Plan de Implementación de la norma ISO/IEC 27001

Nombre Estudiante: Elena Sánchez Hernández

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

RESUMEN EJECUTIVO

Universitat Oberta de Catalunya

Índice

1. Introducción

El presente proyecto tiene por objetivo definir y desarrollar un plan de implementación de la ISO/IEC 27001:2013 en un sistema informático que pertenece a una empresa del sector de la aviación. Para la definición de dicho plan es necesario analizar y evaluar las distintas funciones y áreas de la organización en el ámbito de la seguridad de la información. La organización en la que se engloba este proyecto cuenta con una larga trayectoria en el ámbito del estándar ISO/IEC 27001 pues todos sus sistemas tienen el mandato de implementarlo antes de su puesta en marcha. Así mismo, la organización certifica en el estándar diversos sistemas y servicios pues en el sector en el que opera la seguridad es una cuestión de máxima prioridad.

El sistema en el que se va a implantar el estándar cuenta con gran parte de su infraestructura en la nube pública, siendo un sistema pionero en la organización en este aspecto.

2. Objetivos y alcance del Trabajo

El objetivo que se persigue es el de implantar el Sistema de Gestión de la Seguridad de la Información (SGSI) para el sistema informático mencionado (GoOne) y que este asegure la confidencialidad, integridad y disponibilidad de la información que procesa. Adicionalmente, se persigue que con este proyecto se integren los procesos del sistema con los corporativos y se identifiquen posibles deficiencias en esta integración.

Se busca también, identificar los controles específicos para el sistema en la nube y su correcta gestión. Paralelamente, se busca trazar el sistema de gestión documental adecuado para el SGSI.

Por último, este proyecto busca también, concienciar a la organización de las necesidades de recursos para poder implementar adecuadamente la seguridad de la información en entornos nuevos como es el caso de la nube pública.

3. Resultados

3.1 Análisis Diferencial

El objetivo del proyecto es que el sistema GoOne se implante bajo un Sistema de Gestión de la Seguridad de la Información que cumpla con las normas ISO/IEC 27001, 27002 y 27017 para cloud.

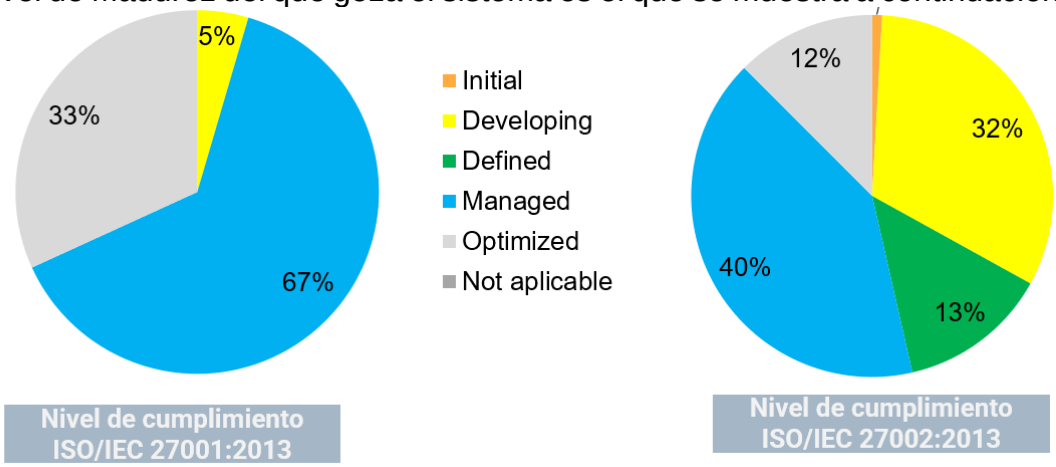
En la compañía la mayoría de los sistemas y procesos cumplen con el estándar 27001 como requisito determinado por la Directiva de Seguridad, así como por requisitos contractuales y legislativos. Sin embargo, el sistema GoOne al ser un desarrollo completamente nuevo con una arquitectura en la nube, el nivel de

implementación inicial respecto a los estándares es poco avanzado. Como se comentó con anterioridad, el proyecto necesita implementar estos estándares desde el diseño. Sin embargo, esto no significa que una vez analizado nos encontremos ante un nivel de madurez muy adecuado, pues como se ha indicado no solo la organización tiene un elevado nivel de madurez respecto al estándar 27001 sino que, además, el proveedor de servicios cloud, AWS, ostenta certificaciones 27001, 27017 o auditorías SOC1. No obstante, con el objetivo de estimar los esfuerzos derivados de la implementación de los estándares y los recursos necesarios, se ha hecho un análisis preliminar del posible estado teniendo en cuenta el nivel de madurez2 de los procesos organizativos respecto a los estándares ISO/IEC 27001, 27002 y 27017:

Nivel	Inicial	En desarrollo	Definido	Gestionado	Optimizado
Personas	Actividades sin personal o sin coordinación.	Liderazgo establecido, comunicación informal	Algunos controles en desarrollo con comunicación limitada	Mayores recursos y concienciación, funciones y responsabilidades claramente definidas	Se apoya la mejora continua de las competencias, los procesos y la tecnología en materia de seguridad
Procesos	No existe un programa formal de seguridad.	Proceso básico de gobernanza y gestión de riesgos, políticas	Procesos y políticas pero con una verificación mínima	Comités formales, procesos de verificación y medición	Procesos más exhaustivos, basados en el riesgo y con una comprensión cuantitativa
Tecnología	A pesar de los problemas de seguridad, no existen controles.	Algunos controles en desarrollo con comunicación limitada	Más controles documentados y desarrollados, pero demasiado dependientes de los esfuerzos individuales	Controles supervisados, medidos para el cumplimiento, pero niveles desiguales de automatización	Controles más exhaustivos, automatizados y sometidos a una mejora continua

Figure 1 - Marco Referencia Niveles Madurez

El Nivel de Madurez del que goza el sistema es el que se muestra a continuación:



[1] *"Programas de conformidad de AWS"* [Fecha de consulta: 3 de Marzo del 2022]. <https://aws.amazon.com/es/compliance/programs/>

[2] Dan Blum "*How to Assess Security Maturity and Make Improvements*", https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/ Fecha de consulta: 3 de Marzo del 2022].

3.2 Sistema de Gestión Documental

El sistema de gestión documental se basa en los siguientes documentos proporcionados por la compañía, los cuales se rigen por la estructura documental proporcionada por la norma ISO/IEC 27001 y cuyos contenidos se encontrarán en los anexos de este documento

- Política de Seguridad de la Información

La política de seguridad es una normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del presente SGSI. La política debería cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.

- Procedimiento de Auditorías Internas

Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

- Gestión de Indicadores

Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.

- Gestión de Roles y Responsabilidades del SGSI

Con el fin de establecer una estructura de roles y responsabilidades que permitan implantar el SGSI de manera exitosa, así como mantenerlo y supervisarlo de manera diligente y adecuada se ha desarrollado el siguiente organigrama específico para el SGSI de GoOne:

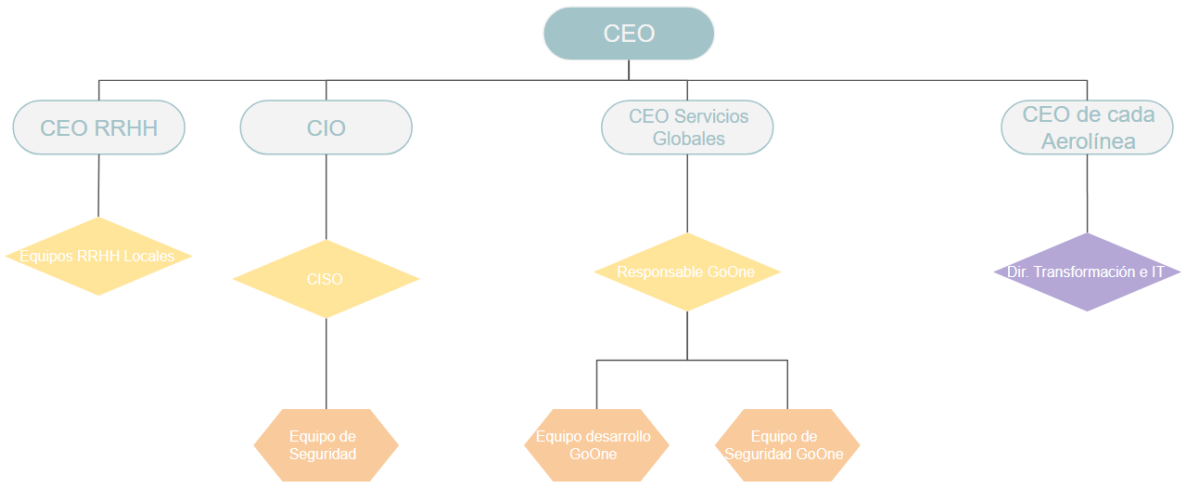


Ilustración 1 - Organigrama SGSI GoOne

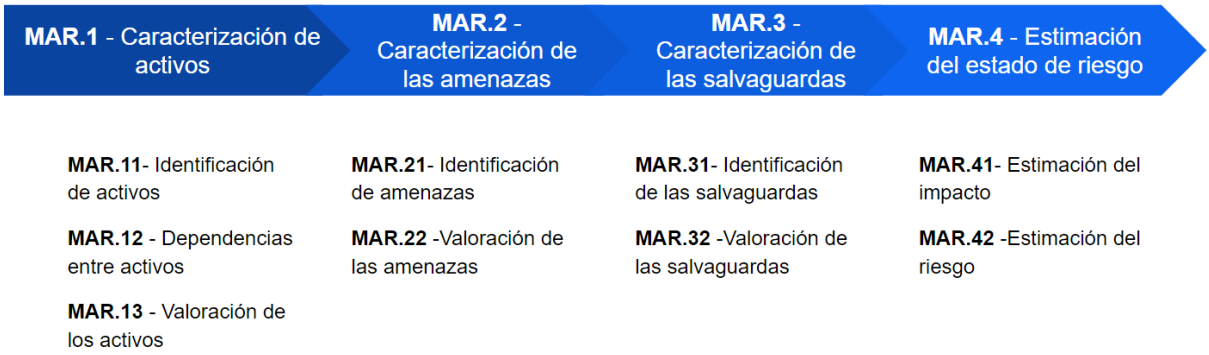
Cabe destacar que el organigrama del SGSI de GoOne parte del organigrama funcional del grupo, incluyendo detalle de aquellas áreas involucradas en el sistema GoOne.

- Metodología de Análisis de Riesgos

Dentro de las distintas necesidades y procesos que han de implementarse dentro de una organización para mantener y asegurar la seguridad de la información se encuentra la gestión de riesgos como pieza clave. La gestión de riesgos es la principal herramienta para detectar aquellas vulnerabilidades y/o amenazas que afectan a los principales activos de una organización.

En este proyecto nos basaremos en MAGERIT como metodología estándar de análisis y gestión de riesgos. Dicha metodología fue definida por el Ministerio de Administraciones Públicas y ha sufrido varias modificaciones desde su publicación hasta la que utilizaremos en este proyecto, la versión V3 publicada en 2012.[3]

Magerit define el proceso de identificación y evaluación del riesgo a través de distintas fases:



- Declaración de Aplicabilidad

Documento que define los controles de seguridad establecidos para el sistema, con la aplicabilidad y el estado actual.

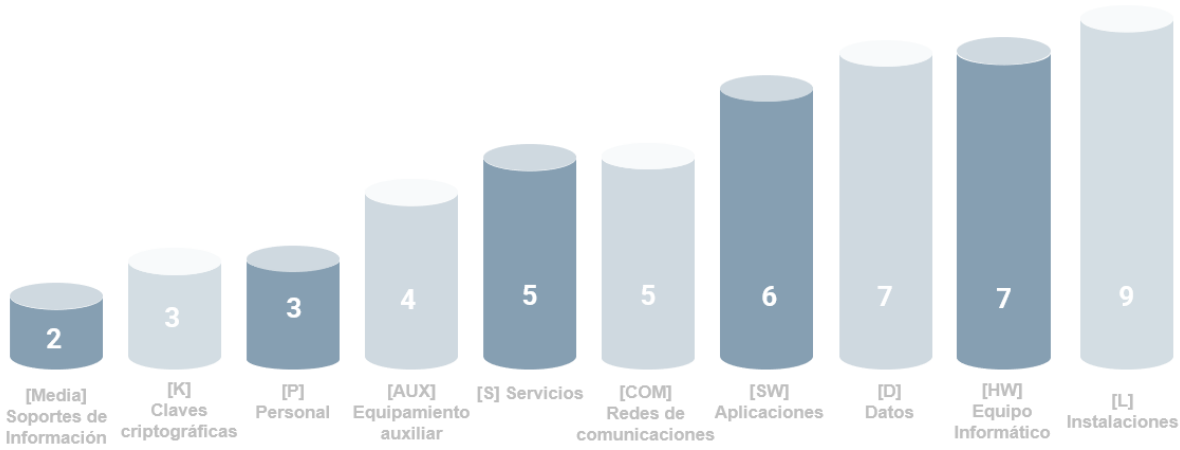
3.3 Análisis de Riesgos

Como parte del proceso de definición e implantación de este SGSI se debe proceder con la evaluación de los activos de nuestro sistema. Para ello vamos a apoyarnos en la metodología definida.

- Inventario, valoración y dimensión de activos

Para realizar el análisis de riesgos atenderemos al primer paso propuesto por Magerit, que es la **Caracterización de los activos (MAR.1)** cuyo punto inicial es la valoración de los activos. En el caso de GoOne el inventario de activos es el que sigue:

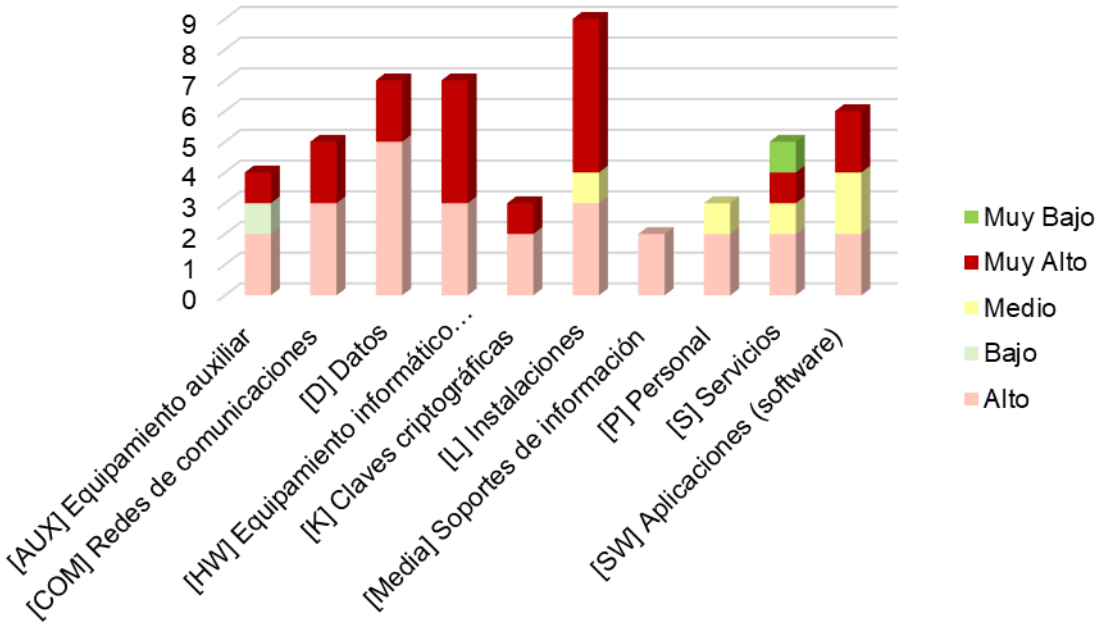
[3] "*Magerit – Libro I- Método*" https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8ixx2gzaM-



Una vez categorizado el activo, pasaremos a la **valoración del activo (MAR.13)** que ayudará a calibrar las medidas necesarias para protegerlo basado en la siguiente tabla de referencia:

Valoración	Rango posibles daños
Muy Alto	Pérdida económica mayor a 50 Millones de euros
Alto	Pérdida económica de entre 8 a 50Millones de euros
Medio	Pérdida económica de entre 1 a 8Millones de euros
Bajo	Pérdida económica de entre 200.000.000 a 1Millones de euros
Muy Bajo	Pérdida económica menor a 200.000.000 euros

Para GoOne el resultado de la valoración de los activos arrojó el siguiente resultado:



Seguidamente se han de valorar los activos en función de una serie de valoraciones respecto a su dimensión que permitan aproximar las posibles consecuencias derivadas de la materialización de una amenaza. Dichas dimensiones son:

Disponibilidad (D), Integridad de los datos (I), **Confidencialidad (C)**. Existen adicionalmente, una escala detallada en Magerit V3.0 para valorar el impacto en cualquiera de las tres dimensiones presentadas:

Valor		Criterio
10	Extremo	Daño muy grave a la organización o Pérdida de personas
7-9	Muy Alto	Daño grave a la organización o Personas con daños graves en su salud
4-6	Alto	Daño importante a la organización o Personas con daños moderados en su salud
1-3	Medio	Daño menor a la organización o Personas con daños leves en su salud
0	Bajo	Irrelevante a efectos prácticos o Ninguna persona afectada

De acuerdo con los criterios anteriores se ha definido el Inventario de los activos incluyendo la correspondiente valoración para las dimensiones .

- Identificación y Valoración de Amenazas

Siguiendo la metodología proporcionada por Magerit V.3 vamos a proseguir con el análisis de riesgos, más concretamente con la segunda fase de **Caracterización de Amenazas (MAR.2).** Dentro de la fase de caracterización de amenazas comenzaremos por la **Identificación de Amenazas (MAR 2.1).** Para ello se va a utilizar el catálogo de amenazas ofrecido por Magerit V.3 Libro II obteniendo las siguientes para GoOne:

Seguidamente vamos a proceder a definir los rangos de probabilidades para las amenazas de manera que se puedan estimar las frecuencias de ocurrencia de cada amenaza, parte de la fase **MAR.2 Caracterización de las amenazas** definida por la metodología Magerit V.3:

Valor		Criterio
3	**Alta**	Ha ocurrido en la propia organización previamente

		Se tiene constancia de su posible materialización en algún momento
2	**Media**	El evento se ha producido en el sector en varias ocasiones
1	**Baja**	Se conoce 1 o 2 eventos similares en el sector

Con todo lo anterior hemos procedido a analizar las amenazas respecto al inventario de activos.

- Impacto Potencial y nivel de riesgo aceptable

Una vez hemos obtenido el detalle de amenazas y respectivos valores para cada activo, vamos a calcular el impacto potencial que conllevaría la materialización de dichas amenazas para la organización:

Impacto potencial = valor del activo X max(valor del impacto)

Una vez analizadas las amenazas y el riesgo de estas respecto a los activos (resultado de multiplicar la frecuencia máxima de ocurrencia por el impacto potencial del activo) de la organización se va a definir un cuadro de decisión de apetito y decisión sobre los riesgos identificados, de manera que la Dirección tenga una herramienta para determinar si un riesgo puede ser aceptado o no.

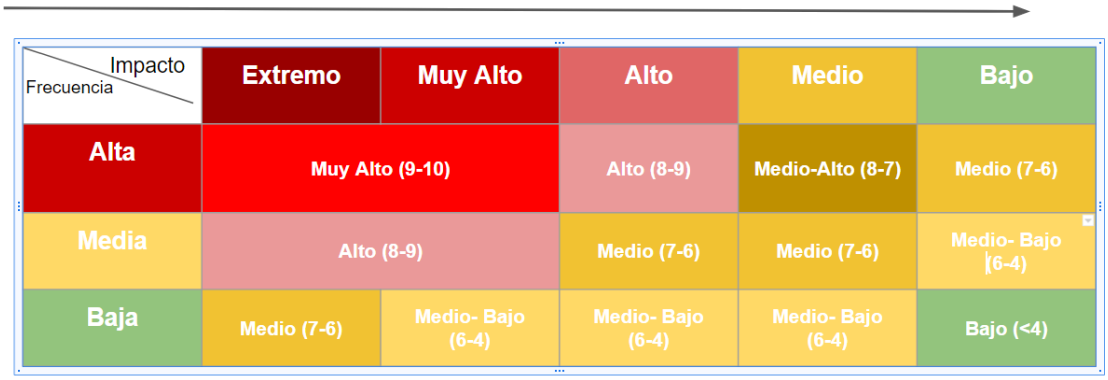
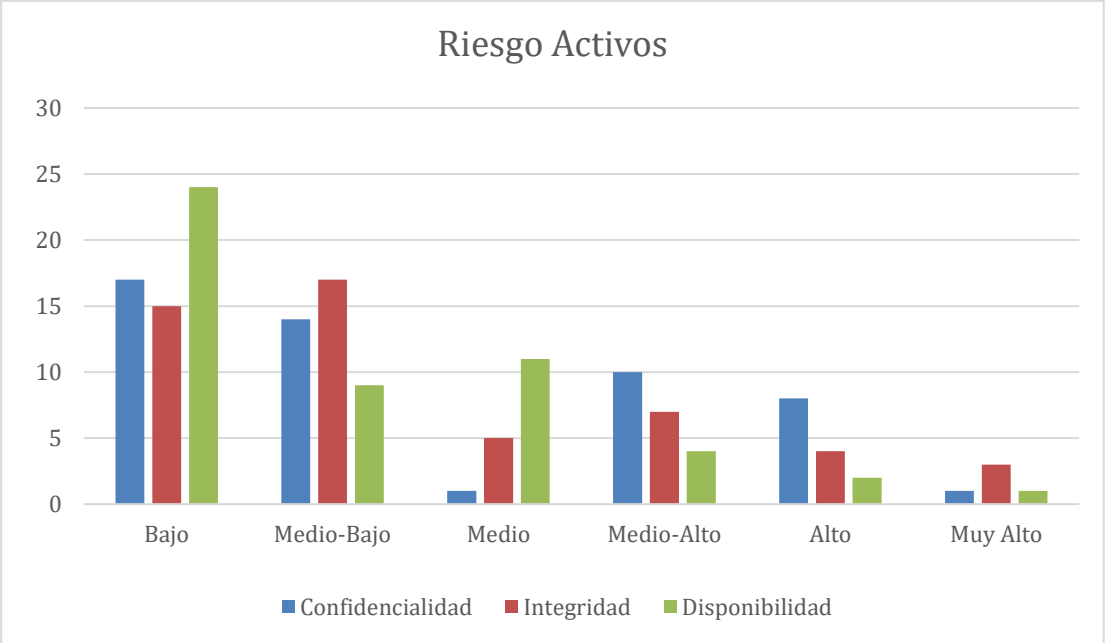


Ilustración 2 – Niveles de Riesgo Aceptable

En el siguiente gráfico observamos que para niveles de riesgo “Muy alto” el número es mayor en cuanto a integridad y que para nieles de riesgo “Alto” el número es mayor en cuanto a confidencialidad se refiere.



3.4 Propuestas de proyectos

Con base a los riesgos detectados y el análisis diferencial existente se han propuesto proyectos que ayuden a reducir el riesgo para aquellos activos con un Riesgo "Muy alto" o "Alto". Además, se ha tenido en cuenta los resultados del análisis diferencial para la propuesta de proyectos, procurando que estos faciliten la mejora del análisis diferencial sobre los estándares objetivo:

- Proyecto I- Definición e implantación de Política de desarrollo seguro de software en la nube
- Proyecto II- Integración del proceso de gestión de identidades y accesos de la nube en el sistema corporativo
- Proyecto III- Creación del modelo operacional para GoOne
- Proyecto IV- Integración inventario de activos en CMDB corporativa
- Proyecto V- Control del servicio del proveedor de nube
- Proyecto VI- Sistema de control sobre el cumplimiento de la política de seguridad de cloud

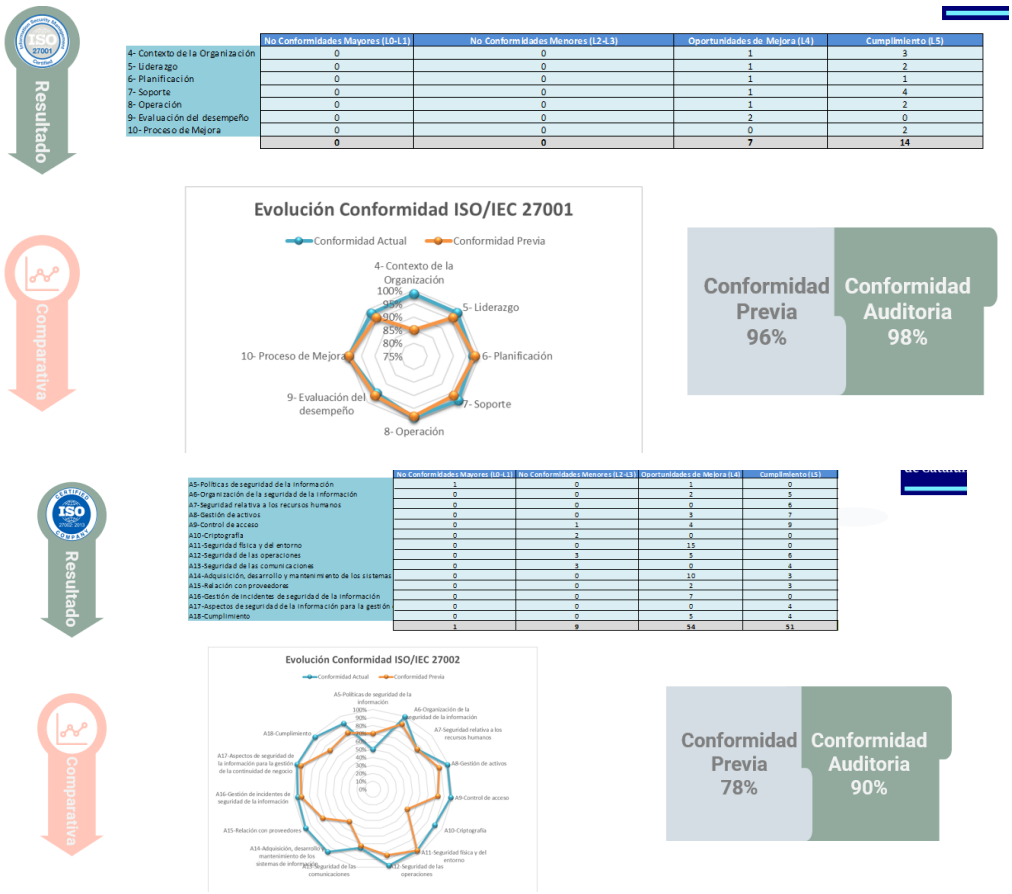
3.5 Auditoría de cumplimiento

Dado que los proyectos propuestos ya han sido implementados la organización y los responsables para el SGSI de GoOne consideran que sería el momento adecuado para realizar una auditoría de cumplimiento respecto a la norma ISO/IEC 27001:2013.

Con este ejercicio se espera confirmar que las planificaciones y expectativas sobre los riesgos y los controles de la norma habrán mejorado tras la implantación de las medidas incluidas en el plan de proyectos.

- Resultado de la Auditoría

Tras la ejecución de la auditoria y los hallazgos que el proceso ha arrojado, se muestra a continuación una vista general de los resultados obtenidos reportados por el informe de Auditoría:



	No Conformidades Mayores (L0-L1)	No Conformidades Menores (L2-L3)	Oportunidades de Mejora (L4)	Cumplimiento (L5)
4- Contexto de la Organización	0	0	1	3
5- Liderazgo	0	0	1	2
6- Planificación	0	0	1	1
7- Soporte	0	0	1	4
8- Operación	0	0	1	2
9- Evaluación del desempeño	0	0	2	0
10- Proceso de Mejora	0	0	0	2
	0	0	7	14

	No Conformidades Mayores (L0-L1)	No Conformidades Menores (L2-L3)	Oportunidades de Mejora (L4)	Cumplimiento (L5)
A5-Políticas de seguridad de la información	1	0	1	0
A6-Organización de la seguridad de la información	0	0	2	5
A7-Seguridad relativa a los recursos humanos	0	0	0	6
A8-Gestión de activos	0	0	3	7
A9-Control de acceso	0	1	4	9
A10-Criptografía	0	2	0	0
A11-Seguridad física y del entorno	0	0	15	0
A12-Seguridad de las operaciones	0	3	5	6
A13-Seguridad de las comunicaciones	0	1	0	4
A14-Adquisición, desarrollo y mantenimiento de los sistemas	0	0	10	3
A15-Relación con proveedores	0	0	2	3
A16-Gestión de incidentes de seguridad de la información	0	0	7	0
A17-Aspectos de seguridad de la información para la gestión	0	0	0	4
A18-Cumplimiento	0	0	5	4
	1	9	54	51

Observamos que en este caso el resultado de conformidades obtenido en la auditoría respecto a la conformidad previa basada en el análisis diferencial es muy significativa. Este resultado, viene en gran medida por las mejoras obtenidas gracias a la implementación del plan de proyectos presentado.

- Destaca en este caso una **No conformidad Mayor** relacionada con el proceso de gestión de políticas de seguridad, en este caso para servicios en la nube:

Control	Observación
A5.1.2 - Revisión de las políticas para la seguridad de la información	Se ha observado que existe un proceso de revisión de la política de seguridad en la nube que se localiza de manera informal y concreta en un grupo de la compañía pero que no se implementa de manera formal y periódica a nivel global.

- Observamos también, nueve **No conformidades Menores** en distintas áreas de control.

Control	Observación
A9.4.2-	Si bien se ha comprobado que existe un procedimiento seguro de inicio de sesión contra las herramientas de

Procedimientos seguros de inicio de sesión	gestión de identidades y accesos corporativas, se recomienda implementar finalmente un sistema de multifactor para entornos en la nube que no solo se limite a usuarios administrativos.
A10.1.1-Política de uso de los controles criptográficos	Se ha comprobado que la política de seguridad en la nube establece la política de controles criptográficos para el entorno sin embargo se ha comprobado que en GoOne este control se ha definido, pero no se ha podido aplicar técnicamente.
A10.1.2-Gestión de claves	Se ha comprobado que a consecuencia de encontrar limitaciones técnicas para la implementación del control de claves en la nube no se está gestionando de manera adecuada, si bien existe un plan para su corrección.
A12.4.1-Registro de eventos	Se ha verificado que se ha definido recientemente el proceso de monitorización de registro de eventos, pero está pendiente de implementar.
A12.4.2-Protección de la información del registro	Se ha verificado que se ha definido recientemente un proceso de captura y gestión segura de registros, pero está pendiente de implementar en los próximos meses.
A12.4.3-Registros de administración y operación	Se ha identificado que existe una configuración de controles de red, pero no se alinea con los controles definidos por las políticas de seguridad.
A13.1.1-Controles de red	Se ha verificado que el equipo de GoOne está detallando formalmente los controles y las necesidades en materia de seguridad de red y segregación de esta pero que no se han implementado en el entorno.
A13.1.2-Seguridad de los servicios de red	Se ha verificado que el equipo de GoOne ha establecido una segregación de redes, pero esta no se ajusta a un proceso formal documentado.
A13.1.3-Segregación en redes	Si bien se ha comprobado que existe un procedimiento seguro de inicio de sesión contra las herramientas de gestión de identidades y accesos corporativas, se recomienda implementar finalmente un sistema de multifactor para entornos en la nube que no solo se limite a usuarios administrativos.

3.6 Conclusiones

Como se ha comprobado gracias a los resultados presentados anteriormente, el Sistema de Gestión de Seguridad auditado para GoOne, goza de un aceptable y favorable madurez. Hemos verificado que el sistema se ha definido correctamente, incluyendo un alcance ajustado y una definición de roles y responsabilidades adecuada.

Cabe destacar, el favorable impacto en los resultados que ha proporcionado el plan de proyectos implantado por la organización y que ha proporcionado una mejora sustancial en la conformidad y cumplimiento respecto los estándares objetivos. Notable mejoría en el área de desarrollo seguro donde se ha comprobado la efectividad del procedimiento de desarrollo implantado o en el área de gestión de activos, donde se ha verificado el nivel de granularidad y exactitud en la gestión de los activos en la nube una vez integrado en la CMDB corporativa.

Sin embargo, se han detectado una serie de no conformidades para las cuales se deberá trazar un plan de remediación y aplicarla a lo largo de los próximos meses, con el fin de evitar próximas no conformidades en el siguiente ejercicio de auditoría.

Finalmente, es importante señalar que, aunque el SGSI ha mostrado tener un nivel de madurez aceptable y favorable en gran parte por el elevado nivel de cumplimiento de los procesos corporativos (auditados ya en varias ocasiones), el nivel de cumplimiento de controles técnicos en la nube es más débil. Se aconseja emplear recursos en mejorar el nivel de capacitación, así como recursos del equipo de GoOne para que se puedan acometer las mejoras propuestas pues fortalecerán no solo el nivel de madurez de las operaciones en la nube, sino que también, mejorará el nivel se seguridad de la información en el entorno. Así mismo, se aconseja considerar una auditoría de tipo SOC para GoOne que verifique de manera más exhaustiva el cumplimiento de sus controles en cuanto a diseño, implementación y eficacia operativa.