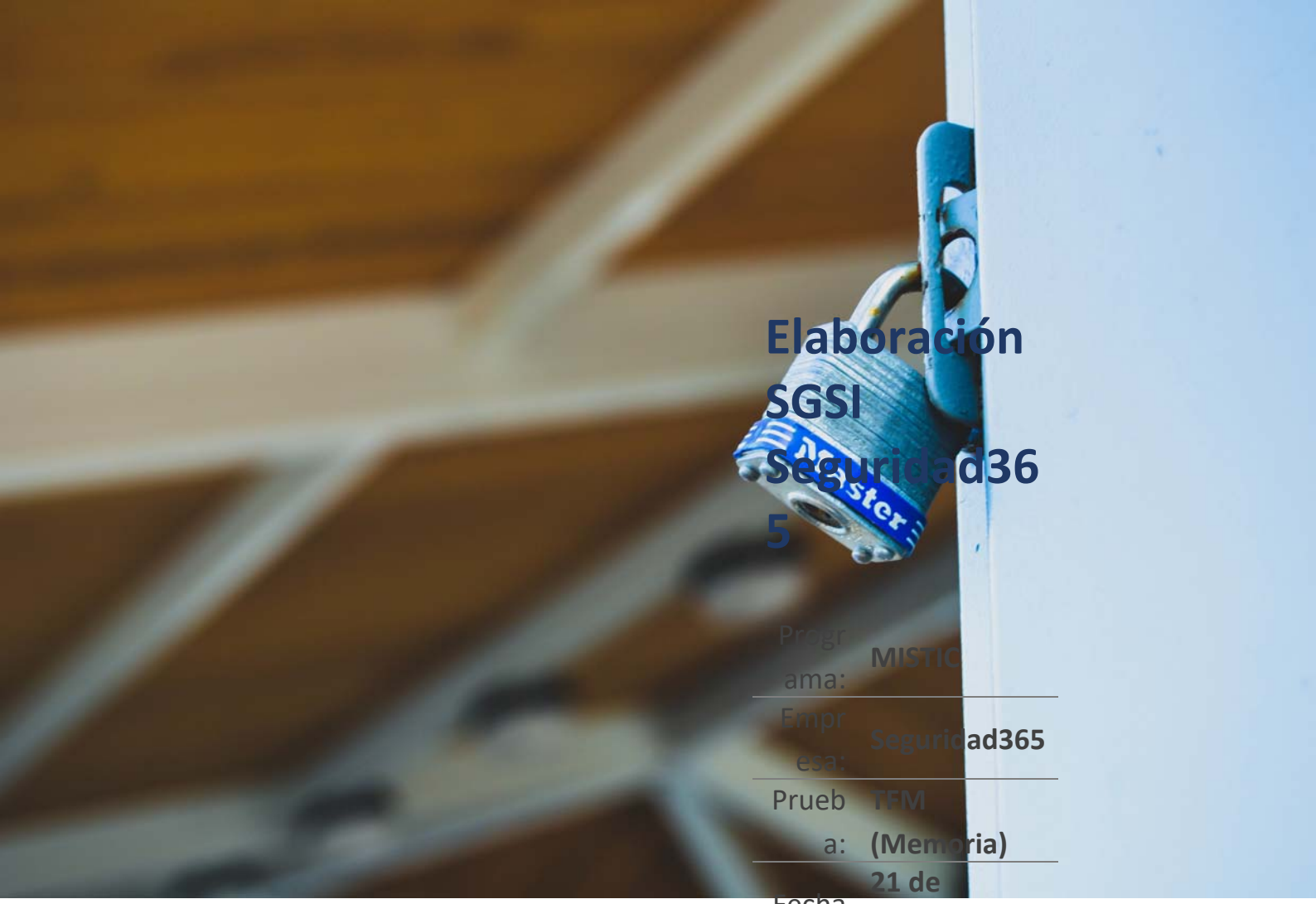

Elaboración SGSI Seguridad365

Programa:	MISTIC
Empresa:	Seguridad365
Prueba:	TFM (Memoria)
Fecha:	21 de diciembre de 2018
Alumno:	José Alberto Catalá Hernansáiz
Universidad:	Universidad Oberta de Cataluña
Consultor:	Antonio José Segovia Henares

UOC
Universitat Oberta de Catalunya

UOC
Universitat Oberta de Catalunya

UAB
Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB
Universitat de les Illes Balears

AGRADECIMIENTOS

A mi mujer y mis hijos. Esas personas a las que tanto quiero y las que tanto tiempo he quitado para sacar adelante este Master.

Y como no, a todos los consultores que siempre han tenido unas palabras de ánimo en esos momentos a los que a uno le fallan las fuerzas.

¡¡¡A todos, muchas gracias!!!

RESUMEN

El proyecto consiste en la elaboración del plan de implementación de un Sistema de Gestión de Seguridad de la Información para una empresa imaginaria (Seguridad365) dedicada a la prestación de servicios de seguridad privada.

El proyecto se ha desarrollado de forma incremental y se ha vertebrado en seis fases, y dando como resultado los siguientes entregables:

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

Para la elaboración del SGSI he utilizado la norma ISO/IEC 27001:2013. Para la elaboración del Análisis de Riesgo he utilizado la metodología Magerit.

Como resultado, la compañía Seguridad365 contaría con un SGSI y estaría preparada para la certificación en la norma ISO/IEC 27001.

ABSTRACT

The project consists in the development of the implementation plan of an Information Security Management System for an imaginary company (Seguridad365) dedicated to delivery of private security services.

The project has been developed incrementally and has been structured in six phases, and resulting in the following deliverables:

- Gap Analysis report
- Documents scheme ISO/IEC 27001
- Risk Assessment
- Project plan
- Compliance audit results
- Conclusion and results

For the development of the ISMS I have used the ISO/IEC 27001: 2013 standard. For the development of the Risk Assessment I have used the Magerit methodology.

As a result, Seguridad365 have an ISMS and would be prepared for ISO / IEC 27001 certification.

Contenido

Ilustraciones

1. Contextualización, Objetivos y Análisis Diferencial

1.1. Introducción

El objetivo del presente documento es fijar las directrices en materia de Seguridad de la Información, en las que se basa el Sistema de Gestión de Seguridad de la Información (SGSI) corporativo de Seguridad365, S.A.

Por otra parte, la consecución de este objetivo se planta como un ciclo de mejora continua (PDCA). De esta manera se espera fijar progresivamente las medidas de protección que permitan minimizar lo máximo posible el riesgo residual asumido por la compañía.

Se trata pues del Documento Marco en materia de seguridad de la información, que incluye a su vez referencias a todos y cada uno de las normativas y procedimientos que dan forma a dicho SGSI.

1.2. Contexto normativo

Aunque existe alguna otra organización que desarrolla estándares para el desarrollo del SGSI, sin duda alguna, la norma desarrollada por la *International Organization for Standardization* (ISO) es la más extendida y la norma elegida por Seguridad365 para el desarrollo de su SGSI.

La familia de normas ISO/IEC 27000 recoge distintas normas, siendo las siguientes las más representativas para el desarrollo del SGSI y las que se aplicarán para el desarrollo de este.

- ISO/IEC 27001. Contiene las especificaciones para la implantación del SGSI. Proviene en origen de la BS 7799-2:2002. Desde entonces ha pasado por distintas versiones, siendo su última versión vigente la ISO/IEC 27001:2013.
- ISO/IEC 27002. Contiene el código de buenas prácticas en la gestión de la Seguridad de la Información. Proviene de la BS 7799 parte 1 y la ISO/IEC 17799. Como la ISO/IEC 27001 ha sido actualizada, siendo la versión vigente la ISO/IEC 27002:2013.

El SGSI se estructura en torno a los 14 dominios y 35 objetivos de la ISO/IEC 27001:2013. De la misma manera se utilizará esta estructura en la Declaración de Aplicabilidad, de forma que se podrá dar una visión alineada estructuralmente.

A continuación, se muestran los dominios de control del Anexo A de la ISO/IEC 27001:2013 que se desarrollan en el SGSI:

- ✓ ***A.5:*** Políticas de Seguridad de la Información.
- ✓ ***A.6:*** Organización de la Seguridad de la Información.
- ✓ ***A.7:*** Seguridad relativa a los Recursos Humanos.
- ✓ ***A.8:*** Gestión de Activos.
- ✓ ***A.9:*** Control de Acceso.
- ✓ ***A.10:*** Criptografía.
- ✓ ***A.11:*** Seguridad Física y del Entorno.
- ✓ ***A.12:*** Seguridad de las Operaciones.
- ✓ ***A.13:*** Seguridad de las Comunicaciones.
- ✓ ***A.14:*** Adquisición, desarrollo y mantenimiento de los sistemas de información.
- ✓ ***A.15:*** Relación con Proveedores.
- ✓ ***A.16:*** Gestión de Incidentes de Seguridad de la Información.
- ✓ ***A.17:*** Aspectos de Seguridad de la Información para la gestión de la Continuidad del Negocio.

✓ ***A.18:*** Cumplimiento.

1.3. Plan de proyecto

La metodología utilizada comúnmente para la implantación de un SGSI es la denominada PDCA que corresponde a las siglas en inglés de *Plan*, *Do*, *Check* y *Act*. Se trata de una estrategia cíclica que siempre está viva, pues una vez implantado el SGSI nos encontraremos siempre en alguna de sus "estaciones". En definitiva, es un proceso que siempre ha de estar vivo, de otra manera nuestro SGSI acabaría desfasado.

A continuación, se muestras un gráfico ilustrativo de las fases PDCA y las tareas que se han de cubrir en cada una de estas fases.

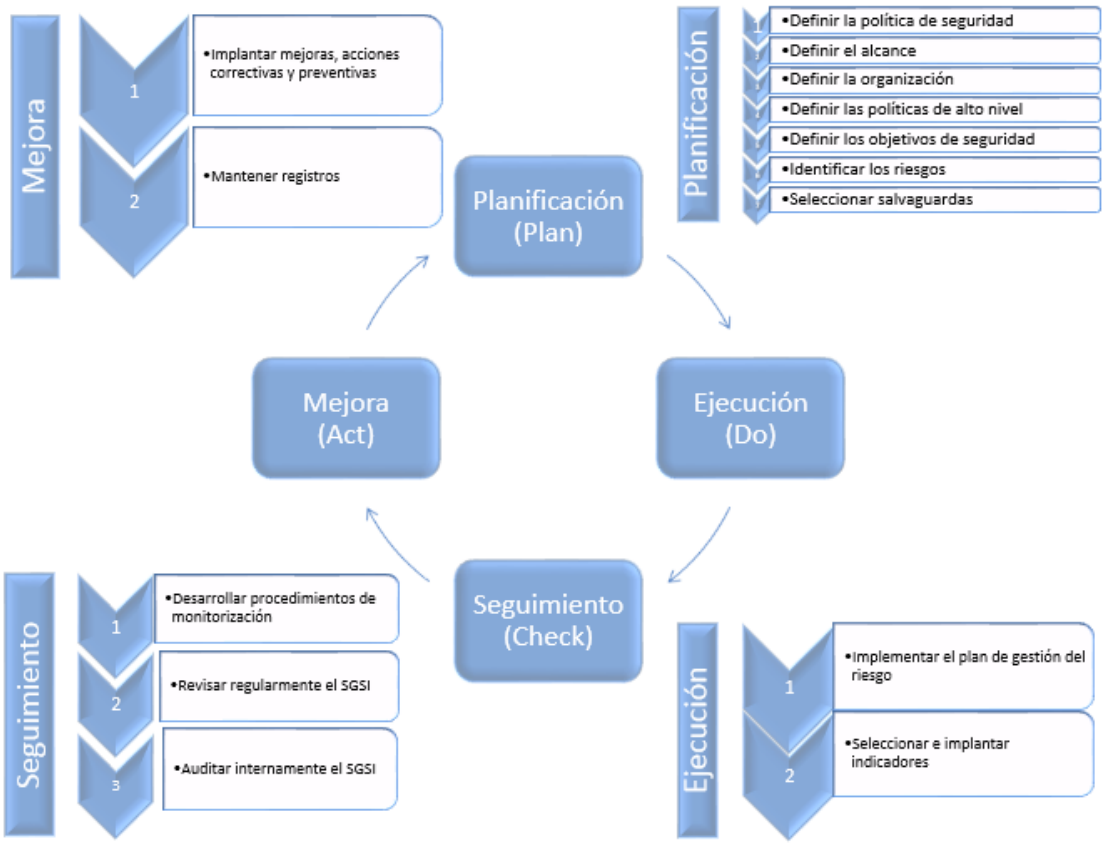

Ilustración 1. Fases del proyecto

1.3.1. Planificación

- ***Definir la política de seguridad.*** La implantación de un SGSI debe ser un facilitador y no debe limitar de ninguna manera los objetivos de negocio. Por este motivo, se intentar dar una visión global (políticas, líneas de actuación, etc.) con relación a la seguridad de la información y como estas políticas no alteran los objetivos de negocio.
- ***Definir el alcance.*** En segundo lugar, se ha de definir el alcance de SGSI. Esta parte es muy importante, ya que definir un alcance muy ambicioso puede acabar con el fracaso del proyecto. Es importante fijar objetivos alcanzables. No hay que olvidar que la implantación de un SGSI es un ciclo de mejora continua y que en futuras iteraciones se podrían añadir nuevos procesos/áreas/departamentos. En este caso, se ha elegido como *driver* los procesos más importantes de negocio o soporte a negocio.
- ***Definir la organización.*** De alguna manera se trata de plasmar un organigrama con relación a las responsabilidades y funciones de cada uno de los implicados en el proceso de implantación

del SGSI. Fundamental como se ha citado con anterioridad la presencia de la dirección de la compañía. Además de describir el negocio, líneas de producto, etc.

- ***Definir las políticas de alto nivel.*** Es una extensión del primer punto "Definir la Política de Seguridad", pero con mayor nivel del detalle.
- ***Definir los objetivos de seguridad.*** Se trata de aterrizar de una forma más detallada cual son los objetivos de la compañía con la implantación del SGSI.
- ***Identificar los riesgos.*** Si vamos a proteger algo, lo primero que tenemos que hacer es determinar lo que queremos proteger, nuestros activos. Esto implica la realización de un análisis de riesgos.
- ***Seleccionar las salvaguardas.*** Una vez realizado el análisis de riesgos, solo queda definir las salvaguardas que harán que esos riesgos disminuyan. En este sentido, es buena práctica la utilización de los controles que ofrece la ISO/IEC 27002.

1.3.2. Ejecución

- ***Implantar el plan de gestión del riesgo.*** Lo primero es empezar a trabajar en lo que se suele denominar "Plan Director de Seguridad de la Información". Donde se define la metodología, los tiempos, los recursos, etc. necesarios para poner en marcha las medidas que se han decidido con anterioridad que son necesarias para proteger la información.
- ***Seleccionar e implantar indicadores.*** Todo lo planificado e implantado no serviría de mucho si no se realizan controles para conocer como ser está incidiendo sobre el problema original. Esto se consigue a través de indicadores, estos indicadores tendrán que ser monitorizados con posterioridad en la fase de seguimiento, pero este es el momento de diseñarlos.

1.3.3. Seguimiento

- ***Desarrollar procedimientos de monitorización.*** Desarrollar procedimientos (si puede ser automatizados) para generar los resultados de los indicadores definidos en la fase de ejecución.
- ***Revisar regularmente el SGSI.*** También de forma periódica, la Dirección deberá verificar la conveniencia, adecuación y eficiencia. Esto se realiza porque se podría dar el caso que, por ejemplo, de que los objetivos de la compañía hubieran cambiado. Como es lógico un cambio así podría genera una revisión completa del SGSI.
- ***Auditar internamente el SGSI.*** De cara a saber que lo que se ha diseñado e implantado es lo adecuado, periódicamente se han de realizar auditorías.

1.3.4. Mejora

- ***Implantar mejoras, acciones correctivas y preventivas.*** Tras una auditoría es muy probable que se encuentren punto de mejora o acciones correctivas o preventivas que implantar.
- ***Mantener registro.*** Para que sea medible la evolución y eficacia del sistema es necesario guardar información sobre su evolución, así como evidencias que permitan corroborar la aplicación de políticas.

1.4. Contexto de Seguridad365

Seguridad365 es una compañía de carácter nacional líder en el sector de la Seguridad Privada. Su personal tiene una marcada vocación de servicio que permite alcanzar un alto nivel de excelencia y calidad de servicio. Su porfolio de servicios y soluciones es amplio y la permite dar cobertura a gran variedad de clientes y sectores empresariales.

Por otra parte, la compañía está regulada por Ley 5/2014, de 4 de abril, de Seguridad Privada (BOE núm. 83, de 5 de abril). Y está sometida a grandes controles por parte del ministerio del interior. En su día a día, Seguridad365 cumple escrupulosamente con la normativa vigente, en un mercado -el de la seguridad privada- muy competitivo.

Además de las regulaciones estatales, Seguridad365 está certificada en la ISO/IEC 9001 y la ISO/IEC 14001. Siguiendo un proceso de mejora continua, la compañía tiene un alto grado de compromiso con el medio ambiente, así como de ofrecer productos y servicios de calidad.

Desde un punto de visto geográfico, Seguridad365 ofrece sus productos y servicios dentro del territorio nacional. Las oficinas centrales están ubicadas en Madrid y cuenta con 30 delegaciones. Estas delegaciones están distribuidas en tres direcciones territoriales:

- ***Área Territorial Norte.*** Dirección ubicada en la sede de Bilbao.
- ***Área Territorial Centro.*** Dirección ubicada en la sede central de Madrid
- ***Área Territorial Sur.*** Dirección ubicada en la sede de Sevilla.

En la sede central de Madrid están localizados los Servicios Centrales (SSCC) de la compañía, entre los que se encuentra la Dirección de TI y el Centro de Proceso de Datos (CPD). Las sedes de la compañía están comunicadas con los SSCC a través de conexiones VPN/IP del operador VodaStar.

Seguridad365 tiene un amplio porfolio de productos que se encuadran en distintos verticales. Uno de los valores de la firma es ofrecer productos de alta calidad a través de la especialización, de manera que cuenta con especialistas en cada uno de estos verticales. Estos verticales son:

- ***Servicios Profesionales de Vigilancia.*** Se trata de personal cualificado y habilitado por el Ministerio del Interior, en el caso de los vigilantes de seguridad. En esta vertical se incluyen otras especializaciones como Escoltas, Auxiliares de servicio, etc.
- ***Servicios Profesionales Itinerantes.*** Se trata de una variante de los Servicios Profesionales de Vigilancia, pero con una la particularidad de compartir tiempo entre distintos clientes. En este caso el vigilante se desplaza entre sedes de distintos clientes. Requiere de cierta especialización tanto en el personal como en la planificación de las operaciones, por lo que se ha consolidado como un vertical independiente.
- ***Servicios de Instalación y Mantenimiento de Sistemas.*** Es personal altamente cualificado que analiza e instala la última tecnología en productos de seguridad. Entre los productos que se combinan para conseguir la mejor solución para cada cliente están los controles de acceso, vigilancia remota, alarmas, dispositivos de extinción de incendios, etc.
- ***Servicios de Monitorización de Sistemas.*** La compañía cuenta con un Centro de Operación y Servicio (COS) donde se monitorizan todos los sistemas instalados y conectados a la Central Receptora de Alarmas (CRA). Este servicio opera 24x7 los 365 días del año.

Con esta diversidad de productos, Seguridad365 es capaz de ofrecer soluciones de seguridad personalizadas y adaptadas a las necesidades de cada cliente.

Para dar soporte a productos tan diferentes, la compañía cuenta con infraestructuras IT y Sistemas de Información muy modernos, adaptables y flexibles. De esta manera es capaz de dar respuesta a problemáticas bien diferentes:

- Gestión contable/financiera a través del ERP Navision de Microsoft.
- Gestión de Nominas a través de PeopleSoft.
- Gestión de turnos de personal operativo a través de ProPlan365.
- Correo electrónico a través de Exchange
- Sistema de recepción de gestión de señales de los sistemas instalados a través de MasterCentral.
- Control de Operativo en Clientes a través de Guadian365
- Portal del Empleado
- Otros sistemas de menos calada pero igualmente necesarios.

Volviendo al compromiso asumido por la compañía con estándares de términos de Calidad como es la ISO/IEC 9001 y habiendo alcanzado mucha madurez en la gestión de esta certificación, la compañía cree necesaria la implantación de un SGSI que permita su certificación en la ISO/IEC 27001. Cada vez una certificación más demandada y valorada por nuestros clientes.

Es determinante fijar un alcance claro del SGSI. En este caso Seguridad365 quiere cubrir con los principales procesos de compañía que están soportados por los Sistemas de Información anteriormente citados. No obstante, en el siguiente epígrafe se describen estos procesos, así como los Sistemas de Información implicados.

1.4.1. Organización

A continuación, se muestra un organigrama que refleja como Seguridad365 está organizada. Los recuadros en color verde identifican los miembros del Comité de Seguridad.

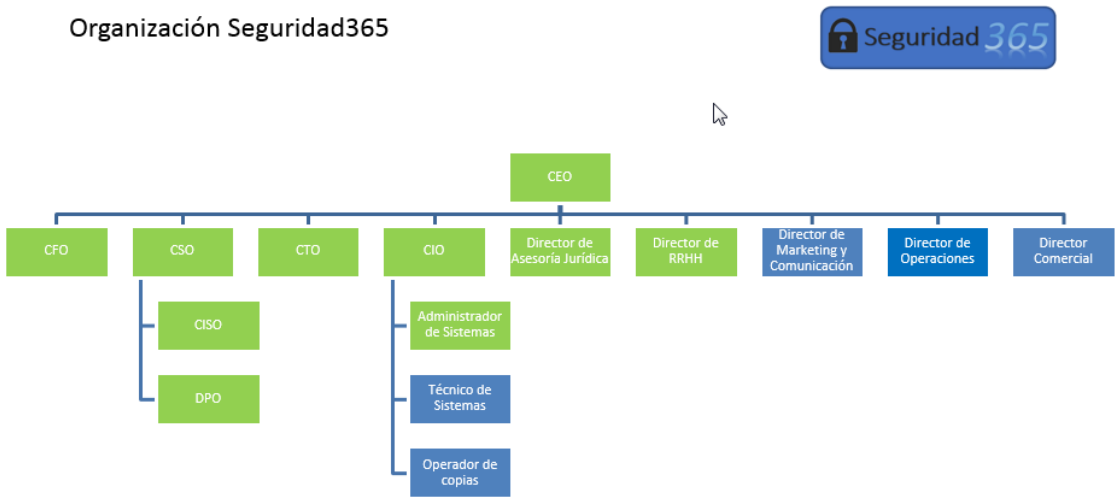

Ilustración 2. Organigrama Seguridad365

- ***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.
- ***Director de Seguridad (CSO).*** En el caso de Seguridad365, compañía dedicada a la Seguridad Privada, cuenta con un Director de Seguridad con múltiples atribuciones. En su equipo cuenta con dos roles necesarios para la implantación y seguimiento del SGSI. Esto roles son el ***Responsable de Seguridad de la información (CISO)*** y el ***Delegado de Protección de Datos (DPO).***
- ***Director de IT (CIO).*** Figura fundamental ya que los Sistemas de Información estas mantenidos por el Departamento de Informática. El CIO cuenta con el soporte de un ***Administrador de Sistemas*** como miembro del Comité de Seguridad para la resolución de cuestiones eminentemente técnicas.
- ***Director Técnico (CTO).*** Si bien no es una figura fundamental para el desarrollo del SGSI, Seguridad365 ha tenido a bien contar con el Director Técnico. Las decisiones tomadas en el Comité de Seguridad pueden tener afectación sobre las soluciones ofrecidas a sus clientes, lo que ha motivado la inclusión de esta figura.
- ***Responsable de Asesoría Jurídica.*** Figura también fundamental por la afectación que puede tener el marco regulatorio (Reglamento Europeo de Protección de Datos, Esquema Nacional de Seguridad, etc.).
- **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). Por este motivo lo veo necesario. De esta figura podrían depender ciertos responsables como el de Calidad, Medio Ambiente, Prevención de riesgos laborales, Selección y Formación, etc. que podrían colaborar con el comité a demanda del responsable de RRHH.

- ***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.

1.4.2. Esquema de Red

A continuación, se muestra un esquema de red básico para mejor entendimiento de los sistemas de Seguridad365. Se entiende mucho mejor tras la lectura del capítulo "Mapa de procesos". En este apartado se encentran los sistemas de información que sustentan dichos procesos.

Esquema de Red Básico

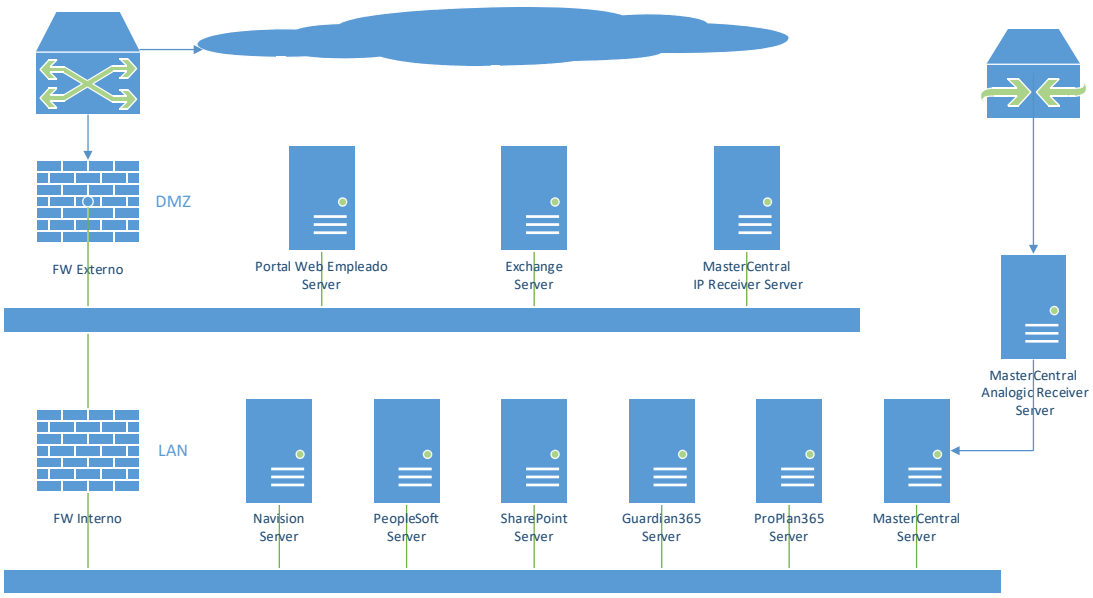

Ilustración 3. Esquema de Red

1.5. Mapa de Procesos

En el punto anterior se describen de manera superficial los Sistemas de Información necesarios para dar cobertura a los principales procesos de negocio y soporte a negocio. Procesos considerados dentro del alcance de SGSI.

A continuación, se detallan estos procesos:

Ilustración 4. SGSI Procesos de Negocio

Como es lógico estos procesos se sustentan en Sistemas de información. Se muestran a continuación:

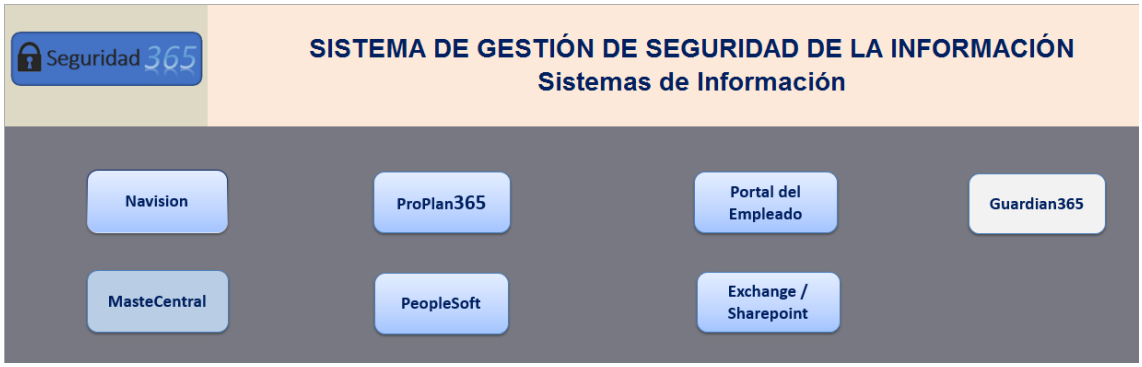

Ilustración 5. SGSI Sistemas de Información

A continuación, se detallan por cada uno de estos Sistemas de Información. Por cada uno, se incluye una valoración de impacto ante un eventual incidente. Se consideran los tres pilares básicos de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad) y por cada uno de ellos el impacto en negocio, imagen corporativa y aspectos legales.

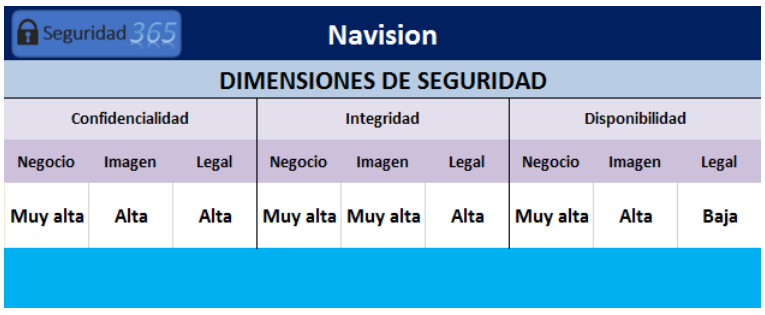

Ilustración 6. SI - Navision

Seguridad 365	ProPlan365								
DIMENSIONES DE SEGURIDAD									
Confidencialidad			Integridad			Disponibilidad			
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	
Muy alta	Alta	Alta	Muy alta	Alta	Alta	Muy alta	Alta	Media	

Ilustración 7. SI - ProPlan365

Seguridad 365	PeopleSoft								
DIMENSIONES DE SEGURIDAD									
Confidencialidad			Integridad			Disponibilidad			
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	
Muy alta	Alta	Alta	Muy alta	Muy alta	Alta	Muy alta	Alta	Media	

Ilustración 8. SI - PeopleSoft

Seguridad 365	Portal del Empleado								
DIMENSIONES DE SEGURIDAD									
Confidencialidad			Integridad			Disponibilidad			
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	
Baja	Media	Alta	Baja	Alta	Alta	Baja	Baja	Baja	

Ilustración 9. SI - Portal del Empleado

Seguridad 365	Exchange / Sharepoint								
DIMENSIONES DE SEGURIDAD									
Confidencialidad			Integridad			Disponibilidad			
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	
Alta	Alta	Muy alta	Alta	Alta	Muy alta	Muy alta	Alta	Baja	

Ilustración 10. SI - Exchange / SharePoint

MasterCentral								
DIMENSIONES DE SEGURIDAD								
Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Alta	Muy alta	Alta	Muy alta	Muy alta	Alta	Muy alta	Muy alta	Muy alta

Ilustración 11. SI - MasterCentral

Guardian365								
DIMENSIONES DE SEGURIDAD								
Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Media	Alta	Alta	Media	Alta	Alta	Baja	Baja	Baja

Ilustración 12. SI - Guardian365

Logicamente para poder dar covertura a estos Sistemas existen multitud de dependencia con otros activos. Hablamos de servidores, infraestructuras de comunicación, personal de IT, control de suministros, etc.

1.6. Objetivos del Plan Director

Seguridad365 pese a no presta servicios de seguridad gestionada IT para sus clientes, está muy sensibilizada con la protección de su información y la de sus clientes. Tratándose de una compañía del sector de la seguridad privada, su sensibilidad es si cabe mayor, pues está acostumbrada a realizar análisis de riesgos para sus clientes y conoce el impacto negativo que tiene cualquier incidente de seguridad.

Por otra parte, muchos de sus clientes están afectados de manera directa por el Esquema Nacional de Seguridad (ENS). De alguna manera, esta circunstancia hace que la compañía esté cada vez más sometida a auditorías externas. La elaboración de un SGSI y la posterior certificación de este supondría estar mejor posicionada ante este tipo de auditorías.

Cada vez es más común que la empresa se presente a concursos donde el pliego de condiciones valora muy positivamente -incluso obliga- a estar certificado en la norma ISO/IEC 27001. Circunstancia que refuerza esta determinación.

Como resumen y de forma esquemática estos son los objetivos del plan director:

- ***Compromiso***. Con la seguridad de la información de sus clientes.
- ***Incrementar la seguridad.*** A través de un ciclo de mejora continua se espera mejorar en términos de Seguridad de la Información, y más allá en aspectos puramente de seguridad informática y continuidad de negocio.
- ***Comercial.*** Permitiendo a la compañía presentarse a concursos que de otra manera no podría.

De alguna manera, Seguridad365 cree que la mejora continua del SGSI y su certificación tendrá consecuencias directas en su:

- ***Competitividad.***

- ***Reputación y confianza*** dentro del sector (clientes, colaboradores, instituciones, etc.)
- ***Beneficio empresarial.***

1.7. Análisis diferencial

Para la realización del Análisis diferencia se plantea la siguiente clasificación según el nivel de madurez de Seguridad365 en relación con cada punto de la norma.

Nivel	Estado	Descripción
L0 (0%)	Inexistente	Cuando la **organización no proporciona un entorno estable** y se basa en la buena voluntad de las personas.
L1 (20%)	Inicial	**No hay comunicación formal sobre procedimientos** y estándares, por lo que las responsabilidades quedan a cargo de cada individuo, dependiendo el resultado del grado de conocimiento de cada uno.
L2 (40%)	Repetible (intuitivo)	La medida está documentada en su correspondiente proceso, normativa, etc. pero no hay evidencias de su cumplimiento, o bien se da el caso contrario, se está realizando, pero no está documentado formalmente y por tanto se hace de manera 'informal' o poco organizada.
L3 (60%)	Definido	La medida está documentada en su correspondiente proceso, normativa, etc. pero no hay evidencias de su cumplimiento, o bien se da el caso contrario, se está realizando, pero no está documentado formalmente y por tanto se hace de manera 'informal' o poco organizada.
L4 (80%)	Gestionado y medible	Los procesos, normativa, instrucciones técnicas, etc. o solo están documentadas, sino que son correctos desde el punto de vista 'compliance', y existen evidencias de su cumplimiento. Se Puede comenzar a utilizar indicadores para medir la eficacia del control y buscar de esta forma la 'mejora continua'
L5 (100%)	Optimizado	Se evidencia la implantación de un **ciclo continuo de revisión y mejora** basado en los indicadores y auditorias anuales.

Ilustración 13. Tabla AD - Leyenda

En el Anexo II se la tabla correspondiente al análisis diferencial. En esta tabla se muestra por cada control de la norma el nivel de cumplimiento y su porcentaje correspondiente, así como el objetivo alcanzable fijado en este primer ciclo de mejora continua.

En la siguiente tabla se muestra un resumen ejecutivo del Análisis Diferencial. En él se puede ver de manera más esquemática el estado actual de cumplimiento de la compañía, así como el objetivo de cumplimiento fijado.

También se incluyen dos gráficos ilustrativos en relación con el estado actual y el objetivo fijado.

Medidas	Madurez (%, p.a.)	Actual	Madurez Objetivo
ISO 27001:2013			
4. CONTEXTO DE LA ORGANIZACIÓN	L2	40,00	80,00
5. LIDERAZGO	L1	20,00	90,00
6. PLANIFICACIÓN	L1-L2	30,00	80,00
7. SOPORTE	L1	20,00	82,00
8. OPERACIÓN	L0-L1	10,00	90,00
9. EVALUACIÓN DEL DESEMPEÑO	L0-L1	10,00	90,00
10. MEJORA	L0-L1	10,00	90,00
ISO 27002:2013			
5. POLÍTICA DE SEGURIDAD	L1	20,00	90,00
6. ASPECTOS ORGANIZATIVOS	L1-L2	33,00	80,00
7. LOS RECURSOS HUMANOS	L2-L3	45,56	60,00
8. GESTIÓN DE ACTIVOS	L2	38,89	74,44
9. CONTROL DE ACCESOS	L2	37,50	85,44
10. CIFRADO	L1	20,00	95,00
11. SEGURIDAD FÍSICA Y AMBIENTAL	L3-L4	70,00	70,00
12. SEGURIDAD EN LA OPERATIVA	L2	38,57	81,07
13. COMUNICACIONES	L2-L3	48,33	79,58
14. ADQUISICIÓN/DESARROLLO SW	L1-L2	28,89	80,56
15. RELACIONES CON SUMINISTRADORES	L1-L2	26,67	78,33
16. GESTIÓN DE INCIDENTES	L2	40,00	80,00

17. CONTINUIDAD DEL NEGOCIO	L4	80,00	80,00
18. CUMPLIMIENTO	L2	36,00	82,17

Ilustración 14. Tabla AD - Resumen

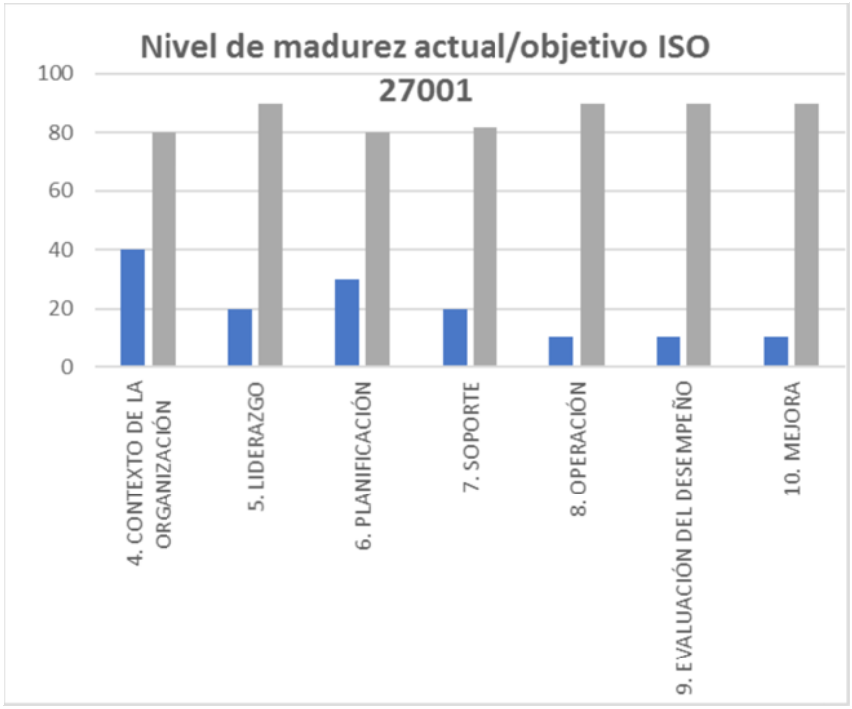

Ilustración 15. Nivel madurez ISO 27001

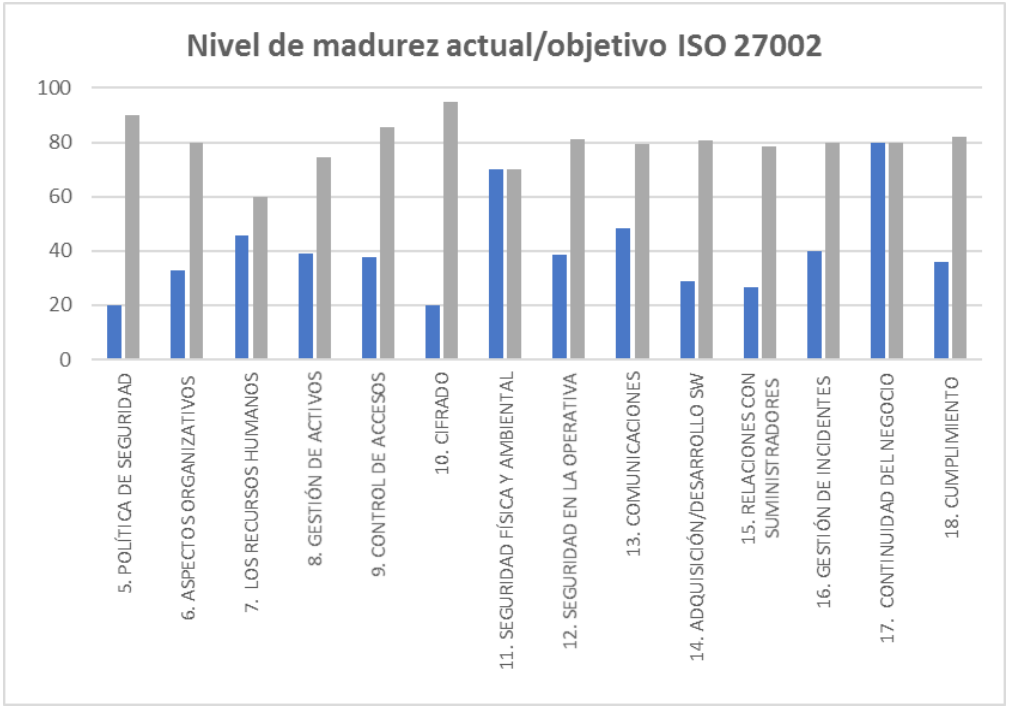

Ilustración 16. Nivel Madurez ISO 27002

1.7.1. Conclusiones

De cara a determinar un indicador de la madurez de la compañía en relación con el objetivo deseable, se han ponderado cada una de las medidas de cada una de las normas. De esta manera nos encontramos con un grado global de 30% respecto al objetivo (83%). Esto indica un grado de madurez relativamente bajo, que implica afrontar un plan de tratamiento y mejora importante, previo a afrontar la auditoría de certificación.

TOTAL 27001	20	86
TOTAL 27002	40	80
TOTAL	30	83

Ilustración 17. Ponderación de la Declaración de Aplicabilidad

2. Sistema de Gestión documental

2.1. Política de Seguridad

2.1.1. Objeto y Alcance

La misión de Seguridad365 es la seguridad, y en este marco, la información y la tecnología que la gestiona se constituyen como un instrumento de alto nivel estratégico, por ello es imprescindible tomar las medidas adecuadas para protegerlos de amenazas que puedan repercutir en confidencialidad, integridad, o de los servicios prestados.

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. Principios Generales que rigen la política

La política de seguridad de la información en Seguridad365 se desarrolla, con carácter general, de acuerdo con los siguientes principios:

a) **Principio de confidencialidad:** se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.

b) ***Principio de integridad:*** se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.

c) ***Principio de disponibilidad:*** se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.

d) ***Principio de gestión del riesgo:*** Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.

e) ***Principio de mejora continua****:* se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico.

f) ***Principio de proporcionalidad en coste****:* la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

g) ***Principio de concienciación y formación****:* se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información.

h) ***Principio de cumplimiento normativo****:* todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

2.1.4. Recursos

La preservación de la seguridad de la información será considerada objetivo común de todas las personas contratadas por Seguridad365, 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.

2.1.5. 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.

2.2. Procedimiento de Auditorías Internas

2.2.1. Objetivo

Definir el procedimiento mediante el cual Seguridad365 planificará, ejecutará y cerrará debidamente documentadas las auditorías internas al SGSI según normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

2.2.2. Metodología

Para la realización de las auditorías internas se tendrán en cuenta las siguientes prerrogativas:

a) El alcance de las auditorías internas se circunscribirá a los procesos identificados en el mapa de procesos de la compañía. Por ende, serán los sistemas de información y las infraestructuras asociadas, el objetivo de estas auditorías.

b) El objetivo será verificar el cumplimiento de lo establecido en el SGSI.

c) 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.

d) 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 3 años. De esta manera, se revisa una parte del sistema cada año, completando un ciclo completo al tercer año. El detalle de esta Programa de auditoría lo podemos encontrar en el Anexo VI.

e) 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.

f) 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.

En procedimiento a seguir queda descrito en la siguiente ilustración:

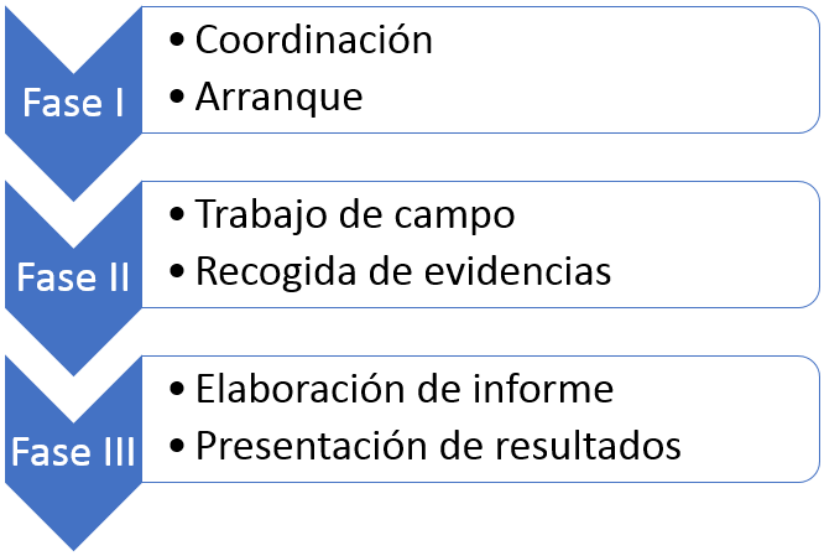

Ilustración 17. Procedimiento Auditoría Interna

En la primera fase se definirá un calendario de auditoría y se reunirá al equipo auditor y a las áreas implicadas para explicar la metodología, el calendario y comunicarles la necesidad de su implicación para poder alcanzar los objetivos.

En la segunda fase se realizará el trabajo de campo. Durante esta fase, la más extensa, se mantendrán reuniones del equipo anterior y las áreas afectados de cara a la extracción de evidencias del cumplimiento de lo establecido en el SGSI.

Por último, en la tercera fase se consolidarán los resultados obtenidos en la fase anterior. En este informe se identificarán claramente las no conformidades, así como las acciones correctivas asociadas. Con toda esta información -debidamente documentada- se elaborará un informe ejecutivo con los

resultados de la auditoría. Posteriormente ser mantendrá una reunión del Comité de Seguridad para dar a conocer estor resultados.

2.2.3. Informe de Auditoría Interna

Ver Anexo I.

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.

CÓDIGO	NOMBRE	DOMINIO	MÉTRICA	PERIODICIDAD	UMBRAL	OBJETIVO	RESPONSABLES
SGSI1	Formación	Personal	Trabajadores que han recibido formación específica en materia de seguridad de la información	Anual	90%	100%	Comité de Seguridad
SGSI2	Umbral de Riesgo	Riesgos	Riesgos por encima del umbral establecido tras análisis (estado potencial) y tratamiento (estado residual)	Anual	5%	0%	CISO
SGSI3	Logs	Control de Acceso	Sistemas/aplicaciones con acceso a datos sensibles sobre los que se realiza registro y alerta periódica de logs de acceso (referido a los Administradores)	Anual	90%	100%	Sistemas
SGSI4	Bajas		Ratio de cuentas de usuario para las que se ha solicitado baja que aún siguen activas	Mensual	5%	0%	Sistemas
SGSI5	Mantenimiento de Sistemas en CPDs	Seguridad Física	Sistemas sometidos a revisión de mantenimiento/inspección	Anual	90%	100%	Resp. Inmuebles
SGSI6	IPS	Comunicaciones	Falsos positivos/negativos detectados por el IPS (Sistema de Detección de Intrusión)	Mensual	95%	100%	Sistemas
SGSI7	Antivirus	Operaciones	Equipos sin antivirus o desactualizado	Mensual	< 10%	< 5%	Sistemas
SGSI8	Vulnerabilidades		Vulnerabilidades críticas no corregidas en plazo		< 15%	< 10%	
SGSI9	Backup		Operaciones de backup fallidas frente al total de registradas en el periodo.		< 10%	< 5%	
SGSI10	Cierre de Incidentes	Incidentes de Seguridad	Media (en horas) que se tarda en cerrar los incidentes de seguridad gestionados en base al procedimiento en la materia	Mensual	< 72 horas	< 48 horas	Comité de Seguridad
SGSI11	Cifrado	Datos/Información	Sistemas de Información categorizados con nivel alto (almacenan datos sensibles) cifrados	Anual	5%	0%	Sistemas
SGS12	Borrado Seguro	Soportes	Soportes que han cambiado de usuario asignado y han sido	Mensual	95%	100%	Sistemas

			sometidos a formateo/borrado seguro				
SGS13	Componentes homologados	Adquisiciones/Software	Componentes comprados de sistemas/aplicaciones no homologados (certificados)	Anual	<10%	< 5%	Resp. de Software
SGS14	Auditorias	Revisión & Mejora	NC/Observaciones abierta en auditorias no tratadas	Anual	2%	0%	CISO
SGS15	Cuadro de Mando Seguridad		% del total de indicadores del SGSI que cumplen el objetivo fijado		> 65%	> 75%	Comité de Seguridad

Ilustración 19. Tabla Gestión de Indicadores

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 labora 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

En el apartado "Contexto de Seguridad365-Organización" se muestra un organigrama de la organización donde se puede ver -en color verde- los miembros del Comité de seguridad. Así mismo, se puede ver el rol y su responsabilidad.

2.6. Declaración de Aplicabilidad

En el Anexo III se adjunta la Declaración de Aplicabilidad. Se trata de una tabla donde se incluyen los controles de seguridad establecidos, así como el detalle de su aplicabilidad en el contexto de la compañía.

2.7. Metodología de Análisis de Riesgos

El presente procedimiento tiene como objeto la definición de responsabilidades, metodología y procedimientos que utiliza Seguridad365 para identificar, evaluar, controlar y medir de forma regular, los riesgos del sistema de gestión de seguridad de la información para asegurar la confidencialidad, integridad, disponibilidad y trazabilidad de la información derivada del funcionamiento de las infraestructuras y servicios prestados por Seguridad365 a sus clientes. Con ello se pretende reducir los riesgos identificados y evaluados en los procesos desarrollados.

A continuación, se detallan las directrices metodológicas seguidas:

- La Gestión de Riesgos es un proceso, y como tal debe incluir actividades de planificación, implantación, seguimiento, evaluación, y planes de actuación dirigidos a la mejora de la situación de seguridad, hacia objetivos más exigentes o corrección de desviaciones.

- Todos los elementos que constituyen la estrategia de gestión de riesgos corporativos deben someterse a ciclos de revisión periódicos que se ejecutan siempre que se produzcan cambios significativos a nivel tecnológico y/ en el alcance de los procesos de negocio actuales.
- La Dirección y/o el CISO deben fijar anualmente un umbral de riesgo aceptable, que debe estar alineado con el propósito y la estrategia de la Organización. En este sentido, la Dirección asume el rol de propietario del riesgo. Esta figura es la que asume la responsabilidad en caso de materializarse un incidente se seguridad producido por la aceptación de los riesgos residuales.
- La Dirección también debe proceder a la aprobación, tras cada proceso de análisis de riesgos que se realice, del Plan de Tratamiento del Riesgo que se elabore, que puede incluir la implantación de medidas de seguridad, ya sean iniciales o aumentado el grado de madurez de las ya aplicadas.
- A fin de conseguir la aplicación práctica de estos principios, la Dirección deberá designar a una persona que coordine la aplicación práctica de estas directrices, así como los recursos necesarios para la operación del Sistema Integrado de Gestión en el que se enmarca este proceso de gestión del riesgo.

2.7.1. Magerit V3

Seguridad365 basa su proceso de análisis de riesgos en la metodología Magerit V3, elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información. Su esquema, desarrollado en los diferentes apartados de este documento, es el siguiente:

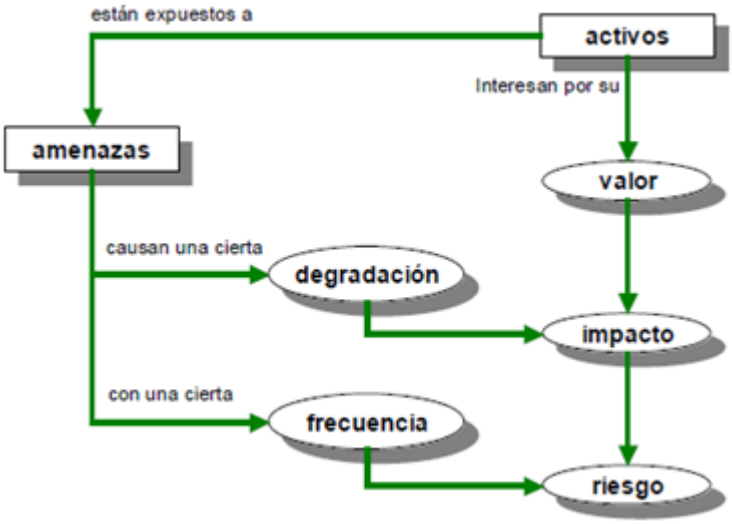

Ilustración 21. Esquema Magerit V3

Magerit, establece un proceso de aproximación metódica para determinar el riesgo siguiendo unas fases pautadas.

- Identificación y Valoración de activos, relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación, especialmente en tres dimensiones asociadas a la seguridad (Disponibilidad, Integridad, Confidencialidad y Trazabilidad).
    - ***Disponibilidad***. Imposibilidad de acceso a la información o uso del servicio por parte del personal autorizado cuando lo necesita.
    - ***Integridad***. Modificación o borrado de información por alguien no autorizado.
    - ***Confidencialidad***. Revelación de información a personas no autorizadas
    - ***Trazabilidad***. Saber quién y cuándo ha hecho qué.

- Determinar a qué amenazas están expuestos los activos identificados, su probabilidad de ocurrencia, y la degradación sufrida en los mismos si se materializa la amenaza.
- Estimar el riesgo actual, definido como el impacto ponderado con la probabilidad de ocurrencia (o expectativa de materialización) de la amenaza, y teniendo presente las medidas o controles de seguridad implantados en la organización.
- Obtener el riesgo residual, tras la aplicación del plan de tratamiento correspondiente.

2.7.2. Identificación y valoración de Activos

Es la primera fase de la metodología Magerit y por tanto del análisis de riesgos.

La actividad de toda organización, pública o privada, se entiende a través de sus procesos, productivos o de prestación de servicio.

Para que toda esta actividad pueda realizarse, son necesarios una serie de activos, entendiendo como tal a los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Pues bien, los activos esenciales al hablar de seguridad de la información son siempre los datos, explotados a través de distintos sistemas de información que prestan soporte a los procesos operativos o servicios de la organización, quedando los demás subordinados a las necesidades de explotación y protección de la información.

Los activos no son únicamente importantes por su valor propio, sino también por todos aquellos activos que dependen de él, por tanto, se deben establecer dependencias entre activos, sistemas de información (datos) y servicios a los que prestan soporte.

En esta fase se han de seguir estos pasos:

- En primer lugar, se identifican todos los sistemas de información que prestan soporte a cada uno de los procesos operativos (POPx) y de soporte (personal, compras, etc.…) de la organización.
- En segundo lugar, se identifican los activos necesarios para la actividad de cada uno de estos sistemas de información. Dichos activos se agrupan en base a las siguientes categorías:
    - Personal (P).
    - Instalaciones (L).
    - Hardware / Equipos Informáticos (HW).
    - Software / Aplicaciones (SW).
    - Redes de comunicaciones (COM).
- En tercer lugar, se identifican las dependencias entre procesos y sistemas de información, y entre éstos y sus activos relacionados. A estas relaciones se les asocia un grado de dependencia, el cual se valora como un porcentaje, estando comprendido entre 0% (activos independientes) y 100% (activos totalmente dependientes).
- Por último, en cuarto lugar, se valoran los activos esenciales, es decir, los sistemas de información. Un activo interesa por su valor, que nada tiene que ver con su coste, sino como el impacto que sobre la organización puede tener una pérdida en cada una de sus dimensiones de seguridad.

  Las dimensiones relevantes desde la perspectiva de la seguridad son las indicadas anteriormente:
    - ***Confidencialidad***: ¿qué daño causaría que se revelase a quien no debe?
    - ***Integridad***: ¿qué perjuicio causaría que estuviera dañado o corrupto?
    - ***Disponibilidad***: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
    - ***Trazabilidad***: ¿quién y cuándo se realizado una determinada modificación?

Las escalas se corresponden de la siguiente forma:

	VALORES POR CADA DIMENSIÓN DE SEGURIDAD	
10	Muy alto	Daño muy grave a la organización
7 - 9	Alto	Daño grave a la organización
4 - 6	Medio	Daño importante a la organización
1 - 3	Bajo	Daño menor a la organización
0	Despreciable	Despreciable irrelevante a efectos prácticos

Ilustración 18. Escala Valoración Activos

El criterio para la estimación de los valores a obtener se basa en el punto 4 del libro 2 "Catálogo de elementos", de la metodología Magerit. Para la valoración de un activo se tienen en cuenta cómo afectaría un incidente de seguridad sobre el mismo desde las siguientes perspectivas:

- Obligaciones legales, normativas, regulatorias…
- Intereses comerciales y económicos
- Valores intangibles pero muy críticos, como la imagen corporativa

Solo se valoran los activos esenciales, pues el resto heredan dicho valor en base a sus relaciones de dependencia, teniendo en cuenta que el valor acumulado sobre un activo es siempre el mayor de los valores que soporta, bien propio, bien de alguno de sus superiores.

2.7.3. Identificación y valoración de Amenazas

La siguiente fase del análisis de riesgos consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren", y de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño.

- El primer paso es por tanto identifican las amenazas a las que están expuestos los activos inventariados en la fase anterior, las cuales son clasificadas en cuatro grandes categorías por la metodología Magerit:
    - Desastres Industriales
    - Origen Industrial
    - Errores no intencionados
    - Ataques deliberados

En el Anexo IV se incluye una tabla que incluye el catálogo de amenazas Magerit.

- El segundo paso es, una vez identificadas todas las amenazas asociadas a cada activo, valorar las mismas en base a dos variables:
    - **Frecuencia**: probabilidad de ocurrencia de la amenaza
    - **Degradación**: en qué porcentaje perdería valor el activo en cada una de sus dimensiones en caso de materialización de la amenaza.

La frecuencia pone en perspectiva la degradación, pues una amenaza puede ser de terribles consecuencias, pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

VALOR		CRITERIO
100%	Muy frecuente (MF)	La amenaza aparece a diario

75%	Frecuente (FR)	La amenaza aparece mensualmente
50%	Normal (No)	La amenaza aparece una vez al año
25%	Poco frecuente (PF)	La amenaza aparece cada varios años
0%	Nunca (NU)	La amenaza nunca aparece

Ilustración 19. Escala Frecuencia

La degradación mide por su parte el daño causado por una amenaza en el supuesto de que ocurriera. Se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción".

VALOR		CRITERIO
100%	Total	El activo resulta totalmente inservible
75%	Alta	Prácticamente inservible
50%	Media	Funcionalmente degradado, rendimiento bajo
25%	Baja	Ligera degradación que no impide el funcionamiento
0%	Despreciable	Activo en perfecto estado

Ilustración 20. Escala Degradación

2.7.4. Determinación del Riesgo

Se denomina riesgo a la medida del daño probable sobre el sistema de información. El riesgo se mide a través de una función del impacto y la frecuencia:

Riesgo = ℜ (impacto, frecuencia)

Donde el impacto refleja el mayor daño posible, mientras que la frecuencia refleja el daño probable.

La variable impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema, calculando ese porcentaje.

El impacto se calcula pues en base al valor del activo, y a su degradación.

Por ejemplo, si un activo vale 8 (Alto en la escala de valoración) y se degrada un 50% (Medio en la escala de degradación) el impacto se calcula de la siguiente forma:

Valor [A+] (que es 8,00) * degradación "M" (que es 50,00) / 100 (es un porcentaje)
= 8,00 x 50,00 / 100 = 4,

Sobre el valor del impacto se aplica la variable probabilidad, obteniendo de esta forma el riesgo. En el ejemplo anterior, si la probabilidad de ocurrencia estimada para una determinada es *"f2""*, y se considera *"f3"* como frecuencia normal, entonces el riesgo será *3*

Para calcular el nivel de riesgo a partir del impacto y la probabilidad de ocurrencia, se suele recurrir a una tabla de doble entrada con escalas de valoración cualitativa.

RIESGO	PROBABILIDAD				
	Muy Baja	Baja	Media	Alta	Muy Alta

IMPACTO						
	Muy Alto	5	6,25	7,5	8,75	10
	Alto	3,75	5	6,25	7,5	8,75
	Medio	2,5	3,75	5	6,25	7,5
	Bajo	1,25	2,5	3,75	5	6,25
	Muy Bajo	0	1,25	2,5	3,75	5

Ilustración 21. Tabla Nivel de Riesgo

En el siguiente cuadro se aprecian las 4 zonas de riesgo que pueden darse mediante la combinación de los valores de impacto y probabilidad:

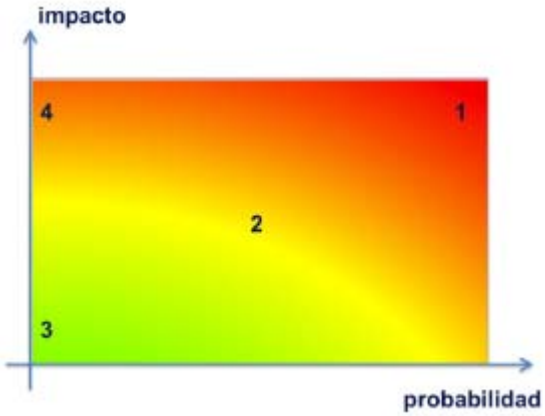

Ilustración 22. Zonas de Riesgo

- Zona 1. Riesgos muy probables y de muy alto impacto.
- Zona 2. Riesgos de probabilidad relativa e impacto medio.
- Zona 3. Riesgos improbables y de bajo impacto.
- Zona 4. Riesgos improbables, pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

El riesgo se clasifica según las siguientes tipologías

- **Riesgo acumulado** es el calculado sobre un activo teniendo en cuenta:
    - El impacto acumulado, que se basa en su valor propio + el de los activos que dependen de él.
    - La frecuencia de la amenaza.

  El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.
- **Riesgo repercutido** es el calculado sobre un activo teniendo en cuenta:
    - El impacto repercutido basado en su propio valor
    - La frecuencia de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio (activos esenciales) permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información.

Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: **definir el umbral de riesgo aceptable.**

Desde otra perspectiva el riesgo se clasifica como:

- **Riesgo actual**, para cuyo cálculo se tienen en cuenta los controles de seguridad presentes en la organización en el momento en que se realiza el análisis de riesgos, disminuyendo de esta forma los parámetros probabilidad y/o degradación asociados a las amenazas. Si no se tuvieran en cuenta dichos controles, el riego obtenido se conoce como 'Riesgo Potencial'.

  A partir del cálculo del riesgo actual tenemos la siguiente casuística:

  - Si los riesgos actuales están por debajo del umbral de riesgo que la organización ha determinado como ampliamente aceptable, no debe hacerse nada adicional.
  - Si están entre ese valor y el tolerable debe decidirse que hacer.
  - Si están por encima del umbral que lo considera intolerable deben tomarse obligatoriamente medidas para minimizar en lo posible el riesgo.

- **Riesgo residual** es el que permanece en la organización una vez implantadas las medidas de seguridad necesarias para disminuir los riesgos por debajo del umbral establecido, en lo que se conoce como Plan de Tratamiento del Riesgo.

  A efectos prácticos, dependiendo de la decisión tomada, ésta afectará al cálculo del riesgo de dos formas:

  Reduciendo la frecuencia de las amenazas, mediante salvaguardas preventivas, que en algunos casos llegan a impedir completamente que la amenaza se materialice.

  Limitando el daño causado mediante salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa, pero las consecuencias se limitan.

3. Análisis de riesgos

El Análisis de Riesgos forma parte de las acciones realizadas para el cumplimiento de los requisitos establecidos por la Norma ISO/IEC 27001, en concreto aquellos relacionados con el análisis de riesgos indicados en los apartados 6.1.2 y 8.2 de la Norma.

3.1. Identificación y valoración de Activos

El análisis de riesgos se centra en los activos esenciales, es decir, aquellos sistemas de información que tratan datos y que por tanto permiten a Seguridad365 desarrollar su actividad.

En el epígrafe Mapa de procesos se identifican los principales Procesos de Negocio, así como los Sistemas de Información que los sustentan.

Por tanto, en la siguiente tabla se identifican los sistemas de información que dan soporte a los procesos operativos y de soporte a negocio. También se vinculan con el clúster de activos subordinados en los que están sustentados.

Agrupación de Activos

Sistema de Información	Clúster
Navision	C1
ProPlan365	C1
Portal del Empleado	C1
Guardian365	C1
PeopleSoft	C1
MasterCentral	C2
Exchange/SharePoint	C1

Ilustración 23. Tabla Agrupación de Activos

A continuación, se muestra una tabla resumen donde se identifican los activos subordinados que permiten soportar los Sistemas de Información.

Inventario de Sistemas de Información y Activos asociados				
Ámbito	Clúster	Descripción	Activo Subordinado	Dependencia
Hardware	C1	Clúster de Servidores	Host	Muy Alta
	C1	Servidor de Base de Datos	SGBD	Muy Alta
	C1	Balanceador de Carga	Equipo virtual	Muy Alta
	C1	Sistema de Almacenamiento	Host	Muy Alta
	C1	Sistema Backup	Servicio de respaldo	Media
Aplicación	C1	Servidor de aplicaciones	Servidor de aplicaciones	Media
	C1	Servidores virtuales de aplicación	Granjas virtuales	Muy Alta
	C1	Servidor de base de datos	SGBD	Baja
Red	C1	Red interna	LAN	Media
	C1	Red externa	DMZ	Baja
Hardware	C2	Servidores físicos SQL	Host	Muy Alta
	C2	Sistema Back-Up	Servicio de respaldo	Muy Alta
Aplicación	C2	Servidor SQL	SGBD	Muy Alta
Red	C2	Red interna	LAN	Muy Alta
Personal	C1, C2	Desarrolladores	Personal	Media
	C1, C2	Técnicos de sistemas	Administradores	Muy Alta
	C1, C2	Usuarios de negocio	Usuarios internos	Muy Alta
Instalaciones	C1, C2	CPD principal	Locales protegidos	Muy Alta

Ilustración 24. Tabla Inventario de Activos

En base a las dos tablas mostradas anteriormente, se puede identificar el grado de dependencia entre un activo concreto (asociado a un clúster) y sus activos subordinados.

En la siguiente tabla se resumen los posibles grados de dependencia.

	Grados de Dependencia	
100%	**Muy alta**	Sería imposible trabajar en el activo dependiente
75%	**Alta**	Sería muy difícil trabajar en el activo dependiente
50%	**Media**	Se podría trabajan en el activo dependiente, pero con muchas dificultades.
25%	**Baja**	Se podría trabajan en el activo dependiente, no siendo su modo de operación óptimo.
0%	**Muy Baja**	No tienen ninguna afectación.

Ilustración 25. Grados de dependencia

Continuando con 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 (Confidencialidad, Integridad, Disponibilidad y Trazabilidad). A continuación, se describe cada una de las dimensiones:

Dimensión	Descripción
Confidencialidad	Revelación de información a personas no autorizadas
Integridad	Modificación de información por alguien no autorizado. Incluye el borrado o eliminación de datos.
Disponibilidad	Imposibilidad de acceso a la información o uso del servicio por parte del personal autorizado cuando lo necesita.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Ilustración 26. Tabla Dimensiones Seguridad

Por cada una de estas dimensiones se valora el impacto que supondría un incidente de seguridad, según los siguientes criterios:

Criterio	Descripción
Negocio	Perdidas económicas, daño para el negocio
Imagen	Daño reputacional/pérdida de imagen y confianza
Legal	Incumplimiento legal, normativo o regulatorio

Ilustración 27. Tabla Valoración según dimensión

Por último, se utiliza la siguiente escala de valores:

	Valores posibles por cada Dimensión / Criterio

9-10	**Muy alto**	Daño muy grave a la organización
7 - 9	**Alto**	Daño grave a la organización
4 - 6	**Medio**	Daño importante a la organización
1 - 3	**Bajo**	Daño menor a la organización
0	**Muy Bajo**	Despreciable irrelevante a efectos prácticos

Ilustración 28. Valores por Dimensión/Criterio

Según los criterios anteriormente citados, esta es la tabla de valoración de los Activos.

Sistema de Información	Confidencialidad			Integridad			Disponibilidad			Trazabilidad		
	Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Navision	MA	A	A	MA	A	A	MA	A	B	A	A	A
Guardian365	M	A	A	M	A	A	B	B	B	A	A	A
ProPlan365	MA	A	A	MA	A	A	MA	A	M	A	A	A
PeopleSoft	MA	A	A	MA	A	A	MA	A	M	A	A	A
Exchange/SharePoint	A	A	MA	A	A	MA	MA	A	B	A	A	A
Portal del Empleado	B	M	A	B	A	A	B	B	B	B	M	A
MasterCentral	A	MA	A	MA	MA	A	MA	MA	MA	A	A	A

Ilustración 29. Tabla de valoración de Activos

3.2. Identificación y valoración de Amenazas

Otra actividad fundamental a la hora de realizar el análisis de riesgos es la identificación y valoración de Amenazas que pueden afectar a los activos de compañía.

Se debe por tanto asociar a cada tipo de activo el conjunto de amenazas/riesgos que le aplican, dentro de las cuatro grandes categorías definidas por la metodología Magerit:

- Desastres Industriales
- Origen Industrial
- Errores no intencionados
- Ataques deliberados

En el Anexo IV podemos encontrar el catálogo de amenazas que contempla la metodología Magerit. No todas estas amenazas afectan de la misma manera a los activos. A posteriori, veremos el nivel de afectación en cada caso.

Por otra parte, en el caso de Seguridad365 se han tomado como activos los distintos Sistemas de Información que sustentan los procesos de negocio o soporte al mismo. De esta manera, algunas de las amenazas no aplican de forma directa a estos activos (por ejemplo, desastres naturales), sin embargo, si afectan a los activos subordinados (por ejemplo, un servidor). Por tanto, a efectos de valoración de estas

amenazas se tienen en cuenta la afectación directa del activo o bien por afectación a alguno de sus activos subordinados. Y siempre se tiene en cuenta el peor de los casos.

Antes las 3 posturas posibles ante el análisis (Peor Escenario, Escenario más Probable, Mejor Escenario) se adoptará la postura del "Escenario más Probable" para ponderar adecuadamente los riesgos y orientar la inversión futura derivada del tratamiento del riesgo a la tipología de amenazas e incidentes más habituales.

Esta valoración se realiza inicialmente en base a tablas y muestra estadísticas o bien al juicio de expertos que son parte relevante en la prestación del servicio, si bien el servicio podrá ir obteniendo datos propios conforme progrese en su nivel de madurez a través de los sucesivos ciclos de revisión y mejora asociados al SGSI.

Una dimensión fundamental a la hora de valorar una amenaza es la frecuencia con la que esta se puede materializar.

La **frecuencia** se valora en base a la siguiente escala y criterio:

VALOR		CRITERIO
100%	Muy frecuente (MF)	La amenaza aparece a diario
75%	Frecuente (FR)	La amenaza aparece mensualmente
50%	Normal (No)	La amenaza aparece una vez al año
25%	Poco frecuente (PF)	La amenaza aparece cada varios años
0%	Nunca (NU)	La amenaza nunca aparece

Ilustración 30. Escala Frecuencia

Por otra parte, para cada una de las dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad y Trazabilidad) se valora la degradación del activo en caso de materializarse la amenaza.

La **degradación** se valora en base a la siguiente escala y criterio.

VALOR		CRITERIO
100%	Total	El activo resulta totalmente inservible
75%	Alta	Prácticamente inservible
50%	Media	Funcionalmente degradado, rendimiento bajo
25%	Baja	Ligera degradación que no impide el funcionamiento
0%	Despreciable	Activo en perfecto estado

Ilustración 31. Escala Degradación

Como resultado, a continuación, se muestra la tabla resumen con las amenazas que pueden afectar a los activos de Seguridad365 o activos subordinados.

TABLA DE AMENAZAS Y VALORACIÓN SOBRE ACTIVOS						
Tipología	**Amenazas**	**Frec.**	**Conf.**	**Integ.**	**Disp.**	**Traz.**

TABLA DE AMENAZAS Y VALORACIÓN SOBRE ACTIVOS							
[N] Desastres Naturales	N1	Fuego	PF	Baja	Baja	Total	Baja
	N2	Daños por agua	PF	Baja	Baja	Alta	Baja
[I] Origen Industrial	I1	Fuego	PF	Baja	Baja	Total	Baja
	I2	Daños por agua	PF	Baja	Baja	Alta	Baja
	I5	Avería de origen físico / lógico	FR	Baja	Baja	Total	Baja
	I6	Corte del suministro eléctrico	NO	Baja	Baja	Alta	Baja
	I7	Condiciones inadecuadas T/ H	NO	Baja	Baja	Alta	Baja
	I8	Fallo de comunicaciones	NO	Media	Media	Total	Media
	I9	Interrupción otros servicios	FR	Baja	Baja	Total	Baja
	I10	Degradación soportes	NO	Baja	Baja	Alta	Baja
[E] Errores	E1	Errores de los usuarios	FR	Media	Media	Alta	Media
	E2	Errores del administrador	FR	Media	Media	Alta	Media
	E3	Errores de monitorización	FR	Alta	Alta	Media	Alta
	E4	Errores de configuración	FR	Media	Media	Alta	Media
	E7	Deficiencias de la organización	FR	Alta	Alta	Alta	Alta
	E8	Difusión de SW dañino	FR	Alta	Alta	Alta	Alta
	E14	Escapes de información	FR	Total	Media	Baja	Alta
	E15	Alteración de la información	FR	Media	Total	Baja	Media
	E18	Destrucción de la información	FR	Baja	Total	Total	Baja
	E19	Divulgación de información	FR	Total	Baja	Baja	Alta
	E20	Vulnerabilidades de los programas	MF	Alta	Alta	Alta	Alta
	E21	Errores de mantenimiento (Sw)	FR	Media	Media	Alta	Media
	E23	Errores de mantenimiento (Hw)	FR	Media	Media	Alta	Media
	E24	Caída del sistema por falta recursos	NO	Baja	Baja	Total	Baja
	E25	Perdida de Equipos	FR	Total	Baja	Baja	Alta
	E28	Indisponibilidad del personal	NO	Baja	Baja	Alta	Baja
[A-] Ataques	A.4	Manipulación de la configuración	FR	Alta	Alta	Alta	Alta
	A.5	Suplantación de la identidad	NO	Total	Total	Alta	Alta
	A.6	Abuso privilegios de acceso	FR	Alta	Alta	Baja	Alta
	A.7	Uso no previsto	FR	Alta	Alta	Alta	Alta
	A.8	Difusión de SW dañino	FR	Alta	Alta	Alta	Alta
	A.10	Alteración de secuencias	FR	Media	Total	Baja	Media
	A.11	Acceso no autorizado	FR	Alta	Total	Baja	Alta
	A.12	Análisis de tráfico	FR	Total	Media	Baja	Alta
	A.14	Intercepción de información	NO	Total	Media	Baja	Alta

TABLA DE AMENAZAS Y VALORACIÓN SOBRE ACTIVOS							
	A.15	Modificación de la información	FR	Media	Total	Baja	Media
	A.18	Destrucción de la información	FR	Baja	Total	Total	Baja
	A.19	Divulgación de información	FR	Total	Baja	Baja	Alta
	A.22	Manipulación de programas	FR	Alta	Alta	Alta	Alta
	A.24	Denegación de servicio	FR	Baja	Baja	Total	Baja
	A.25	Robo	FR	Total	Baja	Baja	Alta
	A.26	Ataque destructivo	FR	Baja	Baja	Total	Baja
	A.29	Extorsión	FR	Alta	Alta	Alta	Alta
	A.30	Ingeniería social	NO	Alta	Alta	Alta	Alta

Ilustración 32. Tabla de Amenazas y Valoración sobre Activos

3.3. Mapa de Riesgos

Se denomina riesgo a la medida del daño probable sobre el sistema de información. El riesgo se mide a través de una función del impacto y la frecuencia:

Riesgo = ℜ (impacto, frecuencia)

La variable impacto se corresponde con la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos, y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema, calculando ese porcentaje.

Para calcular el nivel de riesgo a partir del impacto y la probabilidad de ocurrencia, se suele recurrir a una tabla de doble entrada con escalas de valoración cualitativa.

RIESGO		PROBABILIDAD				
		Muy Baja	Baja	Media	Alta	Muy Alta
IMPACTO	Muy Alto	5	6,25	7,5	8,75	10
	Alto	3,75	5	6,25	7,5	8,75
	Medio	2,5	3,75	5	6,25	7,5
	Bajo	1,25	2,5	3,75	5	6,25
	Muy Bajo	0	1,25	2,5	3,75	5

Ilustración 33.Tabla Nivel de Riesgo

Se aprecia por tanto que el nivel de riesgo puede estar comprendido entre 0 y 10 en la escala definida.

3.3.1. Riesgo Actual

En base a la Metodología descrita en el apartado anterior se presenta a continuación la tabla de niveles de riesgo asociados a los sistemas de información de Seguridad365.

Tipología	Amenazas	Activo

			Navision	Guardian365	ProPlan365	PeopleSoft	Exchange / SharePoint	Portal del Empleado	MasterCentral
[N] Desastres Naturales	N1	Fuego	0,79	0,48	0,85	0,85	0,79	0,4	1,02
	N2	Daños por agua	0,69	0,44	0,73	0,73	0,69	0,36	0,86
[I] Origen Industrial	I1	Fuego	0,79	0,48	0,85	0,85	0,79	0,4	1,02
	I2	Daños por agua	0,69	0,44	0,73	0,73	0,69	0,36	0,86
	I5	Avería de origen físico / lógico	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	I6	Corte del suministro eléctrico	1,38	0,89	1,46	1,46	1,38	0,72	1,72
	I7	Condiciones inadecuadas T/H	1,38	0,89	1,46	1,46	1,38	0,72	1,72
	I8	Fallo de comunicaciones	2,34	1,62	2,45	2,45	2,34	1,29	2,81
	I9	Interrupción otros servicios	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	I10	Degradación soportes	1,38	0,89	1,46	1,46	1,38	0,72	1,72
[E] Errores No Intencionados	E1	Errores de los usuarios	3,2	2,31	3,32	3,32	3,2	1,81	3,75
	E2	Errores del administrador	3,2	2,31	3,32	3,32	3,2	1,81	3,75
	E3	Errores de monitorización	4,02	3,17	4,1	4,1	4,02	2,43	4,45
	E4	Errores de configuración	3,2	2,31	3,32	3,32	3,2	1,81	3,75
	E7	Deficiencias de la organización	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	E8	Difusión de SW dañino	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	E14	Escapes de información	3,71	3,05	3,75	3,75	3,71	2,28	3,95
	E15	Alteración de la información	3,36	2,7	3,4	3,4	3,36	2,1	3,67
	E18	Destrucción de la información	3,55	2,38	3,71	3,71	3,55	1,98	4,34
	E19	Divulgación de información	3,32	2,74	3,36	3,36	3,32	2,02	3,52
	E20	Vulnerabilidades de los programas	5,78	4,38	5,94	5,94	5,78	3,39	6,56
	E21	Errores de mantenimiento (Sw)	3,2	2,31	3,32	3,32	3,2	1,81	3,75
	E23	Errores de mantenimiento (Hw)	3,2	2,31	3,32	3,32	3,2	1,81	3,75
	E24	Caída del sistema por falta recursos	1,59	0,96	1,69	1,69	1,59	0,8	2,03
	E25	Perdida de Equipos	3,32	2,74	3,36	3,36	3,32	2,02	3,52
	E28	Indisponibilidad del personal	1,38	0,89	1,46	1,46	1,38	0,72	1,72
[A-] Ataques Intencionados	A.4	Manipulación de la configuración	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	A.5	Suplantación de la identidad	3,41	2,61	3,49	3,49	3,41	2,03	3,83

	A.6	Abuso privilegios de acceso	3,71	3,05	3,75	3,75	3,71	2,31	3,98
	A.7	Uso no previsto	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	A.8	Difusión de SW dañino	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	A.10	Alteración de secuencias	3,36	2,7	3,4	3,4	3,36	2,1	3,67
	A.11	Acceso no autorizado	4,1	3,36	4,14	4,14	4,1	2,57	4,41
	A.12	Análisis de tráfico	3,71	3,05	3,75	3,75	3,71	2,28	3,95
	A.14	Intercepción de información	2,47	2,03	2,5	2,5	2,47	1,52	2,63
	A.15	Modificación de la información	3,36	2,7	3,4	3,4	3,36	2,1	3,67
	A.18	Destrucción de la información	3,55	2,38	3,71	3,71	3,55	1,98	4,34
	A.19	Divulgación de información	3,32	2,74	3,36	3,36	3,32	2,02	3,52
	A.22	Manipulación de programas	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	A.24	Denegación de servicio	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	A.25	Robo	3,32	2,74	3,36	3,36	3,32	2,02	3,52
	A.26	Ataque destructivo	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	A.29	Extorsión	4,34	3,28	4,45	4,45	4,34	2,54	4,92
	A.30	Ingeniería social	2,89	2,19	2,97	2,97	2,89	1,7	3,28

Ilustración 34. Tabla de Riesgo Actual

Para la formulación del cálculo de riesgo para cada sistema de información se utiliza una hoja de cálculo Excel. En el Anexo V se muestra la tabla utilizada para el caso de Navision.

3.3.2. Riesgo Aceptable

Una vez conocido en nivel de riesgos inicial presente en la organización, la dirección fija el umbral de riesgo aceptable en un valor 4. 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 en aras de rebajas este umbral lo máximo posible hasta alcanzar el riesgo residual.

3.3.3. Riesgo Residual

A continuación, se indican los valores de las amenazas/riesgos esperables sobre cada tipo de activo una vez aplicados los controles ISO/IEC 27001 y ejecutadas las acciones de tratamiento de riesgos identificadas:

Tipología	Amenazas	Activo						
		Navision	Guardian365	ProPlan365	PeopleSoft	Exchange / SharePoint	Portal del Empleado	MasterCentral

[N] Desastres Naturales	N1	Fuego	0,24	0,14	0,26	0,26	0,24	0,24	0,31
	N2	Daños por agua	0,21	0,13	0,22	0,22	0,21	0,22	0,26
[I] Origen Industrial	I1	Fuego	0,24	0,14	0,26	0,26	0,24	0,24	0,31
	I2	Daños por agua	0,21	0,13	0,22	0,22	0,21	0,22	0,26
	I5	Avería de origen físico / lógico	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	I6	Corte del suministro eléctrico	0,41	0,27	0,44	0,44	0,41	0,22	0,52
	I7	Condiciones inadecuadas T/H	0,41	0,27	0,44	0,44	0,41	0,22	0,52
	I8	Fallo de comunicaciones	0,70	0,49	0,74	0,74	0,70	0,39	0,84
	I9	Interrupción otros servicios	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	I10	Degradación soportes	0,41	0,27	0,44	0,44	0,41	0,22	0,52
[E] Errores No Intencionados	E1	Errores de los usuarios	0,96	0,69	1,00	1,00	0,96	0,54	1,13
	E2	Errores del administrador	0,96	0,69	1,00	1,00	0,96	0,54	1,13
	E3	Errores de monitorización	1,21	0,95	1,23	1,23	1,21	0,73	1,34
	E4	Errores de configuración	0,96	0,69	1,00	1,00	0,96	0,54	1,13
	E7	Deficiencias de la organización	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	E8	Difusión de SW dañino	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	E14	Escapes de información	1,11	0,92	1,13	1,13	1,11	0,68	1,19
	E15	Alteración de la información	1,01	0,81	1,02	1,02	1,01	0,63	1,10
	E18	Destrucción de la información	1,07	0,71	1,11	1,11	1,07	0,59	1,30
	E19	Divulgación de información	1,00	0,82	1,01	1,01	1,00	0,61	1,06
	E20	Vulnerabilidades de los programas	1,73	1,31	1,78	1,78	1,73	1,02	1,97
	E21	Errores de mantenimiento (Sw)	0,96	0,69	1,00	1,00	0,96	0,54	1,13
	E23	Errores de mantenimiento (Hw)	0,96	0,69	1,00	1,00	0,96	0,54	1,13
	E24	Caída del sistema por falta recursos	0,48	0,29	0,51	0,51	0,48	0,24	0,61
	E25	Perdida de Equipos	1,00	0,82	1,01	1,01	1,00	0,61	1,06
	E28	Indisponibilidad del personal	0,41	0,27	0,44	0,44	0,41	0,22	0,52
[A-] Ataques Intencionados	A.4	Manipulación de la configuración	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	A.5	Suplantación de la identidad	1,02	0,78	1,05	1,05	1,02	0,61	1,15
	A.6	Abuso privilegios de acceso	1,11	0,92	1,13	1,13	1,11	0,69	1,19
	A.7	Uso no previsto	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	A.8	Difusión de SW dañino	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	A.10	Alteración de secuencias	1,01	0,81	1,02	1,02	1,01	0,63	1,10
	A.11	Acceso no autorizado	1,23	1,01	1,24	1,24	1,23	0,77	1,32
	A.12	Análisis de tráfico	1,11	0,92	1,13	1,13	1,11	0,68	1,19
	A.14	Intercepción de información	0,74	0,61	0,75	0,75	0,74	0,46	0,79
	A.15	Modificación de la información	1,01	0,81	1,02	1,02	1,01	0,63	1,10
	A.18	Destrucción de la información	1,07	0,71	1,11	1,11	1,07	0,59	1,30
	A.19	Divulgación de información	1,00	0,82	1,01	1,01	1,00	0,61	1,06

	A.22	Manipulación de programas	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	A.24	Denegación de servicio	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	A.25	Robo	1,00	0,82	1,01	1,01	1,00	0,61	1,06
	A.26	Ataque destructivo	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	A.29	Extorsión	1,30	0,98	1,34	1,34	1,30	0,76	1,48
	A.30	Ingeniería social	0,87	0,66	0,89	0,89	0,87	0,51	0,98

Ilustración 35. Tabla de Riesgo Residual

3.3.4. Conclusiones

En el siguiente cuadro se aprecian las 4 zonas de riesgo que pueden darse mediante la combinación de los valores de impacto y probabilidad:

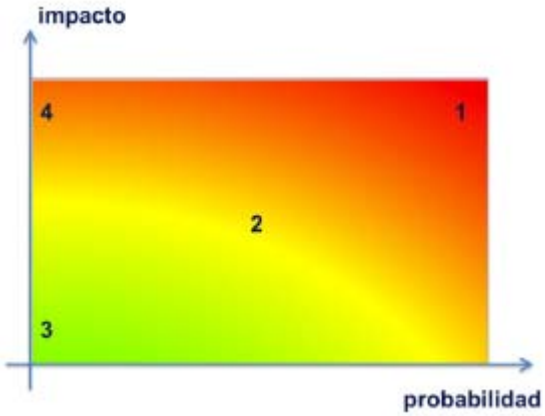

Ilustración 36. Zonas de Riesgo

- Zona 1. Riesgos muy probables y de muy alto impacto.
- Zona 2. Riesgos de probabilidad relativa e impacto medio.
- Zona 3. Riesgos improbables y de bajo impacto.
- Zona 4. Riesgos improbables, pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

Analizando el mapa de riesgos actuales, se puede comprobar que Seguridad365 se encuentra en una

zona de riesgo localizada entre la zona 2 y 3. En conclusión, se puede afirmar que Seguridad365 se encuentra en una situación relativamente saludable. Se compara también la situación de riesgo actual con el riesgo residual al que se tiende alcanzar tras los ciclos futuros de mejora continua.

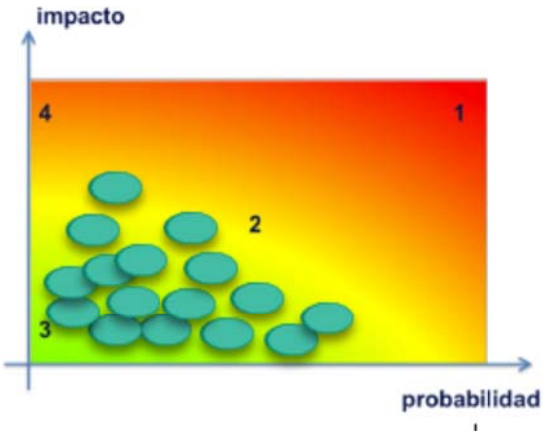

Ilustración 37. Zona de Riesgo Actual

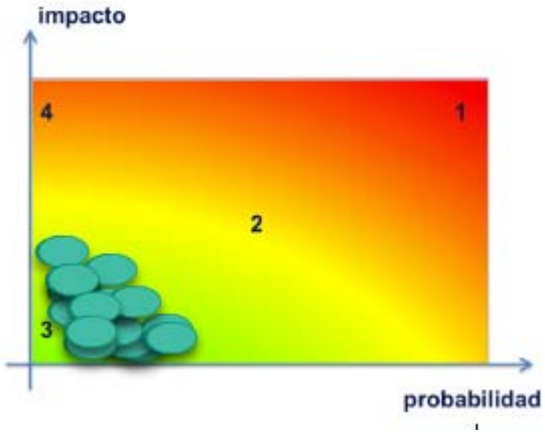

Ilustración 38. Zona de Riesgo Residual

4. Propuestas de mejora

Una vez realizado el Análisis de Riesgos y por tanto el nivel de riesgo actual, el comité de seguridad de Seguridad365 plantea un paquete de mejoras en aras de 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.

4.1. Proyectos de mejora

4.1.1. Medidas Organizativas

Código: **MO-1**	*Proyecto:* **Plan de formación y concienciación a empleados**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 1/2/2019*

Apartado Normativo 4. Contexto de la Organización 5. Liderazgo 7. Soporte *Controles* Políticas de Seguridad (5.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint
Descripción: Elaborar un plan formativo y de capacitación de los empleados para el tratamiento adecuado de los sistemas de información. Incluye una campaña de concienciación del tratamiento de los datos de compañía y en particular de los datos de carácter personal.	
Objetivos: Incorporar acciones formativas genéricas al plan de formación de la compañía. Contratar cursos específicos para personal técnico y/o de compliance (sistemas de Gestión) Elaborar y difundir boletines periódicos de seguridad, buscando el impacto inmediato	
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación

Ilustración 39. MO-1. Plan de formación y concienciación a empleados

Código: **MO-2**	*Proyecto:* **Implantación de sistema de gestión de usuarios y permisos**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 14/2/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Aspectos organizativos de la seguridad de la información (6.1) Control de accesos (9.4)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Análisis diseño y desarrollo de un sistema de gestión de usuarios, permisos y roles.		
Objetivos: 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.		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO	

	• Responsable de formación • CIO

Ilustración 40. MO-2. Implantación de sistema de gestión de usuarios y permisos

Código: **MO-3**	*Proyecto:* **Política de gestión de incidentes de seguridad**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 28/12/2018*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Gestión de incidentes de seguridad de la información (16.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Hasta el momento no se gestionan de manera adecuada los incidentes de seguridad. Se les da tratamiento, peor no se informa a las autoridades competentes.		
Objetivos: Tener una política clara en cuanto al tratamiento de posibles incidentes de seguridad.		
Responsable: • CISO	*Miembros implicados:* • CEO • CIO	

Ilustración 41. MO-3. Política de gestión de incidentes de seguridad

Código: **MO-4**	*Proyecto:* **Normativa de uso de dispositivos móviles y portátiles**	
Presupuesto: N/A - Recursos propios	*Inicio: 17/12/2018*	*Fin: 11/1/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Aspectos organizativos de la seguridad de la información (6.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
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.		

Objetivos: 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. Este proyecto se complementa con el plan formativo que se desarrolla en el proyecto MO-1.

Responsable:	*Miembros implicados:*
• Director de RRHH	• CEO • CISO • Responsable de formación • CIO

Ilustración 42. MO-4. Normativa de uso de dispositivos móviles y portátiles

Código: **MO-5**	*Proyecto:* **Acuerdos de confidencialidad con empleados**	
Presupuesto: N/A - Recursos propios	*Inicio: 28/12/2018*	*Fin: 25/1/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Seguridad Ligada a los Recursos Humanos (7.2, 7.3)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Desarrollo de una política de acuerdo de confidencialidad con respeto al empelado. Hasta el momento los empleados no firman ningún documento que les vincule con la obligación de preservar la información de compañía.		
Objetivos: Disponer de una política que firmará el empleado en su contratación y que tendrán que firmar los actuales empleados. Se espera disminuir el nivel de riesgo por uso inadecuado de la información. También está muy vinculado al plan formativo que se realizará en el proyecto MO-1.		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación • CIO	

Ilustración 43. MO-5. Acuerdos de confidencialidad con empleados

Código: **MO-6**	*Proyecto:* **Acuerdos de confidencialidad con proveedores**	
Presupuesto: N/A - Recursos propios	*Inicio: 14/1/2019*	*Fin: 11/2/2019*

Apartado Normativo 5. Liderazgo *Controles* Políticas de Seguridad (5.1) Relación con suministradores (15.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint
Descripción: Desarrollo de una política de acuerdo de confidencialidad con respeto a los proveedores. Si bien hasta el momento se viene firmando un acuerdo de confidencialidad (NDA), se considera necesario hacer una revisión de este.	
Objetivos: Crear un marco de trabajo con respecto a los proveedores que manejan información de la compañía, que proteja a Seguridad365 de eventuales incidentes de seguridad derivados del uso inadecuado por parte de proveedores.	
Responsable: • Director Asesoría Jurídica	*Miembros implicados:* • CEO • CISO • CFO • Responsable de Compras y Logística

Ilustración 44. MO-6. Acuerdos de confidencialidad con proveedores

4.1.2. Medidas Técnicas

Código: **MT-1**	*Proyecto:* **Instalación de consola centralizada antimalware**	
Presupuesto: 7.000 Euros 15% mantenimiento anual sobre esta cantidad	*Inicio: 3/21/2018*	*Fin: 28/12/2018*
Controles Seguridad en la operativa (12.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Si bien la compañía cuenta con antivirus instalado en servidores y PCs, no cuenta con una consola centralizada que controle el estado del antivirus en cada equipo. De manera que podría estar desactualizado o desinstalado eventualmente.		
Objetivos: Tener mayor control del estado del antivirus y de esta manera evitar posibles problemas con equipos desactualizados o incumpliendo la política de antivirus de la compañía.		

Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO

Ilustración 45. MT-1. Instalación de consola centralizada antimalware

Código: **MT-2**	*Proyecto:* **Implantación de gestor de dispositivos móviles (MDM)**	
Presupuesto: 3.000 Euros (Puesta en marcha) 25 euros por dispositivo anuales.	*Inicio: 10/12/2018*	*Fin: 3/5/2019*
Controles Aspectos normativos de la seguridad de la información (6.2) Gestión de activos (8.1)	*Activos afectados:* • Guardian365 • Exchange/SharePoint	
Descripción: La compañía entrega dispositivos móviles a sus empleados, pero no tiene control alguno sobre el dispositivo una vez entregado. Se afronta la instalación de un gestor de dispositivos móviles (MDM) que permita la administración de estos dispositivos de forma remota.		
Objetivos: Contar con una herramienta que permita aplicar políticas, desplegar aplicaciones, incluso formatear los dispositivos en caso de pérdida o robo.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Ilustración 46. MT-2. Implantación de gestor de dispositivos móviles (MDM)

Código: **MT-3**	*Proyecto:* **Cifrado de dispositivos móviles y portátiles**	
Presupuesto: N/A - Recursos propios	*Inicio: 7/1/2019*	*Fin: 8/3/2019*
Controles Aspectos normativos de la seguridad de la información (6.2) Cifrado (10.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	

Descripción: Hasta el momento no hay una política clara de cifrado de dispositivos móviles y portátiles. De esta manera, nos podemos encontrar con equipos portátiles cifrados a voluntad del usuario. En este momento se quiere forzar por directivas el cifrado del dispositivo.
Objetivos: Conseguir que todo el parque de dispositivos móviles y equipos portátiles estén cifrados.

Responsable:	*Miembros implicados:*
• CIO	• CEO • CISO • CFO

Ilustración 47. MT-3. Cifrado de dispositivos móviles y portátiles

Código: **MT-4**	*Proyecto:* **Implantación de Monitor de Red**	
Presupuesto: 17.000 Euros 20% mantenimiento anual sobre esta cantidad	*Inicio: 17/12/2018*	*Fin: 4/2/2019*
Controles Seguridad en las Telecomunicaciones (13.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de una herramienta que permita a los administradores de sistemas monitorizar la red en busca de posibles comportamientos anómalos que pudieran implicar un riesgo de seguridad para los sistemas de información.		
Objetivos: Detectar posibles ataques o mal funcionamiento de la rede de datos que pudiera afectar a la seguridad de los sistemas de información y por tanto a los datos de la compañía.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Ilustración 48. MT-4. Implantación de Monitor de Red

Código: **MT-5**	*Proyecto:* **Auditoría PenTest**

Presupuesto: 23.000 euros	*Inicio: 7/1/2019*	*Fin: 8/2/2019*
Controles Seguridad en las telecomunicaciones (13.1, 13.2) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.1, 14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Realización de una auditoría técnica de seguridad sobre los sistemas expuestos a Internet, y otra sobre servicios internos que pudieran suponer un riesgo de seguridad.		
Objetivos: Detectar posibles vulnerabilidades técnicas tanto en red interna como externa.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Ilustración 49. MT-5. Auditoría PenTest

Código: **MT-6**	*Proyecto:* **Auditoría de código de los sistemas de información**	
Presupuesto: 175.000 euros	*Inicio: 3/12/2018*	*Fin: 31/5/2019*
Controles Seguridad en la operativa (12.5) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.1, 14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Auditoría de código de los sistemas de información.		
Objetivos: Detectar posibles amenazas derivadas de errores de programación, mala praxis u obsolescencia tecnológica.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Ilustración 50. MT-6. Auditoría de código de los sistemas de información

Código: **MT-7**	*Proyecto:* **Gestor de despliegue de actualizaciones de software y parches de seguridad**	
Presupuesto: 9.000	*Inicio: 4/2/2019*	*Fin: 5/4/2019*
Controles Seguridad en la operativa (12.6) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de un gestor de actualizaciones de software y parches de seguridad. Este trabajo se viene haciendo de manera muy manual con el consiguiente riesgo.		
Objetivos: Tener el parque de PCs y servidores completamente actualizados con las versiones más recientes de software, así como parches de seguridad de SO.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Ilustración 51. MT-7. estor de despliegue de actualizaciones de software y parches de seguridad

Código: **MT-8**	*Proyecto:* **Gestión de eventos e información de seguridad (SIEM)**	
Presupuesto: 12.000 Euros	*Inicio: 24/12/2018*	*Fin: 8/3/2019*
Controles Control de accesos (9.4)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de un correlador de eventos de los distintos sistemas (red, servidores, software, etc.) de manera que se pueda detectar cualquier comportamiento extraño que pueda suponer un riesgo para la compañía.		
Objetivos: Detectar de manera casi instantánea cualquier intrusión u otra anomalía que pudiera suponer un riesgo.		

Responsable:	*Miembros implicados:*
• CIO	• CEO • CISO • CFO

Ilustración 52. MT-8. Gestión de eventos e información de seguridad (SIEM)

4.2. Plan de ejecución

A continuación, se muestra un diagrama de Gantt, donde se plasman los periodos de ejecución de los proyectos de mejora.

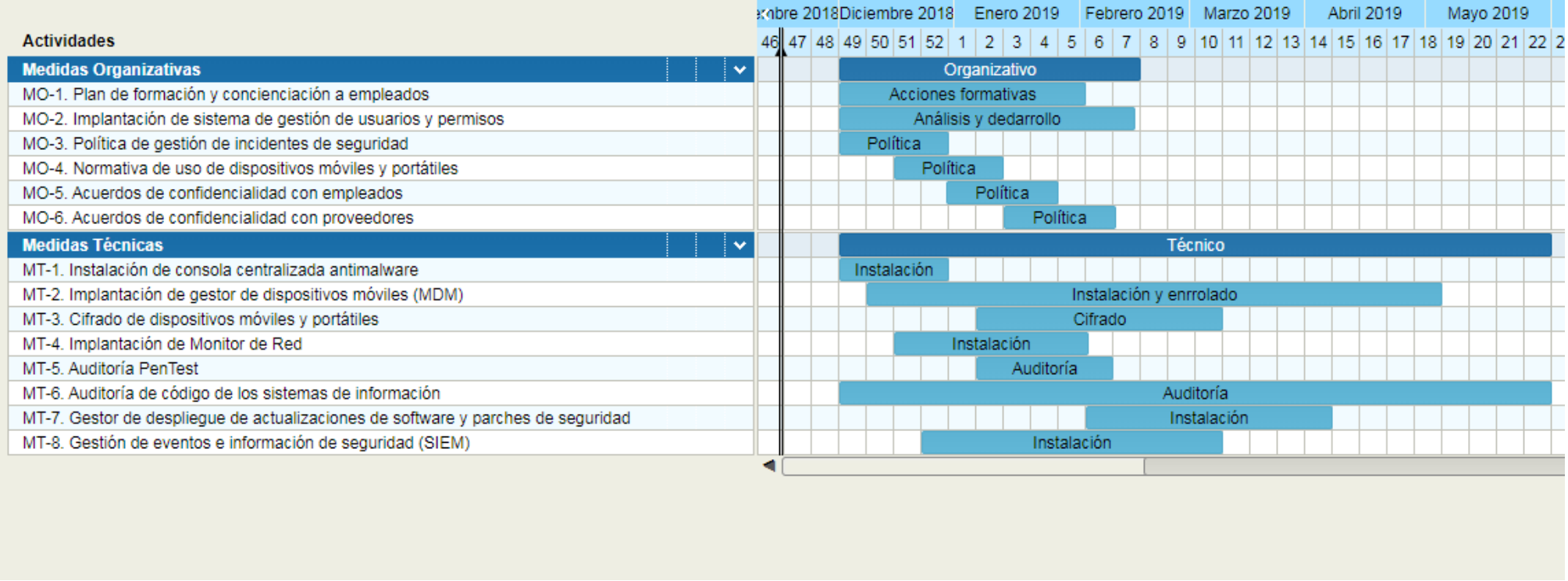

Ilustración 53. Cronograma Plan de Proyectos

4.3. Resultados

Cuando se afrontan una serie de proyectos para elevar el nivel de seguridad, y por tanto disminuir el nivel de riesgo, es difícil concretar como afectará -de forma exacta- al nivel de riesgo de la compañía. Lo que sí está claro es que Seguridad365 pretende con este plan de mejoras acercarse al nivel de riesgo residual planteado durante el Análisis de Riesgos.

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.

5. Auditoría de cumplimiento

La presente auditoria se plantea como una revisión de los aspectos más relevantes de todo SGSI de Seguridad365, desde las perspectivas metodológica, organizativa, y tecnológica. La metodología seguida consiste en evaluar la implantación de las principales directrices y controles normativos, mediante las siguientes comprobaciones:

- Referencia documental respecto al despliegue de la directriz o control correspondiente.
- Corrección desde el punto de vista compliance, lo que se dice que se hace es correcto a efectos normativos.
- Verificación de lo que realmente se hace, a través de las evidencias correspondientes (registros)

Esta auditoría es realizada por una auditora externa de manera que los resultados sean totalmente independientes.

5.1. Metodología

Siguiendo el estándar de la norma ISO/IEC 27000 se han de auditar:

- Aspectos relativos a las directrices dadas en la norma ISO/IEC 27001:2013.
- Aspectos relativos a los dominios y controles de la norma ISO/IEC 27002:2013. Estando esta norma vertebrada en 14 dominio y 35 objetivos de control.

Tal y como se indicó en la fase de propuestas de mejora, los proyectos de mejora -y en general cualquier salvaguarda en aras de reducir el nivel de riesgo-, se dividen en dos tipos de actuaciones:

- ***Medidas organizativas.*** Como podría ser:
  - Formalización de las prácticas mediante documentos escritos o aprobados.
  - Política de personal.
  - Seguridad física.
- ***Medidas técnicas.*** Como aquellas que inciden sobre:
  - Software.
  - Hardware
  - Comunicaciones.

Siendo por tanto estas medidas objetivo de revisión clave en esta auditoría.

Como método de valoración del grado de madurez obtenido en cada directriz de la norma o dominio de esta, se utilizan las siguientes categorías.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0 %	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas.
50%	**L2**	Reproducible , pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Ilustración 54. Categorías de madurez

Siguiendo el programa de auditoría propuesto por el comité de dirección de Seguridad365, las directrices y dominios de norma que se auditan son los que se pueden ver el Anexo VI. En esta ocasión y dado que se trata de una primera auditoría del SGSI, se considera la revisión de todos los dominios de la norma.:

- ✓ ***A.5:*** Políticas de Seguridad de la Información.
- ✓ ***A.6:*** Organización de la Seguridad de la Información.
- ✓ ***A.7:*** Seguridad relativa a los Recursos Humanos.
- ✓ ***A.8:*** Gestión de Activos.
- ✓ ***A.9:*** Control de Acceso.
- ✓ ***A.10:*** Criptografía.
- ✓ ***A.11:*** Seguridad Física y del Entorno.
- ✓ ***A.12:*** Seguridad de las Operaciones.
- ✓ ***A.13:*** Seguridad de las Comunicaciones.
- ✓ ***A.14:*** Adquisición, desarrollo y mantenimiento de los sistemas de información.
- ✓ ***A.15:*** Relación con Proveedores.

- ✓ ***A.16:*** Gestión de Incidentes de Seguridad de la Información.
- ✓ ***A.17:*** Aspectos de Seguridad de la Información para la gestión de la Continuidad del Negocio.
- ✓ ***A.18:*** Cumplimiento.

5.2. Evaluación de la madurez

A continuación, se muestra un cuadro resumen de los resultados de la evaluación de los apartados de la norma ISO/IEC 27001:2013 y los controles de la ISO/IEC 27002:2013.

En el cuadro se muestra el nivel de madurez y tanto por ciento de madurez del epígrafe/dominio correspondiente. Por cada uno se muestra la situación actual y se compara con la situación inicial de madurez de la compañía antes de iniciar el desarrollo del SGSI.

El Anexo VII se puede encontrar el cuadro completo con la valoración de cada uno de los controles.

Medidas	SGSI	Actual		Inicial	
		Madurez	%	Madurez	%
Norma (ISO/IEC 27001:2013)					
4.	CONTEXTO DE LA ORGANIZACIÓN	L2	88 %	L1	40 %
5.	LIDERAZGO	L4	95 %	L1	20 %
6.	PLANIFICACIÓN	L2	85 %	L1	30 %
7.	SOPORTE	L2	78 %	L1	20 %
8.	OPERACIÓN	L2	72 %	L1	10 %
9.	EVALUACIÓN DEL DESEMPEÑO	L2	76 %	L1	10 %
10.	MEJORA	L2	83 %	L1	10 %
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)					
5.	POLÍTICA DE SEGURIDAD	L4	97 %	L1	20 %
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	L2	86 %	L1	33 %
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	L3	94 %	L1	46 %
8.	GESTIÓN DE ACTIVOS	L2	82 %	L1	39 %
9.	CONTROL DE ACCESOS	L2	68 %	L1	38 %
10.	CIFRADO	L2	80 %	L1	20 %
11.	SEGURIDAD FÍSICA Y AMBIENTAL	L4	95 %	L2	70 %
12.	SEGURIDAD EN LA OPERATIVA	L2	76 %	L1	39 %
13.	SEGURIDAD EN LAS TELECOMUNICACIONES	L2	84 %	L1	48 %
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	L2	58 %	L1	29 %
15.	RELACIONES CON SUMINISTRADORES	L3	93 %	L1	27 %
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	L2	69 %	L1	40 %
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L4	98 %	L2	80 %
18.	CUMPLIMIENTO	L2	75 %	L1	36 %

Ilustración 55. Cuadro resumen de Evaluación de Madurez

5.3. Resultados

En el siguiente cuadro se muestra un resumen del nivel de madurez con respecto a las directrices de la norma ISO/IEC 27001:2013 y los dominios de control de la norma ISO/IEC 27002:2013.

		Norma	Controles
L0	Inexistente	0	0
L1	Inicial / Ad-hoc	0	0
L2	Reproducible, pero intuitivo	6	9
L3	Proceso definido	0	2
L4	Gestionado y medible	1	3
L5	Optimizado	0	0

Ilustración 56. Cuadro resumen Nivel de Madurez

De manera más gráfica podemos ver la misma información en los siguientes gráficos de madurez.

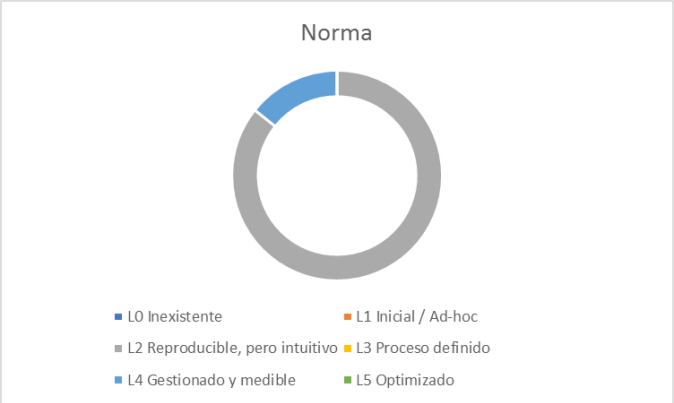

Ilustración 57. Gráfico Madurez Norma

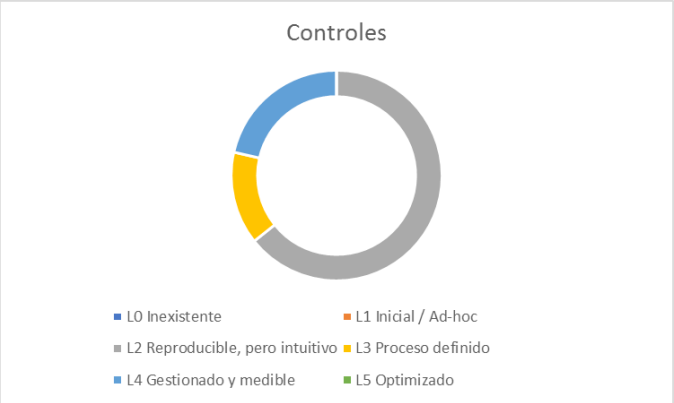

Ilustración 58. Gráfico Madurez Controles

En los siguientes gráficos se peude ver el nivel de cumlimientos en cada uno de las directrices/controles. En ambos gráficos se compara la situación inicial de Seguridad365 antes de iniciar el proceso de implantación del SGSI y la situación actual.

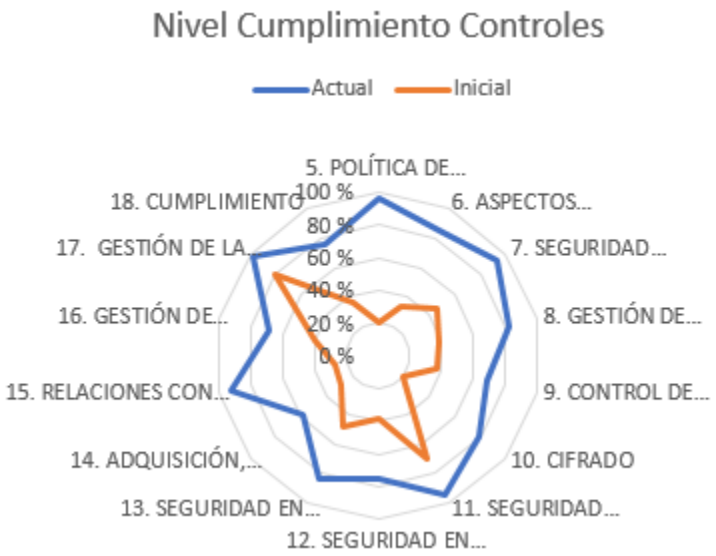

Ilustración 59. Gráfico Nivel de Cumplimiento Norma

Ilustración 60. Gráfico Nivel de Cumplimiento Controles

Como se puede observar en las gráficas anteriores, hay una mejoría considerable en todas las directrices de la norma y los dominios de control. No obstante, nos encontramos con un grado de cumplimiento con posibilidades de mejora. Este es un escenario habitual para compañías, que como Seguridad365, implementan un SGSI y se enfrentan a su primera auditoría de cumplimiento. Será a través de la metodología PDCA, como este nivel de madurez y cumplimento podrá ser optimizado.

No obstante, aun no habiéndose encontrado evidencias que impliquen una no conformidad, se han detectado ciertos aspectos a mejorar o corregir. Los aspectos encontrados se clasifican según el siguiente criterio:

Tipo de comentario	Descripción
No conformidad mayor	Incumplimiento completo del apartado normativo o control
No conformidad menor	Incumplimiento parcial del apartado normativo o control
Observación	No siendo una no conformidad, si no se corrige podría llegar a ser una no conformidad menor
Punto de Mejora	Es una recomendación que aportaría mayor madurez

Ilustración 61. Tipo de comentario

A continuación, se muestra una tabla con los aspectos detectados:

Medidas	SGSI	Tipo	Comentario
Norma (ISO/IEC 27001:2013)			
4.	CONTEXTO DE LA ORGANIZACIÓN		
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	Punto de mejora	Es recomendable definir más claramente el alcance en relación a las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones. Esto debe quedar documentado claramente en la política de Seguridad.
5.	LIDERAZGO		
5.1.	Liderazgo y compromiso.	Punto de	Aunque el compromiso de la Dirección es muy alto, se detecta la

		mejora	falta de asistencia por parte de la Dirección a las reunión del Comité de Seguridad. Sería conveniente demostrar el compromiso de la dirección con la asistencia a este tipo de reuniones.
6.	PLANIFICACIÓN		
6.1.	Acciones para tratar los riesgos y las oportunidades		
6.1.2.	Apreciación de riesgos de seguridad de la información.	Punto de mejora	Aunque se asume que la Dirección es el propietario del riesgo de todos los Sistemas de Información, es aconsejable definir propietarios más concretos. Por ejemplo, en el caso de Navision podría ser el Director Financiero. No obstante, se deja este extremo a criterio del Comité de Seguridad.
7.	SOPORTE		
7.2.	Competencia.	Punto de mejora	En algún caso, no se puede acreditar la realización del curso de concienciación por parte de alguno de los empleados. Se considera que son casos aislados, pero se recomienda poner especial cuidado en el seguimiento de la realización de este tipo de cursos.
8.	OPERACIÓN		
8.1.	Planificación y control operacional.	Observación	La organización debe garantizar que los procesos contratados externamente estén controlados. En este punto se recomienda dejar mejor documentados los procesos realizados por terceros.
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)			
9.2.	Gestión de acceso de usuario:		
9.2.2.	Gestión de los derechos de acceso asignados a usuarios.	Observación	Si bien se ha implementado una aplicación para la gestión de accesos de los usuarios a los distintos sistemas de información, este desarrollo es muy incipiente y con varios puntos de mejora. Por ejemplo, se recomienda automatizar la relación jerárquica de los usuarios.
12.	SEGURIDAD EN LA OPERATIVA		
12.4.	Registro de actividad y supervisión:		
12.4.1.	Registro y gestión de eventos de actividad.	Punto de mejora	Se ha instalado una consola para el control del antivirus. No obstante, se detecta un porcentaje muy bajo de ordenadores que no están reportando su situación con relación a su estado de salud.
14.3.	Datos de prueba:		
14.3.1.	Protección de los datos utilizados en pruebas.	No conformidad menor	Se ha instalado una consola para el control del antivirus. No obstante, se detecta un porcentaje muy bajo de ordenadores que no están reportando su situación con relación a su estado de salud.
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
16.1.	Gestión de incidentes de seguridad de la información y mejoras:		
16.1.2.	Notificación de los eventos de seguridad de la información.	No conformidad menor	De igual manera se ha diseñado un protocolo y un pequeño desarrollo en la plataforma SharePoint para el registro y notificación de incidentes de seguridad. En el tempo que lleva en

			marcha no se han registrado incidentes, aunque sí se han registrado incidentes sucedidos con anterioridad a la implantación del SGSI. Se detecta en algún caso haber excedido el tiempo fijado para la notificación de los incidentes a las autoridades competentes.

6. Presentación de resultados

A continuación, se detallan la documentación que se aporta como entregables de este proyecto.

- ***Memoria descriptiva.*** Se trata del presente documento. Es el documento más detallado, donde se incluye documentación relativa a todas las fases del proyecto, así como los anexos. *CatalaHernansaizJoseAlberto_TFM_Memoria.doc*
- ***Resumen Ejecutivo.*** Se trata de un documento que incluye mis conclusiones sobre la realización del proyecto desde el punto de vista de estudiante. *CatalaHernansaizJoseAlberto_TFM_ResumenEjecutivo.pptx*
- ***Presentación a la dirección.*** También esta bajada en la memoria descriptiva. Está desarrollado en formato presentación y sirve de apoyo para la realización de la vídeo presentación a la dirección. *CatalaHernansaizJoseAlberto_TFM_PresentaciónDirección.pptx*
- ***Concienciación Seguridad de la Información.*** Presentación relativa a aspectos básicos de seguridad de la información. Válida para concienciar y sensibilizar a los empleados. *CatalaHernansaizJoseAlberto_TFM_Concienciación.pptx*
- ***Estado de cumplimiento.*** Presentación del estado de cumplimiento de los controles de seguridad. *CatalaHernansaizJoseAlberto_TFM_EstadoCumplimiento.pptx*

Conclusiones

Considero muy interesante y pedagógico el planteamiento sugerido para la realización de este TFM. El desarrollo de un SGSI es un trabajo un tanto complejo y que requiere el seguimiento de una metodología. El planteamiento incremental de entregas parciales es un método muy acertado, que me ha permitido interiorizar de manera progresiva los conceptos necesarios para su elaboración.

Por otra parte, y en lo que respecta la temática de TFM, considero que tiene mucha aplicación en el mundo empresarial. Cada vez existe más presión en las empresas por contar con un SGSI. Aspectos regulatorios, comerciales o de compromiso empresarial así lo exigen. En este sentido, la utilización de la norma ISO/IEC 27001:2013 es muy adecuada ya que se ha convertido en el estándar de facto para la elaboración de un SGSI.

En particular, quiero resaltar el trabajo realizado para elaborar el Análisis de Riesgos. Quizás sea la parte más importante de todo el trabajo. Conceptualmente es un trabajo que ya habíamos podido ver en otras asignaturas del Master, no obstante, es durante este ejercicio práctico cuando he sido capaz de ponerme en una situación real y hacer por tanto un planteamiento real.

Sin duda, ha sido un buen ejercicio para consolidad el conocimiento adquirido durante el Master y con grandes posibilidades de aplicación en el mundo laboral.

Referencias bibliográficas

UOC. Módulos didácticos MISTIC. Asignatura SGSI

Norma ISO/IEC 27001

Norma ISO/IEC 27002

https://www.pmg-ssi.com/

https://seguinfo.wordpress.com/

http://advisera.com/

https://www.incibe.es/

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8TucHszbmc

https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit /Libro_I_metodo.pdf

Anexos

Anexo I. Informe de auditoría.

Informe de Auditoría Interna

Elaborado por:	Revisado por:	Aprobado por:
CISO	CSO	CEO

Código: (AIxx/año)

Edición: (xx)

Área: (Proceso/Sistema de Información

Fecha Aprobación: (Fecha)

---

1. **Objetivo de auditoría**

Descripción del Proceso o Sistema de información objeto de análisis.

2. Resultados

No conformidad	Acción correctiva

3. **Observaciones**

Apartado dedicado a cualquier observación.

4. **Conclusiones**

Conclusiones del resultado de la auditoría.

Anexo II. Análisis Diferencial

Medidas	SGSI	Madurez Actual	Porcentaje %	Objetivo
Norma (ISO/IEC 27001:2013)				
4.	CONTEXTO DE LA ORGANIZACIÓN	L2	40,00	80,00
4.1.	Comprensión de la organización y de su contexto.	L0	0	80
4.2.	Compresión de las necesidades y expectativas de las partes interesadas.	L0	0	80
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	L4	80	80
4.4.	Sistema de gestión de seguridad de la información (SGSI).	L4	80	80
5.	LIDERAZGO	L1	20,00	90,00
5.1.	Liderazgo y compromiso.	L1	20	90
5.2.	Política.	L1	20	90
5.3.	Roles, responsabilidades y autoridades en la organización.	L1	20	90
6.	PLANIFICACIÓN	L1-L2	30,00	80,00
6.1.	Acciones para tratar los riesgos y las oportunidades	L3	60	80
6.1.1.	Consideraciones generales.	L3	60	80
6.1.2.	Apreciación de riesgos de seguridad de la información.	L3	60	80
6.1.3.	Tratamiento de los riesgos de seguridad de la información.	L3	60	80
6.2.	Objetivos de seguridad de la información y planificación para su consecución.	L0	0	80
7.	SOPORTE	L1	20,00	82,00
7.1.	Recursos.	L1	20	80

7.2.	Competencia.	L1	20	80
7.3.	Concienciación.	L1	20	80
7.4.	Comunicación.	L1	20	90
7.5	Gestión Documental	L3	60	80
8.	OPERACIÓN	L0-L1	10,00	90,00
8.1.	Planificación y control operacional.	L0-1	10	90
8.2.	Apreciación de los riesgos de seguridad.	L0-1	10	90
8.3.	Tratamiento de los riesgos de seguridad de la información.	L0-1	10	90
9.	EVALUACIÓN DEL DESEMPEÑO	L0-L1	10,00	90,00
9.1.	Seguimiento, medición, análisis y evaluación.	L1	10	90
9.2.	Auditoría interna.	L4	10	90
9.3.	Revisión por la dirección.	L1	10	90
10.	MEJORA	L0-L1	10,00	90,00
10.1.	No conformidad y acciones correctivas.	L1	10	90
10.2.	Mejora continua.	L1	10	90
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)				
5.	POLÍTICA DE SEGURIDAD	L1	20,00	90,00
5.1.	Directrices de la Dirección en seguridad de la información:	L1	20	85
5.1.1.	Conjunto de políticas para la seguridad de la información.	L1	20	90
5.1.2.	Revisión de las políticas para la seguridad de la información.	L1	20	80
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	L1-L2	33,00	80,00
6.1	Organización interna:	L1	16	80
6.1.1.	Asignación de responsabilidades para la seguridad de la información.	L1	20	80

6.1.2.	Segregación de tareas.	L2	40	80
6.1.3.	Contacto con las autoridades.	L0	0	80
6.1.4.	Contacto con grupos de interés especial.	L0	0	80
6.1.5.	Seguridad de la información en la gestión de proyectos.	L1	20	80
6.2.	Dispositivos para movilidad y teletrabajo:	L2-L3	50	80
6.2.1.	Política de uso de dispositivos para movilidad.	L2	40	80
6.2.2.	Teletrabajo.	L3	60	80
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	L2-L3	45,56	60,00
7.1.	Antes de la contratación:	L2-L3	50	50
7.1.1.	Investigación de antecedentes.	L2	40	40
7.1.2.	Términos y condiciones de contratación.	L3	60	60
7.2.	Durante la contratación:	L1-L2	27	70
7.2.1.	Responsabilidades de gestión.	L1	20	80
7.2.2.	Concienciación, educación y capacitación en seguridad de la información.	L1	20	80
7.2.3.	Proceso disciplinario.	L2	40	40
7.3.	Cese o cambio de puesto de trabajo.	L3	60	60
8.	GESTIÓN DE ACTIVOS	L2	38,89	74,44
8.1.	Responsabilidad sobre los activos:	L3-L4	70	70
8.1.1.	Inventario de activos.	L3	60	60
8.1.2.	Propiedad de los activos.	L3	60	60
8.1.3.	Uso aceptable de los activos.	L4	80	80
8.1.4.	Devolución de los activos.	L4	80	80
8.2.	Clasificación de la información:	L0	0	80

8.2.1.	Directrices de clasificación.	L0	0	80
8.2.2.	Etiquetado y manipulación de la información.	L0	0	80
8.2.3.	Manipulación de activos.	L0	0	80
8.3.	Manejo de los soportes de almacenamiento:	L2-L3	46,67	73,33
8.3.1.	Gestión de soportes extraíbles.	L0	0	80
8.3.2.	Eliminación de soportes.	L3	60	60
8.3.3.	Soportes físicos en tránsito.	L4	80	80
9.	CONTROL DE ACCESOS	L2	37,50	85,44
9.1.	Requisitos de negocio para el control de accesos:	L1	20	80
9.1.1.	Política de control de accesos.	L1	20	80
9.1.2.	Control de acceso a las redes y servicios asociados.	L1	20	80
9.2.	Gestión de acceso de usuario:	L2	40	89
9.2.1.	Gestión de altas/bajas en el registro de usuarios.	L3	60	80
9.2.2.	Gestión de los derechos de acceso asignados a usuarios.	L3	60	95
9.2.3.	Gestión de los derechos de acceso con privilegios especiales.	L1	20	95
9.2.4.	Gestión de información confidencial de autenticación de usuarios.	L3	60	80
9.2.5.	Revisión de los derechos de acceso de los usuarios.	L1	20	95
9.2.6.	Retirada o adaptación de los derechos de acceso.	L1	20	95
9.3.	Responsabilidades del usuario:	L2	40	85
9.3.1.	Uso de información confidencial para la autenticación.	L2	40	85
9.4.	Control de acceso a sistemas y aplicaciones:	L2-L3	50	88
9.4.1.	Restricción del acceso a la información.	L1-2	20	95

9.4.2.	Procedimientos seguros de inicio de sesión.	L3	60	80
9.4.3.	Gestión de contraseñas de usuarios.	L3	60	80
9.4.4.	Uso de herramientas de administración de sistemas.	L3	60	90
9.4.5.	Control de acceso al código fuente de los programas.	L3	60	95
10.	CIFRADO	L1	20,00	95,00
10.1.	Controles criptográficos:	L1	20	95
10.1.1.	Política de uso de los controles criptográficos.	L1-2	20	95
10.1.2.	Gestión de claves.	L1-2	20	95
11.	SEGURIDAD FÍSICA Y AMBIENTAL	L3-L4	70,00	70,00
11.1.	Áreas seguras:	L3-L4	70	70
11.1.1.	Perímetro de seguridad física.	L3-4	70	70
11.1.2.	Controles físicos de entrada.	L3-4	70	70
11.1.3.	Seguridad de oficinas, despachos y recursos.	L3-4	70	70
11.1.4.	Protección contra las amenazas externas y ambientales.	L3-4	70	70
11.1.5.	El trabajo en áreas seguras.	L3-4	70	70
11.1.6.	Áreas de acceso público, carga y descarga.	L3-4	70	70
11.2.	Seguridad de los equipos:	L3-L4	70	70
11.2.1.	Emplazamiento y protección de equipos.	L3-4	70	70
11.2.2.	Instalaciones de suministro.	L3-4	70	70
11.2.3.	Seguridad del cableado.	L3-4	70	70
11.2.4.	Mantenimiento de los equipos.	L3-4	70	70
11.2.5.	Salida de activos fuera de las dependencias de la empresa.	L3-4	70	70

11.2.6.	Seguridad de los equipos y activos fuera de las instalaciones.	L3-4	70	70
11.2.7.	Reutilización o retirada segura de dispositivos de almacenamiento.	L3-4	70	70
11.2.8.	Equipo informático de usuario desatendido.	L3-4	70	70
11.2.9.	Política de puesto de trabajo despejado y bloqueo de pantalla.	L3-4	70	70
12.	SEGURIDAD EN LA OPERATIVA	L2	38,57	81,07
12.1.	Responsabilidades y procedimientos de operación:	L2-L3	45	70
12.1.1.	Documentación de procedimientos de operación.	L3	60	60
12.1.2.	Gestión de cambios.	L2	40	80
12.1.3.	Gestión de capacidades.	L1	20	80
12.1.4.	Separación de entornos de desarrollo, prueba y producción.	L3	60	60
12.2.	Protección contra código malicioso:	L2	40	90
12.2.1.	Controles contra el código malicioso.	L2-3	40	90
12.3.	Copias de seguridad:	L2	40	80
12.3.1.	Copias de seguridad de la información.	L2-3	40	80
12.4.	Registro de actividad y supervisión:	L1	15	82,5
12.4.1.	Registro y gestión de eventos de actividad.	L0	0	90
12.4.2.	Protección de los registros de información.	L0	0	90
12.4.3.	Registros de actividad del administrador y operador del sistema.	L0	0	90
12.4.4.	Sincronización de relojes.	L3	60	60
12.5.	Control del software en explotación:	L4	80	80
12.5.1.	Instalación del software en sistemas en producción.	L4	80	80
12.6.	Gestión de la vulnerabilidad técnica:	L2-L3	50	85

12.6.1.	Gestión de las vulnerabilidades técnicas.	L1-2	20	90
12.6.2.	Restricciones en la instalación de software.	L4	80	80
12.7.	Consideraciones de las auditorías de los sistemas de información:	L0	0	80
12.7.1.	Controles de auditoría de los sistemas de información.	L0	0	80
13.	SEGURIDAD EN LAS TELECOMUNICACIONES	L2-L3	48,33	79,58
13.1.	Gestión de la seguridad en las redes:	L2-L3	46,67	76,67
13.1.1.	Controles de red.	L2-3	40	90
13.1.2.	Mecanismos de seguridad asociados a servicios de red.	L3	60	60
13.1.3.	Segregación de redes.	L2	40	80
13.2.	Intercambio de información con partes externas:	L2-L3	50	82,5
13.2.1.	Políticas y procedimientos de intercambio de información.	L2	40	80
13.2.2.	Acuerdos de intercambio.	L3	60	80
13.2.3.	Mensajería electrónica.	L2	40	90
13.2.4.	Acuerdo de confidencialidad y secreto.	L3	60	80
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	L1-L2	28,89	80,56
14.1.	Requisitos de seguridad de los sistemas de información:	L2	36,67	80
14.1.1.	Análisis y especificación de los requisitos de seguridad.	L2	40	80
14.1.2.	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	L2-3	50	80
14.1.3.	Protección de las transacciones por redes telemáticas.	L1	20	80
14.2.	Seguridad en los procesos de desarrollo y soporte:	L1-L2	30	76,67
14.2.1.	Política de desarrollo seguro de software.	L1	20	80
14.2.2.	Procedimientos de control de cambios en los sistemas.	L2	40	80

14.2.3.	Revisión técnica de las aplicaciones a efectuar cambios en el sistema operativo.	L3	60	60
14.2.4.	Restricciones a los cambios en los paquetes de software.	L3	60	60
14.2.5.	Uso de principios de ingeniería en protección de sistemas.	L2	40	80
14.2.6.	Seguridad en entornos de desarrollo.	L2	40	80
14.2.7.	Externalización del desarrollo de software.	L2	40	80
14.2.8.	Pruebas de funcionalidad durante el desarrollo de los sistemas.	L2	40	90
14.2.9.	Pruebas de aceptación.	L2	40	90
14.3.	Datos de prueba:	L1	20	85
14.3.1.	Protección de los datos utilizados en pruebas.	L1	20	85
15.	RELACIONES CON SUMINISTRADORES	L1-L2	26,67	78,33
15.1.	Seguridad de la información en las relaciones con suministradores:	L1	33,33	76,67
15.1.1.	Política de seguridad de la información para suministradores.	L1	20	80
15.1.2.	Tratamiento de riesgo dentro de acuerdos de suministradores.	L3	60	70
15.1.3.	Cadena de suministro en tecnologías de la información y comunicaciones.	L1	20	80
15.2.	Gestión de la prestación del servicio por suministradores:	L1	20	80
15.2.1.	Supervisión y revisión de los servicios prestados por terceros.	L1	20	80
15.2.2.	Gestión de cambios en los servicios prestados por terceros.	L1	20	80
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	L2	40,00	80,00
16.1.	Gestión de incidentes de seguridad de la información y mejoras:	L2	40	80
16.1.1.	Responsabilidades y procedimientos.	L2	40	80
16.1.2.	Notificación de los eventos de seguridad de la información.	L2	40	80
16.1.3.	Notificación de puntos débiles de la seguridad.	L2	40	80
16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones.	L2	40	80

16.1.5.	Respuesta a los incidentes de seguridad.	L2	40	80
16.1.6.	Aprendizaje de los incidentes de seguridad de la información.	L2	40	80
16.1.7.	Recopilación de evidencias.	L2	40	80
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L4	80,00	80,00
17.1.	Continuidad de la seguridad de la información:	L4	80	80
17.1.1.	Planificación de la continuidad de la seguridad de la información.	L4	80	80
17.1.2.	Implantación de la continuidad de la seguridad de la información.	L4	80	80
17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	L4	80	80
17.2.	Redundancias:	L4	80	80
17.2.1.	Disponibilidad de instalaciones para el procesamiento de la información.	L4	80	80
18.	CUMPLIMIENTO	L2	36,00	82,17
18.1.	Cumplimiento de los requisitos legales y contractuales:	L2-L3	52	81
18.1.1.	Identificación de la legislación aplicable.	L1	20	90
18.1.2.	Derechos de propiedad intelectual (DPI).	L4	80	80
18.1.3.	Protección de los registros de la organización.	L3	60	60
18.1.4.	Protección de los datos y privacidad de la información personal.	L4	80	80
18.1.5.	Regulación de los controles criptográficos.	L1	20	95
18.2.	Revisiones de la seguridad de la información:	L1	20	83
18.2.1.	Revisión independiente de la seguridad de la información.	L1	20	80
18.2.2.	Cumplimiento de las políticas y normas de seguridad.	L1	20	80
18.2.3.	Comprobación del cumplimiento.	L1-2	20	90

Ilustración 62. Tabla Análisis Diferencial

Anexo III. Declaración de Aplicabilidad

Medidas	SGSI	Aplica/No aplica	Justificación
Norma (ISO/IEC 27001:2013)			
4.	CONTEXTO DE LA ORGANIZACIÓN	Aplica	
4.1.	Comprensión de la organización y de su contexto.	Si	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.
4.2.	Compresión de las necesidades y expectativas de las partes interesadas.	Si	La organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información; y los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	Si	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.
4.4.	Sistema de gestión de seguridad de la información (SGSI).	Si	La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional.
5.	LIDERAZGO	Aplica	
5.1.	Liderazgo y compromiso.	Si	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.
5.2.	Política.	Si	La alta dirección debe establecer una política de seguridad de la información.
5.3.	Roles, responsabilidades y autoridades en la organización.	Si	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.
6.	PLANIFICACIÓN	Aplica	
6.1.	Acciones para tratar los riesgos y las oportunidades	Aplica	

6.1.1.	Consideraciones generales.	Si	Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar.
6.1.2.	Apreciación de riesgos de seguridad de la información.	Si	La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información.
6.1.3.	Tratamiento de los riesgos de seguridad de la información.	Si	La organización debe definir y efectuar un proceso de tratamiento de riesgos de seguridad de la información.
6.2.	Objetivos de seguridad de la información y planificación para su consecución.	Si	La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.
7.	SOPORTE	Aplica	
7.1.	Recursos.	Si	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.
7.2.	Competencia.	Si	La organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas; cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y conservar la información documentada apropiada, como evidencia de la competencia.
7.3.	Concienciación.	Si	Las personas que trabajan bajo el control de la organización deben ser conscientes de la política de la seguridad de la información; su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.
7.4.	Comunicación.	Si	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información, que incluyan: el contenido de la comunicación; cuándo comunicar; a quién comunicar; quién debe comunicar; los

			procesos por los que debe efectuarse la comunicación.
7.5	Gestión Documental	Si	La compañía deberá crear, actualizar y tener control de la información de manera documentada.
8.	OPERACIÓN	Aplica	
8.1.	Planificación y control operacional.	Si	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado 6.1. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinados en el apartado 6.2.
8.2.	Apreciación de los riesgos de seguridad.	Si	La organización debe efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes.
8.3.	Tratamiento de los riesgos de seguridad de la información.	Si	La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.
9.	EVALUACIÓN DEL DESEMPEÑO	Aplica	
9.1.	Seguimiento, medición, análisis y evaluación.	Si	La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.
9.2.	Auditoría interna.	Si	La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca del cumplimiento del sistema de gestión de seguridad de la información.
9.3.	Revisión por la dirección.	Si	La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.
10.	MEJORA	Aplica	
10.1.	No conformidad y acciones correctivas.	Si	Cuando ocurra una no conformidad, la organización debe confeccionar un plan de tratamiento.
10.2.	Mejora continua.	Si	La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información.
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)			

5.	POLÍTICA DE SEGURIDAD	Aplica	
5.1.	Directrices de la Dirección en seguridad de la información:	Aplica	
5.1.1.	Conjunto de políticas para la seguridad de la información.	Si	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
5.1.2.	Revisión de las políticas para la seguridad de la información.	Si	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	Aplica	
6.1	Organización interna:	Aplica	
6.1.1.	Asignación de responsabilidades para la seguridad de la información.	Si	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.
6.1.2.	Segregación de tareas.	Si	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
6.1.3.	Contacto con las autoridades.	Si	Deben mantenerse los contactos apropiados con las autoridades pertinentes.
6.1.4.	Contacto con grupos de interés especial.	Si	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.
6.1.5.	Seguridad de la información en la gestión de proyectos.	Si	La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
6.2.	Dispositivos para movilidad y teletrabajo:	Aplica	
6.2.1.	Política de uso de dispositivos para movilidad.	Si	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
6.2.2.	Teletrabajo.	No (no permitido)	Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	Aplica	
7.1.	Antes de la contratación:	Aplica	

7.1.1.	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.
7.1.2.	Términos y condiciones de contratación.	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.
7.2.	Durante la contratación:	Aplica	
7.2.1.	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.
7.2.2.	Concienciación, educación y capacitación en seguridad de la información.	Si	Todos los empleados de la organización y, cuando corresponda, los contratistas, 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.
7.2.3.	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.
7.3.	Cese o cambio de puesto de trabajo.	Aplica	
8.	GESTIÓN DE ACTIVOS	Aplica	
8.1.	Responsabilidad sobre los activos:	Aplica	
8.1.1.	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.
8.1.2.	Propiedad de los activos.	Si	Todos los activos que figuran en el inventario deben tener un propietario.
8.1.3.	Uso aceptable de los activos.	Si	Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
8.1.4.	Devolución de los activos.	Si	Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

8.2.	Clasificación de la información:	Aplica	
8.2.1.	Directrices de clasificación.	Si	La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
8.2.2.	Etiquetado y manipulación de la información.	Si	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
8.2.3.	Manipulación de activos.	Si	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.	Manejo de los soportes de almacenamiento:	Aplica	
8.3.1.	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.
8.3.2.	Eliminación de soportes.	Si	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
8.3.3.	Soportes físicos en tránsito.	Si	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
9.	CONTROL DE ACCESOS	Aplica	
9.1.	Requisitos de negocio para el control de accesos:	Aplica	
9.1.1.	Política de control de accesos.	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.
9.1.2.	Control de acceso a las redes y servicios asociados.	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.
9.2.	Gestión de acceso de usuario:	Aplica	
9.2.1.	Gestión de altas/bajas en el registro de usuarios.	Si	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
9.2.2.	Gestión de los derechos de acceso asignados a usuarios.	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.
9.2.3.	Gestión de los derechos de acceso con privilegios especiales.	Si	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
9.2.4.	Gestión de información confidencial de autenticación de usuarios.	Si	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
9.2.5.	Revisión de los derechos de acceso de los usuarios.	Si	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
9.2.6.	Retirada o adaptación 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.
9.3.	Responsabilidades del usuario:	Aplica	
9.3.1.	Uso de información confidencial para la autenticación.	Si	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
9.4.	Control de acceso a sistemas y aplicaciones:	Aplica	
9.4.1.	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.
9.4.2.	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.
9.4.3.	Gestión de contraseñas de usuarios.	Si	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
9.4.4.	Uso de herramientas de administración de sistemas.	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.
9.4.5.	Control de acceso al código fuente de los programas.	Si	Se debe restringir el acceso al código fuente de los programas.
10.	CIFRADO	Aplica	
10.1.	Controles criptográficos:	Aplica	
10.1.1.	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.

10.1.2.	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.
11.	SEGURIDAD FÍSICA Y AMBIENTAL	Aplica	
11.1.	Áreas seguras:	Aplica	
11.1.1.	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.
11.1.2.	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.
11.1.3.	Seguridad de oficinas, despachos y recursos.	Si	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
11.1.4.	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.
11.1.5.	El trabajo en áreas seguras.	Si	Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
11.1.6.	Áreas de acceso público, 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.
11.2.	Seguridad de los equipos:	Aplica	
11.2.1.	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.
11.2.2.	Instalaciones de suministro.	Si	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
11.2.3.	Seguridad del cableado.	Si	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
11.2.4.	Mantenimiento de los equipos.	Si	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

11.2.5.	Salida de activos fuera de las dependencias de la empresa.	Si	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
11.2.6.	Seguridad de los equipos y activos 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.
11.2.7.	Reutilización o retirada segura de dispositivos de almacenamiento.	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.
11.2.8.	Equipo informático de usuario desatendido.	Si	Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
11.2.9.	Política de puesto de trabajo despejado y bloqueo de pantalla.	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.
12.	SEGURIDAD EN LA OPERATIVA	Aplica	
12.1.	Responsabilidades y procedimientos de operación:	Aplica	
12.1.1.	Documentación de procedimientos de operación.	Si	Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
12.1.2.	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.
12.1.3.	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.
12.1.4.	Separación de entornos de desarrollo, prueba y producción.	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.
12.2.	Protección contra código malicioso:	Aplica	
12.2.1.	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.
12.3.	Copias de seguridad:	Si	

12.3.1.	Copias de seguridad de la información.	Si	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo con la política de copias de seguridad acordada.
12.4.	Registro de actividad y supervisión:	Aplica	
12.4.1.	Registro y gestión de eventos de actividad.	Si	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
12.4.2.	Protección de los registros de información.	Si	Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
12.4.3.	Registros de actividad del administrador y operador del sistema.	Si	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
12.4.4.	Sincronización de relojes.	Si	Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.
12.5.	Control del software en explotación:	Aplica	
12.5.1.	Instalación del software en sistemas en producción.	Si	Se deben implementar procedimientos para controlar la instalación del software en explotación.
12.6.	Gestión de la vulnerabilidad técnica:	Aplica	
12.6.1.	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.
12.6.2.	Restricciones en la instalación de software.	Si	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
12.7.	Consideraciones de las auditorías de los sistemas de información:	Aplica	
12.7.1.	Controles de auditoría de los 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.
13.	SEGURIDAD EN LAS TELECOMUNICACIONES	Aplica	

13.1.	Gestión de la seguridad en las redes:	Aplica	
13.1.1.	Controles de red.	Si	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
13.1.2.	Mecanismos de seguridad asociados a 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.
13.1.3.	Segregación de redes.	Si	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
13.2.	Intercambio de información con partes externas:	Aplica	
13.2.1.	Políticas y procedimientos de intercambio de información.	Si	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
13.2.2.	Acuerdos de intercambio.	Si	Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
13.2.3.	Mensajería electrónica.	Si	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
13.2.4.	Acuerdo de confidencialidad y secreto.	Si	Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	Aplica	
14.1.	Requisitos de seguridad de los sistemas de información:	Aplica	
14.1.1.	Análisis y especificación de los requisitos de seguridad.	Si	Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
14.1.2.	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Si	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.
14.1.3.	Protección de las transacciones por redes telemáticas.	Si	La información involucrada en las transacciones de servicios de aplicaciones debe ser

			protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.
14.2.	Seguridad en los procesos de desarrollo y soporte:	Aplica	
14.2.1.	Política de desarrollo seguro de software.	Si	Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
14.2.2.	Procedimientos de control de cambios en los sistemas.	Si	La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.
14.2.3.	Revisión técnica de las aplicaciones a efectuar cambios en el sistema operativo.	Si	Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.
14.2.4.	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.
14.2.5.	Uso de principios de ingeniería en protección de sistemas.	Si	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
14.2.6.	Seguridad en entornos de desarrollo.	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.
14.2.7.	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.
14.2.8.	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Si	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
14.2.9.	Pruebas de aceptación.	Si	Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
14.3.	Datos de prueba:	Aplica	
14.3.1.	Protección de los datos utilizados en pruebas.	Si	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
15.	RELACIONES CON SUMINISTRADORES	Aplica	
15.1.	Seguridad de la información en las relaciones con	Aplica	

	suministradores:		
15.1.1.	Política de seguridad de la información para suministradores.	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.
15.1.2.	Tratamiento de riesgo dentro de acuerdos de suministradores.	Si	Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.
15.1.3.	Cadena de suministro en tecnologías de la información y 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.
15.2.	Gestión de la prestación del servicio por suministradores:	Aplica	
15.2.1.	Supervisión y revisión de los servicios prestados por terceros.	Si	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor
15.2.2.	Gestión de cambios en los servicios prestados por terceros.	Si	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 los riesgos.
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Aplica	
16.1.	Gestión de incidentes de seguridad de la información y mejoras:	Aplica	
16.1.1.	Responsabilidades y procedimientos.	Si	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
16.1.2.	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.
16.1.3.	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.
16.1.4.	Valoración de eventos de seguridad de la información y toma de	Si	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se

	decisiones.		clasifican como incidentes de seguridad de la información.
16.1.5.	Respuesta a los incidentes de seguridad.	Si	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
16.1.6.	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.
16.1.7.	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.
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Aplica	
17.1.	Continuidad de la seguridad de la información:	Aplica	
17.1.1.	Planificación de la continuidad de la seguridad de la información.	Si	La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.2.	Implantación de la continuidad de la seguridad de la información.	Si	La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Si	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.
17.2.	Redundancias:	Si	
17.2.1.	Disponibilidad de instalaciones para el procesamiento de la información.	Si	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
18.	CUMPLIMIENTO	Aplica	
18.1.	Cumplimiento de los requisitos legales y contractuales:	Aplica	
18.1.1.	Identificación de la legislación aplicable.	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.

18.1.2.	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.
18.1.3.	Protección de los registros de la organización.	Si	Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.
18.1.4.	Protección de los datos y privacidad de la información personal.	Si	Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.
18.1.5.	Regulación de los controles criptográficos.	Si	Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.
18.2.	Revisiones de la seguridad de la información:	Aplica	
18.2.1.	Revisión independiente de la seguridad de la información.	Si	El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
18.2.2.	Cumplimiento de las políticas y normas de seguridad.	Si	Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable
18.2.3.	Comprobación del cumplimiento.	Si	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Ilustración 63. Tabla Declaración de Aplicabilidad

Anexo IV. Catálogo de amenazas Magerit

Amenazas		
[N-] Desastres Naturales	N.1	Fuego
	N.2	Daños por agua
	N.*	Desastres Naturales
[I-] Origen Industrial	I.1	Fuego
	I.2	Daños por agua
	I.*	Desastres industriales
	I.3	Contaminación mecánica
	I.4	Contaminación electromagnética
	I.5	Avería de origen físico / lógico
	I.6	Corte del suministro eléctrico
	I.7	Condiciones inadecuadas temperatura / humedad
	I.8	Fallo de comunicaciones
	I.9	Interrupción otros servicios
	I.10	Degradación soportes almacenamiento información
	I.11	Emanaciones electromagnéticas
[E-] Errores y Fallos No Intencionados	E.1	Errores de los usuarios
	E.2	Errores del administrador
	E.3	Errores de monitorización

Amenazas		
	E.4	Errores de configuración
	E.7	Deficiencias de la organización
	E.8	Difusión de SW dañino
	E.9	Errores de re-encaminamiento
	E.10	Errores de secuencias
	E.14	Escapes de información
	E.15	Alteración de la información
	E.16	Introducción de info. Incorrecta
	E.17	Degradación de la información
	E.18	Destrucción de la información
	E.19	Divulgación de información
	E.20	Vulnerabilidades de los programas
	E.21	Errores de mantenimiento (software)
	E.23	Errores de mantenimiento (hardware)
	E.24	Caída del sistema por agotamiento recursos
	E.28	Indisponibilidad del personal
[A-] Ataques Intencionados	A.4	Manipulación de la configuración
	A.5	Suplantación de la identidad de usuario
	A.6	Abuso privilegios de acceso
	A.7	Uso no previsto
	A.8	Difusión de SW dañino

Amenazas		
	A.9	Re-encaminamiento de mensajes
	A.10	Alteración de secuencias
	A.11	Acceso no autorizado
	A.12	Análisis de tráfico
	A.13	Repudio
	A.14	Intercepción de información
	A.15	Modificación de la información
	A.16	Introducción de falsa información
	A.17	Corrupción de la información
	A.18	Destrucción de la información
	A.19	Divulgación de información
	A.22	Manipulación de programas
	A.24	Denegación de servicio
	A.25	Robo
	A.26	Ataque destructivo
	A.27	Ocupación Enemiga
	A.28	Indisponibilidad del personal
	A.29	Extorsión
	A.30	Ingeniería social

Ilustración 64. Catálogo de amenazas Magerit

Anexo V. Valoración Navision

Navision																			
Amenazas		Frec.	Conf.	V.Conf	I(Conf)	R(Conf)	Integ.	V.Integ	I(Integ)	R(Integ)	Disp.	V.Disp	I(Disp)	R(Disp)	Traz.	V.Traz	I(Traz)	R(Traz)	Valor
N1	Fuego	25	25	8,33	2,08	0,52	25	8,33	2,08	0,52	100	6,67	6,67	1,67	25	7,50	1,88	0,47	0,79
N2	Daños por agua	25	25	8,33	2,08	0,52	25	8,33	2,08	0,52	75	6,67	5,00	1,25	25	7,50	1,88	0,47	0,69
I1	Fuego	25	25	8,33	2,08	0,52	25	8,33	2,08	0,52	100	6,67	6,67	1,67	25	7,50	1,88	0,47	0,79
I2	Daños por agua	25	25	8,33	2,08	0,52	25	8,33	2,08	0,52	75	6,67	5,00	1,25	25	7,50	1,88	0,47	0,69
I5	Avería de origen físico / lógico	75	25	8,33	2,08	1,56	25	8,33	2,08	1,56	100	6,67	6,67	5,00	25	7,50	1,88	1,41	2,38
I6	Corte del suministro eléctrico	50	25	8,33	2,08	1,04	25	8,33	2,08	1,04	75	6,67	5,00	2,50	25	7,50	1,88	0,94	1,38
I7	Condiciones inadecuadas T/H	50	25	8,33	2,08	1,04	25	8,33	2,08	1,04	75	6,67	5,00	2,50	25	7,50	1,88	0,94	1,38
I8	Fallo de comunicaciones	50	50	8,33	4,17	2,08	50	8,33	4,17	2,08	100	6,67	6,67	3,34	50	7,50	3,75	1,88	2,34
I9	Interrupción otros servicios	75	25	8,33	2,08	1,56	25	8,33	2,08	1,56	100	6,67	6,67	5,00	25	7,50	1,88	1,41	2,38
I10	Degradación soportes	50	25	8,33	2,08	1,04	25	8,33	2,08	1,04	75	6,67	5,00	2,50	25	7,50	1,88	0,94	1,38
E1	Errores de los usuarios	75	50	8,33	4,17	3,12	50	8,33	4,17	3,12	75	6,67	5,00	3,75	50	7,50	3,75	2,81	3,20
E2	Errores del administrador	75	50	8,33	4,17	3,12	50	8,33	4,17	3,12	75	6,67	5,00	3,75	50	7,50	3,75	2,81	3,20
E3	Errores de monitorización	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	50	6,67	3,34	2,50	75	7,50	5,63	4,22	4,02
E4	Errores de configuración	75	50	8,33	4,17	3,12	50	8,33	4,17	3,12	75	6,67	5,00	3,75	50	7,50	3,75	2,81	3,20
E7	Deficiencias de la organización	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
E8	Difusión de SW dañino	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
E14	Escapes de información	75	100	8,33	8,33	6,25	50	8,33	4,17	3,12	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,71
E15	Alteración de la información	75	50	8,33	4,17	3,12	100	8,33	8,33	6,25	25	6,67	1,67	1,25	50	7,50	3,75	2,81	3,36
E18	Destrucción de la información	75	25	8,33	2,08	1,56	100	8,33	8,33	6,25	100	6,67	6,67	5,00	25	7,50	1,88	1,41	3,55
E19	Divulgación de información	75	100	8,33	8,33	6,25	25	8,33	2,08	1,56	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,32
E20	Vulnerabilidades de los programas	100	75	8,33	6,25	6,25	75	8,33	6,25	6,25	75	6,67	5,00	5,00	75	7,50	5,63	5,63	5,78
E21	Errores de mantenimiento (Sw)	75	50	8,33	4,17	3,12	50	8,33	4,17	3,12	75	6,67	5,00	3,75	50	7,50	3,75	2,81	3,20
E23	Errores de mantenimiento (Hw)	75	50	8,33	4,17	3,12	50	8,33	4,17	3,12	75	6,67	5,00	3,75	50	7,50	3,75	2,81	3,20

E24	Caída del sistema por f75 recursos	50	25	8,33	2,08	1,04	25	8,33	2,08	1,04	100	6,67	6,67	3,34	25	7,50	1,88	0,94	1,59
E25	Perdida de Equipos	75	100	8,33	8,33	6,25	25	8,33	2,08	1,56	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,32
E28	Indisponibilidad del personal	50	25	8,33	2,08	1,04	25	8,33	2,08	1,04	75	6,67	5,00	2,50	25	7,50	1,88	0,94	1,38
A.4	Manipulación de la configuración	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
A.5	Suplantación de la identidad	50	100	8,33	8,33	4,17	100	8,33	8,33	4,17	75	6,67	5,00	2,50	75	7,50	5,63	2,81	3,41
A.6	Abuso privilegios de acceso	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,71
A.7	Uso no previsto	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
A.8	Difusión de SW dañino	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
A.10	Alteración de secuencias	75	50	8,33	4,17	3,12	100	8,33	8,33	6,25	25	6,67	1,67	1,25	50	7,50	3,75	2,81	3,36
A.11	Acceso no autorizado	75	75	8,33	6,25	4,69	100	8,33	8,33	6,25	25	6,67	1,67	1,25	75	7,50	5,63	4,22	4,10
A.12	Análisis de tráfico	75	100	8,33	8,33	6,25	50	8,33	4,17	3,12	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,71
A.14	Intercepción de información	50	100	8,33	8,33	4,17	50	8,33	4,17	2,08	25	6,67	1,67	0,83	75	7,50	5,63	2,81	2,47
A.15	Modificación de la información	75	50	8,33	4,17	3,12	100	8,33	8,33	6,25	25	6,67	1,67	1,25	50	7,50	3,75	2,81	3,36
A.18	Destrucción de la información	75	25	8,33	2,08	1,56	100	8,33	8,33	6,25	100	6,67	6,67	5,00	25	7,50	1,88	1,41	3,55
A.19	Divulgación de información	75	100	8,33	8,33	6,25	25	8,33	2,08	1,56	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,32
A.22	Manipulación de programas	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
A.24	Denegación de servicio	75	25	8,33	2,08	1,56	25	8,33	2,08	1,56	100	6,67	6,67	5,00	25	7,50	1,88	1,41	2,38
A.25	Robo	75	100	8,33	8,33	6,25	25	8,33	2,08	1,56	25	6,67	1,67	1,25	75	7,50	5,63	4,22	3,32
A.26	Ataque destructivo	75	25	8,33	2,08	1,56	25	8,33	2,08	1,56	100	6,67	6,67	5,00	25	7,50	1,88	1,41	2,38
A.29	Extorsión	75	75	8,33	6,25	4,69	75	8,33	6,25	4,69	75	6,67	5,00	3,75	75	7,50	5,63	4,22	4,34
A.30	Ingeniería social	50	75	8,33	6,25	3,12	75	8,33	6,25	3,12	75	6,67	5,00	2,50	75	7,50	5,63	2,81	2,89

Ilustración 65. Valoración Navision

Anexo VI. Programa de auditoría

		Revisión		
Norma (ISO/IEC 27001:2013)		Año 1/3	Año 2/3	Año 3/3
4.	CONTEXTO DE LA ORGANIZACIÓN			
5.	LIDERAZGO			
6.	PLANIFICACIÓN			
7.	SOPORTE			
8.	OPERACIÓN			
9.	EVALUACIÓN DEL DESEMPEÑO			
10.	MEJORA			
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)				
5.	POLÍTICA DE SEGURIDAD			
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD			
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
8.	GESTIÓN DE ACTIVOS			
9.	CONTROL DE ACCESOS			
10.	CIFRADO			
11.	SEGURIDAD FÍSICA Y AMBIENTAL			
12.	SEGURIDAD EN LA OPERATIVA			
13.	SEGURIDAD EN LAS TELECOMUNICACIONES			
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
15.	RELACIONES CON SUMINISTRADORES			
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
18.	CUMPLIMIENTO			

Ilustración 66. Programa de auditoría

Anexo VII. Cuadro detalle Evaluación de Madurez

Medidas	SGSI	Actual		Inicial	
		Madurez	%	Madurez	%
Norma (ISO/IEC 27001:2013)					
4.	CONTEXTO DE LA ORGANIZACIÓN	L2	88 %	L1	40 %
4.1.	Comprensión de la organización y de su contexto.	L2	80 %	L0	0 %
4.2.	Compresión de las necesidades y expectativas de las partes interesadas.	L2	83 %	L0	0 %
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	L4	97 %	L2	80 %
4.4.	Sistema de gestión de seguridad de la información (SGSI).	L3	93 %	L2	80 %
5.	LIDERAZGO	L4	95 %	L1	20 %

5.1.	Liderazgo y compromiso.	L4	96 %	L1	20 %
5.2.	Política.	L4	97 %	L1	20 %
5.3.	Roles, responsabilidades y autoridades en la organización.	L3	93 %	L1	20 %
6.	PLANIFICACIÓN	L2	85 %	L1	30 %
6.1.	Acciones para tratar los riesgos y las oportunidades	L2	87 %	L2	60 %
6.1.1.	Consideraciones generales.	L2	83 %	L2	60 %
6.1.2.	Apreciación de riesgos de seguridad de la información.	L2	87 %	L2	60 %
6.1.3.	Tratamiento de los riesgos de seguridad de la información.	L3	92 %	L2	60 %
6.2.	Objetivos de seguridad de la información y planificación para su consecución.	L2	82 %	L0	0 %
7.	SOPORTE	L2	78 %	L1	20 %
7.1.	Recursos.	L2	78 %	L1	20 %
7.2.	Competencia.	L2	84 %	L1	20 %
7.3.	Concienciación.	L2	73 %	L1	20 %
7.4.	Comunicación.	L2	81 %	L1	20 %
7.5	Gestión Documental	L2	73 %	L2	60 %
8.	OPERACIÓN	L2	72 %	L1	10 %
8.1.	Planificación y control operacional.	L2	72 %	L1	10 %
8.2.	Apreciación de los riesgos de seguridad.	L2	77 %	L1	10 %
8.3.	Tratamiento de los riesgos de seguridad de la información.	L2	67 %	L1	10 %
9.	EVALUACIÓN DEL DESEMPEÑO	L2	76 %	L1	10 %
9.1.	Seguimiento, medición, análisis y evaluación.	L2	74 %	L1	10 %
9.2.	Auditoría interna.	L2	83 %	L1	10 %
9.3.	Revisión por la dirección.	L2	72 %	L1	10 %
10.	MEJORA	L2	83 %	L1	10 %
10.1.	No conformidad y acciones correctivas.	L2	78 %	L1	10 %
10.2.	Mejora continua.	L2	87 %	L1	10 %
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)					
5.	POLÍTICA DE SEGURIDAD	L4	97 %	L1	20 %
5.1.	Directrices de la Dirección en seguridad de la información:	L4	97 %	L1	20 %
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	L2	86 %	L1	33 %
6.1	Organización interna:	L2	74 %	L1	16 %
6.1.1.	Asignación de responsabilidades para la seguridad de la información.	L3	94 %	L1	20 %
6.1.2.	Segregación de tareas.	L2	82 %	L1	40 %
6.1.3.	Contacto con las autoridades.	L2	65 %	L0	0 %
6.1.4.	Contacto con grupos de interés especial.	L2	58 %	L0	0 %
6.1.5.	Seguridad de la información en la gestión de proyectos.	L2	72 %	L1	20 %
6.2.	Dispositivos para movilidad y teletrabajo:	L4	98 %	L2	50 %
6.2.1.	Política de uso de dispositivos para movilidad.	L4	95 %	L1	40 %

6.2.2.	Teletrabajo.	L5	100 %	L2	60 %
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	L3	94 %	L1	46 %
7.1.	Antes de la contratación:	L3	90 %	L2	50 %
7.1.1.	Investigación de antecedentes.	L2	88 %	L1	40 %
7.1.2.	Términos y condiciones de contratación.	L3	92 %	L2	60 %
7.2.	Durante la contratación:	L3	93 %	L1	27 %
7.2.1.	Responsabilidades de gestión.	L2	86 %	L1	20 %
7.2.2.	Concienciación, educación y capacitación en seguridad de la información.	L3	94 %	L1	20 %
7.2.3.	Proceso disciplinario.	L4	98 %	L1	40 %
7.3.	Cese o cambio de puesto de trabajo.	L4	98 %	L2	60 %
8.	GESTIÓN DE ACTIVOS	L2	82 %	L1	39 %
8.1.	Responsabilidad sobre los activos:	L2	85 %	L2	70 %
8.1.1.	Inventario de activos.	L2	87 %	L2	60 %
8.1.2.	Propiedad de los activos.	L3	92 %	L2	60 %
8.1.3.	Uso aceptable de los activos.	L2	86 %	L2	80 %
8.1.4.	Devolución de los activos.	L2	75 %	L2	80 %
8.2.	Clasificación de la información:	L2	64 %	L0	0 %
8.2.1.	Directrices de clasificación.	L2	64 %	L0	0 %
8.2.2.	Etiquetado y manipulación de la información.	L2	55 %	L0	0 %
8.2.3.	Manipulación de activos.	L2	72 %	L0	0 %
8.3.	Manejo de los soportes de almacenamiento:	L4	98 %	L1	47 %
8.3.1.	Gestión de soportes extraíbles.	L4	98 %	L0	0 %
8.3.2.	Eliminación de soportes.	L4	98 %	L2	60 %
8.3.3.	Soportes físicos en tránsito.	L4	98 %	L2	80 %
9.	CONTROL DE ACCESOS	L2	68 %	L1	38 %
9.1.	Requisitos de negocio para el control de accesos:	L2	86 %	L1	20 %
9.1.1.	Política de control de accesos.	L2	84 %	L1	20 %
9.1.2.	Control de acceso a las redes y servicios asociados.	L2	88 %	L1	20 %
9.2.	Gestión de acceso de usuario:	L2	59 %	L1	40 %
9.2.1.	Gestión de altas/bajas en el registro de usuarios.	L2	73 %	L2	60 %
9.2.2.	Gestión de los derechos de acceso asignados a usuarios.	L2	66 %	L2	60 %
9.2.3.	Gestión de los derechos de acceso con privilegios especiales.	L2	63 %	L1	20 %
9.2.4.	Gestión de información confidencial de autenticación de usuarios.	L2	74 %	L2	60 %
9.2.5.	Revisión de los derechos de acceso de los usuarios.	L1	35 %	L1	20 %
9.2.6.	Retirada o adaptación de los derechos de acceso.	L1	45 %	L1	20 %
9.3.	Responsabilidades del usuario:	L1	45 %	L1	40 %
9.3.1.	Uso de información confidencial para la autenticación.	L1	45 %	L1	40 %

9.4.	Control de acceso a sistemas y aplicaciones:	L2	83 %	L2	50 %
9.4.1.	Restricción del acceso a la información.	L2	67 %	L1	20 %
9.4.2.	Procedimientos seguros de inicio de sesión.	L4	98 %	L2	60 %
9.4.3.	Gestión de contraseñas de usuarios.	L5	100 %	L2	60 %
9.4.4.	Uso de herramientas de administración de sistemas.	L2	78 %	L2	60 %
9.4.5.	Control de acceso al código fuente de los programas.	L2	72 %	L2	60 %
10.	CIFRADO	L2	80 %	L1	20 %
10.1.	Controles criptográficos:	L2	80 %	L1	20 %
10.1.1.	Política de uso de los controles criptográficos.	L2	79 %	L1	20 %
10.1.2.	Gestión de claves.	L2	80 %	L1	20 %
11.	SEGURIDAD FÍSICA Y AMBIENTAL	L4	95 %	L2	70 %
11.1.	Áreas seguras:	L4	95 %	L2	70 %
11.1.1.	Perímetro de seguridad física.	L4	98 %	L2	70 %
11.1.2.	Controles físicos de entrada.	L4	98 %	L2	70 %
11.1.3.	Seguridad de oficinas, despachos y recursos.	L3	92 %	L2	70 %
11.1.4.	Protección contra las amenazas externas y ambientales.	L3	94 %	L2	70 %
11.1.5.	El trabajo en áreas seguras.	L4	97 %	L2	70 %
11.1.6.	Áreas de acceso público, carga y descarga.	L3	93 %	L2	70 %
11.2.	Seguridad de los equipos:	L3	95 %	L2	70 %
11.2.1.	Emplazamiento y protección de equipos.	L4	95 %	L2	70 %
11.2.2.	Instalaciones de suministro.	L4	97 %	L2	70 %
11.2.3.	Seguridad del cableado.	L3	93 %	L2	70 %
11.2.4.	Mantenimiento de los equipos.	L3	94 %	L2	70 %
11.2.5.	Salida de activos fuera de las dependencias de la empresa.	L4	98 %	L2	70 %
11.2.6.	Seguridad de los equipos y activos fuera de las instalaciones.	L2	87 %	L2	70 %
11.2.7.	Reutilización o retirada segura de dispositivos de almacenamiento.	L3	91 %	L2	70 %
11.2.8.	Equipo informático de usuario desatendido.	L4	98 %	L2	70 %
11.2.9.	Política de puesto de trabajo despejado y bloqueo de pantalla.	L4	99 %	L2	70 %
12.	SEGURIDAD EN LA OPERATIVA	L2	76 %	L1	39 %
12.1.	Responsabilidades y procedimientos de operación:	L2	69 %	L1	45 %
12.1.1.	Documentación de procedimientos de operación.	L2	78 %	L2	60 %
12.1.2.	Gestión de cambios.	L2	56 %	L1	40 %
12.1.3.	Gestión de capacidades.	L2	71 %	L1	20 %
12.1.4.	Separación de entornos de desarrollo, prueba y producción.	L2	69 %	L2	60 %
12.2.	Protección contra código malicioso:	L1	45 %	L1	40 %
12.2.1.	Controles contra el código malicioso.	L1	45 %	L1	40 %
12.3.	Copias de seguridad:	L4	99 %	L1	40 %
12.3.1.	Copias de seguridad de la información.	L4	99 %	L1	40 %
12.4.	Registro de actividad y supervisión:	L2	76 %	L1	15 %
12.4.1.	Registro y gestión de eventos de actividad.	L2	64 %	L0	0 %
12.4.2.	Protección de los registros de información.	L2	56 %	L0	0 %

12.4.3.	Registros de actividad del administrador y operador del sistema.	L2	84 %	L0	0 %
12.4.4.	Sincronización de relojes.	L5	100 %	L2	60 %
12.5.	Control del software en explotación:	L2	88 %	L2	80 %
12.5.1.	Instalación del software en sistemas en producción.	L2	88 %	L2	80 %
12.6.	Gestión de la vulnerabilidad técnica:	L2	89 %	L2	50 %
12.6.1.	Gestión de las vulnerabilidades técnicas.	L2	83 %	L1	20 %
12.6.2.	Restricciones en la instalación de software.	L4	95 %	L2	80 %
12.7.	Consideraciones de las auditorías de los sistemas de información:	L2	65 %	L0	0 %
12.7.1.	Controles de auditoría de los sistemas de información.	L2	65 %	L0	0 %
13.	SEGURIDAD EN LAS TELECOMUNICACIONES	L2	84 %	L1	48 %
13.1.	Gestión de la seguridad en las redes:	L2	82 %	L1	47 %
13.1.1.	Controles de red.	L2	84 %	L1	40 %
13.1.2.	Mecanismos de seguridad asociados a servicios de red.	L2	75 %	L2	60 %
13.1.3.	Segregación de redes.	L2	88 %	L1	40 %
13.2.	Intercambio de información con partes externas:	L2	85 %	L2	50 %
13.2.1.	Políticas y procedimientos de intercambio de información.	L2	84 %	L1	40 %
13.2.2.	Acuerdos de intercambio.	L2	75 %	L2	60 %
13.2.3.	Mensajería electrónica.	L3	94 %	L1	40 %
13.2.4.	Acuerdo de confidencialidad y secreto.	L2	86 %	L2	60 %
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	L2	58 %	L1	29 %
14.1.	Requisitos de seguridad de los sistemas de información:	L2	83 %	L1	37 %
14.1.1.	Análisis y especificación de los requisitos de seguridad.	L2	86 %	L1	40 %
14.1.2.	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	L2	76 %	L2	50 %
14.1.3.	Protección de las transacciones por redes telemáticas.	L2	88 %	L1	20 %
14.2.	Seguridad en los procesos de desarrollo y soporte:	L2	71 %	L1	30 %
14.2.1.	Política de desarrollo seguro de software.	L2	54 %	L1	20 %
14.2.2.	Procedimientos de control de cambios en los sistemas.	L2	56 %	L1	40 %
14.2.3.	Revisión técnica de las aplicaciones a efectuar cambios en el sistema operativo.	L2	67 %	L2	60 %
14.2.4.	Restricciones a los cambios en los paquetes de software.	L2	75 %	L2	60 %
14.2.5.	Uso de principios de ingeniería en protección de sistemas.	L2	66 %	L1	40 %
14.2.6.	Seguridad en entornos de desarrollo.	L2	89 %	L1	40 %
14.2.7.	Externalización del desarrollo de software.	L4	95 %	L1	40 %
14.2.8.	Pruebas de funcionalidad durante el desarrollo de los sistemas.	L2	62 %	L1	40 %
14.2.9.	Pruebas de aceptación.	L2	76 %	L1	40 %
14.3.	Datos de prueba:	L1	20 %	L1	20 %
14.3.1.	Protección de los datos utilizados en pruebas.	L1	20 %	L1	20 %
15.	RELACIONES CON SUMINISTRADORES	L3	93 %	L1	27 %
15.1.	Seguridad de la información en las relaciones con suministradores:	L4	96 %	L1	33 %

15.1.1.	Política de seguridad de la información para suministradores.	L4	98 %	L1	20 %
15.1.2.	Tratamiento de riesgo dentro de acuerdos de suministradores.	L4	99 %	L2	60 %
15.1.3.	Cadena de suministro en tecnologías de la información y comunicaciones.	L3	91 %	L1	20 %
15.2.	Gestión de la prestación del servicio por suministradores:	L3	90 %	L1	20 %
15.2.1.	Supervisión y revisión de los servicios prestados por terceros.	L2	87 %	L1	20 %
15.2.2.	Gestión de cambios en los servicios prestados por terceros.	L3	93 %	L1	20 %
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	L2	69 %	L1	40 %
16.1.	Gestión de incidentes de seguridad de la información y mejoras:	L2	69 %	L1	40 %
16.1.1.	Responsabilidades y procedimientos.	L2	56 %	L1	40 %
16.1.2.	Notificación de los eventos de seguridad de la información.	L2	79 %	L1	40 %
16.1.3.	Notificación de puntos débiles de la seguridad.	L2	64 %	L1	40 %
16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones.	L2	75 %	L1	40 %
16.1.5.	Respuesta a los incidentes de seguridad.	L2	65 %	L1	40 %
16.1.6.	Aprendizaje de los incidentes de seguridad de la información.	L2	87 %	L1	40 %
16.1.7.	Recopilación de evidencias.	L2	54 %	L1	40 %
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L4	98 %	L2	80 %
17.1.	Continuidad de la seguridad de la información:	L4	97 %	L2	80 %
17.1.1.	Planificación de la continuidad de la seguridad de la información.	L4	95 %	L2	80 %
17.1.2.	Implantación de la continuidad de la seguridad de la información.	L4	98 %	L2	80 %
17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	L4	97 %	L2	80 %
17.2.	Redundancias:	L5	100 %	L2	80 %
17.2.1.	Disponibilidad de instalaciones para el procesamiento de la información.	L5	100 %	L2	80 %
18.	CUMPLIMIENTO	L2	75 %	L1	36 %
18.1.	Cumplimiento de los requisitos legales y contractuales:	L2	85 %	L2	52 %
18.1.1.	Identificación de la legislación aplicable.	L2	80 %	L1	20 %
18.1.2.	Derechos de propiedad intelectual (DPI).	L4	98 %	L2	80 %
18.1.3.	Protección de los registros de la organización.	L4	97 %	L2	60 %
18.1.4.	Protección de los datos y privacidad de la información personal.	L4	99 %	L2	80 %
18.1.5.	Regulación de los controles criptográficos.	L2	53 %	L1	20 %
18.2.	Revisiones de la seguridad de la información:	L2	65 %	L1	20 %
18.2.1.	Revisión independiente de la seguridad de la información.	L2	65 %	L1	20 %
18.2.2.	Cumplimiento de las políticas y normas de seguridad.	L2	57 %	L1	20 %
18.2.3.	Comprobación del cumplimiento.	L2	74 %	L1	20 %

Ilustración 67. Cuadro detalle Evaluación de Madurez