación.
14.2.7. Externalización del desarrollo de software	**-**	**-**	No hay software desarrollado externamente

14.2.8. Pruebas funcionales de seguridad de sistemas	**4**	**Cumple**	Las prácticas de desarrollo seguro incluyen pruebas de la seguridad funcional durante el desarrollo.
14.2.9. Pruebas de aceptación de sistemas	**4**	**Cumple**	El procedimiento de desarrollo seguro establece programas de prueba de aceptación y criterios relacionados para nuevos sistemas o actualizaciones.
A.14. Adquisición, desarrollo y mantenimiento de sistemas **A.14.3. Datos de prueba**			
14.3.1. Protección de los datos de prueba	**5**	**Cumple**	No se utilizan datos reales personales o confidenciales.
A.15. Relaciones con los proveedores **A.15.1. Seguridad de la información en las relaciones con los proveedores**			
15.1.1. Política de seguridad de la información en las relaciones con los proveedores	**3**	**Cumple**	Hay cláusulas para garantizar la seguridad de la información en los acuerdos con los proveedores. Falta todavía un control
15.1.2. Requisitos de seguridad en contratos con terceros	**3**	**Cumple**	Hay cláusulas para garantizar la seguridad de la información en los acuerdos. Falta todavía un control
15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones	**3**	**Cumple**	Los acuerdos con los proveedores establecen los requisitos de seguridad. Falta un control
A.15. Relaciones con los proveedores **A.15.2. Gestión de la prestación del servicio de los proveedores**			
15.2.1. Control y revisión de la provisión de servicios del proveedor	**4**	**Cumple**	La provisión de servicios de los proveedores se controla y revisa: se miden sus incumplimientos.
15.2.2. Gestión de cambios en la provisión del servicio del proveedor	**1**	**No cumple**	No existen procedimientos para gestionar los cambios en la provisión del servicio. Se prevé crearlo dentro de un año.
A.16. Gestión de incidentes de seguridad de la información **A.16.1. Gestión de incidentes de seguridad de la información y mejoras**			
16.1.1. Responsabilidades y procedimientos	**5**	**Cumple**	Se han establecido responsabilidades y procedimientos de gestión de los incidentes de seguridad para garantizar una respuesta rápida, efectiva y adecuada.
16.1.2. Notificación de los eventos de seguridad de la información.	**5**	**Cumple**	Trabajadores, contratistas y terceros están adecuadamente formados y conocen su responsabilidad de comunicar cualquier evento de seguridad de la información. Se miden las notificaciones recibidas.
16.1.3. Notificación de puntos débiles de la seguridad	**5**	**Cumple**	Todos deben anotar y notificar los puntos débiles observados o sospechados de existir. Se miden las señalaciones.
16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información	**5**	**Cumple**	El procedimiento indica, en la evaluación de los eventos de seguridad de la información, si clasificarlos como incidentes de seguridad de información. Se ha revisado al menos una vez
16.1.5. Respuesta a incidentes de seguridad de la información.	**5**	**Cumple**	Hay procedimientos documentados para responder a los incidentes de seguridad de la información. Se han revisado al menos una vez

16.1.6. Aprendizaje de los incidentes de seguridad de la información.	**3**	**Cumple**	Aunque se almacenan las informaciones obtenidas de la resolución de incidentes de seguridad, no hay evidencias de su utilización para reducir la probabilidad o el impacto de los incidentes futuros.
16.1.7. Recopilación de evidencias	**2**	**Observación**	Hay un procedimiento de recogidas de evidencias, pero no es cierto que todos cumplan con las directivas.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.1. Continuidad de la seguridad de la información**			
17.1.1. Planificación de la continuidad de la seguridad de la información	**5**	**Cumple**	Se ha desarrollado un documento de continuidad de negocio, que ya ha sido revisado al menos una vez.
17.1.2. Implementar la continuidad de la seguridad de la información	**5**	**Cumple**	Se han documentado los planes establecidos correspondientes a los análisis del control A.17.1.1. Se miden los resultados obtenidos.
17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**5**	**Cumple**	Los planes de continuidad se han ya verificado y revisado al menos una vez.
A.17. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio **A.17.2. Redundancias**			
17.2.1. Disponibilidad de los recursos de tratamiento de la información	**3**	**Cumple**	Hay redundancia para una parte de los recursos (las bases de datos)
A.18. Cumplimiento **A.18.1. Cumplimiento de los requisitos legales y contractuales**			
18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales	**5**	**Cumple**	Se revisa periódicamente la legislación vigente.
18.1.2. Derechos de propiedad intelectual (DPI)	**3**	**Cumple**	Se han implementado unos controles sobre el uso de productos de software patentados, pero no sobre el uso de materiales con respecto a los cuales pueden existir derechos de propiedad intelectual.
18.1.3. Protección de los registros de la organización	**4**	**Cumple**	Los registros están protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado. Todavía faltan indicadores
18.1.4. Protección y privacidad de la información de carácter personal	**3**	**Cumple**	Existe un procedimiento para garantizar la protección y la privacidad de los datos. No existe una metodología para evaluar su evolución.
18.1.5. Regulación de los controles criptográficos	**5**	**Cumple**	Se utilizan controles criptográficos y se han revisado.
A.18. Cumplimiento **A.18.2. Revisiones de la seguridad de la información**			
18.2.1. Revisión independiente de la seguridad de la información	**5**	**Cumple**	Se han realizado, y también se han planificado, revisiones externas independientes.
18.2.2. Cumplimiento de las políticas y normas de seguridad	**5**	**Cumple**	Los directivos revisan periódicamente el cumplimiento de políticas y normas de seguridad.
18.2.3. Comprobación del cumplimiento técnico	**5**	**Cumple**	Se comprueba el cumplimiento técnico de los sistemas de la seguridad de la información.

Anexo 15 – Evaluación de la madurez ISO 27001

ISO 27001 clause	Mandatory requirement for the ISMS	Status	Cumplimiento	Notes
4				
4,1				
4,1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	**L5**	**Cumple**	Existe un SGSI, y se mejora
4,2				
4,2	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security	**L5**	**Cumple**	Se han individuado y documentado el objetivo, los sectores y los procesos involucrados.
4,3				
4,3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	**L5**	**Cumple**	Se han individuado y documentado el objetivo, los sectores y los procesos involucrados.
4,4				
4,4	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	**L5**	**Cumple**	Hay un proceso de mejora continua del SGSI
5	**Leadership**			
5,1				
5,1	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:			
5.1 (a)	ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (b)	ensuring the integration of the information security management system requirements into the organization's processes;	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte

5.1 (c)	ensuring that the resources needed for the information security management system are available;	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (d)	communicating the importance of effective information security management and of conforming to the information security management system requirements;	**L5**	**Cumple**	Se ha comunicado la importancia del objetivo a toda la organización.
5.1 (e)	ensuring that the information security management system achieves its intended outcome(s);	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (f)	directing and supporting persons to contribute to the effectiveness of the information security management system;	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (g)	promoting continual improvement; and	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5.1 (h)	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte
5,2				
5,2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura su soporte.
5,3				
5,3	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	**L5**	**Cumple**	Existe un documento que recoge roles y responsabilidades.

6				
6,1				
6.1.1	**General**			
6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement	**L5**	**Cumple**	Se ha realizado un análisis de riesgos, que se mejora.
6.1.1 (d)	The organization shall plan actions to address these risks and opportunities; and	**L4**	**Cumple**	Los procedimientos existentes no son totalmente exhaustivos.
6.1.1 (e)	The organization shall plan how to: 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	**L4**	**Cumple**	Faltan unos indicadores para poder correctamente evaluar la eficaz de las acciones.
6.1.2				
6.1.2	The organization shall define and apply an information security risk assessment process that:			
6.1.2 (a)	establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	**L5**	**Cumple**	El análisis de riesgos ha permitido establecer el criterio de aceptación.
6.1.2 (b)	ensures that repeated information security risk assessments produce consistent, valid and comparable results;	**L5**	**Cumple**	El SGSI se controla y revisa
6.1.2 (c)	identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	**L5**	**Cumple**	En el SGSI se han asignado los responsables a los riesgos

6.1.2 (d)	analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	**L5**	**Cumple**	Se ha hecho el análisis de riesgos
6.1.2 (e)	evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analyzed risks for risk treatment.	**L5**	**Cumple**	Se ha hecho el análisis de riesgos
6.1.3				
6.1.3	The organization shall define and apply an information security risk treatment process to:			
6.1.3 (a)	select appropriate information security risk treatment options, taking account of the risk assessment results;	**L4**	**Cumple**	Se han tomado medidas contra los riesgos críticos
6.1.3 (b)	determine all controls that are necessary to implement the information security risk treatment option(s) chosen;	**L4**	**Cumple**	Se pueden añadir otros controles
6.1.3 (c)	compare the controls determined in 6.1.3 (b) above with those in Annex A and verify that no necessary controls have been omitted;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
6.1.3 (d)	produce a Statement of Applicability that contains the necessary controls (see 6.1.3.b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
6.1.3 (e)	formulate an information security risk treatment plan; and	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
6.1.3 (f)	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	**L5**	**Cumple**	El plan ha sido aceptato
6,2				
6,2	The organization shall establish information security objectives at relevant functions and levels.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
6,2	The information security objectives shall:	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo

	a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.			
6,2	When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated.	**L3**	**Cumple**	A veces faltan indicaciones sobre como evaluar unos resultados; es necesario también mejorar la gestión de los recursos.
7				
7,1				
7,1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	**L5**	**Cumple**	La dirección se ha comprometido con el objetivo de obtener la certificación y asegura los recursos necesarios.
7,2				
7,2	The organization shall:			
7.2 (a)	determine the necessary competence of person(s) doing work under its control that affects its information security performance;	**L2**	**No Cumple**	A veces las competencias necesarias no se han documentado
7.2 (b)	ensure that these persons are competent on the basis of appropriate education, training, or experience;	**L2**	**No Cumple**	El procedimiento de comprobación no se ha documentado
7.2 (c)	where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and	**L4**	**Cumple**	Se han planificado cursos de formación y se ha contratado una consultoría especializada.
7.2 (d)	retain appropriate documented information as evidence of competence.	**L2**	**No Cumple**	El procedimiento no se ha documentado
7,3				
7,3	Persons doing work under the organization's control shall be aware of:			
7.3 (a)	the information security policy;	**L5**	**Cumple**	Todos los trabajadores la conocen.

7.3 (b)	their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and	**L5**	**Cumple**	Todos los trabajadores la conocen. Se han hecho cursos de formación.
7.3 (c)	the implications of not conforming with the information security management system requirements.	**L5**	**Cumple**	Además de las consecuencias sobre la seguridad, todos los trabajadores conocen las sanciones disciplinarias que podrían sufrir.
7,4				
7,4	The organization shall determine the need for internal and external communications relevant to the information security management system including:			
7.4 (a)	on what to communicate;	**L5**	**Cumple**	Se ha documentado en el SGSI
7.4 (b)	when to communicate;	**L5**	**Cumple**	Se ha documentado en el SGSI
7.4 (c)	with whom to communicate;	**L5**	**Cumple**	Se ha documentado en el SGSI
7.4 (d)	who shall communicate; and	**L5**	**Cumple**	Se ha documentado en el SGSI
7.4 (e)	the processes by which communication shall be effected.	**L5**	**Cumple**	Se ha documentado en el SGSI
7,5				
7.5.1				
7.5.1	The organization's information security management system shall include:			
7.5.1 (a)	documented information required by this International Standard; and	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
7.5.1 (b)	documented information determined by the organization as being necessary for the effectiveness of the information security management system.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
7.5.2				
7.5.2	When creating and updating documented information the organization shall ensure appropriate:			
7.5.2 (a)	identification and description (e.g. a title, date, author, or reference number);	**L3**	**Cumple**	Solo los documentos creados o revisados desde cuándo se ha puesto en marcha el SGSI
7.5.2 (b)	format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	**L3**	**Cumple**	Solo los documentos creados o revisados desde cuándo se ha puesto en marcha el SGSI
7.5.2 (c)	review and approval for suitability and adequacy.	**L3**	**Cumple**	Solo los documentos creados o revisados desde cuándo se ha puesto en marcha el SGSI

7.5.3				
7.5.3	Documented information required by the information security management system and by this International Standard shall be controlled to ensure:			
7.5.3 (a)	it is available and suitable for use, where and when it is needed; and	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
7.5.3 (b)	it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	**L3**	**Cumple**	Se ha documentado en el SGSI
7.5.3	For the control of documented information, the organization shall address the following activities, as applicable:			
7.5.3 (c)	distribution, access, retrieval and use;	**L3**	**Cumple**	Se ha documentado en el SGSI
7.5.3 (d)	storage and preservation, including the preservation of legibility;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
7.5.3 (e)	control of changes (e.g. version control); and	**L3**	**Cumple**	Se ha documentado en el SGSI
7.5.3 (f)	retention and disposition.	**L3**	**Cumple**	Se ha documentado en el SGSI
7.5.3	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	**L2**	**No Cumple**	Falta la documentación del procedimiento
8				
8,1				
8,1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
8,1	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
8,1	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
8,1	The organization shall ensure that outsourced processes are determined and controlled.	**L5**	**Cumple**	El procedimiento aparece documentado.

8,2				
8,2	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.a.	**L5**	**Cumple**	Se hace y revisa periódicamente
8,2	The organization shall retain documented information of the results of the information security risk assessments.	**L5**	**Cumple**	El procedimiento aparece bien documentado.
8,3				
8,3	The organization shall implement the information security risk treatment plan.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
8,3	The organization shall retain documented information of the results of the information security risk treatment.	**L5**	**Cumple**	El procedimiento aparece bien documentado.
9				
9,1				
9,1	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:			
9.1 (a)	what needs to be monitored and measured, including information security processes and controls;	**L4**	**Cumple**	Se pueden mejorar los controles
9.1 (b)	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	**L4**	**Cumple**	Se pueden mejorar los controles
9.1 (c)	when the monitoring and measuring shall be performed;	**L4**	**Cumple**	Se pueden mejorar los controles
9.1 (d)	who shall monitor and measure;	**L5**	**Cumple**	Todos los indicadores tienen su responsable
9.1 (e)	when the results from monitoring and measurement shall be analyzed and evaluated; and	**L5**	**Cumple**	Se ha definido en el SGSI
9.1 (f)	who shall analyze and evaluate these results.	**L5**	**Cumple**	Se ha definido en el SGSI
9,2				
9,2	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:			
9.2 (a)	conforms to	**L5**	**Cumple**	Se hacen auditorias periódicas

	1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;			
9.2 (b)	is effectively implemented and maintained.	**L5**	**Cumple**	Las auditorias se han planificado y al menos una ya hecha
9,2	The organization shall:			
9.2 (c)	plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;	**L5**	**Cumple**	Las auditorias se han planificado
9.2 (d)	define the audit criteria and scope for each audit;	**L5**	**Cumple**	Se ha definido en el SGSI
9.2 (e)	select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	**L5**	**Cumple**	Se ha definido en el SGSI
9.2 (f)	ensure that the results of the audits are reported to relevant management; and	**L5**	**Cumple**	Se ha definido en el SGSI
9.2 (g)	retain documented information as evidence of the audit programme(s) and the audit results.	**L5**	**Cumple**	Se ha definido en el SGSI
9,3				
9,3	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:			
9.3 (a)	the status of actions from previous management reviews;	**L5**	**Cumple**	Se ha definido en el SGSI
9.3 (b)	changes in external and internal issues that are relevant to the information security management system;	**L5**	**Cumple**	Se ha definido en el SGSI
9.3 (c)	feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo

9.3 (d)	feedback from interested parties;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
9.3 (e)	results of risk assessment and status of risk treatment plan; and	**L5**	**Cumple**	Se ha definido en el SGSI
9.3 (f)	opportunities for continual improvement.	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
9,3	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	**L5**	**Cumple**	Se ha definido en el SGSI
10				
10,1				
10,1	When a nonconformity occurs, the organization shall:			
10.1 (a)	react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
10.1 (b)	evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
10.1 (c)	implement any action needed;	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
10.1 (d)	review the effectiveness of any corrective action taken; and	**L5**	**Cumple**	Se ha definido en el SGSI
10.1 (e)	make changes to the information security management system, if necessary.	**L5**	**Cumple**	Se ha definido en el SGSI
10,1	Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:			
10.1 (f)	the nature of the nonconformities and any subsequent actions taken, and	**L4**	**Cumple**	El SGSI se ha puesto en marcha, es necesario mejorarlo
10.1 (g)	the results of any corrective action.	**L5**	**Cumple**	Se ha definido en el SGSI

10,2				
10,2	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	**L4**	**Cumple**	Existe un proceso definido de mejora continua, aunque el SGSI es nuevo y es necesario mejorarlo