Universitat Autònoma de Barcelona

www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 De la empresa TECNOSOFT

Silvia Zugazaga Echebarria

TFM

Elaborado por Silvia Zugazaga Echebarria 2018/2019

Resumen del Trabajo.

El proyecto que se presenta en este documento forma parte del Trabajo Final de Máster del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones. El objetivo es el desarrollo de un Plan de Implementación de un Sistema de Gestión de Seguridad de la Información en la organización ficticia TECNOSOFT, empresa dedicada a la implantación de soluciones informáticas, siguiendo la norma ISO/IEC 27001:2013.

En primer lugar se ha descrito la organización sobre la que se realiza el proyecto y se ha realizado un análisis diferencial respecto a las normas ISO 27001:2013 e ISO 27002:2013 para conocer el punto de partida del proyecto.

En la segunda fase se han definido los documentos necesarios para el cumplimiento normativo de la ISO 27001:2013 política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por la Dirección, gestión de roles y responsabilidades, declaración de aplicabilidad y metodología de análisis de riesgos.

A continuación, en la fase 3, se ha realizado el análisis de riesgos de la organización siguiendo la metodología MAGERIT. Para ello, se han identificado todos los activos de la organización y se han valorado. Posteriormente, se han analizado las posibles amenazas a las que está expuesta la organización y, por último, se ha obtenido el impacto y riesgo potencial de cada uno de los activos identificados.

En la cuarta fase se han planificado diversos proyectos a realizar con el fin de reducir los principales riesgos encontrados y así mejorar el estado de la seguridad de la información de la organización.

En la fase 5, se ha obtenido el grado de madurez de la organización con respecto a las normas ISO 27002:2013 y 27001:2013 y se han presentado los resultados obtenidos.

Tras haber finalizado todas las fases del proyecto, se ha mejorado la seguridad de la información de la organización.

Abstract.

The project presented in this document is part of the Final Master's Project of the Interuniversity Master's Degree in Information and Communications Technology Security. The objective is the development of an Implementation Plan for an Information Security Management System in the fictitious organization TECNOSOFT, a small company dedicated to the implementation of IT solutions, following the ISO / IEC 27001: 2013 standard.

Firstly, the organization on which the project is carried out has been described and a differential analysis has been carried out regarding the ISO 27001: 2013 and ISO 27002: 2013 standards to know the starting point of the project.

In the second phase, the necessary documents have been defined for compliance with the ISO 27001: 2013 security policy, internal auditing procedure, indicator management, review procedure by the Directorate, management of roles and responsibilities, declaration of applicability and risk analysis methodology.

Then, in phase 3, the risk analysis of the organization was carried out following the MAGERIT methodology. For this, all the assets of the organization have been identified and valued. Subsequently, the possible threats to which the organization is exposed have been analyzed and, finally, the impact and potential risk of each of the identified assets has been obtained.

In the fourth phase, several projects have been planned to be carried out in order to reduce the main risks encountered and thus improve the security status of the organization's information.

In phase 5, the degree of maturity of the organization has been obtained with respect to the ISO 27002: 2013 and 27001: 2013 standards and the results obtained have been presented.

After having completed all phases of the project, the security of the organization's information has been improved.

Contenido

Ilustraciones

1. Situación actual: Contextualización, Objetivos y Análisis Diferencial

1.1 Introducción.

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).
El marco legal ha reflejado la importancia de la seguridad de la información (a nivel del estado español, leyes como la 11/2007 artículo 42: "Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad", lo demuestran) . La seguridad no es por tanto un aspecto opcional, sino que debe ser inherente a las actividades de la propia empresa, y constituye un punto de partida ineludible para toda organización en la actualidad.
El planteamiento del proyecto será por tanto, sentar las bases de un Plan de Director de Seguridad para la empresa. Simplificando, y como iremos viendo, nuestro proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción.

Intencionadamente, la lista anterior no contempla aspectos organizativos, que aún así, tocaremos a lo largo del presente proyecto.

1.2. Norma ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

Estructura de la norma ISO 27001:

1. Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

2. Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.
3. Términos y Definiciones: Describe la terminología aplicable a este estándar.
4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
5. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
6. Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
7. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
9. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.
10. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

1.2.1 Planificación:

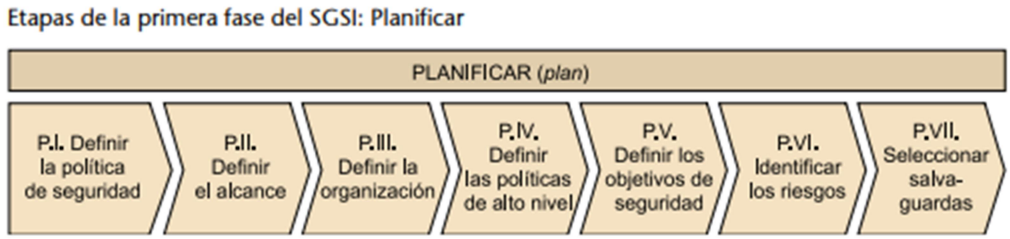

FIGURA1: FASES DE LA PLANIFICACIÓN.[10]

P.I. **Definir la política de seguridad de la información**. La política de seguridad de la información establece los principios y líneas de actuación globales en cuestiones de seguridad de la información, alineados con los objetivos del negocio. La política debe demostrar el compromiso de la Dirección con la seguridad de la información y se debe dar a conocer a todos los usuarios.

P.II. **Definir el alcance**. El primer paso pasa por establecer el alcance del sistema de gestión en términos de procesos, áreas organizativas, emplazamientos y activos.

P.III. **Definir la organización de la seguridad de la información**. Cada organización deberá crear su propio esquema organizativo interno, asegurando en cualquier caso que todas las responsabilidades y funciones en materia de seguridad de la información están correctamente asignadas y garantizando, siempre que sea posible, el principio de segregación de funciones.

P.IV. **Definir las políticas de alto**. Las políticas de alto nivel contemplan en conjunto todas las áreas de seguridad de la información.

P.V. **Definición de objetivos de seguridad de la información** Es necesario establecer objetivos concretos de seguridad de la información, que garanticen que todas las iniciativas en seguridad de la información estén coordinadas y orientadas en una misma dirección, y alineadas con los objetivos del negocio. Los objetivos de seguridad se suelen definir con carácter anual.

P.VI. **Identificación de los riesgos** Es muy importante identificar los activos de información y establecer el riesgo al que están sometidos, a partir de la determinación de cuál sería el impacto para la organización en caso de que se produjera una situación de falta de confidencialidad / privacidad, integridad o disponibilidad de dichos activos.

P.VII. **Selección de salvaguardas** Una vez identificados los riesgos que hay que mitigar (riesgos no asumibles) y los objetivos de seguridad que se desea alcanzar, se deberán seleccionar los controles o salvaguardas necesarias.

1.2.2 DO:

La segunda fase del SGSI se compone básicamente de dos actividades:
• Implantar el plan de gestión del riesgo.
• Seleccionar e implantar indicadores.

D.I. **Implantación del plan de gestión del riesgo**. El Plan de gestión del riesgo determina cómo y cuándo implantar los controles seleccionados y se concreta en el Plan de seguridad de la información, en ocasiones también denominado Plan director de seguridad de la información, que agrupa las acciones en proyectos, las prioriza definiendo acciones a corto y medio plazo (unos 3 años) y realiza una estimación de costes.

D.II. **Selección e implantación de indicadores.** Para que el sistema se mantenga vivo y actualizado, es necesario evaluar su eficacia de forma continuada. Para ello, se deben establecer indicadores que permitan controlar el funcionamiento de las medidas de seguridad de la información implantadas, así como su eficacia y eficiencia, y definir los mecanismos y la periodicidad de medida de dichos indicadores.

1.2.3. CHECK.

La tercera fase del SGSI se compone de 3 etapas:

• C.I **Desarrollar procedimientos de monitorización**.
Es preciso realizar un seguimiento periódico de los indicadores de seguridad de la información, para conocer su estado y evolución y, en definitiva, su eficacia

• C.II. **Revisar regularmente el SGSI**.
La Dirección debe revisar el SGSI a intervalos planificados, para ratificar su conveniencia, adecuación y eficacia. Esta revisión debe ser como mínimo anual, aunque inicialmente se recomienda una periodicidad menor.
• C.III. **Auditar internamente el SGSI.**
La comprobación de la idoneidad del diseño e implantación del SGSI se realiza a través de auditorías. Éstas pueden ser llevadas a cabo internamente, o se pueden contratar auditores externos para efectuarlas.

1.2.4. ACT.

Finalmente, la cuarta y última fase del ciclo del SGSI se compone de las dos actividades siguientes:
• Implantar mejoras y acciones correctivas.
• Mantener registros.

1.3. ISO/IEC 27002

La norma ISO/IEC 27002 se trata de un código de buenas prácticas para la gestión de la seguridad de la información y recoge un completo y amplio catálogo de controles y buenas prácticas en la materia. Es el conjunto de controles que la ISO 27001 toma como referencia a la hora de seleccionar los controles de seguridad.
Esta norma se utiliza en las organizaciones para cubrir cualquiera de los siguientes objetivos:

1. Formular los requerimientos y objetivos de seguridad de la información.
2. Asegurar que los riesgos de seguridad se gestionan de manera efectiva.
3. Asegurar el cumplimiento de las leyes y regulaciones existentes.
4. Implementar y gestionar los controles necesarios para asegurar que se alcanzan los objetivos de seguridad definidos.
5. Definir nuevos procesos de gestión de seguridad o identificar y clarificar los existentes.
6. Conocer el estado de las actividades de gestión de la seguridad por parte de la Dirección.
7. Conocer el grado de cumplimiento de las políticas, directivas y estándares adoptados por la empresa, por parte de auditores internos y/o externos.
8. Establecer políticas, directivas, estándares o procedimientos de seguridad de la información en las relaciones con terceros.
9. Convertir la seguridad de la información en un facilitador del negocio.
10. Proporcionar información relevante sobre el estado de la seguridad de la información a los clientes.

En la primera versión de esta norma, ISO 27002:2005, se incluyeron 11 dominios, 39 objetivos de seguridad y 133 controles.
En 2013 se publicó una nueva versión de esta norma, la ISO 27002:2013 en la que se modificaron la cantidad de dominios y de controles, pasando a ser 14 los dominios y 114 los controles

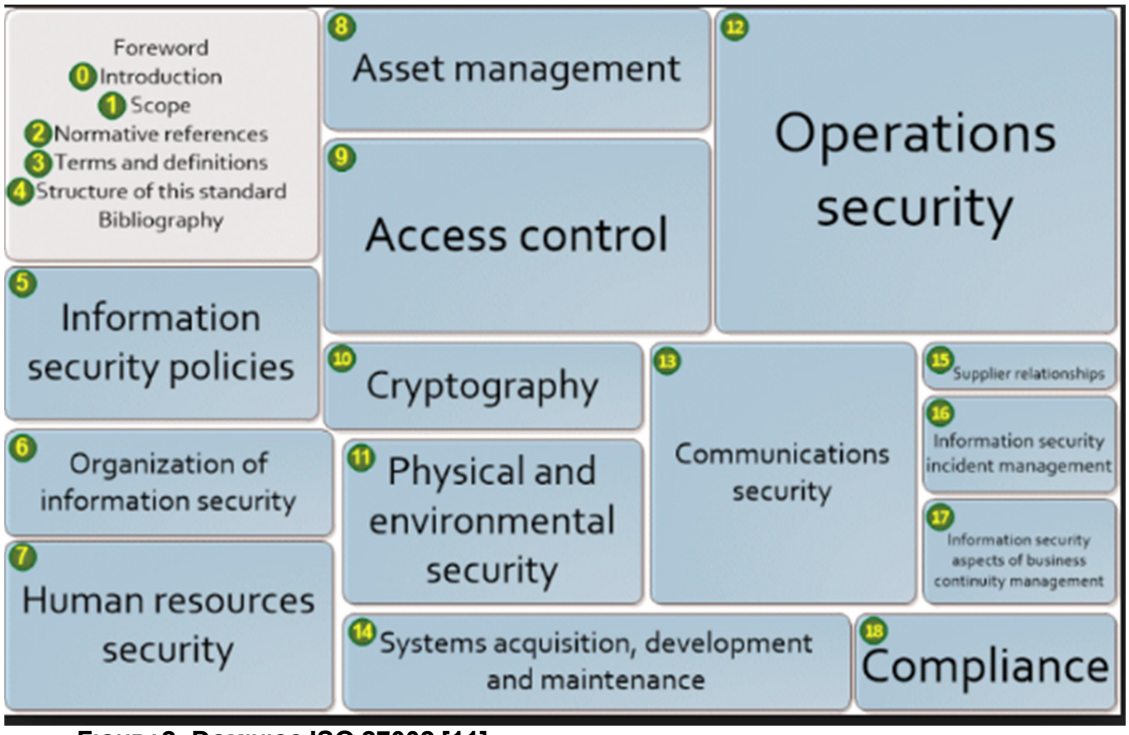

FIGURA2: DOMINIOS ISO 27002 [11]

Ciclo Deming.

El desarrollo de un sistema de gestión de la seguridad de la información se basa en la ISO 27001 y la ISO 27002, así como en el Ciclo de Deming, para garantizar la actualización del sistema y la mejora continua, tal y como se describe en el gráfico siguiente:

Ciclo de Deming aplicado a los sistemas de gestión de seguridad de la información.

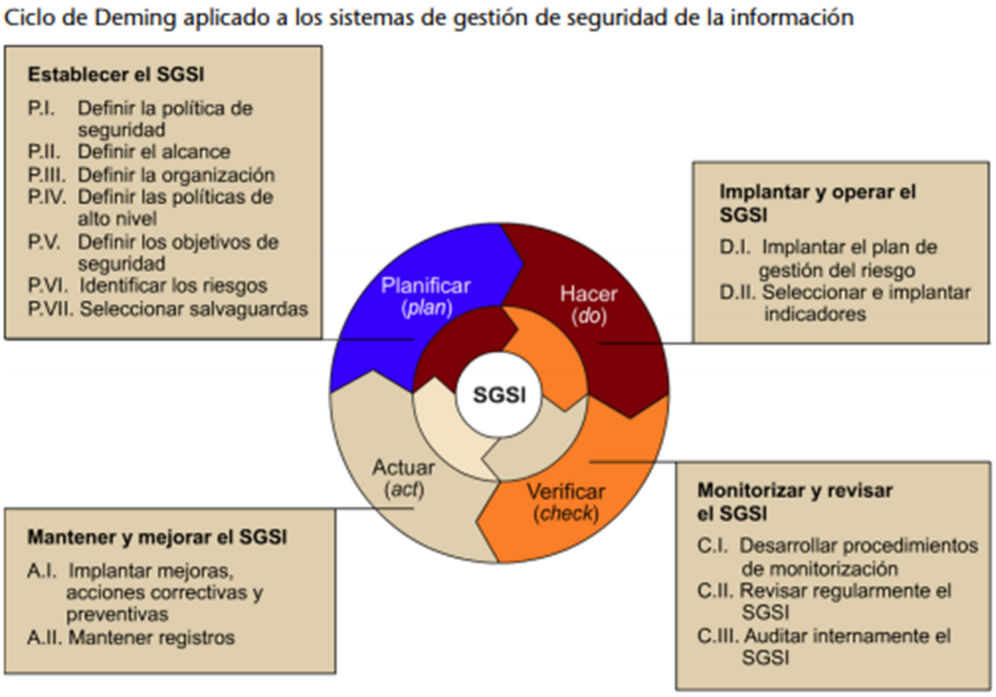

FIGURA3: CICLO DEMING.[10]

1.4 Contextualización.

Para la realización del TFM hemos de realizar el Plan de seguridad de la información para una pequeña compañía del sector de las TIC TECNOSOFT. Esta compañía 10 empleados se dedica al desarrollo e implantación de desarrollos de software en cliente.

- 1 CEO
- 1 responsable de RRHH,
- 1 comercial,
- 2 líderes de proyecto expertos en TI,
- 4 técnicos de desarrollo
- 1 técnico de sistemas.

La empresa posee un CPD principal en la oficina de la organización, y otro CPD secundario externalizado. El CPD primario cuenta con 5 servidores físicos, 2 de los cuales tienen un Windows Server, y los otros 2 se utilizan para máquinas virtuales (VMware). De los 5 servidores, 1 tiene una base de datos ORACLE con la información de clientes y proveedores, y otro tiene también MySQL con

información relevante de la configuración de los diferentes elementos que fabrica la compañía. Por otra parte, la organización posee un firewall, un switch, un punto de acceso Wifi, y una unidad de cinta para las copias de seguridad (5 cintas LTO en total). Cada empleado tiene un portátil y un dispositivo móvil (smartphone). Los empleados tienen instalado en sus equipos el software habitual que tiene por defecto Windows 10. Además, la organización posee 2 medios de almacenamiento externo para compartir información con entidades externas. Se subcontrata el hospedaje de la página web de la organización, y el correo electrónico. También se subcontrata servicio de seguridad física, así como servicio de limpieza.
Al estar ganando peso en la comunidad, la dirección se está preocupando cada vez más por la seguridad de la información, y ha decidido tomar cartas en el asunto de manera activa. Esto no es del todo casual, ya que, al estar cada vez mejor posicionado en el sector, el riesgo de poder sufrir un posible incidente de seguridad y que pueda tener un impacto negativo en la imagen de la empresa, como una denegación de servicio. Por otra parte, la implementación de un sistema de gestión de la seguridad de la información, ahora que la empresa no se encuentra en expansión, permitirá integrar la cultura de seguridad en la misma de una manera temprana y eficaz, haciendo que este sistema pueda crecer con la misma.

Hoy en día, las necesidades de seguridad de las empresas se encuentran basadas en tres fundamentos principales:

Las personas

- Los profesionales de las TIC con formación especializada y acreditada.
- Usuarios con suficiente nivel de educación cómo para poder usar las TIC.

La gestión

- Sistemas de Gestión de Seguridad de la Información basado en la norma ISO-27002.
- Seguridad englobada dentro de todos los procedimientos y los procesos de negocio, así como las actividades de la organización.

Las tecnologías y sistemas de información y comunicaciones.

- Sistemas que cumplen certificaciones de calidad de la seguridad de los productos TIC.

Según el INTECO en un análisis realizado en función del tamaño indica que existe una mayor probabilidad de encontrar profesionales de seguridad en las empresas de mayor dimensión (un 62,8% en las medianas empresas), ya sea en exclusiva (12,4%) o compaginando otras funciones de informática (50,4%). Por su parte, las pequeñas empresas recurren, principalmente, a la gestión externa de la seguridad.
No obstante, al tratarse de una pequeña empresa que cuenta con un personal de perfil técnico especializado (líderes de proyecto y técnicos de sistemas), yo propondría una gestión interna de la seguridad, en el cual la seguridad es gestionada íntegramente por personal propio.

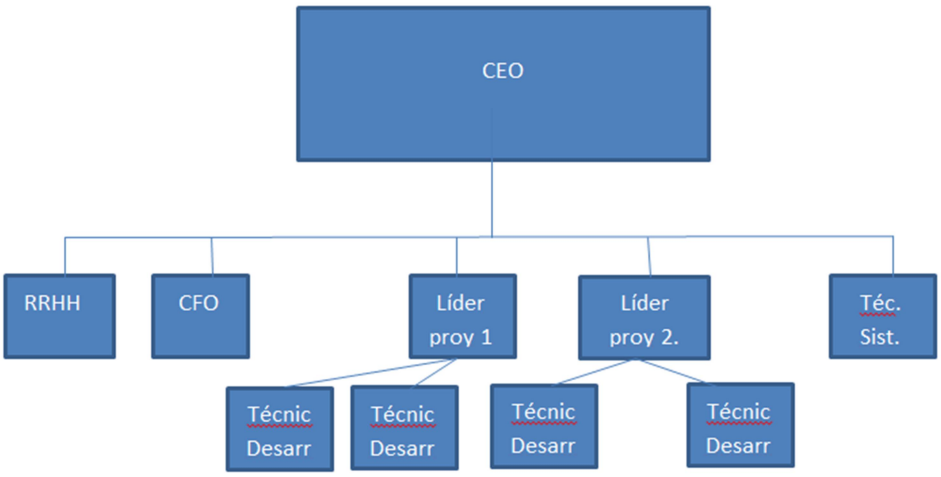

FIGURA 4: ORGANIGRAMA DE LA EMPRESA.

a)***Director General (CEO).*** La dirección general es consciente de la importancia que tiene la elaboración del SGSI y el rol que debe desempeñar en el Comité de Seguridad. Es el máximo responsable de impulsar el proyecto y resolver cualquier conflicto que pudiera surgir.

Responsable de RRHH. Muchas de las decisiones que puede tomar el comité de seguridad, tienen connotaciones para con los empleados de la compañía (por ejemplo, firmar un acuerdo de confidencialidad). De esta figura podrían depender ciertos criterios de Calidad, Medio Ambiente, Prevención de riesgos laborales, Selección y Formación, etc.

Director Financiero (CFO). También necesario por dos motivos. Por ser responsable del ERP. En este sentido es probable que se tengan que aplicar política o hacer adaptaciones, por lo que su presencia puede ayudar a tomar decisiones en este sentido. Por otra parte, el desarrollo del SGSI y realizar los cambios necesarios en los Sistemas de Información, políticas, etc. necesitarán inversiones. La presencia del Director Financiero ayudará en este sentido.

Líderes de proyecto se encargan del Desarrollo de soluciones tecnológicas:

Son los encargados de desarrollar aplicaciones informáticas que ayuden a conseguir los objetivos fijados por el cliente. Otra de las principales funciones que desempeñan es la de dar soporte a las otras secciones con soluciones informáticas que ayuden a mejorar la productividad y tareas que desempeñan.

Clasificar la información de la cual son responsables en función de su criticidad para la compañía en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio, trazabilidad e impacto mediático y determinar el uso que de la información se puede hacer y quién puede acceder a ella.

El técnico de sistemas será Responsable de Sistemas de Seguridad de la Información **CISO**.

Técnicos de Desarrollo, junto con el técnico de sistemas formarán el **Comité de Seguridad de la Información.**

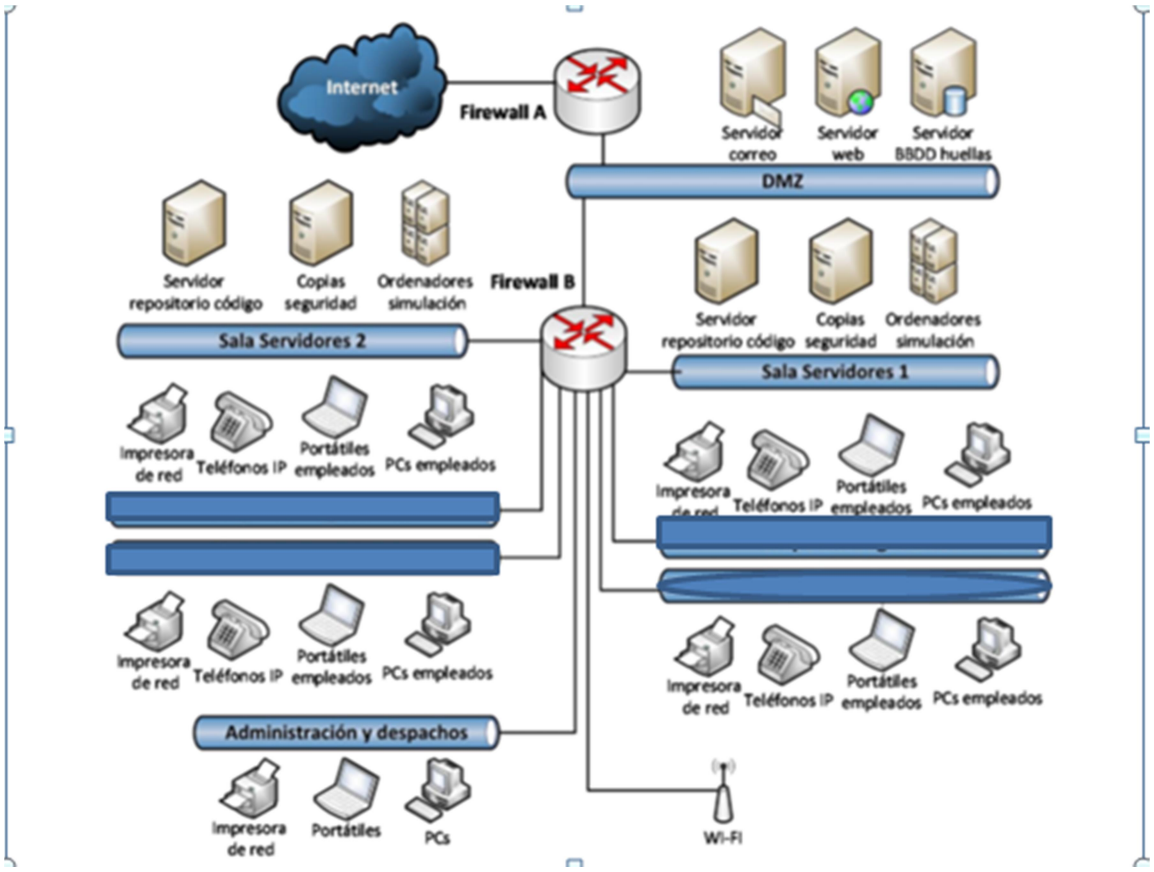

FIGURA 5: ESQUEMA DE RED DE LA EMPRESA.

Se intenta minimizar la cantidad de sistemas a mantener, es por ello que muchos sistemas se encuentran desplegados en la nube o usando servicios en la misma, sin embargo, se ha optado por mantener sistemas dentro de la organización. Así por ejemplo:

- Sistemas de integración continua y de pruebas unitarias: Desplegado en los sistemas de la empresa
- Repositorios de código (GitHub): En GitHub, acceso privado
- Servidores de correo: Uso de Gmail mediante google apps
- CRM: Desplegado en los sistemas de la empresa
- Nóminas y datos de negocio: Almacenados en servidores de la empresa
- Datos de clientes: Almacenados en servidores de la empresa
- Sistemas VPN para interconexión de oficinas: Desplegados en la empresa
- Gestores de tareas y gestión de equipo: Cloud

Servidores Web: Desplegado como servicio Amazon

- Firewall: Desplegado localmente
- Sistemas perimetrales (IDS/IDS): Desplegados en la empresa
- Sistema de correlación de eventos
- Plataforma recolección y correlación de eventos: Desplegados en la empresa
- Almacenaje de información y documentación de trabajo: Cloud
- Paquetes de office (Libreoffice).

1.5 Alcance y objetivos del plan Director.

El plan director de seguridad permitirá establecer un marco de seguridad donde se establecerá el nivel de riesgo asumido, plan de tratamiento de riesgo los cuales nos permitirán establecer la situación actual y donde se quiere llegar respecto a la seguridad de la información:

- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura que ofrece el área de TI.
- Definir directrices en temas de seguridad de la información para el área de TI.
- Definir y planificar los planes de acción a realizar (a corto, mediano y largo plazo) teniendo como referencia la diferencia existente entre el nivel de seguridad actual y el nivel de seguridad objetivo.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.
- Identificar, calificar y hacer un tratamiento adecuado de los riesgos que puedan impactar negativamente la información, los procesos y la organización sobre las redes de telecomunicaciones y los servicios asociados al segmento de hogares, implementando las salvaguardas que permitan reducir el nivel de exposición frente a ataques informáticos.
- Implementación de un equipo de seguridad proactivo, encargado de recolectar y modelar amenazas que afecten a la compañía, incidentes de seguridad mediante las distintas plataformas desplegadas y filtración de datos.
- Mitigar lo máximo posible cualquier incidente de seguridad. Dar el valor estratégico que la seguridad de la información tiene. La dirección teme que pueda ocurrir cualquier evento que pueda poner en peligro o afectar a la imagen de la compañía. Para ello los indicadores de respuesta a incidentes se van a modelar de la siguiente manera:
- Proteger la empresa y la información que posee, para ello se debe implementar y probar un plan de continuidad de negocio. En caso de catástrofe, la empresa deberá estar capacitada para operar parcialmente en 48 horas máximo y estar recuperada completamente en una semana máximo.
- Dar cumplimiento a la normatividad y legislación vigente. Para ello, se propone como objetivo no tener denuncias por incumplimiento de normativa o legislación.
- Fomentar la cultura organizacional, la capacitación y toma de conciencia en seguridad informática mediante la implementación de cursos de formación que serán medidos a través de exámenes.

Para ello se va a seguir una metodología PDCA.

1.6. Análisis diferencial.

El origen de la norma ISO27001 se remonta a 1998 y se basa en la BSI (British Standard Institution) norma británica certificable. La primera versión certificable de la ISO 27001 fue publicada el 15 de octubre de 2005.
ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 27002 para su posible aplicación en el SGSI que implante cada organización justificando los motivos de exclusión de aquellos que finalmente no sean necesarios. ISO 27002 es para ISO 27001, por tanto, una relación de controles necesarios para garantizar la seguridad de la información.

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo; la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002 es un conjunto de buenas prácticas en seguridad de la información. Contiene 114 controles aplicables (en relación a la gestión de la continuidad de negocio, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, entre otros muchos, que ayudarán a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información.
A partir del 1 de julio de 2007, ISO 17799:2005 pasó a denominarse ISO 27002:2005, cambiando únicamente su nomenclatura. Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 dominios, 35 objetivos de control y 114 controles.

Para la realización del Análisis diferencial se plantea la siguiente clasificación según el nivel de madurez en relación con cada punto de la norma.
Se va a utilizar como modelo de evaluación de las medidas de seguridad ya implantadas en la organización el Modelo de Madurez de Capacidades (CCM) definido por el Software Engineering Institute. La aplicación de este modelo de madurez permite establecer criterios objetivos para la evaluación de la eficacia de los controles gracias a la repetitividad de la medida, permitiendo así analizar su evolución en el tiempo.
En el presente apartado se va a realizar un análisis de madurez de las medidas de seguridad ya implantadas en la organización en relación a la seguridad de la información.

L0	0%	Inexistente	• Ausencia total de proceso reconocible. • La organización no ha reconocido la existencia del problema.
L1	10%	Inicial	• La organización ha reconocido la existencia del problema y la necesidad de resolverlo. • No hay procesos estandarizados pero sí hay métodos ad hoc que tienden a ser aplicados de manera individual. • Resultados impredecibles y pobremente controlados.
L2	50%	Repetible	• Los procesos se han desarrollado y diferentes personas siguen procedimientos similares realizando la misma tarea. • No hay comunicación formal de procesos estándar y la responsabilidad recae en la persona. • Existe la posibilidad de que haya errores debido a la alta confianza en los conocimientos de las personas.
L3	90%	Definido	• Los procedimientos han sido estandarizados, documentados y comunicados. Son conocidos y bien entendidos. • El seguimiento de los procesos se ha dejado en mano de la persona y es complicado que se detecten desviaciones. • Los procedimientos no son sofisticados.
L4	95%	Administrado	• Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acciones en aquellos que no estén funcionando correctamente. • Los procesos se encuentran en constante mejora y proveen buenas prácticas.
L5	100%	Optimizado	• Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejora continua y diseño de madurez de la organización.

Tabla 1. Niveles de capacidad del Modelo de Madurez de Capacidades (CCM)

ISO 27001:

Estado de Implementación ISO 27001

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas
4	**Contexto de la organización**			
4,1	**Comprensión de la organización y de su contexto**			
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial		
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**			
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Repetible		
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Repetible		
4,3	**Determinación del alcance del SGSI**			
4,3	Determinar y documentar el alcande del SGSI	Definido		Documentación obligatoria ¿Existe el documento?
4,4	**SGSI**			
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Definido		
5	**Liderazgo**			
5,1	**Liderazgo y compromiso**			
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Definido		
5,2	**Política**			
5,2	Documentar la Política de Seguridad de la Informacion	Definido		
5,3	**Roles, responsabilidades y autoridades en la organización**			
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Definido		
6	**Planificación**			
6,1	**Acciones para tratar los riesgos y oportunidades**			
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Definido		
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Definido		
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Definido		
6,2	**Objetivos de seguridad de la información y planificación para su consecución**			
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Repetible		
7	**Soporte**			
7,1	**Recursos**			
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Definido		
7,2	**Competencia**			
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Definido		
7,3	**Concienciación**			
7,3	Implementar un programa de concienciación de seguridad	Repetible		

7,3	Implementar un programa de concianciación de seguridad	Repetible
7,4	**Comunicación**	
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Repetible
7,5	**Información documentada**	
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Inicial
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprovacion a los documentos	Inicial
7.5.3	Mantener un control adecuado de la documentación	Inicial
8	**Operación**	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Repetible
8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios	Repetible
8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Repetible
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Repetible
9,2	**Auditoría interna**	
9,2	Planificar y realizar una auditoria interna del SGSI	Definido
9,3	**Revisión por la dirección**	
9,3	La administración realiza una revision periodica del SGSI	Definido
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

TABLA 2: ANÁLISIS GAP 27001

Gráfico resumen:

Estado	Significado	Proporción de requerimientos SGSI	de Controles de Seguridad
? Desconocido	No ha sido verificado	0%	100%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	7%	0%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	15%	0%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	33%	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	44%	0%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	0%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo.	0%	0%

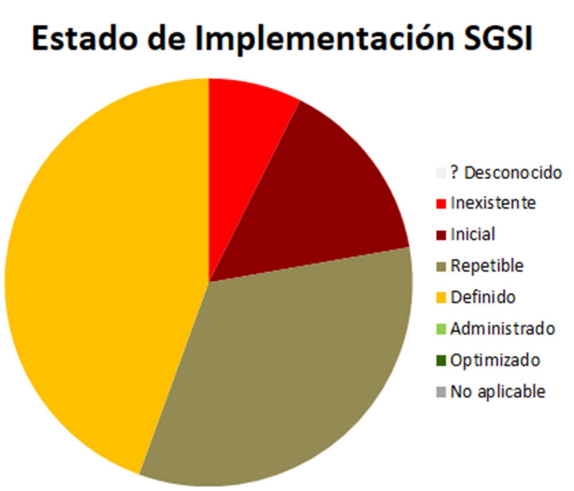

FIGURA6 RESULTADOS ANÁLISIS ISO27001

Conclusiones: Se muestra el estado actual de los controles ISO 27001 comparado con el estado óptimo.
En este caso se ve que en la mayoría de los niveles el estado es Definido o Administrado.
Se ve que no existe procedimiento relacionado con la evaluación de desempeño.
Se cuenta con planes de auditoría interna escasos en relación con la seguridad de la información. Esto conlleva por tanto a que la claúsula de mejora también se encuentre en un estado casi inexistente, mostrando la necesidad de generar procesos que ayuden en su formulación y mejora.

Si hacemos una media de la situación de los distintos controles de cada dimensión y cambiamos la escala para verla en porcentaje, obtenemos una evaluación general de cada dimensión de la **ISO 27002**.

CONTROL			Evaluación	Valor	Total
A.5 Information security policies					4
	A.5.1 Management direction for information security				4
	A.5.1.1	Policies for information security	4 - Gestionado	4	
	A.5.1.2	Review of the policies for informatio security	4 - Gestionado	4	
A.6 Organization of information security					1
	A.6.1 Internal organization				2
	A.6.1.1	Information security roles and responsibilities	3 - Definido	3	
	A.6.1.2	Segregation of duties	3 - Definido	3	
	A.6.1.3	Contact with authorities	4 - Gestionado	4	
	A.6.1.4	Contact with special interest groups	0 - No existente	0	
	A.6.1.5	Information security in project management	0 - No existente	0	
	A.6.2 Mobile devices and teleworking				0
	A.6.2.1	Mobile device policy	0 - No existente	0	
	A.6.2.2	Teleworking	0 - No existente	0	
A.7 Human resource security					1,333333333
	A.7.1 Prior to employment				0
	A.7.1.1	Screening	0 - No existente	0	
	A.7.1.2	Terms and conditions of employment	0 - No existente	0	
	A.7.2 During employment				0
	A.7.2.1	Management responsibilities	0 - No existente	0	
	A.7.2.2	Information security awareness, education and training	0 - No existente	0	
	A.7.2.3	Disciplinary process	0 - No existente	0	
	A.7.3 Termination and change of employment				4
	A.7.3.1	Termination or change of employment responsibilities	4 - Gestionado	4	
A.8 Asset management					0
	A.8.1 Responsibility for asset				0
	A.8.1.1	Inventory of assets	0 - No existente	0	
	A.8.1.2	Ownership of assets	0 - No existente	0	
	A.8.1.3	Acceptable use of assets	0 - No existente	0	
	A.8.1.4	Return of assets	0 - No existente	0	
	A.8.2 Information classification				0
	A.8.2.1	Classification of information	0 - No existente	0	
	A.8.2.2	Labelling of informa tion	0 - No existente	0	
	A.8.2.3	Handling of assets	0 - No existente	0	
	A.8.3 Media handling				0
	A.8.3.1	Management of removable media	0 - No existente	0	
	A.8.3.2	Disposal of media	0 - No existente	0	
	A.8.3.3	Physical media transfer	0 - No existente	0	
A.9 Access control					3,525
	A.9.1 Business requirements of access control				4
	A.9.1.1	Access control policy	5 - Optimizado	5	
	A.9.1.2	Access to networks and network services	3 - Definido	3	
	A.9.2 User access management				4,5
	A.9.2.1	User registration and de-registration	5 - Optimizado	5	
	A.9.2.2	User access provisioning	4 - Gestionado	4	
	A.9.2.3	Management of privileged access rights	4 - Gestionado	4	
	A.9.2.4	Management of secret authentication information of use	4 - Gestionado	4	

50			A.9.2.5	Review of user access rights	5 - Optimizado	5
51			A.9.2.6	Removal or adjustment of access rights	5 - Optimizado	5
52		A.9.3 User responsibilities				4
53			A.9.3.1	Use of secret authentication information	4 - Gestionado	4
54		A.9.4 System and application access control				1,6
55			A.9.4.1	Information access restriction	4 - Gestionado	4
56			A.9.4.2	Secure log-on procedures	1 - Inicial	1
57			A.9.4.3	Password managment system	1 - Inicial	1
58			A.9.4.4	Use of privileged utility programs	1 - Inicial	1
59			A.9.4.5	Access control to program source code	1 - Inicial	1
60	A.10 Cryptography					
61		A.10.1 Cryptographic controls				4
62			A.10.1.1	Policy on the use of cryptographic controls	4 - Gestionado	4
63			A.10.1.2	Key management	4 - Gestionado	4
64	A.11 Physical and environmental security					0
65		A.11.1 Secure areas				0
66			A.11.1.1	Physical security perimeter	0 - No existente	0
67			A.11.1.2	Physical entry controls	0 - No existente	0
68			A.11.1.3	Securing offices, rooms and facilities	0 - No existente	0
69			A.11.1.4	Protecting against external and environmental threats	0 - No existente	0
70			A.11.1.5	Working in secure areas	0 - No existente	0
71			A.11.1.6	Delivery and loading areas	0 - No existente	0
72		A.11.2 Equipment				0
73			A.11.2.1	Equipment siting and protection	0 - No existente	0
			A.11.2.1	Equipment siting and protection	0 - No existente	0
			A.11.2.2	Supporting utilities	0 - No existente	0
			A.11.2.3	Cabling security	0 - No existente	0
			A.11.2.4	Equipment maintenance	0 - No existente	0
			A.11.2.5	Removal of assets	0 - No existente	0
			A.11.2.6	Security of equipment and assets off-premises	0 - No existente	0
			A.11.2.7	Secure disposal or reuse of equipment	0 - No existente	0
			A.11.2.8	Unattended user equipment	0 - No existente	0
			A.11.2.9	Clear desk and clear screen policy	0 - No existente	0
A.12 Operations security						2,142857143
	A.12.1 Operational procedures and responsibilities					5
			A.12.1.1	Documented operating procedures	5 - Optimizado	5
			A.12.1.2	Change management	5 - Optimizado	5
			A.12.1.3	Capacity management	5 - Optimizado	5
			A.12.1.4	Separation of development, testing and operational env	5 - Optimizado	5
	A.12.2 Protection from malware					0
			A.12.2.1	Controls against malware	0 - No existente	0
	A.12.3 Backup					5
			A.12.3.1	Information backup	5 - Optimizado	5
	A.12.4 Logging and monitoring					0
			A.12.4.1	Event logging	0 - No existente	0
			A.12.4.2	Protection of log information	0 - No existente	0
			A.12.4.3	Administrator and operator logs	0 - No existente	0
			A.12.4.4	Clock synchronisation	0 - No existente	0
	A.12.5 Control of operational software					4

	A.12.5 Control of operational software				4
		A.12.5.1	Installation of software on operational systems	4 - Gestionado	4	
	A.12.6 Technical vulnerability management				0
		A.12.6.1	Management of technical vulnerabilities	0 - No existente	0	
		A.12.6.2	Restrictions on software installation	0 - No existente	0	
	A.12.7 Information systems audit considerations				1
		A.12.7.1	Information systems audit controls	1 - Inicial	1	
A.13 Communications security					1,5
	A.13.1 Network security management				3
		A.13.1.1	Network controls	3 - Definido	3	
		A.13.1.2	Security of network services	3 - Definido	3	
		A.13.1.3	Segregation in networks	3 - Definido	3	
	A.13.2 Information transfe				0
		A.13.2.1	Information transfer policies and procedures	0 - No existente	0	
		A.13.2.2	Agreements on information transfer	0 - No existente	0	
		A.13.2.3	Electronic messaging	0 - No existente	0	
		A.13.2.4	Confidentiality or nondisclosure agreements	0 - No existente	0	
A.14 System acquisition, development and maintenance					0,888888867
	A.14.1 Security requirements of information systems				0
		A.14.1.1	Information security requirements analysis and specifica	0 - No existente	0	
		A.14.1.2	Securing application services on public networks	0 - No existente	0	
		A.14.1.3	Protecting application services transactions	0 - No existente	0	
	A.14.2 Security in development and support processes				2,6666666
		A.14.2.1	Secure development policy	2 - Repetible	2	
		A.14.2.2	System change control procedures.	4 - Gestionado	4	
		A.14.2.2	System change control procedures.	4 - Gestionado	4	
		A.14.2.3	Technical review of applications after operating platform	3 - Definido	3	
		A.14.2.4	Restrictions on changes to software packages	3 - Definido	3	
		A.14.2.5	Secure system engi neering principles	2 - Repetible	2	
		A.14.2.6	Secure development environment	3 - Definido	3	
		A.14.2.7	Outsourced development	1 - Inicial	1	
		A.14.2.8	System security testing	3 - Definido	3	
		A.14.2.9	System acceptance testing	3 - Definido	3	
	A.14.3 Test data				0
		A.14.3.1	Protection of test data	0 - No existente	0	
A.15 Supplier relationships					2,8333333
	A.15.1 Information security in supplier relationships				2,6666666
		A.15.1.1	Information security policy for supplier relationships	4 - Gestionado	4	
		A.15.1.2	Addressing security within supplier agreements	4 - Gestionado	4	
		A.15.1.3	Information and communication technology supply chain	0 - No existente	0	
	A.15.2 Supplier service delivery management				3
		A.15.2.1	Monitoring and review of supplier services	3 - Definido	3	
		A.15.2.2	Managing changes to supplier services	3 - Definido	3	
A.16 Information security incident management					3,14
	A.16.1 Management of information security incidents and improvement				3,14
		A.16.1.1	Responsibilities and procedures	3 - Definido	3	
		A.16.1.2	Reporting information security events	3 - Definido	3	
		A.16.1.3	Reporting information security weaknesses	3 - Definido	3	
		A.16.1.4	Assessment of and decision on information security ever	3 - Definido	3	
		A.16.1.5	Response to information security incidents	3 - Definido	3	

		A.16.1.5	Response to information security incidents	3 - Definido	3	
		A.16.1.6	Learning from information security incidents	3 - Definido	3	
		A.16.1.7	Collection of evidence	4 - Gestionado	4	
A.17 Information security aspects of business continuity management						2,5
	A.17.1 Information security continuity					4
		A.17.1.1	Planning information security continuity	4 - Gestionado	4	
		A.17.1.2	Implementing information security continuity	4 - Gestionado	4	
		A.17.1.3	Verify, review and evaluate information security continu	4 - Gestionado	4	
	A.17.2 Redundancies					1
		A.17.2.1	Availability of infor mation processing facilities	1 - Inicial	1	
A.18 Compliance						0,9666665
	A.18.1 Compliance with legal and contractual requirements					0,6
		A.18.1.1	Identification of applicable legislation and contractual re	0 - No existente	0	
		A.18.1.2	Illectual property rights	0 - No existente	0	
		A.18.1.3	Protection of records	2 - Repetible	2	
		A.18.1.4	Privacy and protection of personally identifiable informa	1 - Inicial	1	
		A.18.1.5	Regulation of cryptographic controls	0 - No existente	0	
	A.18.2 Information security reviews					1,333333
		A.18.2.1	Independent review of information security	1 - Inicial	1	
		A.18.2.2	Compliance with security policies and standards	2 - Repetible	2	
		A.18.2.3	Technical compliance review	1 - Inicial	1	

TABLA3: GAP 27002_2013.

Tabla resumen:

	Valor	Objetivo
A.5 Information security policies	4	5
A.6 Organization of information security	1	3
A.7 Human resource security	1,333333333	3
A.8 Asset management	0	3
A.9 Access control	3,525	4
A.10 Cryptography	0	4
A.11 Physical and environmental security	0	3
A.12 Operations security	2,142857143	3
A.13 Communications security	1,5	3
A.14 System acquisition, development and maintenance	0,888888867	3
A.15 Supplier relationships	2,8333333	3
A.16 Information security incident management	3,14	3
A.17 Information security aspects of business continuity management	2,5	3
A.18 Compliance	0,9666665	3

TABLA4: TABLA RESUMEN DE LOS ANÁLISIS ISO 27002/2013

Gráfico:

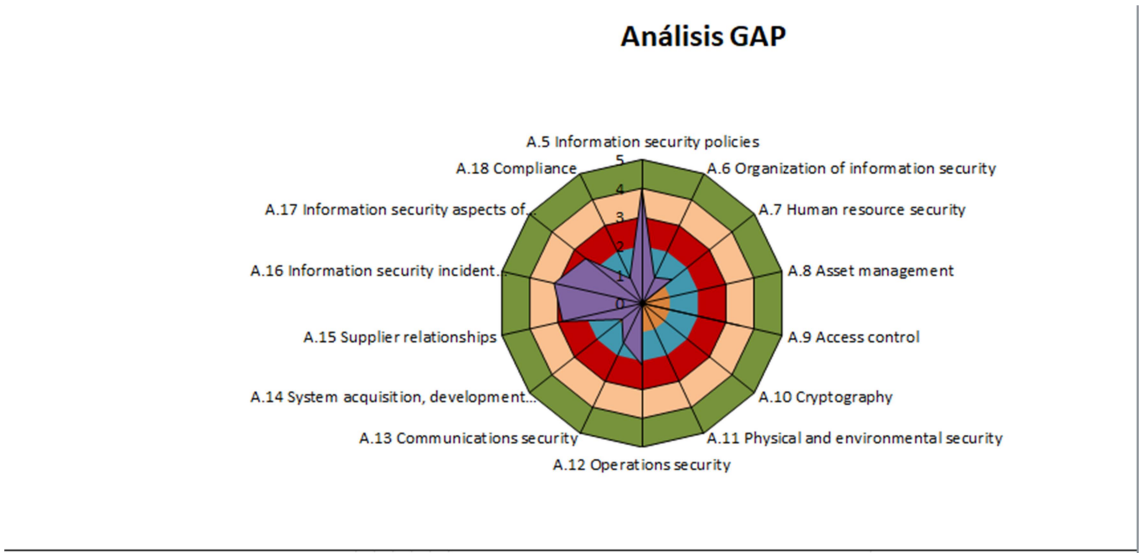

FIGURA7: GRÁFICO DEL ANÁLISIS GAP 27002/2013

Conclusiones: Se muestra el estado actual de los controles ISO 27002:2013 comparado con el estado óptimo.
La línea azul representa el estado actual del cumplimiento de los controles, la línea naranja un posible cumplimiento a medio o largo plazo y por último la línea verde representa un nivel de cumplimiento óptimo. Los números que se muestran en la gráfica hacen referencia a los diferentes dominios en la ISO 27002:2013.
Nuestro objetivo va a ser mejorar los valores de la empresa para llegar al menos al nivel Gestionado(4) o Definido (3) en todas las categorías.
Con relación a los controles del Anexo A de la ISO 27002:2013, se evidencia claramente que la organización de la seguridad de la información, la criptografía y la continuidad del negocio no son prioridad para la empresa. Con respecto a la seguridad ligada a los RRHH, se evidencia un desconocimiento de los procesos realizados por el departamento de RRHH.

2. SISTEMA DE GESTIÓN DOCUMENTAL

2.1. Política de Seguridad

2.1.1 Objeto y Alcance

El objetivo de este documento es establecer las directrices en seguridad de la información de la empresa TECNOSOFT. Todo el personal que trabaja en la organización debe conocer todas las normas indicadas en el presente documento y velar por su cumplimiento. Estas medidas serán de naturaleza organizativa, física y lógica, ya que la seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora que debe ser controlado y gestionado.
Por ello, esta política será de aplicación a todos los recursos y procesos de negocio corporativos.

2.1.2 Marco normativo

La presente política de seguridad se desarrolla en el marco normativo establecido por las siguientes leyes y normas:

- Normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013
- Reglamento Europeo de Protección de Datos Personales
- Real decreto 3/2010 del Esquema Nacional de Seguridad

2.1.3. Recursos

La preservación de la seguridad de la información será considerada objetivo común de todas las personas contratadas por TECNOSOFT, y serán las personas, junto con la tecnología y los procesos, el pilar fundamental para el mantenimiento de la seguridad de la información.
Aparte, la Dirección adquiere el compromiso de dotar a la función de seguridad con los roles necesarios para asegurar su buen hacer, eficiencia, y progresión respecto a la madurez en la implantación de las medidas de seguridad pertinentes.

2.1.4 Desarrollo

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

a) Políticas de seguridad de la información, constituido por el presente documento y el manual de seguridad.

b) Normativas de obligado cumplimiento, asociados a diferentes ámbitos normativos de ISO 27001, esquema de referencia del SGSI corporativo.

c) Procedimientos operativos, documentos que describen explícitamente y paso a paso como realizar una cierta actividad.

d) Instrucciones o procedimientos técnicos, propios del área de sistemas.

2.1.5. Software.

Todos los equipos deben de tener instalado el antivirus utilizado por TECNOSOFT y tenerlo habilitado en todo momento.
El antivirus deberá de estar siempre actualizando con la última versión disponible.

Está prohibida la instalación de software no aprobado por TECNOSOFT.

Ningún equipo podrá tener instalado software que no disponga de licencia.

Para la instalación de nuevo software o actualización del existente es necesario comunicarlo primero al técnico de cada grupo que debe aprobar dicha instalación.

2.1.6. Accesos físicos

1. El acceso físico de los trabajadores a las distintas oficinas de TECNOSOFT se permitirá a través de un sistema de tarjetas situado en las puertas que dan acceso los pasillos donde se encuentran las salas y despachos de los distintos grupos de trabajo.

2. El personal ajeno a la empresa que desee acceder a las instalaciones deberá rellenar sus datos en una lista de visitas al entrar a las instalaciones del grupo al que visita, siendo el técnico del grupo el responsable de dicha lista. El jefe del grupo será el responsable del visitante durante el tiempo que dure su estancia en TECNOSOFT. Al salir de las instalaciones, el visitante deberá firmar en la lista de visitas cómo que se marcha de las instalaciones.

3. El acceso a los despachos de los jefes de grupo y dirección se realizará utilizando una llave que sólo tendrán los que trabajen en cada uno de los despachos.

4. El acceso a las salas de los grupos de investigación se realizará utilizando una llave que poseerán todos los trabajadores de cada sala.

5. El acceso a los laboratorios de los grupos de investigación se realizará también utilizando una llave. Esta llave sólo la tendrán el jefe y el técnico de cada grupo.

6. Tanto el jefe como el técnico de cada grupo disponen de las llaves de todas las salas de su grupo. En caso de que ambos estén de vacaciones a la vez, se designará a una persona responsable de dichas llaves.

7. Los accesos a las salas de servidores. Sólo tendrán acceso a estas salas el responsable de seguridad, el técnico del centro y los técnicos de los grupos de investigación.

2.1.7. Equipos y hardware.

1. Cada trabajador es responsable de su equipo asignado y debe realizar un buen uso del mismo.
2. Todos los equipos deben estar protegidos por contraseña.
3. El equipo debe bloquearse cada vez que el trabajador se aleje de él.
4. Los sistemas de almacenamiento que se utilicen se extraerán siempre de manera segura.
5. Los ordenadores portátiles dispondrán de un sistema de seguridad para evitar que alguien se los pueda llevar.
6. Si algún trabajador necesita sacar algún equipo de TECNOSOFT de las instalaciones debe comunicárselo al técnico de su grupo junto a una justificación y éste lo debe aprobar.
7. El trabajador que saque equipos de las instalaciones de TECNOSOFT se hace responsable de lo que le suceda tanto al equipo como a la información que contenga dicho equipo.
8. Si se detecta algún comportamiento anómalo en algún equipo debe informarse de manera inmediata al técnico del grupo correspondiente.
9. Los dispositivos de almacenamiento que no se vayan a usar deberán ser entregados al técnico de cada grupo. Este decidirá si se reutiliza o se retira definitivamente. En cualquier caso, el técnico de grupo deberá realizar un formateo completo del dispositivo

2.1.8. Acceso a internet.

1. Los trabajadores deben realizar un uso responsable de este recurso.

2. Está prohibido visitar páginas web con contenido ilícito.

3. Está prohibido el acceso, uso o instalación de servicios de mensajería instantánea que no sean los empleados por TECNOSOFT.

4. Está prohibida la descarga, uso o instalación de cualquier programa de descarga o intercambio P2P de música, películas, etc., así como juegos o software no aprobado por el equipo técnico de TECNOSOFT.

2.1.9. Correo electrónico

1. Todo el personal de TECNOSOFT dispone de una dirección de correo electrónica de la organización.

2. La cuenta de correo electrónico sólo podrá ser utilizada para temas relacionados con el trabajo que desempeñan en TECNOSOFT.

3. No está permitido utilizar el correo electrónico de la empresa como correo electrónico personal.

4. No está permitido realizar SPAM con el correo electrónico de TECNOSOFT.

5. Si se recibe un correo electrónico sospechoso debe seguirse el procedimiento definido por TECNOSOFT para comprobar si el correo es seguro o no.

2.1.10. Software

1. Todos los equipos deben de tener instalado el antivirus utilizado por TECNOSOFT y tenerlo habilitado en todo momento. El antivirus deberá de estar siempre actualizando con la última versión disponible.

2. Está prohibida la instalación de software no aprobado por TECNOSOFT.

3. Ningún equipo podrá tener instalado software que no disponga de licencia.

4. Para la instalación de nuevo software o actualización del existente es necesario comunicarlo primero al técnico de cada grupo que debe aprobar dicha instalación.

2.1.11. Copias de seguridad.

1. Se deberán realizar copias de seguridad diarias de todos los servidores de TECNOSOFT. Los técnicos son los responsables de que las copias de los servidores que tienen a su cargo se realicen correctamente.
2. Los trabajadores deberán realizar copias de seguridad de sus equipos regularmente.
3. Las copias de seguridad se almacenarán en un edificio diferente al que alberga las oficinas de TECNOSOFT.

2.1.12. Información.

1. No está permitido sacar fuera de las instalaciones de TECNOSOFT información restringida o confidencial sin haber obtenido un permiso previamente.
2. Los trabajadores deben mantener su puesto de trabajo limpio de información restringida o confidencial.
3. Los trabajadores deben recoger los documentos impresos de las impresoras en el momento de mandarlos a imprimir.
4. Los documentos con información restringida o confidencial no se tirarán en la papelera ordinaria sino que se utilizará el destructor de papeles situado en las oficinas de los grupos de investigación.

5. Está prohibido el uso de información confidencial para autenticarse en cualquiera de los sistemas de la organización.

2.1.13. Contraseñas.

1. Las contraseñas que se utilicen en TECNOSOFT deben de tener entre 8 y 15 caracteres entre los que tienen que haber mayúsculas, minúsculas, números y símbolos.

2. Las contraseñas se cambiarán cada 3 meses y no se podrá utilizar como nueva contraseña ninguna de las tres últimas utilizadas.

3. Ningún trabajador puede comunicar a otro la contraseña de acceso a su equipo ni debe tenerla apuntada en ningún papel al alcance de la vista de otros.

2.2. Auditorías internas.

Se define el procedimiento mediante el cual TECNOSOFT planificará, ejecutará y cerrará debidamente documentadas las auditorías internas al SGSI según normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

a) La periodicidad de la auditoría interna será de carácter anual, realizándose durante el primer semestre del año. Dejando así el segundo semestre para la realización de la auditoría externa. Y permitiendo así la corrección de las no conformidades encontradas durante la auditoría interna.

b) Dada la carga de trabajo que implicaría hacer una revisión total del sistema cada año, se ha diseñado un Programa de Auditoría basado en ciclos de 2 años. De esta manera, se revisa una parte del sistema cada año, completando un ciclo completo al segundo año.

c) El equipo auditor estará formado por la Dirección de Seguridad. Recayendo el liderazgo sobre la figura del CISO. Se requerirá la colaboración de las distintas áreas de la compañía en función del proceso/sistema auditado, siendo imprescindible la colaboración del Área de Sistemas dependiente de la Dirección de IT.

d) Las auditorías internas serán lideradas por el CISO, cuenta con una dilatada experiencia profesional como auditor jefe en la norma ISO/IEC 27001. Ha participado en múltiples auditorías internas y cuenta con las siguientes certificaciones.

a. Certificado de Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001.

b. Certificado del Curso Auditor Interno de Seguridad de la Información ISO 27001.

Los requisitos mínimos que deben cumplir los miembros del equipo auditor son los siguientes:

- Ser independiente de la organización.
- Capacidad de comunicación.
- Conocimientos de informática y/o telecomunicaciones.
- Conocer tanto la norma ISO 27001:2013 como la ISO 27002:2013.
- Experiencia en la realización auditorías de seguridad de la información.
- Capacidad para elaborar informes.

2.2.1. Fases.

Las auditorías internas constarán de tres fases:

Preparación de la auditoría

Se trata de la fase inicial de la auditoría y en ella se llevará a cabo una primera reunión entre el auditor jefe y el director general y el responsable de seguridad de TECNOSOFT para establecer de una manera clara cuales son los objetivos de la auditoría que se va a realizar y lo que se espera de ésta.
Tras la primera reunión se determinarán los procedimientos de comunicación entre el equipo auditor y los responsables de TECNOSOFT.

Se realizará a continuación el inventariado de las políticas de empresa que afecten a la auditoría y que serán comprobadas.
Por último, se definirán las pruebas que se van a realizar durante la auditoría.

Ejecución de la auditoría
En esta fase el equipo auditor llevará a cabo las diferentes tareas para la correcta realización de la auditoría interna.
Estas tareas serán:

1. Recolección de la información necesaria:

- Documentación de la empresa con información sobre los requisitos del negocio.
- Leyes y regulaciones.
- Política de seguridad.
- Documentación con los controles de seguridad implantados.

2. Ejecución de pruebas:

- Se buscarán fallos en la documentación de la empresa.
- Se realizarán entrevistas con los trabajadores.
- Se ejecutarán las pruebas técnicas que se consideren oportunas.

3. Elaboración del informe de auditoría.

Reporting de la auditoría

En esta fase el auditor jefe comunicará a TECNOSOFT el informe de auditoría con los resultados y conclusiones obtenidas tras haber realizado todas las pruebas pertinentes.

2.2.2. Informe de auditoría.

En esta sección del informe se consigna lo siguiente:

- una breve caracterización de la organización auditada referida a las principales actividades que desarrolla y otros aspectos que puedan resultar de interés;
- los objetivos de la Auditoría, así como las causas de incumplimiento de alguno de los objetivos previstos;
- el alcance debe expresar la profundidad y cobertura del trabajo que se haya realizado para cumplir los objetivos;
- la declaración en el informe de que la Auditoría se realizó de conformidad con estas normas; si es necesario modificar esa declaración cuando no se haya cumplido con las normas que sean de aplicación, el auditor interno debe modificar la declaración para manifestar una salvedad, e incluir en el alcance las causas del incumplimiento de forma clara, concisa y comprensible; y
- las limitaciones en el alcance pueden estar relacionadas, entre otras, con situaciones como las siguientes:

  - imposibilidad de aplicar determinado procedimiento previsto en el programa de trabajo diseñado, que se considere necesario o deseable;
  - inadecuados registros primarios de la información;

- La metodología debe explicar claramente los programas de trabajo diseñados, las técnicas que se han empleado para efectuar los análisis requeridos y obtener la evidencia necesaria para cumplir con los objetivos de la Auditoría; y el informe se dirige al máximo nivel de dirección al que está subordinado el auditor interno.
- Conclusiones

  En esta sección se deben tener en cuenta los criterios generales siguientes:

  - las conclusiones son deducciones lógicas basadas en los hallazgos de los auditores; la fuerza de las conclusiones de los auditores depende de lo persuasivo de la evidencia de los hallazgos y lo convincente de la lógica usada para formular dichas conclusiones;

- no deben constituir la repetición de lo consignado en la sección Resultados del propio informe, sino una síntesis de los hechos y situaciones fundamentales comprobadas; cuidando de incluir un hecho o hallazgo que no haya sido reflejado en otra sección del informe;
- debe reflejarse, de forma general, las causas fundamentales que originaron el error, irregularidad o fraude planteado, así como las consecuencias directas e indirectas que pudieran derivarse de estos hallazgos; y
- se expone la calificación otorgada de acuerdo con los resultados del servicio de Auditoría ejecutado.

- Grado de adecuación del SGSI con la norma ISO 27002:2013.
- No conformidades detectadas.
- Recomendaciones de mejora.

La empresa deberá de realizar una serie de auditorías internas que permitan revisar en el tiempo, la mejora continua y posteriores certificaciones. En tal sentido, se efectuará al menos una auditoría anual completa, para la revisión de los controles previstos en la ISO/IEC 27002:2013:

Control	Fecha de Realización (mes)											
	1	2	3	4	5	6	7	8	9	10	11	12
5. Políticas de seguridad		X										
6. Aspectos organizativos de la seguridad de la información		X										
7. Seguridad ligada a los recursos humanos		X										
8. Gestión de activos				X								
9. Control de accesos				X								
10. Cifrado				X								
11. Seguridad física y ambiental						X						
12. Seguridad en las operaciones						X						
13. Seguridad en las telecomunicaciones						X						
14. Adquisición, desarrollo y mantenimiento de los sistemas de información								X				
15. Relaciones con suministradores								X				
16. Gestión de incidentes en la seguridad de la información								X				
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio											X	
18. Cumplimiento											X	

TABLA 5: CONTROLES DE AUDITORÍA POR MES.

Es decir, la auditoría se realizará cada año, dividida en secciones que se realizarán trimestralmente según la siguiente planificación:

Primer Trimestre:
- Auditoría de las Políticas de Seguridad.
- Auditoría de la Organización de la Seguridad de la Información.
- Auditoría de la Seguridad relacionada con RRHH.

Segundo Trimestre:
- Auditoría de la Gestión de Activos.
- Auditoría de Control de los accesos.

- Auditoría del Cifrado.
- Auditoría de la Seguridad Física y Ambiental.
- Auditoría de la Seguridad de la Operativa.
- Auditoría de la Seguridad de las Comunicaciones.

Tercer Trimestre:

- Auditoría de la gestión y Mantenimiento de los SI.
- Relaciones con proveedores.
- Auditoría de la gestión de incidentes de la seguridad de la información.

Cuarto Trimestre:

- Auditoría de seguridad de la información en gestión de la continuidad del negocio.
- Auditoría del Cumplimiento.

En el ANEXO III tenemos un ejemplo de Informe de Auditoría

2.2.3 Hallazgos en la auditoría interna

Como resultado de la auditoría, poder distinguir entre:

- No conformidad: pueden ser conformidades mayores (incumplimiento de requisitos de la norma ISO/IEC 27001:2013 que impedirían la certificación de SGSI de no ser resueltas) o no conformidades leves. Ambas se resuelven mediante acciones correctivas.
- Posibles no conformidades: indican el riesgo de un potencial incumplimiento. Se resuelven mediante acciones preventivas.
- Mejoras: para aquellos aspectos que no suponen incumplimiento, el auditor fijará un criterio mínimo aconsejable de nivel de cumplimiento y las acciones de mejora recomendadas para alcanzar dicho nivel.

Ejemplos de algunas No Conformidades Mayores serían:

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
7	Soporte		
7.5	Información documentada	No Conformidad mayor	No está cumplimentada toda la información requerida. Requerimientos legales y contractuales y algunos procedimientos operacionales
8	Operación		
8.1.	Planificación y control operacional	No Conformidad mayor	No se planifican y controlan acciones para el tratamiento de riesgos.
8.3	Tratamiento de los riesgos de seguridad de la información	No Conformidad mayor	No hay evidencia de información documentada de los resultados de tratamiento de los riesgos residuales.
9	Evaluación del desempeño		

9.1.	Seguimiento, medición, análisis y evaluación	No Conformidad mayor	No están documentadas evidencias de seguimiento medición, análisis y evaluación del desempeño del sistema de gestión.

TABLA 6: NO CONFORMIDADES MAYORES.

Ejemplos de algunas No Conformidades Menores serían

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
4	Contexto de la organización		
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	No Conformidad menor	No está cumplimentados todos os requisitos legales y contractuales
6	Planificación		
6.1.	Acciones para tratar los riesgos y oportunidades	No Conformidad menor	No están documentados los criterios para llevar a cabo apreciaciones de riesgo
7	Soporte		
7.2	Competencia	No Conformidad menor	No están documentadas las evidencias de competencia.
8	Operación		
8.2	Apreciación de riesgos de seguridad de la información	No Conformidad menor	No hay evidencias de los resultados de apreciación de riesgo

TABLA 7: NO CONFORMIDADES MENORES.

2.3. Gestión de indicadores.

En la siguiente tabla se especifican los distintos indicadores que se tendrán en cuenta para para medir la eficacia de los controles de seguridad implantados. En la tabla se pueden encontrar los siguientes datos:

- Código identificativo del control.
- Nombre identificativo.
- Dominio de pertenencia.
- Descripción de la métrica.

- Periodicidad de aplicación.
- Objetivo fijado para valorar positivamente su cumplimiento.
- Responsable de su cumplimiento.

ID	NOMBRE	DOMINIO	METRICA	PERIODICIDAD	UMBRAL	RESPONSABLE
SEG1	Política de seguridad	Verificar que se realiza la revisión de las políticas de seguridad por parte de la Dirección	A.5.1.1	Anual	2-1	Comité de Seguridad
SEG2	Roles	Verificar si los roles y responsabilidades en cuanto a seguridad de la información están definidos.	A.6.1.1.	Anual	100-90	Comité de Seguridad
SEG3	Móviles	cumplimiento de las políticas respecto a los dispositivos móviles	A.6.2.1	Semestral	0-15	CISO
SEG4	Formación	Trabajadores que han recibido formación específica en materia de seguridad de la información	A.7.2.2	Anual	70-80	Comité de Seguridad
SEG5	Activos inventariados	Inventariado de activos	A.8.1.1	Semestral	80-90	CISO
SEG6	Control accesos red	Medida de la cantidad de accesos no autorizados a la red de la organización	A.9.1.2	Mensual	100-90	CISO
SEG7	Derechos de acceso de usuario	Medida de la eficacia del proceso de otorgar/quitar los permisos a los usuarios	A.9.2.1, A.9.2.2, A.9.2.5, A.9.2.6	Mensual	100-90	CISO
SEG8	Controles criptográficos.	Medida de la eficacia de la política de encriptación de datos sensibles	A.10.1.1	Semestral	100-90	CISO

SEG9	Control accesos oficinas	Medida de la eficacia de las medidas de seguridad físicas	A.11.1.2, A.11.1.3, A.11.1.6	Semanal	100-90	CISO
SEG10	Revisión antiincendios.	Verificar que se realizan las revisiones a los sistemas contra incendios	A.11.1.4	Anual	90-80	CISO
SEG11	Fallas de energía	Medida de la eficacia de los equipos UPS de la organización	A.11.2.2	Semestral	100-90	CISO
SEG12	Cableado	Medida de la seguridad del cableado de la organización	A.11.2.3	Semestral	100-90	CISO
SEG13	Copias de seguridad de los equipos de trabajo.	Medida de la eficacia de las copias de seguridad de los equipos de los trabajadores	A.12.3.1	Trimestral	90-80	Técnicos
SEG14	Copias de seguridad servidores	Medida de la eficacia de las copias de seguridad de los servidores	A.12.3.1	Trimestral	100-90	CISO
SEG15	Antivirus	Medida de la cantidad de equipos que no disponen de antivirus instalados	A.12.2.1	Mensual	100-90	CISO
SEG16	Licencias de software	Medida de la cantidad de software con licencia instalado en los equipos de trabajo	A.12.5.1, A.18.1.2	Semestral	90-80	CISO
SEG17	Comunicaciones externas	Verificar el correcto cumplimiento de las políticas de intercambio de información con el exterior	A.13.2.2, A.13.2.3	Anual	100-90	CISO

TABLA8 : INDICADORES DE LOS CONTROLES DE MEDIDAS DE SEGURIDAD.

2.4. Procedimiento de Revisión por la Dirección.

La revisión del Sistema de Gestión de Seguridad de la Información es una tarea necesaria de cara a asegurarse de su conveniencia, adecuación y eficacia. Esta es una labor que ha de realizar la dirección de la compañía en colaboración con el Comité de Seguridad.
Esta labor se ha de hacer con una periodicidad anual y ha de reflejar la evolución que ha tenido el Sistema durante este último año. De la misma manera que se realiza un Análisis Diferencial en el proceso de elaboración del SGSI, anualmente se tiene que conocer cuál es el estado con respecto a la revisión anterior. De esta manera, el informe deberá contener los siguientes aspectos:

- Estado de las acciones tomadas en la revisión anterior y su evolución.
- Cambios producidos en la organización que puedan afectar al SGSI. Por ejemplo, la existencia de nuevos procesos de negocio o activos.
- Informes relativos a las no conformidades que hubieran podido producir, acciones correctivas, indicadores relativos al cumplimiento con el sistema, resultado de auditorías internas/externas y cumplimiento con los objetivos de seguridad fijados.
- Apreciaciones del Comité de Seguridad.
- Evolución del plan de tratamiento de riesgos
- Oportunidades de mejora.

Al tratarse de un proceso de revisión cíclico, el informe de revisión contará con un apartado de conclusiones -principalmente cambios producidos en el SGSI o bien oportunidades de mejora- que serán objeto de seguimiento en futuras revisión.
Así mismo se almacenará una copia firmada por la dirección y el resto de los miembros del Comité de Seguridad como evidencia de esta revisión ante futuras auditorías.

2.5. Gestión de Roles y Responsabilidades.

2.5.1.2 técnicos de Desarrollo, junto con el técnico de sistemas formarán el Comité de Seguridad de la Información

- Implantar las directrices del Comité de Dirección.
- Desarrollo de algunos objetivos de control del SGSI
- Asignar roles y funciones en materia de seguridad.
- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).
- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.
- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

2.5.2. *El técnico de sistemas será Responsable de Sistemas de Seguridad de la Información CISO, y como tal sus responsabilidades serán:*

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

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

• Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el área de Organización/RR. HH., en el cual se recogerá quién asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.

• Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.
• Desarrollo de algunos objetivos de control del SGSI
• Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.

• Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección. Elevar el mapa de riesgos y el Plan de seguridad de la información al CSI

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

• Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando. Una vez aprobado dicho plan y el presupuesto por el CSI, el RSI deberá gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.

• Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.

• Velar por el cumplimiento legal (LOPD, RD 3/2010 Esquema Nacional de Seguridad, Basilea, SOX...), coordinando las actuaciones necesarias con las unidades responsables.

• Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al CSI si corresponde.

• Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.

• Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al CSI si corresponde.

• Desarrollo de algunos objetivos de control del SGSI.

• Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El RSI debe analizar y mantener actualizado dicho cuadro de mando, presentándolo al CSI con la periodicidad que se establezca.

2.5.3. *Técnicos de grupo*

Los técnicos de grupo tienen las siguientes responsabilidades en materia de seguridad:

- Notificar al técnico del centro de investigación de los incidentes de seguridad detectados en el grupo de investigación.
- Administrar los equipos del grupo.

- Realizar el mantenimiento de los equipos del grupo.
- Dar permisos de acceso a los miembros del grupo a equipos, red, etc.
- Controlar el cumplimiento de las normas definidas en la política de seguridad dentro de su grupo.
- Revisar la correcta realización de las copias de seguridad de los servidores del grupo.
- Autorizar y controlar el acceso al laboratorio del grupo.
- Apuntar y supervisar los accesos a las instalaciones de personal ajeno a la empresa

2.5.4. Personal en general

El personal de TECNOSOFT tiene las siguientes obligaciones y responsabilidades:

- Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la empresa.
- Mantener la confidencialidad de la información.
- Hacer un buen uso de los activos de la organización.
- Respetar la legislación y regulación vigentes.
- Notificar al técnico de grupo correspondiente las anomalías o incidentes de seguridad así como las situaciones sospechosas.

2.6. Declaración de aplicabilidad.

Se recoge la relación de controles de la ISO/IEC 27002:2013 y se especifica, para cada uno de ellos, si se va a aplicar o no al SGSI de TECNOSOFT. Además, se detalla la descripción de cómo se implementa en caso de que se vaya a aplicar.

Sección	CONTROLES	APLICA	JUSTIFICACION
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	SI	Se debe definir un conjunto de políticas de seguridad de la información que sean aprobadas por la dirección y comunicadas a todos los trabajadores
A5.1.2	Revisión de las políticas para la seguridad de la información	SI	La política de seguridad deben ser revisadas periódicamente o cuando ocurran cambios significativos.
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	SI	Se deben asignar los distintos roles y responsabilidades en cuanto a seguridad de la información. La Dirección tiene que comprometerse con la implementación del SGSI y velar por el cumplimiento de las políticas.
A6.1.2	Segregación de tareas	SI	Las tareas están definidas, pero no están claramente asignadas al personal involucrado en el SGSI Según las responsabilidades que se les han asignado. Tampoco se realiza ningún tipo de seguimiento
A6.1.3	Contacto con las autoridades	SI	Se deben mantener los contactos apropiados con las autoridades pertinentes. La Dirección debe revisar las claúsulas que tienen desarrolladas en la actualidad para ver si cumplen lo establecido.
A6.1.4	Contacto con grupos de interés especial	SI	Se debe mantener contacto con asociaciones o grupos especializados en seguridad.

A6.1.5	Seguridad de la información en la gestión de proyectos	SI	No existe documentación oficial relativa a estableer unos requisitos de seguridad en las nuevas iniciativas y proyectos que surgen en la organización. La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	SI	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
A6.2.2	Teletrabajo	SI	Se deben implementar medidas de seguridad para proteger la información tratada en los lugares desde los que se teletrabaja.
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	SI	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos. RRHH suele verificar la veracidad de los datos.
A7.1.2	Términos y condiciones del empleo	SI	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	SI	La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	Todos los empleados de la organización deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.
A7.2.3	Proceso disciplinario	SI	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	SI	Se deben definir las responsabilidades y deberes que tienen los empleados al cambiar de contrato o terminar con él.
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	SI	Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. Se debe revisar que todos los activos que entran dentro del alcance del SGSI estén inventariados.
A8.1.2	Propiedad de los activos	SI	Todo activo del inventario debe tener un propietario que será el responsable de dicho activo.
A8.1.3	Uso aceptable de los activos	SI	Se deben definir las reglas de uso de los activos. Se debería de comunicar por email esta política para que llegue a todos

A8.1.4	Devolución de activos	SI	Todos los empleados deben devolver los activos que tengan a su cargo al terminar el contrato con la organización.
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	SI	La información debe ser clasificada en base a los requisitos legales, valor, criticidad, susceptibilidad a divulgación o modificación no autorizada.
A8.2.2	Etiquetado de la información	SI	Se debe definir el procedimiento para el etiquetado de la información.
A8.2.3	Manipulado de la información	SI	Se deben definir el procedimiento para el manejo de activos.
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	SI	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A8.3.2	Eliminación de soportes	SI	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A8.3.3	Soportes físicos en tránsito	SI	Se deben definir el procedimiento para la gestión de soportes extraíbles.
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	SI	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
A9.1.2	Acceso a las redes y a los servicios de red	SI	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	SI	Se debe implementar un proceso de altas y bajas en el registro de usuarios.
A9.2.2	Provisión de acceso de usuario	SI	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A9.2.3	Gestión de privilegios de acceso	SI	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A9.2.5	Revisión de los derechos de acceso de usuario	SI	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A9.2.6	Retirada o reasignación de los derechos de acceso	SI	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	SI	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	SI	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A9.4.2	Procedimientos seguros de inicio de sesión	SI	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A9.4.3	Sistema de gestión de contraseñas	SI	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A9.4.4	Uso de utilidades con privilegios del sistema	SI	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A9.4.5	Control de acceso al código fuente de los programas	SI	Se debe restringir el acceso al código fuente de los programas.
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	SI	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
A10.1.2	Gestión de claves	SI	Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	SI	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
A11.1.2	Controles físicos de entrada	SI	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A11.1.3	Seguridad de oficinas, despachos y recursos	SI	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A11.1.4	Protección contra las amenazas externas y ambientales	SI	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A11.1.5	El trabajo en áreas seguras	SI	Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
A11.1.6	Áreas de carga y descarga	SI	Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	SI	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.
A11.2.2	Instalaciones de suministro	SI	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
A11.2.3	Seguridad del cableado	SI	El cableado de potencia y el de telecomunicaciones debe estar protegido para evitar ser interceptado o dañado.

A11.2.4	Mantenimiento de los equipos	SI	Los equipos deben de ser mantenidos correctamente para asegurar siempre su integridad y disponibilidad.
A11.2.5	Retirada de materiales propiedad de la empresa	SI	Se debe definir un procedimiento para sacar los activos fuera de la empresa.
A11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
A11.2.7	Reutilización o eliminación segura de equipos	SI	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
A11.2.8	Equipo de usuario desatendido	SI	Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	SI	Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
A12.1.2	Gestión de cambios	SI	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.
A12.1.3	Gestión de capacidades	SI	Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	SI	Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	SI	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	SI	Se deben hacer copias de seguridad de la información y del software realizado y ponerlas a prueba regularmente.
A12.4	**Registros y supervisión**		

A12.4.1	Registro de eventos	SI	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
A12.4.2	Protección de la información del registro	SI	Se deben proteger las instalaciones e información de registro contra la alteración y el acceso no autorizado.
A12.4.3	Registros de administración y operación	SI	Se deben registrar las actividades del administrador del sistema así como proteger y revisar regularmente dichos registros.
A12.4.4	Sincronización del reloj	SI	Todos los relojes de la organización deben de estar sincronizados.
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	SI	Se deben establecer procedimientos para controlar la instalación de software en los sistemas operativos.
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	SI	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A12.6.2	Restricción en la instalación de software	SI	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

A12.7	**Consideraciones sobre la auditoría de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	SI	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	SI	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A13.1.2	Seguridad de los servicios de red	SI	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A13.1.3	Segregación en redes	SI	Los distintos grupos dentro de la organización deben separarse en redes.
A13.2	**Intercambio de información**		

A13.2.1	Políticas y procedimientos de intercambio de información	SI	Se deben definir políticas para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A13.2.2	Acuerdos de intercambio de información	SI	Los acuerdos deben tener en cuenta la transferencia segura de la información entre la empresa y las partes externas.
A13.2.3	Mensajería electrónica	SI	Se debe proteger adecuadamente la información incluida en mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o no revelación	SI	Se deben identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad que reflejen las necesidades de la organización para la protección de la información.

A14	[illegible]		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	Se deben incluir 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.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI	La información que pasa por redes públicas debe protegerse de actividades fraudulentas, modificación no autorizada, divulgación, etc.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	Se debe proteger la información en las transacciones de los servicios de las aplicaciones para evitar alteración, divulgación, modificación no autorizada, etc.
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	SI	Se deben establecer reglas para el desarrollo de software que se realiza en la empresa.
A14.2.2	Procedimiento de control de cambios en sistemas	SI	Los cambios a los sistemas se deben controlar mediante procedimientos de control de cambios.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	Se deben revisar las aplicaciones críticas cuando se cambian las plataformas de operación y ponerlas a prueba para asegurar que no hay impacto adverso.
A14.2.4	Restricciones a los cambios en los paquetes de software	SI	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.
A14.2.5	Principios de ingeniería de sistemas seguros	SI	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
A14.2.6	Entorno de desarrollo seguro	SI	Se debe establecer un ambiente de desarrollo seguro.
A14.2.7	Externalización del desarrollo de software	SI	Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.
A14.2.8	Pruebas funcionales de seguridad de sistemas	SI	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
A14.2.9	Pruebas de aceptación de sistemas	SI	Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	SI	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.Datos pseudomizados.
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.

A15.1.2	Requisitos de seguridad en contratos con terceros	SI	• Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor		Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	SI	• I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora
A16.1.2	Notificación de los eventos de seguridad de la información	SI	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A16.1.3	Notificación de puntos débiles de la seguridad	SI	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI	Se deben evaluar los eventos de seguridad de la información y decidir si se van a clasificar como incidentes de seguridad de la información.

A16.1.5	Respuesta a incidentes de seguridad de la información	SI	Se debe dar respuesta a los incidentes de seguridad de acuerdo a los procedimientos establecidos.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A16.1.7	Recopilación de evidencias	SI	La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.
A17			
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Se deben determinar los requisitos de seguridad de la información y la continuidad de la gestión de ésta en situaciones adversas.
A17.1.2	Implementar la continuidad de la seguridad de la información		La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión
A17.1.3		SI	Se deben verificar periódicamente los controles de continuidad de seguridad implementados.
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A18	**Cumplimiento**		
A18.1			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	SI	Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
A18.1.3	Protección de los registros de la organización	SI	Los registros deben protegerse contra pérdida, destrucción, acceso no autorizado, falsificación y liberación no autorizada de acuerdo con los requisitos legislativos.
A18.1.4	Protección y privacidad de la información de carácter personal	SI	Se debe asegurar la privacidad y protección de la información de carácter personal de acuerdo a como dicta la ley.
A18.1.5	Regulación de los controles criptográficos	SI	Se deben usar controles criptográficos de acuerdo a la legislación pertinente
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	SI	La seguridad de la información de la organización debe revisarse de manera independiente periódicamente o cuando ocurran cambios significativos
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	La Dirección debe revisar regularmente el cumplimiento del procesamiento y procedimientos de información.
A18.2.3	Comprobación del cumplimiento técnico	SI	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

TABLA 9: APLICABILIDAD DE LOS CONTROLES DE LA ISO/IEC 27002:2013

2.7. Metodología gestión de riesgos.

La metodología de análisis de riesgos elegida por la empresa es MAGERIT que tiene como característica fundamental que los riesgos que se plantean para una organización se expresan directamente en valores económicos, lo que ayudará a la toma de decisiones por parte de la Dirección de la empresa.

MAGERIT

Esta metodología fue elaborada por el MAP (Ministerio de Administraciones Públicas) con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos. Con posterioridad ha sido aplicable a cualquier organización. Esta metodología puede ser aplicada a cualquier organización, independientemente de que se encuentre en el Estado español o en otro país. Al mismo tiempo, esta metodología ha desarrollado una herramienta que ayuda a su aplicación. Como soporte a esta metodología, existen las herramientas de entorno de análisis de riesgos (EAR), que soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (metodología de análisis y gestión de riesgos de los sistemas de información) y está desarrollada y financiada parcialmente por el CCN. Esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente, lo que una ventaja y un inconveniente:

• El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Esto hace que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

• Por el contrario, el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

Fases de MAGERIT:

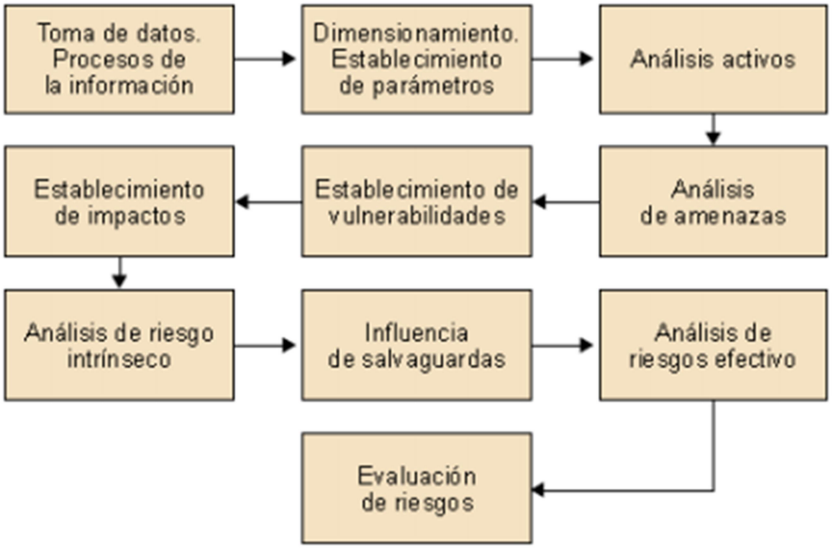

FIGURA8: PROCESOS MAGERIT **[10]**

1. **Toma de datos y procesos de información** En esta primera fase –la más importante de toda la metodología–, debe definirse el alcance que se ha de estudiar o analizar, ya que, dependiendo de éste, será más o menos costoso el proceso. A mayor alcance, mayor es el número de riesgos analizables.

2. **Establecimiento de parámetros** La segunda fase es la más importante en la metodología MAGERIT. Consiste en el establecimiento de parámetros que se utilizarán durante todo el proceso de análisis de riesgos.
Los parámetros que deben identificarse son los siguientes:
• Valor de los activos
• Vulnerabilidad
• Impacto
• Efectividad del control de seguridad.

3. **Análisis de activos** Esta fase del estudio consiste en identificar cuáles son los activos que posee la organización y que necesita para llevar a cabo sus actividades. En esta fase es muy importante haber dejado claramente identificado el alcance del análisis de riesgos, puesto que solamente se deberían analizar aquellos activos que estén dentro de dicho alcance.
Cuando se habla de activos analizables hay que pensar en los siguientes tipos de activos:
• Activos físicos.
• Activos lógicos.
• Activos de personal.
• Activos de entorno infraestructura.
• Activo intangibles.

4. **Análisis de amenazas**. Hay que tener presente que las amenazas dependen mucho de la organización, así como de las características de ésta, en el sentido de que hay que analizar las amenazas que afectarían a los activos que posee una organización en concreto.

5. **Establecimiento de las vulnerabilidades**. Por vulnerabilidades se entienden aquellos agujeros que tenemos en nuestra seguridad y que permiten que una amenaza pueda dañar un activo. Es importante tener claro que, sin vulnerabilidad, la amenaza no puede dañar nuestros activos y también que las vulnerabilidades por sí mismas no provocan daños, sino que éstos son siempre provocados por las amenazas.
6. **Valoración de impactos**. A la hora de analizar los impactos deberían tenerse en consideración los siguientes aspectos:
• El resultado de la agresión de una amenaza sobre un activo
• El efecto sobre cada activo para poder agrupar los impactos en cadena según la relación de activos.

7. **Análisis de riesgos intrínseco**. Para este estudio, únicamente es necesario realizar una multiplicación de los valores que hemos indicado hasta ahora:
Riesgo = Valor del activo × Vulnerabilidad × Impacto.

8. **Influencia de las salvaguardas**. Una vez que tenemos identificados los riesgos actuales a los que se encuentra expuesta la organización, se entra en la fase de gestión de riesgos, que consiste en tratar de escoger la mejor solución de seguridad que me permita reducirlos. Para ello existen dos tipos fundamentales de controles de seguridad o salvaguardas:
• Preventivas. Son aquellas medidas de seguridad que reducen las vulnerabilidades
• Correctivas. Son aquellas medidas de seguridad que reducen el impacto de las amenazas.

9. **Análisis de riesgos efectivos** Será el resultado de estudiar cómo se reducirían los riesgos con cada una de las medidas de protección (controles o salvaguardas) que hemos identificado; es decir, se debería calcular el riesgo definitivo, dándose como resultado el riesgo efectivo que tendría la organización para cada una de las amenazas identificadas.

10. **Gestión de riesgos** Esta última fase consiste en la toma de decisiones por parte de la organización sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquélla. Recordemos que, a la hora de gestionar los riesgos en una organización, existen tres decisiones que pueden tomarse:
• Reducirlos
• Transferirlos
• Aceptarlos.

FIGURA9 PROCESO DE GESTIÓN DE RIESGOS. [12]

Este análisis permite identificar y analizar cada uno de los procesos del negocio y determinar los riesgos a los que están expuestos cada uno de ellos, a su vez se consiguen identificar amenazas y vulnerabilidades.

MAGERIT es una metodología elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la precepción de que la Administración toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.
La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o os servicios que se prestan gracias a ella son valiosos, MAGERIT permite saber cuánto valor está en juego y ayudará a protegerlo.
Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.
MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Previamente para poder llevar a cabo el análisis del riesgo es imprescindible hacer previamente un inventario de todos los activos (todos aquellos que su pérdida, daño o modificación pueda afectar al negocio), relacionados con las IS/IT.

A la hora de gestionar riesgos debe elaborarse un plan de acción.
Establecimiento del contexto El análisis de riesgos se realiza en el marco de la gestión integral del riesgo institucional. En el ámbito del SGSI el alcance del análisis de riesgos es el del SGSI, es decir, un conjunto de activos de información, que asisten a los procesos institucionales, que constituyen el alcance del SGSI. En este proceso, el riesgo se determina en forma cualitativa, a partir de la Probabilidad, de que se materialice una amenaza, por el Impacto, que ocasione en la institución, a través de los procesos que asiste. La valoración de los dos factores se realiza con base en escalas (alta, media, baja, muy naja y raro). El riesgo resultante se clasifica en 4 niveles, (desastres naturales, de origen industrial, errores y fallos no intencionados, ataques intencionados). Los activos con riesgo extremo e intolerable deben ser llevados por lo menos al nivel tolerable, y aquellos activos críticos con nivel de riesgo tolerable deben ser llevados al nivel aceptable.

Identificación de riesgos Comprende la identificación de los riesgos de los activos de información, por lo que demanda del inventario de estos activos incluyendo su valor, determinado a partir de sus tres dimensiones de seguridad (Disponibilidad, Integridad y Confidencialidad) como mínimo.

Probabilidad		
Valor	Grado	Descripción
1	Raro	Puede ocurrir una vez cada 2 años
2	Muy baja	Al año
3	Baja	En 6 meses
4	Media	Al mes
5	Alta	A la semana

FIGURA10: CUADRO DE PROBABILIDADES DE INCIDENTES.

Impacto		
Valor	*Nivel*	*Descripción*
1	Insignificante	Impacta levemente en la operatividad del proceso
2	Menor	Impacta en la operatividad del proceso
3	Moderado	Impacta en la operatividad del macro proceso
5	Mayor	Impacta en la operatividad de los procesos
8	Desastroso	Impacta fuertemente en la operatividad de los procesos

FIGURA11: IMPACTO DE LOS INCIDENTES EN LA ORGANIZACIÓN.

Aceptación/Tolerancia		
Valor	*Nivel*	*Descripción*
1	Aceptable	Retenido
2	Tolerable	Para activos no críticos, pero intolerable para críticos
3	Intolerable	Atención inmediata y monitoreo permanente.
4	Extremo	Tratado como intolerable, pero a nivel de Gerencia General.

FIGURA12: NIVELES DE RIESGO Y SU DESCRIPCIÓN

Categorías de Activos de Información		
Identificador	*Categoría*	*Ejemplos*
STI	Servicios TI	Aplicación + infraestructura TI de soporte.
SW	Software / Aplicaciones	Aplicaciones, sistemas operativos, herramientas de desarrollo y utilitarios
HW	Hardware / equipos	Servidores (S.O.), PCs, routers, hubs, firewalls, medio magnético, gabinetes, cajas fuertes, salas, mobiliario, sistema de alarma, etc.
SI	Soportes de información	SAN, discos, cintas, USB, CD, DVD.
COM	Redes de comunicaciones	Medios de transporte que llevan datos de un sitio a otro
DAT	Datos / Información	BD, archivos de datos, contratos y acuerdos, documentación del sistema, información de investigación, manuales de usuario, material de entrenamiento, de operación, procedimientos de soporte, planes de continuidad y contingencia, acuerdos
AUX	Equipamiento auxiliar	Equipamiento de soporte a los sistemas de información (UPS, Generados, Aire acondicionado, cableado, etc.)
INS	Locales / Instalaciones	Lugares donde se hospedan los sistemas de Información, registros vitales y comunicaciones
PER	Personal / RR.HH.	Personas, calificaciones, experiencia y capacidades (usuarios, proveedores, personal de TI)
SRV	Servicios generales	Vigilancia, servicios de impresión, computación, telecomunicaciones, eléctrica, agua, etc.

TABLA10: TIPOS DE CATEGORÍAS DE ACTIVOS PRESENTES EN LA ORGANIZACIÓN.[10]

Los activos están expuestos a amenazas, que pueden materializarse (explotando vulnerabilidades) con determinada frecuencia o probabilidad, dependiendo de la eficacia de los controles o salvaguardas vigentes. Para la determinación de riesgos, este proceso utiliza el catálogo de amenazas de MAGERIT, y las vulnerabilidades y controles identificados por los administradores de activos, con base en su experiencia e información de los fabricantes. Las amenazas están organizadas en las categorías consignadas en la tabla siguiente, y pueden afectar a más de un tipo de activo.

Categorías de Amenazas	
Identificador	*Tipo*
N	Desastres naturales
I	De origen industrial
E	Errores y fallos no intencionados
A	Ataques intencionados

TABLA 11: DISTINTAS CATEGORÍAS DE AMENAZAS A NUESTRA ORGANIZACIÓN.

Áreas de Impacto										
N°	Áreas							Peso Relativo		
1	Objetivo Estratégicos / Funciones							30%		
2	Financiero							20%		
3	Objetivo y Metas del Proceso u otros Procesos Vinculados							10%		
4	Reputación / Imagen / Credibilidad							30%		
5	Situación y Bienestar del Personal							10%		
	1	2	3	4	5	6	7	8	9	10
RTO	**TR**	**10'**	**30'**	**1 h**	**2 h**	**4 h**	**8 h**	**2 d**	**5 d**	**15 d**
Impacto										

TABLA 12: IMPACTO DE LAS AMENAZAS SOBRE PROCESOS DE LA ORGANIZACIÓN

3. ANÁLISIS DE RIESGOS

3.1 Introducción.

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Permite determinar cómo es, cuánto vale y cómo de protegido se encuentra un sistema, siguiendo los objetivos, estrategia y política de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la Dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.
El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente. El análisis cualitativo es recomendable hacerlo en primer lugar, utiliza una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; y la probabilidad de que se produzcan estas consecuencias.
Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos, aquellos sujetos a un riesgo máximo.

El análisis cuantitativo es más detallado y utiliza una escala con valores numéricos para las consecuencias y probabilidad, permitiendo:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora de seguridad.

3.2. Inventario de activos.

El primer paso para realizar un análisis de riesgos es la identificación de los activos que están dentro del alcance del SGSI de la organización y que son necesarios para llevar a cabo sus actividades.

De acuerdo con la metodología MAGERIT clasificaremos los activos en diferentes ámbitos:

- Instalaciones [L]: Lugares donde se hospedan los sistemas de información y comunicaciones.
- Hardware [HW]: Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
- Aplicación [SW]: Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
- Información/Datos [D]: La información que permite a la organización prestar sus servicios.
- Red [COM]: Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
- Servicios [S]: Servicios prestados por el sistema.
- Equipamiento auxiliar [AUX]: Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con éstos.
- Personal [P]: Personas relacionadas con los sistemas de información.

AMBITO	CODIGO	ACTIVO	PROPIETARIO
HW	HW1	Equipos de comunicaciones	Técnico de sistemas
	HW2	Robot de cintas	CISO
	HW3	PC del puesto usuario	Empleado propietario
	HW4	Servidores del CPD principal	CISO
	HW5	Servidores CPD externalizado.	CISO
	HW6	Portátiles	Empleado propietario
	HW7	Teléfonos VOIP y centralita	CISO
	HW8	Routers	CISO
	HW9	Switches	CISO
	HW10	Impresoras en red	CISO
Instalaciones [L]	L1	Centro de datos	CISO
	L2	CPD externo	CISO
	L3	Cuarto de racks	CISO
	L4	Oficinas	Director
	L5	Despachos	Director
[SW]	SW1	Windows server	CISO
	SW2	Servidores de B.D mySQL	CISO
	/3	Microsoft Office	CISO
	SW4	Antivirus	CISO
	SW5	Aplicaciones internas	Técnicos de desarrollo
	SW6	Página web de la empresa	Técnicos de desarrollo
	SW7	Correo electrónico	CISO

	SW8	Software de Nóminas	Técnicos de desarrollo
	SW9	Repositorio de código	Técnicos de desarrollo
Información [D]	D1	Base de datos de proveedores	CISO
	D2	Base de datos de clientes	CISO
	D3	Base de datos con información de datos de configuración	CISO
	D4	Copias de seguridad de servidores	CISO
Comunicación[COM]	COM1	Cableado eléctrico	CISO
	COM2	Cableado de telecomunicaciones	CISO
	COM3	Servicio VOIP	CISO
	COM4	Servicio Internet	CISO
	COM5	Red inalámbrica	SO
SERVICIOS [S]	S1	Correo electrónico	CISO
	S2	Acceso remoto	CISO
	S3	Página web	CISO
AUX	AUX1	Sistema de climatización	CISO
	AUX2	Sistema de detección incendios	CISO
	AUX3	Sistema de alimentación ininterrumpido SAI	CISO
	AUX4	Extintores	CISO
	AUX5	Terminales móviles	CISO
Personal [P]	P1	Director General	Dirección General
	P2	Director Financiero	Dirección General

	P3	Responsable de RRHH	Dirección General
	P4	Técnicos de Desarrollo	Dirección General
	P5	Técnico de Sistemas	Dirección General
	P6	Personal de limpieza	Dirección General
	P7	Personal de seguridad	Dirección General

TABLA 13: TABLA DEL LISTADO DE LOS ACTIVOS.

Equipamiento - Hardware

• Equipos de comunicaciones.- Se consideran todos los equipos que conforman la red de voz y datos ubicados en el centro de datos que son administrados por personal de infraestructura.
• Robot de cintas.- Equipo físico que realiza los respaldos en cinta de la información de los servidores ubicado en el centro de datos y es administrado por el personal de infraestructura.
• Computador de personal.- Equipo de computación que utiliza el personal para trabajar.
• CPD-Principal-Servidores(Windows server 2008, y máquinas VMware).- Se consideran todos los equipos físicos de tipo torre y rack que alojan algún programa o aplicación, se encuentran dentro del centro de datos y son administrados por el personal de infraestructura y sistemas.
• CPD-externalizado-Servidores.- Se consideran todos los equipos físicos de tipo torre y rack que alojan algún programa o aplicación, se encuentran fuera de la organización en una empresa externa subcontratada, y son administrados por personal externo de infraestructura y sistemas, con la supervisión del personal del CPD principal.
- Impresoras de red.
- Portátiles.

Equipamiento - Software

• Sistemas académicos, financieros y administrativos.- Se consideran a los sistemas prioritarios para la administración de la organización que son gestionados por los desarrolladores.
• Almacenamiento – bases de datos.- Se considera a la información almacenada y respaldada originada de los datos de los servicios prestados, esto es administrado por administrador de bases de datos. Servidores de B.D mySQL. También se consideran a las cintas magnéticas que almacenan la información respaldada.
• Correo electrónico.- se considera al sistema de correo electrónico.
• Virtualización.- se considera al servicio que permite el funcionamiento de los servidores virtuales.

- Microsoft Office
- Antivirus
- Microsoft Windows Server

Comunicaciones.

• Internet.- Se considera al servicio y demás elementos necesarios para lograr el acceso hacia el Internet.
• Red alámbrica.- se considera a las conexiones alámbricas ya sean de fibra óptica o cable UTP.
• Red inalámbrica.- se considera a la señal de red emitida por los puntos de acceso.
• Enlace con proveedor.- se considera al servicio y equipos que conlleva la comunicación exitosa con el proveedor de Internet.

Equipamiento Auxiliar.

• UPS.- se consideran a las baterías que protegen a los servidores y equipos de comunicación de fallos eléctricos.
• Generador eléctrico.- se considera al dispositivo que genera energía eléctrica cuando no hay servicio eléctrico.
• Equipos de climatización.- se consideran a los elementos que mantienen la temperatura adecuada en el centro de datos y cuartos de rack.
• Cableado eléctrico.- se considera a la red eléctrica existente entre el centro de datos, cuarto de rack y cuarto del generador eléctrico.

- Extintores
- Terminales móviles.

Instalaciones.

- Centro de datos.- es el lugar donde se concentran todos los servidores y equipos de comunicación.
- Sistemas de almacenamiento externo.
- Cuarto de rack.- o cuarto de telecomunicaciones, están ubicados en los diferentes edificios de la organización y es donde se encuentran los equipos de comunicación que tienen un enlace directo con el centro de datos.

Despachos.

Personal.

- Equipo de desarrollo.- se considera al personal encargado de desarrollar las aplicaciones o sistemas.
- Equipo técnico.- se considera al personal encargado de dar asesoría técnica.
- Administradores.- se consideran a los jefes de cada área.
- Personal de Seguridad física subcontratada.
- Servicio subcontratado de limpieza.

3.3 Valoración de los activos.

Una vez hemos identificado los activos, tenemos en cuenta las dependencias que existen entre ellos. De forma que un riesgo alto en los niveles inferiores implicará un riesgo alto en los niveles superiores.
En primer lugar se van a analizar las dependencias entre activos. Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior, es decir, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

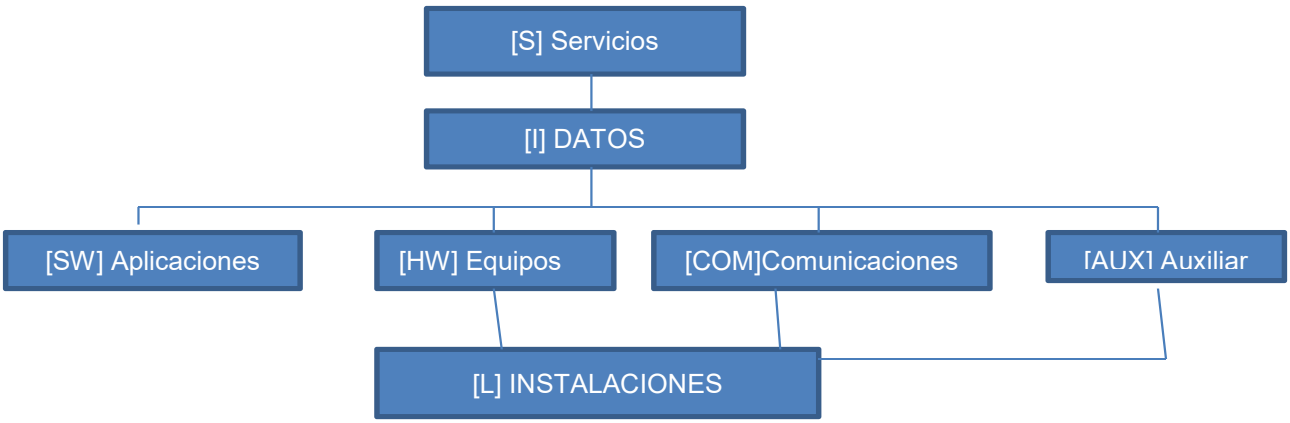

FIGURA13: ESQUEMA DE LA RELACIÓN DE LOS TIPOS DE ACTIVOS.

A continuación se va a realizar la valoración de cada uno de los activos inventariados. A la hora de asignar un valor a cada activo se van a tener en cuenta las siguientes consideraciones:

El valor de reposición del activo en caso de que éste se pierda o no pueda ser utilizado.

El tiempo que se necesita desde que se adquiere el nuevo activo hasta que se pone a punto para que pueda utilizarse.

El valor que pierde la organización durante el tiempo en el que no se puede utilizar el activo.

El valor que pierde potencialmente la organización por no poder disponer del activo durante un tiempo.

En la Tabla 12 se muestra la escala de la valoración de activos que se va a utilizar.
Más abajo en la tabla 13, se usará este valor de los activos.

Valoración de los activos		
Valor	Niveles	Rango en euros
MA	Muy Alto	350.000 - 100.000
A	Alto	100.000 – 50.000
M	Medio	50.000 – 10.000
B	Bajo	10.000 - 1000
MB	Muy Bajo	1000 - 0

TABLA 14: ESCALA DE VALORACIÓN DE ACTIVOS.

Este procedimiento de valoración de activos va a permitir realizar la asignación de un valor tanto cualitativo como cuantitativo a cada uno de los activos identificados.

3.3. Dimensiones de seguridad.

La valoración de los activos, esta se realiza en base a la valoración que da la organización a cada uno de sus Sistemas de Información en relación a las dimensiones de seguridad (Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad). A continuación, se describe cada una de las dimensiones:

Autenticidad [A]: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

Confidencialidad [C]: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Integridad [I]: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que los datos fueran modificados fuera de control?

Disponibilidad [D]: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría el activo si no estuviera disponible?

Trazabilidad [T]: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

Para valorar los activos en las dimensiones anteriores usaremos la ANTERIOR tabla de valoración.

3.4. Tabla resumen de valoración.

Se han especifican los valores de cada uno de los activos de la empresa tanto de manera general como respecto a las cinco dimensiones de la seguridad de la información.

AMBITO	CODIGO	ACTIVO	VALORACION	VALOR	DIMENSION SEGURIDAD				
					C	I	D	A	T
HW	HW1	Equipos de comunicaciones	B	10000	6	3	8		
	HW2	Robot de cintas							
	HW3	PC del puesto usuario	B	10000	8	4	2		
	HW4	Servidores del CPD principal	M	50000	3	6	6		
	HW5	Servidores CPD externalizado.	M	50000	3	6	6		
	HW6	Portátiles	B	10000	8	5	3		
	HW7	Teléfonos VOIP y centralita	B	10000	6	3	8		
	HW8	Routers	MB	1000	3	2	7		
	HW9	Switches	MB	1000	6	5	6		
	HW10	Impresoras en red	MB	500	3	2	3		

Instalaciones [L]	L1	Centro de datos	M	50000	6	5	9		
	L2	CPD externo							
	L3	Cuarto de racks	MB	1000	4	3	5		
	L4	Oficinas	MA	350000	6	5	9		
	L5	Despachos	MA	100000	6	5	9		
[SW]	SW1	Windows server	MB	1000	3	5	5		
	SW2	Servidores de B.D mySQL	MB	500	3	5	5		
	SW3	Microsoft Office	MB	1000	3	5	5		
	SW4	Antivirus	MB	1000	3	5	7		
	SW5	Aplicaciones internas	M	50000	6	8	9		
	SW6	Página web de la empresa	M	50000	8	9	9		
	SW7	Correo electrónico	M	50000	3	6	6		
	SW8	Software de Nóminas	M	50000	6	7	8		
	SW9	Repositorio de código	MB	1000	2	4	4		
Información [D]	D1	Base de datos de proveedores	MA	100000	8	9	7	8	8
	D2	Base de datos de clientes	MA	350000	9	9	9	9	9
	D3	Base de datos con información de datos de configuración	MA	100000	6	7	6	8	8
	D4	Copias de seguridad de servidores	MA	100000	6	8	7	7	7
Comunicación[COM]	COM1	Cableado eléctrico	B	10000	6	0	8		
	COM2	Cableado de telecomunicaciones	M	50000	8	5	9		
	COM3	Servicio VOIP	B	10000	6	0	8		
	COM4	Servicio	M	50000	8	5	9		

		Internet							
	COM5	Red inalámbrica	M	50000	8	5	9		
SERVICIOS [S]	S1	Correo electrónico	M	50000	8	9	8		
	S2	Acceso remoto	MB	1000	8	8	7	8	7
AUX	AUX1	Sistema de climatización	B	10000	0	0	8		
	AUX2	Sistema de detección incendios	A	10000	0	0	9		
	AUX3	Sistema de alimentación ininterrumpido SAI	A	10000	0	0	9		
	AUX4	Extintores	A	1000	0	0	9		
	AUX5	Terminales móviles	MB	1000	8	7	6	7	6
Personal [P]	P1	Director General	MA	350000			9		
	P2	Director Financiero	MA	200000			9		
	P3	Responsable de RRHH	MA	200000			9		
	P4	Técnicos de Desarrollo	A	100000			9		
	P5	Técnico de Sistemas	A	100000			9		
	P6	Personal de limpieza	M	50000			7		
	P7	Personal de seguridad	M	50000			8		

TABLA 15: TABLA DE VALORES DE LOS ACTIVOS.

3.5. Análisis de amenazas.

Todos los activos de una organización están expuestos a diversas amenazas que pueden afectar a los distintos aspectos de la seguridad de la empresa. Por este motivo en este apartados se van a analizar qué amenazas pueden afectar a qué activos de TECNOSOFT. Posteriormente, se va a estimar cuán vulnerable es cada uno de los activos a la materialización de la amenaza así como la estimación de la frecuencia de la misma.

Se va a utilizar la metodología MAGERIT para realizar este análisis de amenazas. Las amenazas están clasificadas en los siguientes grupos:

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

Desastres naturales[N]	N1	Fuego
	N2	Inundaciones
	N3	Tormentas
	N4	Terremotos
Accidentes industriales[I]	I1	Incendio
	I2	Fuga de agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación electromagnética
	I7	Contaminación industrial
	I8	Avería
	I9	Corte suministro eléctrico
	I10	Humedades
	I11	Fallo del servicio comunicaciones
	I12	Degradación soportes.
	I13	Emanaciones electromagnéticas.
Errores y fallos no intencionados[E]	E1	Errores de los técnicos
	E2	Errores de configuración
	E3	Deficiencias de organización
	E4	Difusión de software dañino
	E5	Fugas de información
	E6	Errores de mantenimiento software
	E7	Errores de mantenimiento hardware
	E8	Caída del sistema
	E9	Pérdida de equipos
	E10	Personal no disponible
	E11	Vulnerabilidades del software
	E12	Destrucción de la información
	E13	Alteración accidental de la información
	E14	Errores de secuencia
	E15	Errores de reencaminamiento

Ataques intencionados [A]	A1	Manipulación de los registros de actividad
	A2	Manipulación de configuración
	A3	Suplantación de identidad
	A4	Abuso de privilegios de acceso
	A5	Difusión de software dañino
	A6	Reencaminamiento de mensajes
	A7	Alteración de la secuencia
	A8	Acceso no autorizado
	A9	Análisis de tráfico
	A10	Repudio
	A11	Interceptación de la información
	A12	Modificación de la información
	A13	Divulgación errónea de la información
	A14	Manipulación del software
	A15	Manipulación de equipos
	A16	Destrucción de la información
	A17	Denegación de servicio
	A18	Robo
	A19	Extorsión
	A20	Ingeniería social

TABLA 16: TABLA DE LAS DIFERENTES AMENAZAS.

La frecuencia la calcularemos según la siguiente tabla:

Vulnerabilidad	ID	Rango	Valor
Frecuencia muy alta	MA	1 vez al día	1
Frecuencia alta	A	1 vez a la semana	0.5
Frecuencia media	M	1 vez al mes	0.1
Frecuencia baja	B	1 vez cada 6 meses	0.02
Frecuencia muy baja	MB	1 vez al año	0.005

TABLA 17: TABLA DE FRECUENCIA DE AMENAZAS.

La valoración del impacto de la amenaza sobre la seguridad de un activo la calcularemos teniendo en cuenta la siguiente tabla:

Impacto	ID	Valor
Muy alto	MA	100%
Alto	A	75%
Medio	M	50%
Bajo	B	20%
Muy bajo	MB	5%

TABLA 18: TABLA DE VALORACIÓN DE IMPACTO DE AMENAZA EN SEGURIDAD.

El análisis de las amenazas que afectan a cada uno de los activos de TECNOSOFT, detallando en ella la frecuencia de ocurrencia de cada amenaza sobre cada activo y el impacto que tendría la ocurrencia de cada una de las amenazas sobre cada una de las cinco dimensiones de seguridad de cada activo.

Tipo	Amenaza	Activo	Frec	Valor	A	C	I	D	T
Desastres naturales	Incendio [N1]	Instalaciones [I]	MB	0.005				100	
		Hardware[HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Cableado telecomunicaciones[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	
	Inundación [N2]	Instalaciones[I]	MB	0.005				75	
		Hardware[HW]	MB	0.005				75	
		Equipamiento auxiliar[AUX]	MB	0.005				75	
	Tormenta eléctrica [N3]	Hardware [HW]	MB	0.005				75	
		Cableado eléctrico[COM]	MB	0.005				50	
		Equipamiento auxiliar[AUX]	MB	0.005				50	
	Terremoto [N4]	Hardware [HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	
Origen industrial [I]	Incendio [I1]	Hardware [HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	
		Instalaciones[I]	MB	0.005				100	
		Cableado telecomunicaciones[COM]	MB	0.005				100	
	Inundación[I2]	Hardware [HW]	MB	0.005				75	
		Instalaciones[I]	MB	0.005				75	
		Equipamiento auxiliar[AUX]	MB	0.005				75	
	Sobrecarga eléctrica	Hardware [HW]	MB	0.005				75	
	[I3]	Cableado[COM]	MB	0.005				50	
		Equipamiento auxiliar[AUX]	MB	0.005				50	
	Explosión [I4]	Hardware [HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	
		Instalaciones	MB	0.005				100	
		Cableado teleco[COM]	MB	0.005				100	
	Derrumbe[I5]	Hardware [HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				50	
		Equipamiento auxiliar[AUX]	MB	0.005				50	
		Instalaciones	MB	0.005				80	
		Cableado teleco[COM]	MB	0.005				50	
	Contaminación electromagnética[I6]	Hardware[HW]	MB	0.005				75	
		Equipamiento auxiliar[AUX]	MB	0.005				75	

	Contaminación industrial [I7]	Hardware[HW]	MB	0.005				50	
		Equipamiento auxiliar[AUX]	MB	0.005				50	
	Avería [I8]	Instalaciones	B	0.02				50	
		Hardware[HW]	B	0.02				50	
		Software[SW]	B	0.02				50	
		Equipamiento auxiliar[AUX]	B	0.02				20	
		Servicios[S]	B	0.02				50	
	Corte suministro eléctrico [I9]	Hardware[HW]	B	0.02				50	
		Equipamiento auxiliar[AUX]	B	0.02				5	
	Humedades [I10]	Hardware[HW]	B	0.02				50	
		Equipamiento auxiliar[AUX]	B	0.02				5	
		Servicios[S]	B	0.02				5	
	Fallo servicio comunicaciones [I11]	VOIP [COM]	M	0.1				100	
		Internet [COM]	M	0.1				100	
		Red inalámbrica [COM]	M	0.1				100	
		Correo electrónico [S]	M	0.1				100	
	Degradación de soportes [I12]	Servidor repositorio de código [HW]	MB	0.005				75	
		Servidor de copias de seguridad [HW]	MB	0.005				75	
	Emanaciones electromagnéticas [I13]	Instalaciones [I]	MB	0.005		20			
		Hardware[HW]	MB	0.005		50			
Errores y fallos no intencionados	Errores de los técnicos [E1]	Instalaciones [I]	B	0.02		20	20	50	
		Hardware[HW]	B	0.02		20	50	10	
		Software [SW]	B	0.02		50	75	50	
		Servicios[S]	B	0.02		50	75	50	
		Equipamiento auxiliar[AUX]	B	0.02		20	20	50	
		Datos[D]	B	0.02		75	75	50	
Errores y fallos no intencionados	Errores de configuración [E2]	Software [SW]	B	0.02				50	
		Datos[D]	B	0.02				50	
	Deficiencias de organización[E3]	Personal[P]	M	0.1				75	
		Instalaciones	M	0.1				75	
		Datos[D]	M	0.1				75	
	Difusión de software dañino [E4]	Software [SW]	MB	0.005			50	75	75
		Datos[D]	MB	0.005			50	50	50
	Fugas de información [E5]	Instalaciones	B	0.02		25			
		Datos[D]	B	0.02		25			
		Software [SW]	B	0.02		100			
		Servicios [S]	B	0.02		25			
	Errores de mantenimiento de software[E6]	Software [SW]	B	0.02			50	75	

	Errores de mantenimiento de hardware[E7]	Hardware[HW]	B	0.02				75	
	Caída del sistema [E8]	VOIP [COM]	B	0.02				100	
		Internet[COM]	B	0.02				100	
		Red [COM] inalámbrica	B	0.02				100	
		Servicios[S]	B	0.02				100	
	Perdida de equipos [E9]	Hardware[HW]	B	0.02				100	
		Equipamiento auxiliar[AUX]	B	0.02				100	
	Personal no disponible [E10]	Personal[P]	A	0.5				100	
	Vulnerabilidades del software [E11]	Software[SW]	M	0.1		75	25	75	
		Datos[D]	M	0.1		75	25	75	
	Destrucción de la información [E12]	Datos[D]	B	0.02				100	
	Alteración accidental de la información[E13]	Datos[D]	M	0.1			80		
	Errores de secuencia[E14]	VOIP [COM]	MB	0.005		50			
		Internet[COM]	MB	0.005		50			
		Red [COM] inalámbrica	MB	0.005		50			
		Servicios[S]	MB	0.005		50			
	Errores de encaminamiento[E15]	VOIP [COM]	MB	0.005		50			
		Internet[COM]	MB	0.005		50			
		Red [COM] inalámbrica	MB	0.005		50			
		Servicios[S]	MB	0.005		50			
Ataques intencionados [A]	Manipulación de los registros de actividad[A1]	Datos[D]	MB	0.005					75
	Manipulación de configuración[A2]	Datos[D]	MB	0.005	80	80	80		
	Suplantación de identidad[A3]	VOIP[COM]	B	0.02	80	80	50		
		Software[SW]	B	0.02	100	80	50		
		Datos[D]	B	0.02	100	80	50		
		Red inalámbrica[COM]	B	0.02	80	80	50		
	Abuso de privilegios de acceso[A4]	Instalaciones[I]	B	0.02		80	50	50	
		Hardware [HW]	B	0.02		80	50	50	
		Equipamiento auxiliar [AUX]	B	0.02		80	50	50	

	Datos[D]	B	0.02		100	50	50	
	Software[SW]	B	0.02		100	50	50	
	Servicios [S]	B	0.02		80	50	50	
Difusión de software dañino[A5]	Software[SW]	MB	0.005		80	80	80	
Reencaminamiento de mensajes[A6]	Servicios	MB	0.005		50			
	Red inalámbrica[COM]	MB	0.005		50			
	VOIP [COM]	MB	0.005		50			
	Internet[COM]	MB	0.005		50			
Alteración de la secuencia[A7]	Servicios	MB	0.005				50	
	Red inalámbrica[COM]	MB	0.005				50	
	VOIP [COM]	MB	0.005				50	
	Internet[COM]	MB	0.005				50	
Acceso no autorizado[A8]	Instalaciones [I]	B	0.02		50		10	
	Hardware[HW]	B	0.02		50		10	
	Equipamiento auxiliar [AUX]	B	0.02		50		10	
	Software[SW]	B	0.02		80		80	
	Red[COM]	B	0.02		80		80	
	Servicios[S]	B	0.02		80		80	
	Datos[D]	B	0.02		100		80	
Análisis de tráfico[A9]	Datos[D]	MB	0.005		50			
Repudio[A10]	Servicios[S]	MB	0.005					80
Interceptación de la información[A11]	Datos[D]	B	0.02		100			

	Modificación de la información[A12]	Instalaciones[I]	MB	0.005			50		
		Datos[D]	MB	0.005			100		
		Servicios[S]	MB	0.005			50		
		Software[SW]	MB	0.005			80		
	Divulgación errónea de la información[A13]	Personal[P]	M	0.1		25			
		Datos[D]	M	0.1		100			
	Manipulación del software[A14]	Software[SW]	MB	0.005			80	80	
	Manipulación de equipos[A15]	Hardware[HW]	MB	0.005		50		50	
		Equipamiento auxiliar[AUX]	MB	0.005		50		50	
		Software[SW]	MB	0.005		50		50	
	Destrucción de la información[A16]	Datos[D]	MB	0.005				100	
		Software[SW]	MB	0.005				100	
	Denegación de servicio [A17]	Software[SW]	B	0.02				100	
		VOIP[COM]	B	0.02				100	
		Internet[COM]	B	0.02				100	
		Red inalámbrica[COM]	B	0.02				100	
		Servicios[S]	B	0.02		25		100	
	Robo[A18]	Hardware[HW]	MB	0.005		80		100	
		Equipamiento auxiliar[AUX]	MB	0.005		25		100	
		Datos[D]	MB	0.005		100		100	
		Red[COM]	MB	0.005		60		100	
		Servicios[S]	MB	0.005		25		100	
	Extorsión[A19]	Personal[P]	MB	0.005		25	25	25	
	Ingeniería social[A20]	Personal[P]	MB	0.005		25	25	25	

TABLA 19: TABLA DE VALORACIÓN DE IMPACTO DE AMENAZA EN ACTIVOS Y FRECUENCIA.

Si hacemos un estudio de los datos obtenidos en la tabla, vemos que para todos los Activos el impacto más alto de todas las Amenazas es sobre la Disponibilidad, seguido por la Confidencialidad, a continuación la Integridad, Accesibilidad y por último la Trazabilidad.

3.7. Impacto potencial.

El impacto potencial permitirá a la organización priorizar el plan de acción y, a su vez, evaluar cómo se verá modificado este valor una vez se apliquen las contramedidas oportunas.

El impacto potencial se calcula siguiendo la siguiente fórmula:

Impacto potencial = Valor del activo * Valor del impacto de la amenaza.

Aplicando esta fórmula a los datos que ya tenemos de las tablas anteriores. Cogemos como valor de impacto el más alto de la tabla anterior.

COD	ACTIVO	VALORACION					IMPACTO					Impacto potencial				
		C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
HW1	Equipos de comunicaciones	6	3	8			75	50	100			4.5	1.5	8		
HW2	Robot de cintas	6	3	8			75	50	100			4.5	1.5	8		
HW3	PC del puesto usuario	8	4	2			75	50	100			6	2	2		
HW4	Servidores del CPD principal	3	6	6			75	50	100			2.25	3	6		
HW5	Servidores CPD externalizado.	3	6	6			75	50	100			2.25	3	6		
HW6	Portátiles	8	5	3			75	50	100			6	2.5	3		
HW7	Teléfonos VOIP y centralita	6	3	8			75	50	100			4.5	1.5	8		
HW8	Routers	3	2	7			75	50	100			2.25	1	7		
HW9	Switches	6	5	6			75	50	100			4.5	2.5	6		
HW10	Impresoras en red	3	2	3			75	50	100			2.25	1	3		
L1	Centro de datos	6	5	9			75	50	100			4.5	2.5	9		
L2	CPD externo	6	5	9			75	50	100			4.5	2.5	9		
L3	Cuarto de racks	4	3	5			75	50	100			4.5	1.5	5		
L4	Oficinas	6	5	9			75	50	100			4.5	2.5	9		
L5	Despachos	6	5	9			75	50	100			4.5	2.5	9		
SW1	Windows server	3	5	5			100	75	100	75		3	3.75	5		
SW2	S. O. Ubuntu	3	5	5			100	75	100	75		3	3.75	5		
SW3	Microsoft Office	3	5	5			100	75	100	75		3	3.75	5		
SW4	Antivirus	3	5	7			100	75	100	75		3	3.75	7		

D3	Base de datos con información de datos de configuración	6	7	6	8	8	100	100	100	100	75	6	7	6	8	6
D4	Copias de seguridad de servidores	6	8	7	7	7	100	100	100	100	75	6	8	7	7	5.25
COM1	Cableado eléctrico	6	0	8			75	50	100	75		4.5	0	8		
COM2	Cableado de telecomunicaciones	8	5	9			75	50	100	75		6	2.5	9		
COM3	Servicio VOIP	6	0	8			75	50	100	75		4.5	0	8		
COM4	Servicio Internet	8	5	9			75	50	100	75		6	2.5	9		
COM5	Red inalámbrica	8	5	9			75	50	100	75		6	2.5	9		
S1	Correo electrónico	8	9	8			75	50	100	75	75	6	4.5	8		
S2	Acceso remoto	8	8	7	8	7	75	50	100	75	75	6	4	7	6	5.25
AUX1	Sistema de climatización	0	0	8			50	50	100			0	0	8		
AUX2	Sistema de detección incendios	0	0	9			50	50	100			0	0	9		
AUX3	Sistema de alimentación ininterrumpido SAI	0	0	9			50	50	100			0	0	9		
AUX4	Extintores	0	0	9			50	50	100			0	0	9		
AUX5	Terminales móviles	8	7	6	7	6	50	50	100			4	3.5	6		
P1	Director General			9			20	20	100					9		
P2	Director Financiero			9			20	20	100					9		
P3	Responsable de RRHH			9			20	20	100					9		
P4	Técnicos de Desarrollo			9			20	20	100					9		
P5	Técnico de Sistemas			9			20	20	100					9		
P6	Personal de limpieza			7			20	20	100					7		
P7	Personal de seguridad			8			20	20	100					8		

TABLA 20: TABLA DE VALORACIÓN DE IMPACTO POTENCIAL EN LOS ACTIVOS.

3.6. Nivel de Riesgo Aceptable y Residual.

Con los datos calculados en los apartados anteriores y sabiendo que los riesgos no pueden eliminarse por completo, es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o no para cada uno de los activos.

Por una parte, se debe establecer el riesgo aceptable, es decir, el nivel de riesgo a partir del cual la organización considera una amenaza importante y debe aplicar controles para reducirlo.

Riesgo residual: Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una compañía nunca puede erradicarse totalmente.

Para calcular el riesgo de cada uno de los activos se va a utilizar la siguiente fórmula:

Riesgo = Impacto potencial * Frecuencia.

Utilizaremos la siguiente tabla para el cálculo del riesgo:

Riesgo	Frecuencia					
		MB(0,002)	B(0,005)	M(0,015)	A(0,075)	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

TABLA 21: TABLA DE CÁLCULO DEL RIESGO.

Aplicándolo a todos los activos de la empresa:

COD	ACTIVO	Impacto potencial					Frecuencia		Riesgo				
		C	I	D	A	T	F	Valor	C	I	D	A	T
HW1	Equipos de comunicaciones	4.5	1.5	8			M	0,015	0.06	0.02	0.12		
HW2	Robot de cintas	4.5	1.5	8			M	0,015	0.06	0.02	0.12		
HW3	PC del puesto usuario	6	2	2			M	0,015	0.09	0.03	0.03		
HW4	Servidores del CPD principal	2.25	3	6			M	0,015	0.03	0.04	0.09		
HW5	Servidores CPD externalizado.	2.25	3	6			M	0,015	0.03	0.04	0.09		
HW6	Portátiles	6	2.5	3			M	0,015	0.09	0.03	0.04		

HW7	Teléfonos VOIP y centralita	4.5	1.5	8			M	0,015	0.06	0.02	1.2		
HW8	Routers	2.25	1	7			M	0,015	0.03	0.015	0.10		
HW9	Switches	4.5	2.5	6			M	0,015	0.06	0.03	0.09		
HW10	Impresoras en red	2.25	1	3			M	0,015	0.03	0.015	0.04		
L1	Centro de datos	4.5	2.5	9			M	0,015	0.06	0.03	0.13		
L2	CPD externo	4.5	2.5	9			M	0,015	0.06	0.03	0.13		
L3	Cuarto de racks	4.5	1.5	5			M	0,015	0.06	0.02	0.07		
L4	Oficinas	4.5	2.5	9			M	0,015	0.06	0.03	0.13		
L5	Despachos	4.5	2.5	9			M	0,015	0.06	0.03	0.13		
SW1	Windows server	3	3.75	5			M	0,015	0.04	0.05	0.07		
SW2	S.O. Ubuntu	3	3.75	5			M	0,015	0.04	0.05	0.07		
SW3	Microsoft Office	3	3.75	5			M	0,015	0.04	0.05	0.07		
SW4	Antivirus	3	3.75	7			M	0,015	0.04	0.05	0.10		
SW5	Aplicaciones internas	6	6	9			M	0,015	0.09	0.09	0.13		
SW6	Página web de la empresa	8	6.75	9			M	0,015	0.12	0.10	0.13		
SW7	Correo electrónico	3	4.5	6			M	0,015	0.04	0.06	0.09		
SW8	Software de Nóminas	6	5.25	8			M	0,015	0.09	0.07	0.12		
SW9	Repositorio de código	2	3	7			M	0,015	0.03	0.04	0.10		
D1	Base de datos de proveedores	8	9	7	8	6	M	0,015	0.12	0.13	0.10	0.12	0.09
D2	Base de datos de clientes	9	9	9	9	6.75	M	0,015	0.13	0.13	0.13	0.13	0.10
D3	Base de datos con información de datos de configuración	6	7	6	8	6	M	0,015	0.09	0.10	0.09	0.12	0.09
D4	Copias de seguridad de servidores	6	8	7	7	5.25	M	0,015	0.09	0.12	0.10	0.10	0.07

COM 1	Cableado eléctrico	4.5	0	8			MB	0,002	0.009	0	0.01		
COM 2	Cableado de telecomunicaciones	6	2.5	9			MB	0,002	0.01	0.005	0.018		
COM 3	Servicio VOIP	4.5	0	8			MB	0,002	0.009	0	0.01		
COM 4	Servicio Internet	6	2.5	9			MB	0,002	0.01	0.005	0.018		
COM 5	Red inalámbrica	6	2.5	9			MB	0,002	0.01	0.005	0.018		
S1	Correo electrónico	6	4.5	8			M	0,015	0.09	0.06	0.12		
S2	Acceso remoto	6	4	7	6	5.25	M	0,015	0.09	0.04	0.10	0.09	0.07
AUX1	Sistema de climatización	0	0	8			M	0,015	0	0	0.12		
AUX2	Sistema de detección incendios	0	0	9			M	0,015	0	0	0.13		
AUX3	Sistema de alimentación ininterrumpido SAI	0	0	9			M	0,015	0	0	0.13		
AUX4	Extintores	0	0	9			M	0,015	0	0	0.13		
AUX5	Terminales móviles	4	3.5	6			M	0,015	0.04	0.05	0.09		
P1	Director General			9			A	0,075			0.675		
P2	Director Financiero			9			A	0,075			0.675		
P3	Responsable de RRHH			9			A	0,075			0.675		
P4	Técnicos de Desarrollo			9			A	0,075			0.675		
P5	Técnico de Sistemas			9			A	0,075			0.675		
P6	Personal de limpieza			7			A	0,075			0.52		
P7	Personal de seguridad			8			A	0,075			0.6		

TABLA 22: TABLA DE CÁLCULO DEL RIESGO SOBRE CADA ACTIVO.

Algunos de los activos de la empresa tienen un nivel de riesgo alto o muy alto y habrá que reducir el nivel de riesgo de cada uno de ellos.

Una vez conocido en nivel de riesgos inicial presente en la organización, la dirección fija el umbral de riesgo aceptable el riesgo medio, bajo o muy bajo. De manera que se trabajará en base al ciclo PDCA en controles que permitan rebajar los niveles de riesgo por debajo de este valor. No obstante, se trabajará en acciones de tratamiento para rebajar este umbral lo máximo posible hasta alcanzar el riesgo residual.
Los riesgos que en primer lugar se deben de intentar bajar, son aquellos tipificados con un valor Muy Alto, es decir, lo que aplican al personal, seguidos de los que se deben a los Datos, quedando en último lugar los debidos a las comunicaciones.
Los ordenamos por orden de prioridad según el nivel del riesgo:

ACTIVO	C	I	A	D	T
Director General[P1]			0.675		
Director Financiero[P2]			0.675		
Responsable de RRHH [P3]			0.675		
Técnicos de Desarrollo [P4]			0.675		
Técnicos de sistemas [P5]			0,675		
Personal de seguridad[P7]			0.6		
Personal de limpieza[P6]			0.52		
Base de datos de clientes[D2]	0.13	0.13	0.13	0.13	0.10
Base de datos de proveedores[D1]	0.12	0.13	0.10	0.12	0.09
Copias de seguridad de servidores[D4]	0.09	0.12	0.10	0.10	0.07
Base de datos con información de datos de configuración[D3]	0.09	0.10	0.09	0.12	0.09
Acceso remoto [S2]	0.09	0.04	0.10	0.09	0.07
Página web de la empresa [SW6]	0.12	0.10	0.13		
Aplicaciones internas [SW5]	0.09	0.09	0.13		
Software de nóminas [SW8]	0.09	0.07	0.12		
Terminales móviles [AUX5]	0.04	0.05	0.09		
Correo electrónico[SW7]	0.04	0.06	0.09		
Windows server [SW1]	0.04	0.05	0.07		
Equipo DE comunicaciones [HW1]	0.06	0.02	0.12		
Robot de cintas [HW2]	0.06	0.02	0.12		

Teléfonos VOIP y centralita[HW7]	0.06	0.02	0.12		
Switches[HW9]	0.06	0.03	0.09		
PC puesto usuario [HW3]	0.09	0.03	0.03		
Servidores del CPD principal[HW4]	0.03	0.04	0.09		
Servidores CPD externalizado.[HW5]	0.03	0.04	0.09		
Portatiles [HW6]	0.09	0.03	0.04		
Repositorio de código [SW9]	0.03	0.04	0.10		
Routers [HW8]	0.03	0.015	0.10		
Servicio internet [COM4]	0.01	0.005	0.018		
Red inalámbrica[COM5]	0.01	0.005	0.018		
Cableado de telecomunicaciones[COM2]	0.01	0.005	0.018		
Sistema de detección incendios[AUX2]	0	0	0.13		
Sistema de alimentación ininterrumpido SAI[AUX3]	0	0	0.13		
Extintores[AUX4]	0	0	0.13		
Sistema de climatización [AUX1]	0	0	0.12		
Cableado eléctrico[COM1]	0.009	0	0.01		
Impresoras en red[HW10]	0.03	0.015	0.04		
Servicio VOIP[COM3]	0.009	0	0.01		

TABLA 23: TABLA RESUMEN DE CÁLCULO DEL RIESGO SOBRE CADA ACTIVO PRIORIZADA.

Conclusiones:

Analizando los riesgos actuales, se puede comprobar que la empresa se encuentra en una zona de riesgo localizada entre la zona baja y media. En conclusión, se puede afirmar que la empresa se encuentra en una situación relativamente saludable.

3.7. Resultados.

Teniendo en cuenta el nivel de riesgo aceptable, nos quedaremos con los activos cuyas amenazas superan el nivel Bajo y Medio. A continuación se muestra la tabla de activos con sus amenazas por encima del nivel de riesgo aceptable (M).
El bloque de Activos sobre el que la empresa es más urgente que actúe en cuanto a las amenazas a las que está expuesta es, principalmente los activos de carácter Personal:

ACTIVO	C	I	A	D	T
Director General[P1]			0.675		
Director Financiero[P2]			0.675		
Responsable de RRHH [P3]			0.675		
Técnicos de Desarrollo [P4]			0.675		
Técnicos de sistemas [P5]			0,675		
Personal de seguridad[P7]			0.6		
Personal de limpieza[P6]			0.52		
Base de datos de clientes[D2]	0.13	0.13	0.13	0.13	0.10

TABLA 24: TABLA ACTIVOS SOBRE LOS QUE HAY QUE ACTUAR.

Seguido de las amenazas a las que están expuestos los activos de Datos y Software:

ACTIVO	C	I	A	D	T
Base de datos de proveedores[D1]	0.12	0.13	0.10	0.12	0.09
Copias de seguridad de servidores[D4]	0.09	0.12	0.10	0.10	0.07
Base de datos con información de datos de configuración[D3]	0.09	0.10	0.09	0.12	0.09
Acceso remoto [S2]	0.09	0.04	0.10	0.09	0.07
Página web de la empresa [SW6]	0.12	0.10	0.13		
Aplicaciones internas [SW5]	0.09	0.09	0.13		
Software de nóminas [SW8]	0.09	0.07	0.12		

TABLA 25: TABLA ACTIVOS SOBRE LOS QUE ES MENOS URGENTE ACTUAR.

4. PROPUESTAS DE PROYECTOS.

4.1. Introducción.

Una vez realizado el Análisis de Riesgos donde se han identificado los activos, amenazas, el impacto de dichas amenazas sobre los activos y por tanto el nivel de riesgo actual, el comité de seguridad de TECNOSOFT plantea un paquete de mejoras para elevar el nivel de seguridad. El objetivo de este paquete de mejoras es que el nivel de riesgo actual sea igual o inferior al nivel de riesgo aceptable.
Las mejoras planteadas han sido catalogadas en dos tipos de actuaciones, las relativas a aspectos organizativos y las estrictamente técnicas.
Se van a plantear un conjunto de recomendaciones, incidiendo en la mejora de la gestión de la seguridad y optimización de recursos o mejora de procesos.

4.2. Propuestas.

Cuando se afrontan una serie de proyectos para elevar el nivel de seguridad, y por tanto disminuir el nivel de riesgo, es difícil concretar cómo afectará al nivel de riesgo de la compañía.
En futuras revisiones del SGSI y del Análisis de Riesgos, se podrá observa con mayor concreción como esta serie de medidas han afectado al nivel de riesgo.

Propuesta 1: Mejorar Política de seguridad	
Objetivo	Mejorar la política de seguridad de la información de TECNOSOFT
Descripción	Revisión de la política de seguridad de TECNOSOFT para buscar puntos de

	mejora. La política de seguridad tiene que ser aprobado por el equipo de Dirección y la tienen que llevar a cabo todos los empleados.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos Servicios: todos los activos Equipamiento auxiliar: todos los activos
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad, Integridad , Disponibilidad
Responsable	Responsable de seguridad
Controles	Políticas de Seguridad de la Información.
Indicadores	Política de seguridad [SEG1]
Duración	11 días
Coste	Euros/hora personal responsable de seguridad Euros/hora comité de seguridad Euros/hora equipo de Dirección

Propuesta2: Plan de continuidad	
Objetivo	Definir un plan de Continuidad del negocio de TECNOSOFT en caso de ocurrir un desastre.
Descripción	Partimos del análisis de riesgos para descubrir los procesos más críticos.Identificados los procesos, se plasman en un documento que será aprobado por la Dirección de TECNOSOFT. El Comité de Seguridad hace un seguimiento de dicho documento para mejorar el Plan de Continuidad.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos

	Servicios: todos los activos Equipamiento auxiliar: todos los activos
Dimensiones de seguridad cuyo riesgo se reduce	Disponibilidad
Responsable	Responsable de seguridad
Controles	Continuidad de Seguridad de la información.
Indicadores	Continuidad de negocio.
Duración	31 días
Coste	Euros/hora personal responsable de seguridad Euros/hora comité de seguridad Euros/hora equipo de Dirección

Propuesta3: Formación a los empleados en Seguridad	
Objetivo	Concienciar a los empleados de TECNOSOFT en materia de seguridad de información.
Descripción	Estableceremos un calendario de formación en seguridad a los empleados de TECNOSOFT. Se indicará a los empleados los principios básicos de seguridad de la información a adoptar por TECNOSOFT. El curso será impartido por el responsale de seguridad. Cada año se establecerá un calendario de formación en seguridad.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos Servicios: todos los activos Equipamiento auxiliar: todos los activos
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad Disponibilidad Integridad

	Integridad
Responsable	Responsable de seguridad
Controles	Sensibilización, educación y formación en seguridad de la información.
Indicadores	Formación [SEG4]
Duración	11 días
Coste	Euros/hora personal responsable de seguridad Euros/hora empleados
Propuesta4: Mejora de la gestión de incidentes de seguridad	
Objetivo	Establecer procedimientos de notificación y actuación ante incidentes de seguridad de la información, con objeto de que sean resueltos lo más eficaz y rápidamente posible.
Descripción	Definiremos con claridad el procedimiento de notificación de incidentes de seguridad que puedan encontrar los empleados de TECNOSOFT en cualquier sistema de la organización. Se describirán las responsabilidades de cada empleado en lo que a los incidentes de seguridad se refiere, indicando cómo debe actuar cada empleado en cada caso, dependiendo de su puesto en la organización. También se definirá el proceso de actuación para resolver los incidentes de seguridad que puedan surgir. Se guardarán y registrarán todos los incdentes de seguridad que vayan surgiendo en la origanización para estudirarlos y tomar nota de cómo se r esolvieron.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos Servicios: todos los activos Equipamiento auxiliar: todos los

	activos
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad Disponibilidad Integridad Integridad
Responsable	Responsable de seguridad
Controles	Gestión de incidentes de seguridad de la información
Indicadores	Puntos débiles de seguridad Incidentes.
Duración	16 días

Propuesta5: Revisión de seguridad de la información	
Objetivo	Comprobar el cumplimiento de las medidas de seguridad por parte de TECNOSOFT
Descripción	Se contratará a un auditor externopara que realice una auditoría de seguridad de la información de la organización para tener una opinión independiente sobre el estado de la seguridad de la organización, así como de una valoración de las posibles mejoras a llevar a cabo. Tanto la Dirección como el Responsable de Seguridad revisarán el cumplimiento de los procedimientos de seguridad establecidos por la organización que les involucren. Este proceso se revisará anualmente.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos Servicios: todos los activos Equipamiento auxiliar: todos los activos
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad Disponibilidad Integridad

	Integridad Trazabilidad
Responsable	Responsable de seguridad Auditor externo Dirección
Controles	Revisiones de seguridad de la información.
Indicadores	Auditorías internas
Duración	36 días
Coste	Euros/hora del equipo de dirección. Euros/hora del responsable de seguridad. Euros/hora del auditor externo.
Propuesta6: Mejora en la relación con los proveedores	
Objetivo	Comprobar que los proveedores de TECNOSOFT disponen de medidas de seguridad adecuadas en los servicios que ofrecen a la organización.
Descripción	Se comprueba que los proveedores cumplen los acuerdos establecidos cn TECNOSOFT. Se monitorizan las conexiones para monitorizar las conexiones con terceras partes y el riesgo que estas pueden conllevar, para poder mitigarlas.
Activos cuyo riesgo se reduce	Datos:D1,D2,D3,D4 Red Servicios
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad Disponibilidad Integridad Integridad
Responsable	Responsable de seguridad
Controles	Relaciones con proveedores

Indicadores	Revisión de los servicios ofrecidos por los proveedores.
Duración	11 días
Coste	Euros/hora del responsable de seguridad

Propuesta7: Monitorización del sistema	
Objetivo	Comprobar el cumplimiento de las medidas de seguridad por parte de TECNOSOFT con el fin de evitar amenazas.
Descripción	Se van a implantar soluciones para proteger los registros obtenidos de la monitorización de accesos no autorizados o alteraciones.
Activos cuyo riesgo se reduce	Instalaciones:L1,L2,L3,L4 Aplicación:SW1,SW2,SW6 Datos:D1,D2,D3,D4 Red Servicios
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad Integridad Trazabilidad
Responsable	Responsable de seguridad
Controles	Gestión de la capacidad Registro y Seguimiento. Control de acceso al código fuente del programa.
Indicadores	Registros de actividad
Duración	11 días
Coste	Euros/hora del responsable de seguridad
Propuesta8: Protección de los datos con técnicas criptográficas	
Objetivo	Asegurar la protección de la autenticidad, confidencialidad e integridad de datos de TECNOSOFT.

Descripción	Se implantan controles criptográficos en todos los servciicos de la organización que contengan información confidencial, y en los equipos de lo empleados para asegurar la confidencialidad e integridad de la información de la organización, así como la ocurrencia de cualquier amenaza que ponga en peligro las dimensiones de seguridad
Activos cuyo riesgo se reduce	Datos: [D1], [D2], [D3], [D4
Dimensiones de seguridad cuyo riesgo se reduce	Autenticidad [A] Confidencialidad [C] Integridad [I]
Responsable	Responsable de seguridad
Controles	Controles criptográficos.
Indicadores	Controles criptográficos.
Duración	21 días
Coste	Euros/hora del responsable de seguridad

Propuesta9: Implantación de sistema de gestión de usuarios y permisos	
Objetivo	Gestionar de forma adecuada el ciclo de vida de los usuarios, así como los permisos y roles otorgados a cada uno. Tener trazabilidad de los cambios de permiso de los usuarios. Verificar con la colaboración del Área de Formación, que un usuario tiene la formación necesaria para contar con determinados permisos.
Descripción	Análisis diseño y desarrollo de un sistema de gestión de usuarios, permisos y roles.
Activos cuyo riesgo se reduce	Personal
Dimensiones de segridad cuyo riesgo se reduce	Confidencialidad Integridad Trazabilidad
Responsable	Director de RRHH
Controles	Aspectos organizativos de la seguridad de la información (6.1) Control de accesos (9.4)

Indicadores	Registros de actividad
Duración	42 días
Coste	Euros/hora del responsable de seguridad
Propuesta10: Normativa de uso de dispositivos móviles y portátiles	
Objetivo	Crear conciencia de uso adecuado de los dispositivos con los que la compañía dota a sus empleados. Por tanto, se espera que los empleados hagan un uso más adecuado y por tanto se eleve el umbral de seguridad en lo que a uso adecuado de dispositivo se refiere.
Descripción	Desarrollar una política de uso de dispositivos móviles y equipos portátiles. Hasta el momento no se hace firmar ningún documento a los empleados cuando reciben un dispositivo móvil o equipo portátil.
Dimensiones de segridad cuyo riesgo se reduce	Autenticidad [A] Confidencialidad [C] Integridad [I]
Responsable	Director de RRHH
Controles	Políticas de Seguridad (5.1) Aspectos organizativos de la seguridad de la información (6.2)
Duración	11 días
Coste	Euros/hora del responsable de seguridad

Propuesta11: Mejora en los desarrollos.	
Objetivo	Incluir controles de seguridad en los desarrollos realizados en TECNOSOFT
Descripción	Se va a definir un documento en el que se expliquen las reglas para el desarrollo de software en la organización. Se van a implantar procedimientos de control de cambios para los desarrollos. Se van a definir los principios para la construcción de software seguro que todo empleado deberá conocer y seguir así como las pruebas básicas que se deben realizar a todo software para asegurar su seguridad.

Activos cuyo riesgo se reduce	Software Datos
Dimensiones de segridad cuyo riesgo se reduce	Confidencialidad Integridad Disponibilidad
Responsable	Responsable de seguridad.
Controles	Seguridad en procesos de desarrollo y soporte.
Indicadores	Incidentes
Duración	16 días
Coste	Euros/hora del responsable de seguridad
Propuesta12: Mejora en los requisitos y comunicaciones.	
Objetivo	Identificar y analizar los requisitos de seguridad necesarios para cualquier proyecto que se realice en TECNOSOFT así como proteger la información que se comunica por las redes de la organización.
Descripción	Se deberá realizar un análisis de requisitos de seguridad para los sistemas de información existentes en la organización y se tendrá que hacer también para los nuevos sistemas que aparezcan en la empresa. Se van a establecer medidas para proteger todas las comunicaciones y transacciones que se realicen por las redes de la organización así como por las redes públicas.
Activos cuyo riesgo se reduce	Red: [COM3], [COM4], [COM5] Servicios: [S1], [S2], [S3] Datos: [D1], [D2], [D3], [D4
Dimensiones de segridad cuyo riesgo se reduce	Autenticidad [A] Integridad [I]
Responsable	Responsable de seguridad
Controles	Requisitos de seguridad de los sistemas de información.

	Políticas y procedimientos de transferencia de información. Acuerdos de transferencia de información. Mensajería electrónica Seguridad de la información en la gestión de proyectos.
Indicadores	Incidentes. Comunicaciones externas
Duración	26 días
Coste	Euros/hora del responsable de seguridad
Propuesta 13: Mejorar en la Gestión de Activos.	
Objetivo	Tener conocimiento preciso de todos los activos de TECNOSOFT
Descripción	A partir del inventario de activos realizado se asignará a cada activo un propietario o responsable de éste y se llevará a cabo la clasificación y etiquetado de todos los activos. Se va a redactar un documento en el que se expliquen las normas de uso adecuado de los activos así como el procedimiento a seguir si un empleado necesita manipular un activo o sacarlo fuera de las instalaciones de la organización.
Activos cuyo riesgo se reduce	Instalaciones:todos los activos Hardware: todos los activos Aplicación: todos los activos Datos: todos los activos Red: todos los activos Servicios: todos los activos Equipamiento auxiliar: todos los activos
Dimensiones de seguridad cuyo riesgo se reduce	Confidencialidad, Integridad , Disponibilidad
Responsable	Responsable de seguridad
Controles	Gestión de activos. Retiro de activos.

Indicadores	Inventario de activos Mal uso de activos Extravío de activos
Duración	12 días
Coste	Euros/hora del responsable de seguridad Euros/hora investigador

TABLA 26: TABLA DE PROPUESTAS DE MEJORA.

4.3. Planificación del proyecto de mejora.

A continuación, se muestra un diagrama, donde se plasman los periodos de ejecución de los proyectos de mejora, durante un tiempo de 6 meses, dejando el período de agosto para las vacaciones.

FIGURA14: PLANIFICACIÓN DEL PROYECTO DE MEJORA.

4.2. Resultados.

Los proyectos propuestos en esta fase tienen como objetivo principal la reducción del riesgo de los activos analizados en la fase anterior. Además, con la realización de estos proyectos se va a conseguir una mejora del estado de los dominios de la ISO/IEC 27002:2013.

A continuación, se muestra la comparación entre la situación inicial de los controles de la ISO 27002 que se obtuvo en la fase 1 y la situación que se espera obtener tras la realización de los proyectos.

CONTROL				Situación inicial	Situación esperada
A.5 Information security policies					
	A.5.1 Management direction for information security				
		A.5.1.1	Policies for information security	4 - Gestionado	5 - Optimizado
		A.5.1.2	Review of the policies for informatio security	4 - Gestionado	5 - Optimizado
A.6 Organization of information security					
	A.6.1 Internal organization				
		A.6.1.1	Information security roles and responsibilities	3 - Definido	4 - Gestionado
		A.6.1.2	Segregation of duties	3 - Definido	4 - Gestionado
		A.6.1.3	Contact with authorities	4 - Gestionado	5 - Optimizado
		A.6.1.4	Contact with special interest groups	0 - No existente	3 - Definido
		A.6.1.5	Information security in project management	0 - No existente	3 - Definido
	A.6.2 Mobile devices and teleworking				
		A.6.2.1	Mobile device policy	0 - No existente	3 - Definido
		A.6.2.2	Teleworking	0 - No existente	3 - Definido
A.7 Human resource security					
	A.7.1 Prior to employment				
		A.7.1.1	Screening	0 - No existente	3 - Definido
		A.7.1.2	Terms and conditions of employment	0 - No existente	3 - Definido
	A.7.2 During employment				
		A.7.2.1	Management responsibilities	0 - No existente	3 - Definido
		A.7.2.2	Information security awareness, education and training	0 - No existente	3 - Definido
		A.7.2.3	Disciplinary process	0 - No existente	3 - Definido
	A.7.3 Termination and change of employment				
		A.7.3.1	Termination or change of employment responsibilities	4 - Gestionado	5 - Optimizado
A.8 Asset management					
	A.8.1 Responsibility for asset				
		A.8.1.1	Inventory of assets	0 - No existente	3 - Definido
		A.8.1.2	Ownership of assets	0 - No existente	3 - Definido
		A.8.1.3	Acceptable use of assets	0 - No existente	3 - Definido
		A.8.1.4	Return of assets	0 - No existente	3 - Definido
	A.8.2 Information classification				
		A.8.2.1	Classification of information	0 - No existente	3 - Definido
		A.8.2.2	Labelling of informa tion	0 - No existente	3 - Definido
		A.8.2.3	Handling of assets	0 - No existente	3 - Definido
	A.8.3 Media handling				
		A.8.3.1	Management of removable media	0 - No existente	3 - Definido
		A.8.3.2	Disposal of media	0 - No existente	3 - Definido
		A.8.3.3	Physical media transfer	0 - No existente	3 - Definido
A.9 Access control					
	A.9.1 Business requirements of access control				
		A.9.1.1	Access control policy	5 - Optimizado	5 - Optimizado
		A.9.1.2	Access to networks and network services	3 - Definido	4 - Gestionado
	A.9.2 User access management				
		A.9.2.1	User registration and de-registration	5 - Optimizado	5 - Optimizado
		A.9.2.2	User access provisioning	4 - Gestionado	5 - Optimizado
		A.9.2.3	Management of privileged access rights	4 - Gestionado	5 - Optimizado
		A.9.2.4	Management of secret authentication information of us	4 - Gestionado	5 - Optimizado

		A.9.2.5	Review of user access rights	5 - Optimizado	5 - Optimizado
		A.9.2.6	Removal or adjustment of access rights	5 - Optimizado	5 - Optimizado
	A.9.3 User responsibilities				
		A.9.3.1	Use of secret authentication information	4 - Gestionado	5 - Optimizado
	A.9.4 System and application access control				
		A.9.4.1	Information access restriction	4 - Gestionado	5 - Optimizado
		A.9.4.2	Secure log-on procedures	1 - Inicial	3 - Definido
		A.9.4.3	Password managment system	1 - Inicial	3 - Definido
		A.9.4.4	Use of privileged utility programs	1 - Inicial	3 - Definido
		A.9.4.5	Access control to program source code	1 - Inicial	3 - Definido
A.10 Cryptography					
	A.10.1 Cryptographic controls				
		A.10.1.1	Policy on the use of cryptographic controls	4 - Gestionado	5 - Optimizado
		A.10.1.2	Key management	4 - Gestionado	5 - Optimizado
A.11 Physical and environmental security					
	A.11.1 Secure areas				
		A.11.1.1	Physical security perimeter	0 - No existente	3 - Definido
		A.11.1.2	Physical entry controls	0 - No existente	3 - Definido
		A.11.1.3	Securing offices, rooms and facilities	0 - No existente	3 - Definido
		A.11.1.4	Protecting against external and environmental threats	0 - No existente	3 - Definido
		A.11.1.5	Working in secure areas	0 - No existente	3 - Definido
		A.11.1.6	Delivery and loading areas	0 - No existente	3 - Definido
	A.11.2 Equipment				
		A.11.2.1	Equipment siting and protection	0 - No existente	3 - Definido
		A.11.2.2	Supporting utilities	0 - No existente	3 - Definido
		A.11.2.3	Cabling security	0 - No existente	3 - Definido
		A.11.2.4	Equipment maintenance	0 - No existente	3 - Definido
		A.11.2.5	Removal of assets	0 - No existente	3 - Definido
		A.11.2.6	Security of equipment and assets off-premises	0 - No existente	3 - Definido
		A.11.2.7	Secure disposal or reuse of equipment	0 - No existente	3 - Definido
		A.11.2.8	Unattended user equipment	0 - No existente	3 - Definido
		A.11.2.9	Clear desk and clear screen policy	0 - No existente	3 - Definido
A.12 Operations security					
	A.12.1 Operational procedures and responsibilities				
		A.12.1.1	Documented operating procedures	5 - Optimizado	5 - Optimizado
		A.12.1.2	Change management	5 - Optimizado	5 - Optimizado
		A.12.1.3	Capacity management	5 - Optimizado	5 - Optimizado
		A.12.1.4	Separation of development, testing and operational env	5 - Optimizado	5 - Optimizado
	A.12.2 Protection from malware				
		A.12.2.1	Controls against malware	0 - No existente	3 - Definido
	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	3 - Definido
		A.12.4.2	Protection of log information	0 - No existente	3 - Definido
		A.12.4.3	Administrator and operator logs	0 - No existente	3 - Definido
		A.12.4.4	Clock synchronisation	0 - No existente	3 - Definido
	A.12.5 Control of operational software				

		A.12.5.1	Installation of software on operational systems	4 - Gestionado	5 - Optimizado
	A.12.6 Technical vulnerability management				
		A.12.6.1	Management of technical vulnerabilities	0 - No existente	3 - Definido
		A.12.6.2	Restrictions on software installation	0 - No existente	3 - Definido
	A.12.7 Information systems audit considerations				
		A.12.7.1	Information systems audit controls	1 - Inicial	3 - Definido
A.13 Communications security					
	A.13.1 Network security management				
		A.13.1.1	Network controls	3 - Definido	4 - Gestionado
		A.13.1.2	Security of network services	3 - Definido	4 - Gestionado
		A.13.1.3	Segregation in networks	3 - Definido	4 - Gestionado
	A.13.2 Information transfe				
		A.13.2.1	Information transfer policies and procedures	0 - No existente	3 - Definido
		A.13.2.2	Agreements on information transfer	0 - No existente	3 - Definido
		A.13.2.3	Electronic messaging	0 - No existente	3 - Definido
		A.13.2.4	Confidentiality or nondisclosure agreements	0 - No existente	3 - Definido
A.14 System acquisition, development and maintenance					
	A.14.1 Security requirements of information systems				
		A.14.1.1	Information security requirements analysis and specifica	0 - No existente	3 - Definido
		A.14.1.2	Securing application services on public networks	0 - No existente	3 - Definido
		A.14.1.3	Protecting application services transactions	0 - No existente	3 - Definido
	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.	4 - Gestionado	5 - Optimizado
		A.14.2.3	Technical review of applications after operating platforn	3 - Definido	4 - Gestionado
		A.14.2.4	Restrictions on changes to software packages	3 - Definido	4 - Gestionado
		A.14.2.5	Secure system engi neering principles	2 - Repetible	4 - Gestionado
		A.14.2.6	Secure development environment	3 - Definido	4 - Gestionado
		A.14.2.7	Outsourced development	1 - Inicial	3 - Definido
		A.14.2.8	System security testing	3 - Definido	4 - Gestionado
		A.14.2.9	System acceptance testing	3 - Definido	4 - Gestionado
	A.14.3 Test data				
		A.14.3.1	Protection of test data	0 - No existente	3 - Definido
A.15 Supplier relationships					
	A.15.1 Information security in supplier relationships				
		A.15.1.1	Information security policy for supplier relationships	4 - Gestionado	5 - Optimizado
		A.15.1.2	Addressing security within supplier agreements	4 - Gestionado	5 - Optimizado
		A.15.1.3	Information and communication technology supply chai	0 - No existente	3 - Definido
	A.15.2 Supplier service delivery management				
		A.15.2.1	Monitoring and review of supplier services	3 - Definido	4 - Gestionado
		A.15.2.2	Managing changes to supplier services	3 - Definido	4 - Gestionado
A.16 Information security incident management					
	A.16.1 Management of information security incidents and improvement				
		A.16.1.1	Responsibilities and procedures	3 - Definido	4 - Gestionado
		A.16.1.2	Reporting information security events	3 - Definido	4 - Gestionado
		A.16.1.3	Reporting information security weaknesses	3 - Definido	4 - Gestionado
		A.16.1.4	Assessment of and decision on information security eve	3 - Definido	4 - Gestionado
		A.16.1.5	Response to information security incidents	3 - Definido	4 - Gestionado
		A.16.1.6	Learning from information security incidents	3 - Definido	4 - Gestionado
		A.16.1.7	Collection of evidence	4 - Gestionado	5 - Optimizado
A.17 Information security aspects of business continuity management					
	A.17.1 Information security continuity				
		A.17.1.1	Planning information security continuity	4 - Gestionado	5 - Optimizado
		A.17.1.2	Implementing information security continuity	4 - Gestionado	5 - Optimizado
		A.17.1.3	Verify, review and evaluate information security contin	4 - Gestionado	5 - Optimizado
	A.17.2 Redundancies				
		A.17.2.1	Availability of infor mation processing facilities	1 - Inicial	3 - Definido
A.18 Compliance					
	A.18.1 Compliance with legal and contractual requirements				
		A.18.1.1	Identification of applicable legislation and contractual re	0 - No existente	3 - Definido
		A.18.1.2	Illectual property rights	0 - No existente	3 - Definido
		A.18.1.3	Protection of records	2 - Repetible	4 - Gestionado
		A.18.1.4	Privacy and protection of personally identifiable inform	1 - Inicial	3 - Definido
		A.18.1.5	Regulation of cryptographic controls	0 - No existente	3 - Definido
	A.18.2 Information security reviews				
		A.18.2.1	Independent review of information security	1 - Inicial	3 - Definido
		A.18.2.2	Compliance with security policies and standards	2 - Repetible	4 - Gestionado
		A.18.2.3	Technical compliance review	1 - Inicial	3 - Definido

TABLA 27: TABLA COMPARATIVA, ANTES Y DESPUÉS DE APLICAR MEDIDAS.

5. AUDITORÍA DEL CUMPLIMIENTO.

5.1. Introducción.

En esta fase se va a realizar la auditoría de cumplimiento, que tiene como objetivo la evaluación del estado de la seguridad de la información de TECNOSOFT tras haber finalizado con éxito todas las fases anteriores. Para ello, se evaluará el grado de madurez en lo que respecta a los diferentes dominios y controles planteados por la ISO/IEC 27002:2013.

Antes de empezar a realizar la auditoría de cumplimiento, vamos a suponer que los proyectos propuestos en la fase anterior se han implementado correctamente en la organización. Por lo tanto, se partirá de ese supuesto para llevar a cabo la evaluación de la seguridad de TECNOSOFT.

5.2. Metodología.

Para evaluar correctamente la madurez de la seguridad de la información de TECNOSOFT se va a utilizar el estándar ISO/IEC 27002:2013, puesto que se trata de un estándar internacionalmente conocido y es perfectamente válido para la mayoría de organizaciones.

Como se ha mencionado en capítulos anteriores, el estándar ISO/IEC 27002:2013 está formado por 114 controles o salvaguardas organizadas en 14 dominios y 35 objetivos de control. Para comprobar el estado de la seguridad de la organización, se evaluará el nivel de madurez de cada uno de los controles existentes en la norma. Para ello, se volverá a utilizar el Modelo de Madurez de Capacidades (CCM) que se utilizó para realizar el análisis diferencial del estado inicial de la seguridad de TECNOSOFT, que se encuentra definido en la Tabla 1.

Los niveles que se van a utilizar para evaluar el grado de madurez de cada uno de los controles.

Nivel	Efectividad	Significado
L0	0%	Inexistente
L1	10%	Inicial
L2	50%	Repetible
L3	90%	Definido
L4	95%	Administrado
L5	100%	Optimizado

TABLA 28: TABLA DE NIVELES CMM

5.3. Evaluación de la madurez.

A continuación, en la Tabla 29, se muestra el nivel de madurez de cada uno de los controles de la ISO 27002:2013 así como la justificación de dicho nivel.

Sección	Control ISO 27002:2013	JUSTIFICACION	CMM
A5	**Políticas de seguridad de la información**		
A5.1	Directrices de gestión de la seguridad de la información		
A5.1.1	Políticas para la seguridad de la información	Se ha comprobado que existe una política de seguridad y que se le aplican mejoras .	L5
A5.1.2	Revisión de las políticas para la seguridad de la información	Existe un proyecto anual de mejora de la política de seguridad que ya ha sido aplicado al menos una vez.	L5
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Existe un documento en el que se asignan los roles de los empleados en lo referente a la seguridad de la información cuya evolución se comprueba anualmente a través de un indicador	L4
A6.1.2	Segregación de tareas	Existe un documento en el que se describen las tareas de los empleados en lo referente a la seguridad de la información y se ha comprobado que éstas se están realizando correctamente por las personas adecuadas, gracias a los indicadores de acuerdo al documento	L4
A6.1.3	Contacto con las autoridades	Se ha comprobado que ha existido contacto con las autoridades. Sin embargo, no hay ningún documento formal que indique cómo se debe realizar este contacto ni cuándo, ni existen	L2
A6.1.4	Contacto con grupos de interés especial	Se ha comprobado que ha existido contacto con grupos de interés relacionados con la seguridad de la información. Sin embargo, no hay ningún	L2
A6.1.5	Seguridad de la información en la gestión de proyectos	Se ha comprobado que se han realizado análisis de requisitos para los sistemas y procesos existentes y que se realizan para los nuevos procesos.	L3
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	Existen normas definidas y empleados por los trabajadores respecto al uso de dispositivos móviles, así como indicadores para seguir su evolución y mejorar esta política	L4
A6.2.2	Teletrabajo	Existen algunas normas no escritas para el teletrabajo, pero no una política específica que especifique el procedimiento a seguir.	L2
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Se ha comprobado que los miembros de administración investigan sobre los posibles candidatos antes de contratarlos. Sin embargo, no se ha podido demostrar que este proceso se revise y mejore cada cierto tiempo.	L4
A7.1.2	Términos y condiciones del empleo	Se ha comprobado que se definen correctamente los términos y condiciones de las nuevas contrataciones antes de llevarlas a cabo. Sin embargo, no se ha podido demostrar que este	L4
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Se ha comprobado que se comunica a los empleados la política de seguridad así como la necesidad de aplicarla. Sin embargo, no se ha comprobado que se revisen las responsabilidades.	L4
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Existe un programa de formación que está en constante mejora gracias a los indicadores que controlan la evolución de este control.	L5

A7.2.3	Proceso disciplinario	Se ha comprobado que hay definido un proceso disciplinario para cuando un empleado no cumpla las normas y que se realiza un seguimiento de éste con el objetivo de mejorarlo.	L5
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Existe un procedimiento de actuación para cuando un empleado abandona la empresa. Se ha comprobado que se está llevando a cabo de manera adecuada. Sin embargo, no se ha podido demostrar que este proceso esté bajo constante mejora.	L4
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Se ha comprobado que existe un inventario de activos y que existe un procedimiento para ir inventariando los nuevos activos.	L5
A8.1.2	Propiedad de los activos	Se ha comprobado que todos los activos tienen un propietario y que existe un procedimiento para asignar el propietario de los nuevos activos.	L5
A8.1.3	Uso aceptable de los activos	Existe un documento en el que se definen las normas de uso de los activos. Se ha comprobado que los empleados están siguiendo estas reglas. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore, pese a que existen indicadores para controlar la evolución de este control.	L4
A8.1.4	Devolución de activos	Existen normas a seguir para la devolución de activos. Sin embargo, éste no es muy claro.	L2
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Los activos están clasificados. Sin embargo, no existe un documento en el que estén definidas las directrices de clasificación.	L2
A8.2.2	Etiquetado de la información	Los activos están etiquetados. Sin embargo, no existe un documento en el que estén definidas las directrices de etiquetado. Existen definidas algunas normas para el tratamiento de la información, pero se recomienda revisarlas y mejorarlas.	L3
A8.2.3	Manipulado de la información	Las normas de manipulación de activos están definidas y se ha comprobado que se siguen de manera adecuada y se puede seguir quien lleva a cabo la manipulación de cada activo.	L4
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Existen procedimientos para la utilización y gestión de los soportes extraíbles. Sin embargo, no existe una métrica que permita conocer si se está aplicando correctamente.	L3
A8.3.2	Eliminación de soportes	No se han encontrado procedimientos concretos para la eliminación de los soportes. Se reconoce que existe el problema y que hay que mejorarlo.	L1
A8.3.3	Soportes físicos en tránsito	Existen procedimientos para el tratamiento de soportes físicos que se sacan fuera de la organización y existen medidas para controlar la evolución de este control.	L4

A9	Control de acceso		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Existe una política de control de accesos definida y seguida por todos los trabajadores. Esta política es revisada por la dirección junto al resto de políticas cada cierto tiempo	L5
A9.1.2	Acceso a las redes y a los servicios de red	Se ha comprobado que hay implantados controles de acceso a las redes y servicios así como indicadores con los que seguir su evolución y mejorar los accesos a las redes y servicios	L5
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Existe un procedimiento a seguir para dar de alta y de baja usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.	L5
A9.2.2	Provisión de acceso de usuario	Existe un procedimiento a seguir para otorgar y quitar derechos a los usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.	L5
A9.2.3	Gestión de privilegios de acceso	Existe un procedimiento a seguir para otorgar y quitar derechos especiales a los usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.	L5
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Existen normas a seguir referentes a este control que son conocidas por los empleados. Sin embargo, no se ha encontrado un documento en el que se defina formalmente el procedimiento.	L2
A9.2.5	Revisión de los derechos de acceso de usuario	Se ha comprobado que los derechos de acceso de los usuarios se revisan de vez en cuando. Sin embargo, no existe ningún documento formal que indique cada cuanto se debe realizar ni el responsable de hacerlo.	L2
A9.2.6	Retirada o reasignación de los derechos de acceso	Se ha comprobado que los derechos de acceso de los usuarios se retiran de manera adecuada. Sin embargo, no existe ningún documento formal que indique el procedimiento a seguir ni para retirar los derechos de acceso ni para adaptarlos en el caso de que cambien los derechos de un usuario.	L2
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Se ha comprobado que a los usuarios se les exige la no utilización de información confidencial para autenticarse. Se ha comprobado que se está llevando a cabo de manera adecuada. Sin embargo, no existen indicadores para medir este control eficazmente.	L3
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Hay puestas en marcha medidas para evitar el acceso a usuarios no autorizados. Sin embargo, no existe ningún documento formal que indique cada cuanto se debe realizar ni el responsable de hacerlo.	L4

A9.4.2	Procedimientos seguros de inicio de sesión	Se ha comprobado que existen procedimientos seguros de inicio de sesión en todos los sistemas de la organización. Sin embargo, se deben implantar indicadores para comprobar su evolución e intentar mejorarlos.	L3
A9.4.3	Sistema de gestión de contraseñas	Se ha comprobado que existe una política de contraseñas y que los sistemas de gestión de contraseñas aseguran el uso de contraseñas de calidad.	L5
A9.4.4	Uso de utilidades con privilegios del sistema	El software instalado en los equipos está totalmente controlado y ningún empleado sin derechos de administrador puede hacer uso ni modificar las herramientas de administración. Sin embargo, no existen indicadores que midan su evolución.	L3
A9.4.5	Control de acceso al código fuente de los programas	Se ha comprobado que el acceso al código fuente de los programas está restringido y que se controla a través de monitorización. Además, existen indicadores para comprobar su evolución y así mejorarlo.	L5
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Se ha comprobado que hay implantados controles criptográficos en todos los sistemas de la organización. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore, pese a que existen indicadores para controlar la evolución de este control.	L4
A10.1.2	Gestión de claves	Existen procedimientos para el control de las claves criptográficas utilizadas y estos se están aplicando correctamente. Sin embargo, no existe ningún indicador para controlar la evolución y no se ha podido demostrar que este proceso se revise y/o se mejore.	L3
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Existen medidas de seguridad que aseguran el perímetro de la organización. Se ha comprobado que se controla su evolución, se revisa y se intenta mejorar	L5
A11.1.2	Controles físicos de entrada	Existen controles físicos en todas las entradas a las instalaciones de la organización . Se ha comprobado que se controla su evolución, se revisa y se intenta mejorar.	L5
A11.1.3	Seguridad de oficinas, despachos y recursos	Existen controles físicos en todas las salas de la organización y éstos se controlan y se encuentran en constante mejora.	L5
A11.1.4	Protección contra las amenazas externas y ambientales	Existen medidas de protección contra las amenazas externas y ambientales así como medidas para comprobar su evolución y mejorarlo.	L5
A11.1.5	El trabajo en áreas seguras	Existen buenas prácticas respecto a este control pero no existe un documento formal.	L2
A11.1.6	Áreas de carga y descarga	Existen buenas prácticas respecto a este control pero no existe un documento formal.	L2

A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Los equipos se encuentran emplazados en lugares con control de acceso así como protegidos de posibles amenazas ambientales. Existe documentación sobre este control. Sin embargo no existen controles para comprobar su evolución.	L3
A11.2.2	Instalaciones de suministro	Existen medidas para proteger los equipos contra fallos del suministro eléctrico y éstas son controladas y en constante mejora.	L5
A11.2.3	Seguridad del cableado	No existen cables a la vista en toda la instalación y existen indicadores para medir el número de cables visibles	L4
A11.2.4	Mantenimiento de los equipos	Existe un procedimiento de mantenimiento de equipos así como un responsable para ello. También existen indicadores para comprobar la correcta realización de este procedimiento y poder aplicar mejoras	L5
A11.2.5	Retirada de materiales propiedad de la empresa	Existe un procedimiento a seguir para cuando se quieren sacar activos fuera de las instalaciones de la organización. Existe un procedimiento para comunicar que se va a sacar un activo, por lo que este control se puede medir. Sin embargo, no se ha podido demostrar que el proceso se revise y mejore.	L4
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Existe una política de uso aceptable de activos que debe aplicarse a todos los activos en general. Sin embargo, se debería especificar en un documento las medidas de seguridad a tomar en el caso concreto de que se saque un activo fuera de las instalaciones de la organización.	L3
A11.2.7	Reutilización o eliminación segura de equipos	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no existen indicadores para medir su evolución.	L3
A11.2.8	Equipo de usuario desatendido	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no se puede medir este control por la falta de métricas.	L3
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no se puede medir este control puesto que no hay ningún indicador que refleje su evolución.	L3
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	No existe un documento formal donde se encuentren documentados los procedimientos operativos. Sin embargo, los empleados sí que siguen métodos propios.	L2
A12.1.2	Gestión de cambios	No existe ningún proceso formal para controlar los cambios que afectan a la seguridad de la información de la organización. Sin embargo, sí que se tienen algunos registros de cambios que se han ido haciendo	L2
A12.1.3	Gestión de capacidades	Los sistemas de la organización se encuentran monitorizados. Sin embargo, no se han encontrado evidencias de que con los registros obtenidos se ajuste el uso de los recursos de los sistemas.	L3
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Se separan los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	L3

A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Existen implantadas medidas contra código malicioso en todos los equipos de la organización, así como indicadores para medir su funcionamiento. Este proceso está en constante mejora.	L5
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Existe un procedimiento formal a seguir para realizar las copias de seguridad y existen métricas para comprobar su funcionamiento y evolución. Además, se ha comprobado que este control está en constante mejora.	L5
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Se ha comprobado que los eventos de actividad se registran y existen métricas para comprobar su funcionamiento y evolución. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore.	L4
A12.4.2	Protección de la información del registro	Se ha comprobado que los registros de información que se crean y guardan están correctamente protegidos. Sin embargo, no se ha encontrado una métrica para comprobar el funcionamiento y evolución de este control.	L4
A12.4.3	Registros de administración y operación	Se ha comprobado que los eventos de actividad de los administradores se registran y existen métricas para comprobar su funcionamiento y evolución. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore.	L4
A12.4.4	Sincronización del reloj	Los relojes de los sistemas de la organización están correctamente sincronizados.	L5
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Existen procedimientos a seguir para instalar software en los sistemas. Se controla la evolución de este control utilizando un indicador. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore	L4
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Se obtiene información sobre las vulnerabilidades pero no existe un proceso formal para ello que indique con qué frecuencia se debe obtener esta información. Cada uno de los empleados responsables de esta tarea lo hace a su propia manera y buscando la información en sitios distintos.	L2
A12.6.2	Restricción en la instalación de software	Existen controles para evitar que cualquier usuario pueda instalar cualquier software en los ordenadores e indicadores que sirven para comprobar el estado de este control así como su evolución.	L4
A12.7	**Consideraciones sobre la auditoría de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	L4

A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Se realizan controles de red de vez en cuando y no siempre de la misma manera.	L2
A13.1.2	Seguridad de los servicios de red	La organización conoce la necesidad de aplicar mecanismos de seguridad asociados a servicios de red pero todavía no existen ningún procedimiento respecto a este control	L1
A13.1.3	Segregación en redes	Se ha comprobado que existen diferentes redes para los diferentes grupos y salas de servidores. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.	L4
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Existe una política respecto a cómo se debe realizar el intercambio de información entre los empleados y con el exterior. Existe un indicador para medir este control y esto se revisa y se mejora periódicamente	L5
A13.2.2	Acuerdos de intercambio de información	Hay definidas normas a seguir para realizar las transferencias de información de manera segura. Existe un indicador para comprobar la evolución de este control.	L4
A13.2.3	Mensajería electrónica	La información incluida en mensajería electrónica está debidamente protegida. Existe un indicador para comprobar la evolución de este control.	L4
A13.2.4	Acuerdos de confidencialidad o no revelación	Existen acuerdos de confidencialidad con los empleados de la organización. Sin embargo, éstos no se revisan regularmente.	L3
A14	[illegible]		
A14.1	[illegible]		
A14.1.1	[illegible]	Se ha comprobado que se realizan análisis de requisitos a los sistemas de la organización. Sin embargo, faltan indicadores para comprobar la evolución de este control.	L3
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Existen medidas implantadas para proteger las comunicaciones por redes públicas.	L3
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Existen medidas implantadas para proteger las transacciones que se realicen por las redes de la organización.	L3
A14.2	[illegible]		
A14.2.1	Política de desarrollo seguro	Existe un documento con la política de desarrollo de software seguro. Sin embargo, no existen indicadores para controlar la evolución de este control	L3
A14.2.2	Procedimiento de control de cambios en sistemas	Existe un procedimiento de control de cambios para los desarrollos. Sin embargo, no existen indicadores para controlar que este procedimiento se está llevando a cabo correctamente	L3

A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No existe un procedimiento a seguir tras haber realizado cambios en el sistema operativo de algún equipo de la organización. Es el empleado el que las realiza y no sigue ningún procedimiento, sino que realiza las pruebas que considera oportunas	L2
A14.2.4	Restricciones a los cambios en los paquetes de software	Existen controles para evitar la instalación de software indebido. Este control se mide a través de un indicador y se revisa y mejora periódicamente.	L5
A14.2.5	Principios de ingeniería de sistemas seguros	No existe un documento en el que se establezcan los principios de seguridad en ingeniería de sistemas. Sin embargo, la organización está al corriente de este problema y sabe que debe mejorar este control.	L1
A14.2.6	Entorno de desarrollo seguro	Los entornos de desarrollo se encuentran protegidos adecuadamente con medidas de seguridad.	L3
A14.2.7	Externalización del desarrollo de software	Se establecen los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	L3
A14.2.8	Pruebas funcionales de seguridad de sistemas	Se han definido en un documento las pruebas básica que se deben realizar a todo software para asegurar su seguridad. Sin embargo, no existen un indicador concreta para medir si está funcionando correctamente.	L3
A14.2.9	Pruebas de aceptación de sistemas	Se realizan pruebas a los sistemas. Sin embargo, no existe un documento formal que indique la metodología a seguir y cada empleado lo realiza cómo y cuándo le parece adecuado.	L2
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Los datos utilizados en pruebas se encuentran protegidos	L3
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Existen documentos en los que aparecen los acuerdos con los suministradores. Sin embargo, no existen indicadores para este control.	L3
A15.1.2	Requisitos de seguridad en contratos con terceros	Los requisitos de seguridad con los suministradores están establecidos en el acuerdo con éstos. Sin embargo, no existen indicadores para este control.	L3
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	El acuerdo con los suministradores incluye los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios.	L3
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	La organización monitorea las conexiones con terceras partes y deja registros para comprobar su estado y evolución. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.	L4
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No existe un proceso formal de administración de cambios en los servicios prestados por los proveedores.	L2

A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Las responsabilidades y los procedimientos para gestionar los incidentes de seguridad están documentados de manera adecuada. Además, existen métricas para controlar la evolución de los incidentes y procesos de mejora de estos procedimientos.	L5
A16.1.2	Notificación de los eventos de seguridad de la información	Se ha comprobado que existe un procedimiento a seguir para notificar los incidentes de seguridad. Sin embargo, no existe un indicador con el que se pueda medir correctamente si este control se está llevando a cabo correctamente.	L3
A16.1.3	Notificación de puntos débiles de la seguridad	Existe un procedimiento a seguir para notificar los puntos débiles de la seguridad de la organización. La evolución de este control se está midiendo con un indicador. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.	L4
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No existe un procedimiento formal para valorar y clasificar los incidentes de seguridad que surgen. Para ello, cada empleado encargado de tratar los incidentes utiliza su propio método de valoración.	L2
A16.1.5	Respuesta a incidentes de seguridad de la información	Existe un procedimiento a seguir de actuación ante cualquier incidente de seguridad así como métricas para medir su evolución. Estos incidentes se revisan periódicamente y se mejoran.	L5
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Existen una base de datos en la que se guarda la información de los incidentes ocurridos con el objetivo de aprender de ellos y mejorar la seguridad. Sin embargo, no existe ninguna métrica para comprobar que se está utilizando esta información con el fin expuesto.	L3
A16.1.7	Recopilación de evidencias	Se ha comprobado que algunos empleados recopilan las evidencias de los incidentes. Sin embargo, no todos lo hacen ni existe un documento formal que indique el procedimiento a llevar a cabo para este fin.	L2
A17	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Existe un documento en el que se encuentra definido el plan de continuidad de negocio de la organización. Este documento se revisa y mejora periódicamente. Sin embargo, todavía no se ha revisado por primera vez por lo que no se puede afirmar que se encuentra en constante mejora.	L4
A17.1.2	Implementar la continuidad de la seguridad de la información	Se han implantado las medidas oportunas para asegurar la continuidad de negocio en caso de desastre. Se puede seguir la evolución de estas medidas gracias a la existencia de indicadores que sirven para mejorarlas constantemente.	L5
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Existe un plan de seguimiento y evaluación del plan de continuidad de negocio. Sin embargo, éste todavía no se ha llevado a cabo ninguna vez.	L4
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	N.A.	L0

A18	Cumplimiento		
A18.1	Cumplimiento de los requisitos legales y contractuales		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se ha comprobado que se revisa periódicamente la legislación vigente aplicable.	L5
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Se ha comprobado que existen procedimientos que garantizan el cumplimiento de los derechos de propiedad intelectual. Además, hay implantados indicadores para comprobar su funcionamiento y evolución y así mejorar este control.	L5
A18.1.3	Protección de los registros de la organización	Los registros de la organización están debidamente protegidos, existiendo indicadores que así lo demuestran. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.	L4
A18.1.4	Protección y privacidad de la información de carácter personal	La información personal identificable está adecuadamente protegida y tratada de acuerdo a la legislación vigente. Sin embargo, no existe una métrica para comprobar su evolución.	L3
A18.1.5	Regulación de los controles criptográficos	Existen controles criptográficos de acuerdo a la legislación vigente para proteger la información de la organización. También se dispone de un indicador para controlarlo. Sin embargo, no se ha podido demostrar que se revise este control.	L4
A18.2	Revisiones de la seguridad de la información		
A18.2.1	Revisión independiente de la seguridad de la información	Se ha realizado una revisión externa independiente del estado de la seguridad de la información de la organización de la que existen indicadores para comprobar su evolución. Además, este proceso se revisa y se mejora de manera periódica.	L5
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Se lleva a cabo la revisión de las políticas y normas de seguridad y se encuentran en constante mejora	L5
A18.2.3	Comprobación del cumplimiento técnico	Se lleva a cabo la revisión del cumplimiento de las políticas y normas establecidas por la organización. Este proceso se revisa y mejora de manera periódica.	L5

TABLA 29 CONTROLES DE LA ISO 27002:2013

A continuación, en la Tabla 30, se muestra el nivel de madurez de cada una de las secciones de la ISO 27001:2013 así como la justificación de cada nivel.

Sección	Requerimientos ISO 27001	CMM	JUSTIFICACION
4	Contexto de la organización		
4,1	Comprensión de la organización y de su contexto		
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Optimizado	Se ha comprobad o que se la organización y su contexto han sido comprendidas adecuadamente
4,2	Comprensión de las necesidades y expectativas de las partes interesadas		Se ha comprobad o que se han determinado todas las necesidades y expectativas dentro y fuera de la organización que afectan al SGSI.
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Optimizado	
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Optimizado	
4,3	Determinación del alcance del SGSI		
4,3	Determinar y documentar el alcande del SGSI	Optimizado	El alcance ha sido definido correctamente.
4,4	SGSI		
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Optimizado	La organización ha implantado correctamente un SGSI que está en proceso de mejora continua.

5	**Liderazgo**		
5,1	**Liderazgo y compromiso**		
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Optimizado	Se ha comprobado que existe un gran compromiso por parte de la dirección en materia de seguridad de la información.
5,2	**Política**		
5,2	Documentar la Política de Seguridad de la Informacion	Optimizado	Existe definida una política de seguridad que está en constante mejora.
5,3	**Roles, responsabilidades y autoridades en la organización**		
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Optimizado	Existe un documento en el que se definen los roles y responsabilidades de todos los empleados de la organización respecto a la seguridad de la información.
6	**Planificación**		
6,1	**Acciones para tratar los riesgos y oportunidades**		
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Optimizado	Se ha realizado un análisis de riesgos para identificar los activos y valorarlos, identificar las posibles amenazas, el impacto de éstas y el riesgo de cada uno de los activos identificados, todo esto siguiendo una metodología documentada.
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Optimizado	Se ha realizado un análisis de riesgos que ha dado como resultado la valoración de los riesgos de la seguridad de la información de la organización.
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Administrado	Se han realizando proyectos para tratar los riesgos obtenidos. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
6,2	**Objetivos de seguridad de la información y planificación para su consecución**		
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Optimizado	Los objetivos de seguridad de la información son claros en la organización y existe una planificación para mejorar la seguridad con el fin de conseguir dichos objetivos.
7	**Soporte**		
7,1	**Recursos**		
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Definido	La disponibilidad de recursos es buena. Sin embargo, se puede mejorar.
7,2	**Competencia**		
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Administrado	Las competencias de cada uno están claramente definidas y se llevan a cabo correctamente. Sin embargo, puesto que el SGSI se acaba de poner
7,3	**Concienciación**		
7,3	Implementar un programa de concianciación de seguridad	Administrado	Se ha logrado la concienciación en materia de seguridad de todos los empleados de la organización. Sin embargo, puesto que el SGSI se
7,4	**Comunicación**		
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Administrado	Existe una buena comunicación respecto a la seguridad de la información. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100%
7,5	**Información documentada**		
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Repetible	Existe documentación de la información. Sin embargo, algunos de los procesos no están documentados formalmente.
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprovacion a los documentos	Repetible	Algunos de los documentos se actualizan periódicamente y se van creado nuevos, como documentos de pruebas. Sin embargo, no existe un procedimiento formal a seguir y cada empleados lo realiza a su manera
7.5.3	Mantener un control adecuado de la documentación	Repetible	Existe control de la información documentada., pero no de toda la información . No existe definida una manera clara de realizar el control de la información documentada referente a la seguridad de la información de la organización
8	**Operación**		
8,1	**Planificación y control operacional**		
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Administrado	Las operaciones y los requisitos de seguridad están planificadas y controladas. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
8,2	**Apreciación de los riesgos de seguridad de la información**		
8,2	Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios	Optimizado	Se ha realizado un análisis de riesgos que ha dado como resultado la valoración de los riesgos de la seguridad de la información de la organización.
8,3	**Tratamiento de los riesgos de seguridad de la información**		
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Administrado	Se han realizando proyectos para tratar los riesgos obtenidos. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.

9	**Evaluación del desempeño**		
9,1	**Seguimiento, medición, análisis y evaluación**		
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Administrado	Existe una planificación para llevar un seguimiento y evaluación del SGSI y se puede comprobar su evolución gracias a los controles implantados y los indicadores de dichos controles. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
9,2	**Auditoría interna**		
9,2	Planificar y realizar una auditoria interna del SGSI	Administrado	Existe un plan de realización de auditorías internas que ya se ha puesto en marcha y que se puede comprobar su evolución. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto

9,3	Revisión por la dirección		
9,3	La administración realiza una revision periodica del SGSI	Administrado	Existe planificado un plan de revisión del SGSI por la dirección y hay controles implantados respecto a este punto así como indicadores para comprobar su evolución. Sin embargo, puesto que el SGSI se acaba de
10	Mejora		
10,1	No conformidad y acciones correctivas		
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Administrado	Se identifican no conformidades y las respectivas acciones correctivas para corregirlas cuando se realizan las revisiones y auditorías. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha
10,2	Mejora continua		
10,2	Mejora continua del SGSI	Administrado	Existe un proceso definido de mejora continua. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.

TABLA 30 CONTROLES DE LA ISO 27001:2013

5.2. Resultados.

En este apartado se van a mostrar los resultados obtenidos en el apartado anterior en forma de gráficas. En primer lugar, en la Imagen, se muestra el porcentaje de madurez de los controles ISO 27002:2013 implantados en TECNOSOFT.

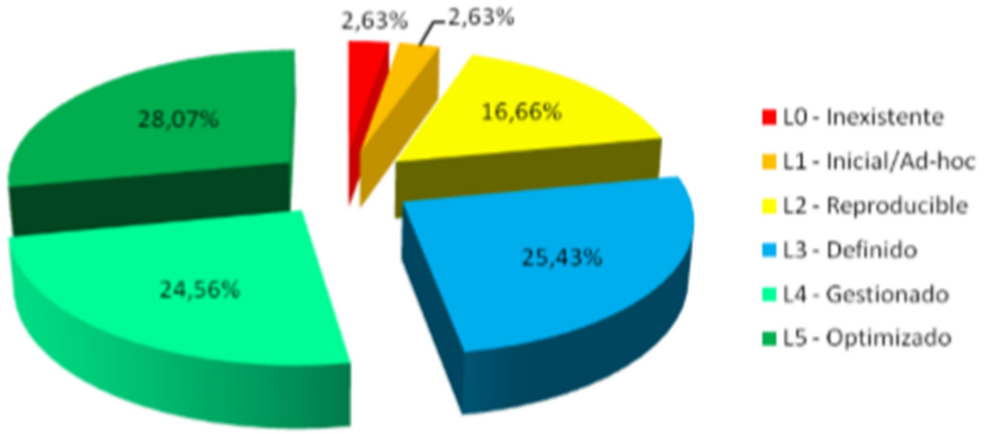

FIGURA 15: GRADO DE MADUREZ DE LOS CONTROLES ISO 27002:2013

Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	0%	0%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	0%	0%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	11%	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	4%	0%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	41%	0%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	44%	0%

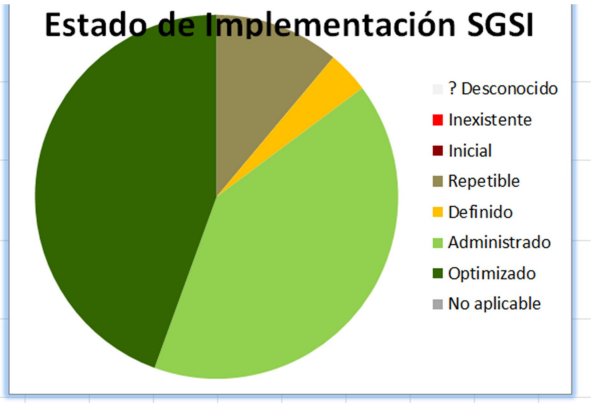

FIGURA 16: GRADO DE MADUREZ DE LOS CONTROLES ISO 27001:2013

Por otra parte, a partir de la Tabla 27 y conociendo la efectividad correspondiente a cada nivel CMM, se obtiene la Tabla 29, en la que se muestra el grado de madurez de cada uno de los controles y el total de cada uno de los dominios que forman parte de la ISO 27002:2013. Se observa que la efectividad de cada uno de los controles es significativamente mejor que la efectividad de dichos controles al inicio del proyecto, que aparecen en la Tabla3 y Figura 6

	Valor
A.5 Information security policies	5
A.6 Organization of information security	2,6
A.7 Human resource security	4,22
A.8 Asset management	3,22
A.9 Access control	3,88
A.10 Cryptography	3,5
A.11 Physical and environmental security	3,83
A.12 Operations security	3,36
A.13 Communications security	3,17
A.14 System acquisition, development and maintenance	2,93
A.15 Supplier relationships	3
A.16 Information security incident management	3,43
A.17 Information security aspects of business continuity management	2,17
A.18 Compliance	4,6

TABLA 31 GRADO DE MADUREZ DE LOS DOMINIOS ISO 27002:2013 TRAS AUDITORÍA

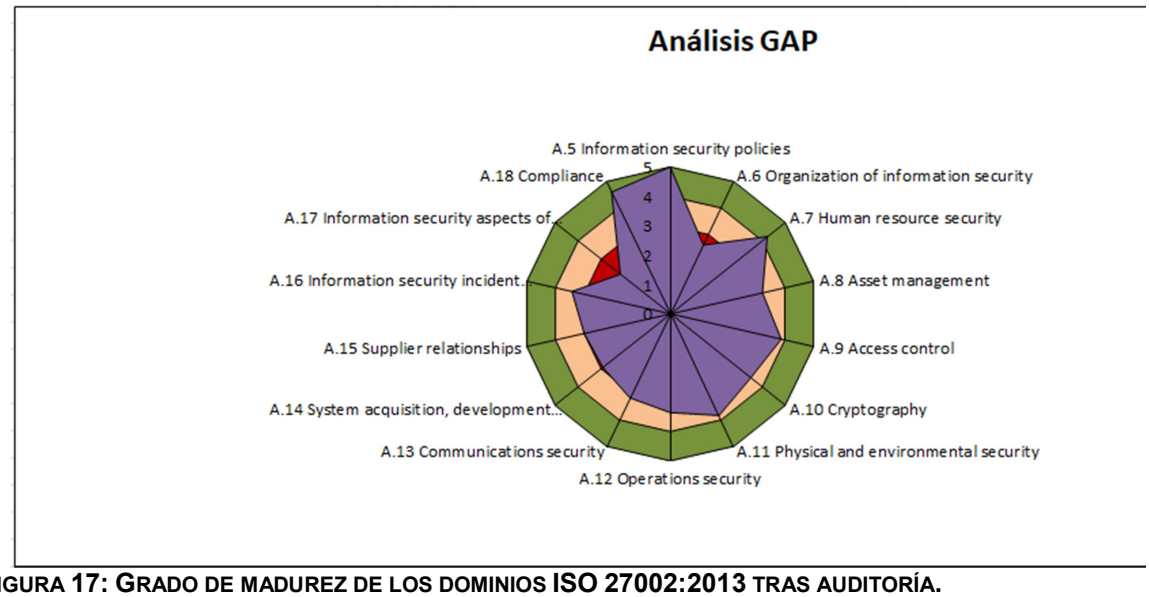

FIGURA 17: GRADO DE MADUREZ DE LOS DOMINIOS ISO 27002:2013 TRAS AUDITORÍA.

Comparando el nivel de madurez obtenido con el nivel de madurez que se planteó como objetivo al inicio del proyecto, vemos que el nivel obtenido se aproxima al objetivo, incluso lo sobrepasa en algunos dominios. Sin embargo, para otros dominios aún quedan mejoras que hacer para llegar al objetivo fijado.
Vemos que, en general, el estado obtenido de la mayoría de los dominios tras la auditoría es similar al esperado tras la realización de los proyectos. Asimismo, volvemos a observar que hay que seguir trabajando en la mejora de algunos dominios para conseguir alcanzar el objetivo fijado al principio de este proyecto.
En la Tabla 30 se muestra el grado de madurez de cada una de las secciones que forman parte de la ISO 27001:2013. Estos datos se han obtenido a partir de la Tabla 28 y de la efectividad de los niveles CCM. Se observa que la efectividad de cada una de las secciones es significativamente mejor que la efectividad de dichas secciones al inicio del proyecto.

ISO 27001:2013	Efectividad
4. Contexto de la Organización	100%
5. Liderazgo	100%
6. Planificación	98’75%
7. Soporte	75%
8. Operación	96’6%
9. Evaluación	95%
10.Mejora	95%

TABLA 32 GRADO DE MADUREZ ISO 27001:2013

Observamos que el estado obtenido de la ISO 27001:2013 es muy similar al objetivo que se planteó al principio del proyecto, incluso en algunas secciones es superior al objetivo planteado.

No conformidades con la norma ISO 27002:2013

A continuación, en la Tabla 31, se muestran las no conformidades (NC) con la norma ISO 27002:2013 encontradas durante la realización de la auditoría de cumplimiento así como las acciones correctivas recomendadas a seguir para mejorar el estado de los controles con no conformidades.

CONTROL	No Conformidad	Descripción	Acción Correctiva
Contacto con las autoridades	menor	No existe documento formal que indique el procedimiento a seguir para contactar con las autoridades. Tampoco existe una programación para realizar dicho contacto.	Definir un procedimiento a seguir para contactar con las autoridades así como planificar el momento de los contactos
Contacto con grupos de especial interés	menor	No existe documento formal que indique el procedimiento a seguir para contactar con grupos de interés. Tampoco existe una programación para realizar dicho contacto	Definir un procedimiento a seguir para contactar con los grupos de interés así como planificar el momento de los contactos.
Teletrabajo	mayor	No existe un documento formal en el que se describan las normas a seguir para	Definir un documento en el que se incluyan todas las normas a seguir cuando

		cuando se teletrabaja.	un empleado teletrabaje.
Devolución de activos	mayor	Las normas a seguir para llevar a cabo la devolución de activos no es claro y no existe un indicador con el que se pueda controlar si estas normas se están cumpliendo.	Elaborar un nuevo documento con las normas bien explicadas e implantar un indicador para comprobar si la devolución de los activos se está realizando correctamente.
Clasificación de la información	mayor	No existe un documento en el que se indiquen los criterios a seguir para clasificar los activos.	Redactar un documento en el que se encuentren definidas las directrices de clasificación de los activos de la organización
Etiquetado de la información	mayor	No están definidas en ningún sitio las directrices de etiquetado de los activos.	Redactar un documento con las directrices a seguir para el etiquetado de los activos. Revisar y mejorar las normas de tratamiento de la información
Gestión de medios extraíbles.	Menor	No es posible conocer que se está aplicando correctamente el control.	Implantar un indicador para medir la evolución de este control
Disposición de medios.	Mayor	No existe ningún procedimiento a seguir para llevar a cabo la eliminación de soportes extraíbles.	Implantar un procedimiento claro de eliminación de soportes extraíbles.
Gestión de la información de autenticación secreta de los usuarios.	Mayor	No existe un documento en el que se defina cómo gestionar la información confidencial de autenticación de usuarios.	Redactar el documento en el que definan las normas referentes al uso de información confidencial en la autenticación de usuario.

Revisión de los derechos de acceso de los usuarios.	Mayor	No existe un documento en el que se especifique cuándo ni cómo se revisan los derechos de acceso de los usuarios	Redactar el documento en el que se incluya quién es el encargado de revisar los derechos de acceso de los usuarios, cada cuánto se lleva a cabo la revisión y cómo se realiza.
Eliminación o ajuste de los derechos de acceso.	Mayor	No existe un documento en el que se explique el procedimiento a seguir para retirar o adaptar los derechos de acceso de los usuarios.	Redactar el documento en el que se incluya quién es el encargado de modificar los derechos de acceso de los usuarios, en qué momento y cómo se realiza.
Procedimientos de inicio de sesión seguros	Menor	No existen indicadores para comprobar que los procedimientos seguros de inicio de sesión están funcionando correctamente.	Implantar indicadores para medir este control a lo largo del tiempo.
Gestión de claves.	Menor	No existen indicadores para comprobar la evolución de la gestión de claves.	Implantar indicadores para medir este control a lo largo del tiempo.
Trabajando en áreas seguras. Áreas de entrega y carga.	Mayor	No existe un documento formal.	Redactar un documento formal para cada uno de estos controles e informar a todos los empleados de su existencia
Seguridad de equipos y activos fuera de las instalaciones.	Mayor	No existe un documento en el que se especifiquen las medidas de seguridad a tomar para cuando se saca un activo fuera de las instalaciones de la organización.	Redactar el documento con las normas a seguir e informar a todos los empleados de estas normas.
Procedimientos operativos	Mayor	No existe un documento formal donde se encuentren documentados los	Redactar un documento con los procedimientos de operación.

documentados.		procedimientos operativos.	
Gestión del Cambio.	Mayor	No existe ningún proceso formal para controlar los cambios que afectan a la seguridad de la información de la organización.	Crear registros con los cambios que se vayan realizando.
Gestión de la Capacidad.	Mayor	Falta de evidencias de que con los registros obtenidos de la monitorización se ajuste el uso de los recursos de los sistemas.	Implantar indicadores para comprobar el uso de los recursos de los sistemas.
Gestión de vulnerabilidades técnicas.	Mayor	No existe un proceso para identificar las vulnerabilidades técnicas del software.	Implantar un proceso automático que identifique las vulnerabilidades del software existente.
Controles de red.	Mayor	No existe un procedimiento a seguir ni ninguna planificación para realizar los controles de la red.	Planificar y ejecutar controles de red de manera periódica.
Seguridad de los servicios de red.	Mayor	No existen mecanismos de seguridad asociados a servicios de red.	Contratar una segunda conexión con otro proveedor para conseguir redundancia.
Revisión técnica de aplicaciones después de la plataforma operativa.	Mayor	No existe un procedimiento a seguir tras haber realizado cambias en el sistema operativo de algún equipo de la organización.	Establecer un procedimiento a seguir para cuando se realizan cambios en los sistemas operativos y realizarlo cada vez que se realiza un cambio en el sistema operativo de un equipo de la organización.
Sistema seguro de principios de ingeniería	Mayor	No existe un documento en el que se establezcan los principios de seguridad en ingeniería de sistemas	Redactar un documento con los principios de seguridad en ingeniería de sistemas.
Pruebas de aceptación del	Mayor	No existe un documento formal que indique la metodología	Redactar un documento con los pasos a seguir a la hora

sistema		a seguir para realizar las pruebas de los desarrollos.	de realizar las pruebas necesarias a los desarrollos.
Gestión de cambios en los servicios del proveedor.	Mayor	No existe un proceso formal de administración de cambios en los servicios prestados por los proveedores.	Definir el proceso de administración de cambios en los servicios prestados por proveedores.
Evaluación y decisión sobre eventos de seguridad de la información.	Mayor	No existen directrices para clasificar los incidentes de seguridad según su importancia o prioridad.	Definir los criterios de valoración de incidencias así como las directrices a seguir para clasificarlas de la manera más eficiente posible.
Recogida de pruebas.	Mayor	No existe un documento en el que se especifique cuándo hay que recoger evidencias ni cómo se debe hacer.	Redactar un documento con el procedimiento a seguir para recopilar evidencias e informar a todos los empleados de este documento y de la importancia de la recopilación.

TABLA 33 NO CONFORMIDADES CON LA NORMA ISO 27002:2013

No conformidades con la norma ISO 27001:2013

A continuación, en la Tabla 33, se muestran las no conformidades (NC) con la norma ISO 27001:2013 encontradas durante la realización de la auditoría de cumplimiento así como las acciones correctivas recomendadas a seguir para mejorar el estado de las secciones con no conformidades.

CONTROL	No Conformidad	Descripción	Acción Correctiva
Recursos	menor	La disponibilidad de recursos es mejorable.	Se debe mejorar la disponibilidad de los recursos de la organización.
Proveer documentación requerida por el estándar más la requerida por la organización	Mayor	Algunos de los procesos no están documentados formalmente	Documentar todos los procesos relacionados con la seguridad de la información que se lleven a cabo en la organización.
Proveer un título, autor, formato consistente, revisión y	mayor	No existe un procedimiento formal a seguir para la creación	Definir un procedimiento a seguir para la creación y

aprobación a los documentos		y actualización de documentos.	actualización de documentos.
Mantener un control adecuado de la documentación	mayor	No existe definida una manera clara de realizar el control de la información documentada referente a la seguridad de la información de la organización.	Definir el procedimiento a seguir para realizar el control de la documentación

TABLA 34 NO CONFORMIDADES CON LA NORMA ISO 27001:2013

5.5. Conclusiones.

Comparando el nivel de madurez obtenido con el nivel de madurez que se planteó como objetivo al inicio del proyecto, vemos que el nivel obtenido se aproxima al objetivo, incluso lo sobrepasa en algunos dominios. Sin embargo, para otros dominios aún quedan mejoras que hacer para llegar al objetivo fijado.
Vemos que, en general, el estado obtenido de la mayoría de los dominios tras la auditoría es similar al esperado tras la realización de los proyectos. Asimismo, volvemos a observar que hay que seguir trabajando en la mejora de algunos dominios para conseguir alcanzar el objetivo fijado al principio de este proyecto.
En la Tabla 30 se muestra el grado de madurez de cada una de las secciones que forman parte de la ISO 27001:2013. Estos datos se han obtenido a partir de la Tabla 28 y de la efectividad de los niveles CCM. Se observa que la efectividad de cada una de las secciones es significativamente mejor que la efectividad de dichas secciones al inicio del proyecto.

6. CONCLUSIONES

6.1. Introducción.

Tras haber realizado con éxito todas las fases anteriores, se puede concluir que se han cumplido los objetivos propuestos al inicio de este proyecto, es decir, mejorar la seguridad de la información de la organización gracias a la implementación de un Plan de Seguridad.

6.2. Objetivos de la Fase.

Se ha establecido el estado inicial de la seguridad de la información de la organización así como los objetivos a alcanzar tras la implantación del SGSI.

Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2013.
Como evidencia el análisis diferencial realizado al inicio de este proyecto, la organización, aunque contaba con múltiples controles de seguridad específicos, no se englobaban en un SGSI que involucrara a todos sus estamentos, ni disponía de buena parte de los mecanismos formales que se deben contemplar en un sistema de gestión de seguridad de la información.

Tras la realización de las actividades descritas en el proyecto, se puede concluir que su objetivo principal, puesta en marcha del SGSI, de manera que la seguridad se tenga en cuenta en todos los procesos de la organización y, por tanto, mejorar la seguridad global de la organización, ha sido plenamente conseguido.
La implementación del SGSI de TECNOSOFT se ha realizado siguiendo las directrices de la norma ISO/IEC 27001:2013 y el código de buenas prácticas que describe la norma ISO/IEC 27002:2013, que establece una serie de puntos a desarrollar y cumplir.
Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información.
Existe el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

Buena parte de esos puntos se han alcanzado.
A continuación mostramos los objetivos conseguidos y aspectos pendientes.

6.2.1 Objetivos conseguidos.

Entre los objetivos podemos destacar:

- Se ha definido y se ha puesto en marcha un SGSI del que inicialmente carecía la organización.
- Se ha definido y desarrollado el esquema documental necesario para sustentar el SGSI.
- Se ha definido la metodología y se ha realizado el análisis de riesgos necesario para evaluar las amenazas que afectan a distintos activos de la organización.
- Se han definido y ejecutado diversos proyectos, tanto tecnológicos como organizativos y de gestión, que han permitido mejorar la seguridad global de la organización.
- Se ha mejorado la formación y concienciación de todos los empleados de la organización, lo que a su vez contribuye a disminuir los riesgos y mejorar la seguridad de la organización.
- Se han definido los roles y responsabilidades relativas a seguridad de la información.
- Se han definido indicadores para evaluar el cumplimiento de los controles de seguridad definidos.

6.2.2. Aspectos pendientes.

Es necesario avanzar en el desarrollo del SGSI en los siguientes aspectos:

- Definir e implementar la política de seguridad de proveedores.
- Definir e implementar procedimientos para la correcta gestión de la seguridad desde el punto de vista de los recursos humanos.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información: RRHH, TI, etc…
- Identificar distintas áreas y clasificarlas en función de sus necesidades en cuanto a seguridad.
- Definir e implementar procedimientos para la autorización de retirada de materiales de las oficinas.

Adicionalmente, no debemos perder de vista el hecho de que el SGSI se debe contemplar bajo un modelo de mejora continua, de manera que se debe revisar y evaluar periódicamente, y cuando se detecten deficiencias, se deben de tomar las medidas correctoras que garanticen la seguridad y protección de la información.

6.3. Presentación de resultados.

Como resultado del trabajo Fin de Máster se han generado los siguientes entregables:

- Memoria del proyecto, que es este documento. Incluye los anexos indicados en el índice.
- Resumen ejecutivo. Documento adicional, que muestra las principales conclusiones del proyecto.
- Presentación a la dirección. Documento adicional, que incluye conceptos de seguridad con el objetivo de concienciar y sensibilizar al personal en materia de seguridad de la información.
- Presentación con el resumen del estado del proyecto.

- Vídeo de presentación del proyecto. Describe las distintas etapas y el proceso llevado a cabo para la realización del TFM

7. ANEXOS.

7.1. ANEXO I tabla ISO 27001:2013.

Estado de Implementación ISO 27001

Sección	Requerimientos ISO 27001	Estado	
4	**Contexto de la organización**		
4,1	**Comprensión de la organización y de su contexto**		
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial	
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**		
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Repetible	
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Repetible	
4,3	**Determinación del alcance del SGSI**		
4,3	Determinar y documentar el alcande del SGSI	Definido	
4,4	**SGSI**		
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Definido	
5	**Liderazgo**		
5,1	**Liderazgo y compromiso**		
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Definido	
5,2	**Política**		
5,2	Documentar la Política de Seguridad de la Informacion	Definido	

5,3	**Roles, responsabilidades y autoridades en la organización**	
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Definido
6	**Planificación**	
6,1	**Acciones para tratar los riesgos y oportunidades**	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Definido
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Definido
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Definido
6,2	**Objetivos de seguridad de la información y planificación para su consecución**	
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Repetible
7	**Soporte**	
7,1	**Recursos**	
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Definido
7,2	**Competencia**	
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Definido
7,3	**Concienciación**	
7,3	Implementar un programa de concianciación de seguridad	Repetible
7,4	**Comunicación**	
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Repetible
7,5	**Información documentada**	
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Inicial
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprovacion a los documentos	Inicial
7.5.3	Mantener un control adecuado de la documentación	Inicial
8	**Operación**	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Repetible
8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios	Repetible

8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Repetible
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Repetible
9,2	**Auditoría interna**	
9,2	Planificar y realizar una auditoria interna del SGSI	Definido
9,3	**Revisión por la dirección**	
9,3	La administración realiza una revision periodica del SGSI	Definido
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

27

TABLA 35: TABLA ISO 27001:2013

7. 2. ANEXO II tabla ISO 27002:2013

CONTROL				Valor	Total
A.5 Information security policies					4
	A.5.1 Management direction for information security				4
		A.5.1.1	Policies for information security	4	
		A.5.1.2	Review of the policies for informatio security	4	
A.6 Organization of information security					1
	A.6.1 Internal organization				2
		A.6.1.1	Information security roles and responsibilities	3	
		A.6.1.2	Segregation of duties	3	
		A.6.1.3	Contact with authorities	4	
		A.6.1.4	Contact with special interest groups	0	
		A.6.1.5	Information security in project management	0	
	A.6.2 Mobile devices and teleworking				0
		A.6.2.1	Mobile device policy	0	
		A.6.2.2	Teleworking	0	
A.7 Human resource security					1,333333333
	A.7.1 Prior to employment				0
		A.7.1.1	Screening	0	
		A.7.1.2	Terms and conditions of employment	0	
	A.7.2 During employment				0
		A.7.2.1	Management responsibilities	0	
		A.7.2.2	Information security awareness, education and training	0	
		A.7.2.3	Disciplinary process	0	
	A.7.3 Termination and change of employment				4
		A.7.3.1	Termination or change of employment responsibilities	4	
A.8 Asset management					0
	A.8.1 Responsibility for asset				0
		A.8.1.1	Inventory of assets	0	
		A.8.1.2	Ownership of assets	0	
		A.8.1.3	Acceptable use of assets	0	
		A.8.1.4	Return of assets	0	
	A.8.2 Information classification				0
		A.8.2.1	Classification of information	0	
		A.8.2.2	Labelling of informa tion	0	

		A.8.2.3	Handling of assets	0	
	A.8.3 Media handling				0
		A.8.3.1	Management of removable media	0	
		A.8.3.2	Disposal of media	0	
		A.8.3.3	Physical media transfer	0	
A.9 Access control					3,525
	A.9.1 Business requirements of access control				4
		A.9.1.1	Access control policy	5	
		A.9.1.2	Access to networks and network services	3	
	A.9.2 User access management				4,5
		A.9.2.1	User registration and de-registration	5	
		A.9.2.2	User access provisioning	4	
		A.9.2.3	Management of privileged access rights	4	
		A.9.2.4	Management of secret authentication information of users	4	
		A.9.2.5	Review of user access rights	5	
		A.9.2.6	Removal or adjustment of access rights	5	
	A.9.3 User responsibilities				4
		A.9.3.1	Use of secret authentication information	4	
	A.9.4 System and application access control				1,6
		A.9.4.1	Information access restriction	4	
		A.9.4.2	Secure log-on procedures	1	
		A.9.4.3	Password managment system	1	
		A.9.4.4	Use of privileged utility programs	1	
		A.9.4.5	Access control to program source code	1	
A.10 Cryptography					
	A.10.1 Cryptographic controls				4
		A.10.1.1	Policy on the use of cryptographic controls	4	
		A.10.1.2	Key management	4	
A.11 Physical and environmental security					0
	A.11.1 Secure areas				0
		A.11.1.1	Physical security perimeter	0	
		A.11.1.2	Physical entry controls	0	
		A.11.1.3	Securing offices, rooms and facilities	0	
		A.11.1.4	Protecting against external and environmental threats	0	
		A.11.1.5	Working in secure areas	0	
		A.11.1.6	Delivery and loading areas	0	
	A.11.2 Equipment				0
		A.11.2.1	Equipment siting and protection	0	
		A.11.2.2	Supporting utilities	0	
		A.11.2.3	Cabling security	0	
		A.11.2.4	Equipment maintenance	0	
		A.11.2.5	Removal of assets	0	
		A.11.2.6	Security of equipment and assets off-premises	0	
		A.11.2.7	Secure disposal or reuse of equipment	0	
		A.11.2.8	Unattended user equipment	0	

		A.11.2.9	Clear desk and clear screen policy	0	
A.12 Operations security					2,142857143
	A.12.1 Operational procedures and responsibilities				5
		A.12.1.1	Documented operating procedures	5	
		A.12.1.2	Change management	5	
		A.12.1.3	Capacity management	5	
		A.12.1.4	Separation of development, testing and operational environments	5	
	A.12.2 Protection from malware				0
		A.12.2.1	Controls against malware	0	
	A.12.3 Backup				5
		A.12.3.1	Information backup	5	
	A.12.4 Logging and monitoring				0
		A.12.4.1	Event logging	0	
		A.12.4.2	Protection of log information	0	
		A.12.4.3	Administrator and operator logs	0	
		A.12.4.4	Clock synchronisation	0	
	A.12.5 Control of operational software				4
		A.12.5.1	Installation of software on operational systems	4	
	A.12.6 Technical vulnerability management				0
		A.12.6.1	Management of technical vulnerabilities	0	
		A.12.6.2	Restrictions on software installation	0	
	A.12.7 Information systems audit considerations				1
		A.12.7.1	Information systems audit controls	1	
A.13 Communications security					1,5
	A.13.1 Network security management				3
		A.13.1.1	Network controls	3	
		A.13.1.2	Security of network services	3	
		A.13.1.3	Segregation in networks	3	
	A.13.2 Information transfe				0
		A.13.2.1	Information transfer policies and procedures	0	
		A.13.2.2	Agreements on information transfer	0	
		A.13.2.3	Electronic messaging	0	
		A.13.2.4	Confidentiality or nondisclosure agreements	0	
A.14 System acquisition, development and maintenance					0,888888867
	A.14.1 Security requirements of information systems				0
		A.14.1.1	Information security requirements analysis and specification	0	
		A.14.1.2	Securing application services on public networks	0	
		A.14.1.3	Protecting application services transactions	0	
	A.14.2 Security in development and support processes				2,6666666
		A.14.2.1	Secure development policy	2	
		A.14.2.2	System change control procedures.	4	
		A.14.2.3	Technical review of applications after operating platform	3	
		A.14.2.4	Restrictions on changes to software packages	3	
		A.14.2.5	Secure system engi neering principles	2	
		A.14.2.6	Secure development environment	3	

		A.14.2.7	Outsourced development	1	
		A.14.2.8	System security testing	3	
		A.14.2.9	System acceptance testing	3	
	A.14.3 Test data				0
		A.14.3.1	Protection of test data	0	
A.15 Supplier relationships					2,8333333
	A.15.1 Information security in supplier relationships				2,6666666
		A.15.1.1	Information security policy for supplier relationships	4	
		A.15.1.2	Addressing security within supplier agreements	4	
		A.15.1.3	Information and communication technology supply chain	0	
	A.15.2 Supplier service delivery management				3
		A.15.2.1	Monitoring and review of supplier services	3	
		A.15.2.2	Managing changes to supplier services	3	
A.16 Information security incident management					3,14
	A.16.1 Management of information security incidents and improvements				3,14
		A.16.1.1	Responsibilities and procedures	3	
		A.16.1.2	Reporting information security events	3	
		A.16.1.3	Reporting information security weaknesses	3	
		A.16.1.4	Assessment of and decision on information security events	3	
		A.16.1.5	Response to information security incidents	3	
		A.16.1.6	Learning from information security incidents	3	
		A.16.1.7	Collection of evidence	4	
A.17 Information security aspects of business continuity management					2,5
	A.17.1 Information security continuity				4
		A.17.1.1	Planning information security continuity	4	
		A.17.1.2	Implementing information security continuity	4	
		A.17.1.3	Verify, review and evaluate information security continuity	4	
	A.17.2 Redundancies				1
		A.17.2.1	Availability of infor mation processing facilities	1	
A.18 Compliance					0,9666665
	A.18.1 Compliance with legal and contractual requirements				0,6
		A.18.1.1	Identification of applicable legislation and contractual requirements	0	
		A.18.1.2	Illectual property rights	0	
		A.18.1.3	Protection of records	2	
		A.18.1.4	Privacy and protection of personally identifiable information	1	
		A.18.1.5	Regulation of cryptographic controls	0	
	A.18.2 Information security reviews				1,333333
		A.18.2.1	Independent review of information security	1	
		A.18.2.2	Compliance with security policies and standards	2	
		A.18.2.3	Technical compliance review	1	

TABLA 36 TABLA ISO 27002:2013

7.3. ANEXO III Informe de Auditoría.

1. INTRODUCCION

Este informe de auditoría interna pretende determinar el grado de cumplimiento del Sistema de Gestión de Seguridad TECNOSOFT con la norma ISO/IEC 27001:2013.
Es el resultado de la primera auditoría interna del SGSI de TECNOSOFT que se realiza como parte del plan de auditoría establecido por la organización para la implantación y mejora de su SGSI.

2. ALCANCE

El plan Director de Seguridad que se desea implantar en TENOSOFT pretende adecuar a la norma ISO/IEC 27001:2013 todos los procesos y procedimientos tanto organizativos como técnicos relacionados con los Sistemas de Información de la organización.
Esta auditoría abarca todos los Sistemas de Información que incluye el SGSI de TECNOSOFT que son:

- Servicios Financieros.
- Recursos Humanos.
- Tecnologías de la información.

La auditoría se realiza sobre todos los dominios y controles que establece la norma ISO/IEC 27001:2013

3. CRITERIOS.

Esta auditoría sigue los criterios establecidos por:

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

4. PLAN DE AUDITORÍA.

La auditoría de cumplimiento se ha realizado conforme a la siguiente planificación:

Primer Trimestre:

- Auditoría de las Políticas de Seguridad.

Auditoría de la Organización de la Seguridad de la Información.

- Auditoría de la Seguridad relacionada con RRHH.

Segundo Trimestre:

- Auditoría de la Gestión de Activos.
- Auditoría de Control de los accesos.
- Auditoría del Cifrado.
- Auditoría de la Seguridad Física y Ambiental.
- Auditoría de la Seguridad de la Operativa.
- Auditoría de la Seguridad de las Comunicaciones.

Tercer Trimestre:

- Auditoría de la gestión y Mantenimiento de los SI.
- Relaciones con proveedores.
- Auditoría de la gestión de incidentes de la seguridad de la información.

Cuarto Trimestre:

- Auditoría de seguridad de la información en gestión de la continuidad del negocio.

Auditoría del Cumplimiento.

5. REGISTROS DE AUDITORÍA.

a) Documentación consultada.

Para la realización de esta auditoría se ha consultado la siguiente documentación:

- Contexto, requerimientos y alcance del SGSI
- Declaración de aplicabilidad.
- Roles y Responsabilidades de Seguridad.
- Inventario de activos.
- Plan de continuidad de negocio.
- Análisis de Riesgos.
- Política de Seguridad.
- Política de control de acceso.
- Política de seguridad de dispositivos móviles.
- Política de uso aceptable de activos.
- Política de contraseñas.
- Procedimiento de gestión de incidentes.
- Procedimiento de Continuidad del negocio.
- Procedimiento de operación de TI.

b) Personal entrevistado.

El siguiente personal ha sido entrevistado durante la auditoría de cumplimiento.

- Responsable de Seguridad
- Responsable de RRHH
- Responsable de TI
- Personal de Desarrollo

6. RESULTADO DE AUDITORÍA.

A continuación se muestran los hallazgos de auditoría detectados para los requerimientos ISO 27001:2013. Se contemplan dos tipos de hallazgos:
No Conformidad Mayor. Incumplimiento de un requisito normativo que vulnera o pone en serio riesgo la integridad del Sistema de Gestión.
No Conformidad Menor. Desviación mínima en relación a los requisitos normativos que no afecta a la eficiencia e integridad del Sistema de Gestión.

No Conformidades Mayores serían:

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
7	Soporte		
7.5	Información documentada	No Conformidad mayor	No está cumplimentada toda la información requerida. Requerimientos legales y contractuales y algunos procedimientos operacionales
8	Operación		
8.1.	Planificación y control operacional	No Conformidad mayor	No se planifican y controlan acciones para el tratamiento de riesgos.

8.3	Tratamiento de los riesgos de seguridad de la información	No Conformidad mayor	No hay evidencia de información documentada de los resultados de tratamiento de los riesgos residuales.
9	Evaluación del desempeño		
9.1.	Seguimiento, medición, análisis y evaluación	No Conformidad mayor	No están documentadas evidencias de seguimiento medición, análisis y evaluación del desempeño del sistema de gestión.

TABLA 37 TABLA DE NO CONFORMIDADES MAYORES.

No Conformidades Menores serían

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
4	Contexto de la organización		
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	No Conformidad menor	No está cumplimentados todos os requisitos legales y contractuales
6	Planificación		
6.1.	Acciones para tratar los riesgos y oportunidades	No Conformidad menor	No están documentados los criterios para llevar a cabo apreciaciones de riesgo
7	Soporte		
7.2	Competencia	No Conformidad menor	No están documentadas las evidencias de competencia.
8	Operación		
8.2	Apreciación de riesgos de seguridad de la información	No Conformidad menor	No hay evidencias de los resultados de apreciación de riesgo

TABLA 38 TABLA DE NO CONFORMIDADES MENORES.

7. OPORTUNIDADES DE MEJORA.

Es necesario avanzar en el desarrollo del SGSI en los siguientes aspectos:

- Definir e implementar la política de seguridad de proveedores.

- Definir e implementar procedimientos para la correcta gestión de la seguridad desde el punto de vista de los recursos humanos.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información: RRHH, TI, etc…
- Identificar distintas áreas y clasificarlas en función de sus necesidades en cuanto a seguridad.
- Definir e implementar procedimientos para la autorización de retirada de materiales de las oficinas.

Adicionalmente, no debemos perder de vista el hecho de que el SGSI se debe contemplar bajo un modelo de mejora continua, de manera que se debe revisar y evaluar periódicamente, y cuando se detecten deficiencias, se deben de tomar las medidas correctoras que garanticen la seguridad y protección de la información.

8. PLANIFICACION DE LA FUTURA AUDITORÍA.

Se aconseja seguir el plan de auditoría definido en TECNOSOFT y realizar una nueva auditoría interna en el primer semestre del 2020.
El período de tiempo hasta esa nueva auditoría se debe utilizar para definir nuevos proyectos orientados a la mejora del SGSI , y en concreto a las oportunidades de mejora identificadas en el punto anterior.
Se aconseja priorizar y definir dichos proyectos de mejora para su implantación en un espacio temporal que permita evaluar su impacto en el SGSI en la siguiente auditoría de cumplimiento.

Glosario

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Activo: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditor: Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización y su justificación, así como la justificación de las exclusiones de controles.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evidencia: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Impacto: El coste para la empresa de un incidente, que puede o no ser medido en términos estrictamente financieros.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

ISO/IEC 27000: Revisión de los estándares de la serie 27000.

ISO/IEC 27001: Especificaciones para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27002: Código de buenas prácticas en la gestión de la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten ser protegidos de potenciales riesgos.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.

PDCA (plan-do-check-act): Método de mejora continua de la calidad. También conocido como ciclo Deming.

No repudio: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Plan de continuidad de negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Proceso: Conjunto de actividades que transforman unas entradas en salidas.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Mecanismo de protección frente a las amenazas. Existen diferentes tipos dependiendo si se desea prevenir o corregir un incidente.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza

Referencias:

[1]http://www.isaca.org/chapters7/Madrid/Certification/Pages/Page2.aspx
[2] WIKIPEDIA
[3]HTtps://www.isaca.org/info/certificationlanding/cisa/cisa.html?cid=SEM_1226586&appeal=sem&gclid=EAIaIQob
ChMIseaR-tb03QIV1vhRCh0SAw_KEAAYASAAEgKENPD_BwE&gclsrc=aw.ds
[4]http://www.isaca.org/chapters7/Madrid/Certification/Pages/Page3.aspx
[5] http://www.isaca.org/chapters7/Madrid/Certification/Pages/Page4.aspx
[6] http://www.intedya.com/internacional/513/noticia-iso-20000-vs-itil.html
[7] https://cursos.com/seguridad-informacion-profesion-futuro/
[8] https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf.
[9] http://evaluries.blogspot.com/
[10] Recursos UOC
[11] https://www.isaca.org/
[12]http://compromiso.sena.edu.co/imagenes/files_upload_3/files/Gestion%20del%20riesgo%20-%20Identificacion%20de%20peligros.pdf