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

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

Título del Trabajo Final

Nombre Estudiante: Elena Sánchez Hernández

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

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

Fecha entrega: 25 Mayo 2022

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un plan de Implementación de la norma ISO/IEC 27001*
Nombre del autor:	*Elena Sánchez Hernández*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	05/2022
Titulación:	Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	Castellano
Palabras clave	*SGSI, Cloud, Seguridad*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El presente proyecto persigue como objetivo definir un Plan Director para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro un sistema basado en la nube pública. Es por ello, que dicho SGSI se basa en la norma ISO/IEC 27001:2013, así como en las guías de buenas prácticas ISO/IEC 27002:2013 ISO/IEC 27017:2015.

La definición e implantación del SGSI se ha basado en una contextualización y análisis inicial de la organización, el sistema objetivo y su cumplimiento respecto a la norma. De manera complementaria se ha realizado un análisis exhaustivo de los activos principales del sistema y los riesgos y amenazas asociados a estos basado en la metodología Magerit. Todo ello, con el fin de obtener una lista de prioridades respecto a los riesgos del sistema que permitiese trazar un plan de proyectos destinado a mitigar esos riesgos más prioritarios, así como mejorar el cumplimiento de aquellos controles más deficientes detectados en el análisis diferencial inicial.

Finalmente, el proyecto ha concluido con la revisión del cumplimiento mediante un ejercicio de auditoría interna permitiendo verificar el favorable estado de cumplimiento del SGSI y si este asegura de manera adecuada la confidencialidad, integridad y disponibilidad de la información.

Abstract (in English, 250 words or less):

The objective of this project is to define a Master Plan for the implementation of an Information Security Management System (ISMS) within a public cloud-based system. Therefore, the ISMS is based on the ISO/IEC 27001:2013 standard, as well as on the ISO/IEC 27002:2013 ISO/IEC 27017:2015 best practice guides.

The definition and implementation of the ISMS was based on an initial contextualization and analysis of the organization, the target system and its compliance with the standard. In addition, an exhaustive analysis of the main assets of the system and the risks and threats associated with them has been carried out based on Magerit methodology. All this, in order to obtain a list of priorities with respect to system risks that would allow to draw up a project plan aimed at mitigating these priority risks, as well as to improve compliance with the most deficient controls detected in the initial differential analysis.

Finally, the project concluded with a compliance review through an internal audit exercise to verify the positive state of compliance of the ISMS and whether it adequately ensures the confidentiality, integrity and availability of information.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

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.

1.2 Objetivos 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 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.

1.3 Enfoque y método seguido

Para la realización de este proyecto se va a seguir un enfoque metodológico basado en la experiencia de la organización con el estándar y los procesos de implantación que se corresponderán parcialmente con las fases en las que se acometerá el proyecto:

1. Análisis del cumplimiento inicial
2. Definición y/o adecuación del Sistema de Gestión documental
3. Análisis de Riesgos basado en la metodología Magerit
4. Decisión sobre riesgos detectados
5. Propuesta e implementación del plan de proyectos

6. Auditoría interna

1.4 Planificación del Trabajo

El presente trabajo se desarrollará en el plazo de 3 meses naturales, llevando a cabo entregas quincenales (aproximadamente) de cada una de las fases, pudiendo efectuar mejoras y correcciones en cada fase de entregas anteriores.

1.5 Breve sumario de productos obtenidos

Los entregables del presente proyecto, incluirán los siguientes productos:

- Resumen ejecutivo
- Memoria del proyecto (este documento) junto con los siguientes anexos:
    1. Anexo I: Análisis diferencial
    2. Anexo II: Política de Seguridad de la Información
    3. Anexo III: Procedimiento de Auditoría
    4. Anexo IV: Gestión de Indicadores
    5. Anexo V: Declaración de Aplicabilidad
    6. Anexo VI: Inventario Activos
    7. Anexo VII: Identificación y Valoración de Amenazas
    8. Anexo VIII: Impacto Potencial de los Activos
    9. Anexo IX: Análisis de Riesgo
    10. Anexo X: Detalle controles post-proyectos
    11. Anexo XI: Informe Ejecutivo Auditoría Interna
    12. Anexo XII: Detalle Resultados Auditoría
- Presentación del proyecto
- Video de presentación del proyecto

1.6 Breve descripción de los otros capítulos de la memoria

Fase 1: SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

- **Introducción:** Fase de planteamiento del proyecto para sentar las bases del Plan Director de Seguridad del sistema.
- **Conociendo la ISO/IEC 27002:** documentación y análisis del estándar para aplicarlo más adelante.
- **Contextualización:** Se presenta el marco empresarial en el que se desarrolla el proyecto y el sistema objeto.
- **Objetivos del plan director:** Definición de los objetivos dentro del margo organizativo.
- **Análisis Diferencial:** Análisis del estado inicial de cumplimiento del sistema objeto.

- **Resultados:** Definición y presentación de los resultados sobre el estado inicial del cumplimiento.

Fase 2: SISTEMA DE GESTIÓN DOCUMENTAL

- **Introducción:** sobre el esquema documental para el cumplimiento normativo.
- **Esquema documental:** Definición del listado de documentos que forman parte del esquema documental del SGSI.

Fase 3: ANÁLISIS DE RIESGOS

- **Introducción:** sobre el proceso de análisis de riesgos a grandes rasgos.
- **Inventario de activos:** Estudio de los activos asociados al sistema objeto.
- **Valoración de activos:** Determinación del valor de los activos identificados para el sistema.
- **Dimensiones de la seguridad:** Estudio de la criticidad de cada activo mediante las principales dimensiones de la seguridad.
- **Análisis de amenazas:** Estudio de las amenazas que pueden afectar al sistema.
- **Impacto potencial:** Análisis del impacto potencial sobre la posible materialización de las amenazas identificadas.
- **Nivel de riesgo aceptable y riesgo residual:** Definición criterio de determinación del nivel de riesgo y marco de decisión.
- **Resultado:** Conclusiones y presentación de resultados del análisis de riesgos.

Fase 4: PROPUESTAS DE PROYECTOS

- **Introducción:** sobre el proceso de propuestas de proyectos y selección/priorización de estos.
- **Propuestas:** Presentación del portfolio de proyectos presentados basados en los resultados obtenidos hasta el momento.

Fase 5: AUDITORÍA DE CUMPLIMIENTO

- **Introducción:** una vez se han implementado los proyectos se ha de evaluar el estado del cumplimiento del sistema.
- **Metodología:** se define la metodología del proceso de auditoría.
- **Evaluación de madurez:** se evalúa la madurez de los controles y procesos respecto al estándar ISO/IEC 27001 y los controles del anexo A.
- **Resultado:** Conclusiones y presentación de resultados del ejercicio de auditoría.

Fase 6: PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

- **Introducción:** una vez se ha llegado a este punto es momento de analizar los hitos alcanzados y formalizar los resultados.
- **Objetivos de la fase y entregables:** se define la documentación que ha de acompañar a todo el proceso de implementación del SGSI.

2. Situación actual: Contextualización, Objetivos y Análisis Diferencial

2.1 Conociendo los estándares ISO/IEC 27002 e ISO/IEC 27017

Los estándares ISO/IEC son desarrollados por organizaciones internacionales, gubernamentales y no gubernamentales, así como por miembros de ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional). Todos ellos conforman el comité técnico ISO/IEC JTC 1 que trabaja en las normas y estándares Internacionales para la Seguridad de la Información. [1]

Dentro de este comité técnico se han desarrollado los Estándares Internacionales para el Sistema de Gestión de Seguridad de la Información (ISMS) que conforman hoy en día la familia de estándares con secuencia 27000.[2]

En este proyecto nos vamos a enfocar en el estándar ISO/IEC 27001 como referencia para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI), así como herramienta de apoyo para la definición de normas de gestión de la seguridad de la información. Adicionalmente, vamos a complementarnos con el estándar ISO/IEC 27002 cuyos objetivos son desarrollar una serie de normas organizativas para la seguridad, prácticas para la gestión de esta y proporcionar confianza a los principales actores (internos y externos). Dicho estándar se publicó por primera vez en 2005 bajo la referencia ISO/IEC 17799:2005 y que posteriormente en 2007 adoptó la secuencia que conocemos hoy en día, ISO/IEC 27002.

La norma consta de 14 dominios dentro de los cuales encontraremos 35 objetivos de seguridad y 114 controles (en su totalidad).[3]

Recientemente, se ha publicado una actualización del estándar ISO/IEC 27002 en el que se han reducido significativamente el número de controles, a 93, así como el número de categorías de cara a hacer del estándar. Además, se han añadido 11 controles relacionados con áreas relativamente nuevas que no cubría la versión anterior:

- Inteligencia de amenazas.
- Seguridad de la información en la nube.
- Continuidad del negocio.
- Seguridad física y su supervisión.
- Configuración.
- Eliminación de la información.

---

[1] "ISO/IEC 27001" https://www.iso.org/isoiec-27001-information-security.html [Fecha de consulta: 27 de Febrero del 2022].

[2] ESTÁNDAR ISO/IEC INTERNACIONAL 17799, *tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información*

[3] ESTÁNDAR ISO/IEC INTERNACIONAL 17799, *tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información*

[4] Silvia Garre Gui, Antonio José Segovia Henares, Arsenio Tortajada Gallego (septiembre 2020). *"Implantación de un sistema de gestión de la seguridad de la información (SGSI)"* (Tercera edición). Fundació Universitat Oberta de Catalunya (FUOC)

- Encriptación de datos.
- Prevención de fugas de datos.
- Seguimiento y monitoreo.
- Filtrado web.
- Codificación segura.

Mencionar, también, que esta última publicación de la norma ISO/IEC 27002 añade una clasificación por tipo de control y función: preventivos, detectivos o correctivos.

Adicionalmente, vamos a incorporar a este proyecto la norma ISO/IEC 27017 la cual incluye un código de buenas prácticas para la seguridad de la información específicas enfocadas a la provisión y el uso de servicios cloud. Este estándar está basado en la bien conocida ISO/IEC 27002, fue publicado en el año 2015 y ratificada en el 2021.

2.2 Contexto

La empresa seleccionada para este trabajo se enmarca en el sector de la aviación comercial, siendo un grupo integrado por distintas aerolíneas bajo un mismo conglomerado empresarial. Entre sus marcas se encuentran tanto aerolíneas tradicionales como de bajo coste. Adicionalmente, cuenta con diversas marcas destinadas al sector de cargo o transporte aéreo.

El grupo cuenta con alrededor de 650 aeronaves, opera en 250 destinos y tiene una media de volumen de pasajeros anualmente de 120.453.000. Adicionalmente, sus ingresos anuales se acercan a 27 millones de euros, en el año previo a la pandemia.

Desde que el grupo se formó, se ha ido definiendo y consolidando una estructura de gobierno central que permita establecer un marco común estratégico e integrado de cara a poder alinear los objetivos de las aerolíneas integradas con los objetivos del grupo. Con esta finalidad y paralelo a esta estructura de gobierno central se han ido conformando una serie de servicios centrales e integrados al servicio de las aerolíneas que les permiten no solo cumplir con el marco de gobierno del grupo, sino que, además, les permite adoptar una estandarización de procesos clave dentro de la operativa.

Debido al sector en el que se opera y la seguridad que este requiere las compañías integradas en el grupo partían de unos estándares de seguridad de IT maduros, no solo por la confianza que eso les otorga en el mercado sino por las estrictas regulaciones internacionales que han de cumplirse. Todo esto acompañado con las numerosas auditorías a las que deben someterse de manera periódica.

Transcurridos ya siete años desde la formación del grupo y con una estructura de gobierno central consolidada y adoptada de manera eficiente por todas las marcas del grupo, en gran medida por la integración de servicios centrales, el estado de seguridad de la compañía y de sus marcas podría considerarse maduro.

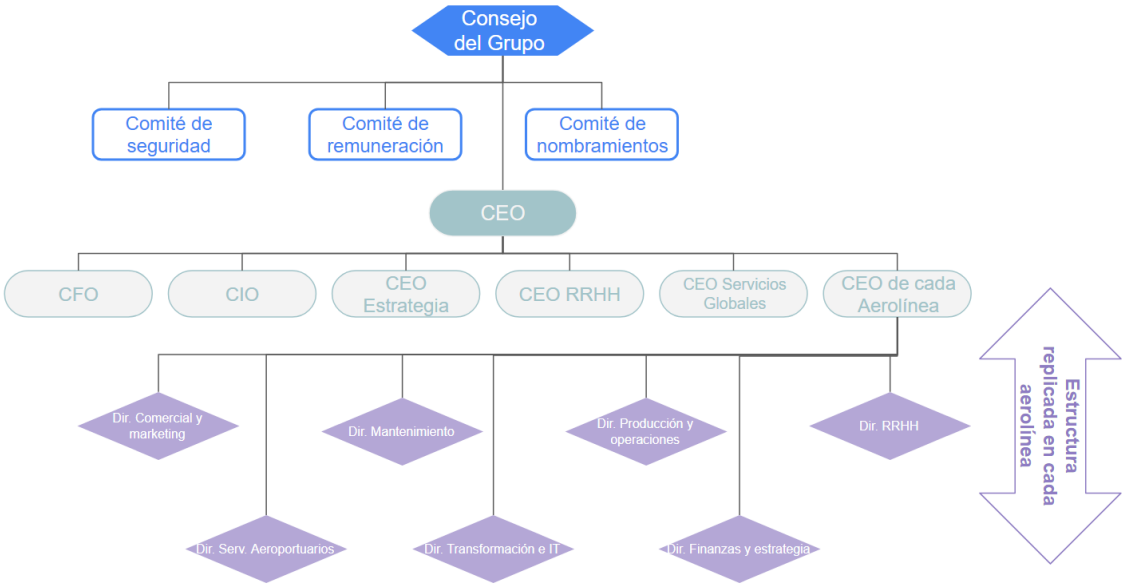

Ilustración 1 - Organigrama Funcional

Entre los mandatos y medidas establecidas desde el gobierno central de la compañía se encuentra la definición de política corporativa de seguridad, así como un marco de seguridad basado en ISO 27001. El CISO global de la compañía (dependiente del CIO) junto con las oficinas de seguridad del resto de aerolíneas se aseguran de que los procedimientos globales y su aplicación a nivel aerolínea se alineen con los estándares definidos y se apliquen adecuadamente.

Dentro de las estrategias de transformación del grupo empresarial que vienen determinadas por las decisiones del CEO en conjunto con el consejo del grupo se encuentra la de integrar las operaciones de todas las aerolíneas sobre un mismo sistema (GoOne System), de manera que el proceso sea estándar para todas ellas y se asegure una alineación respecto a los principales objetivos que se pretenden cubrir:

- Unificación proceso operaciones aéreas
- Maximización de la eficiencia operativa ofrecida por las aeronaves
- Mejora de la eficiencia sostenible de las aeronaves (cumplir con restricciones de gasto de combustible, ser más eficientes en el uso del combustible)

Debido a la pandemia de la COVID y al gran impacto que esta ha supuesto en el sector de la aviación comercial [4]la compañía ha decidido que este sistema se desarrolle en la nube dentro en la modalidad de Infraestructura como Servicio (IaaS- Infrastructure as a Service) de manera que les permita tener una infraestructura dinámica y escalable que se pueda adaptar a la demanda de manera ágil. Además, el sistema se encontrará en dos localizaciones para poder

[4] "Impacto en la aviación de la pandemia de COVID-19"https://es.wikipedia.org/wiki/Impacto_en_la_aviaci%C3%B3n_de_la_pandemia_de_COVID-19 [Fecha de consulta: 27 de Febrero del 2022].

cubrir requisitos de disponibilidad, recuperación de desastres y privacidad de datos.

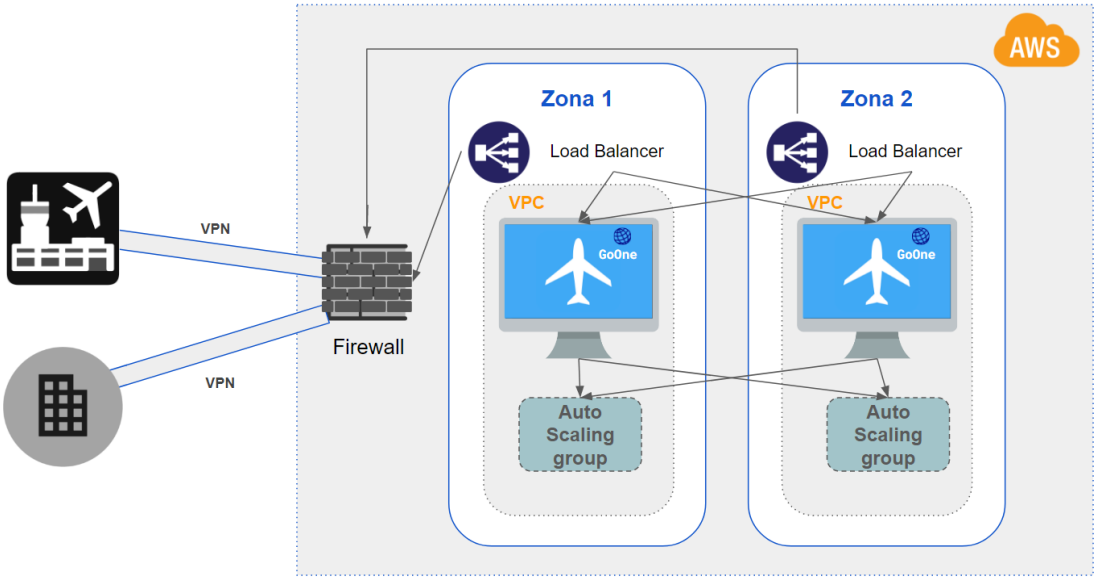

Ilustración 2 - Arquitectura simple del sistema GoOne

El programa para implantar este sistema viene esponsorizado por el CIO y el CEO y se liderará desde el área de servicios globales que serán los dueños del producto. Adicionalmente, se creará un grupo de trabajo dentro de cada aerolínea para participar tanto en las fases diseño e implementación del producto.

2.3 Objetivos del Plan Director

Existe el mandato por directiva de seguridad que todos los nuevos sistemas/productos se diseñen bajo el marco de políticas de seguridad de la compañía y se establezca un marco de SGSI basado en ISO 27001. Además, el CISO de la compañía ha promovido que puesto que este será el primer producto en la nube de la compañía se incluya en el SGSI el estándar ISO 27017 para controles de seguridad en la nube. Por lo tanto, el sistema ha de diseñarse e implementarse de acuerdo a los requisitos de ambos estándares para que una vez implementado, se lleve a cabo la certificación por parte de un organismo externo.

El objetivo que se persigue es que se asegure que el sistema garantice la confidencialidad, integridad y disponibilidad de la información, de manera que la seguridad de la información sea debidamente gestionada con este propósito.[5] Además, este requisito es primordial dentro del marco de continuidad y recuperación ante desastres pues ayudará a minimizar ciertos riesgos.

Por otro lado, es importante añadir que este programa es esponsorizado desde la oficina del CIO y desde la oficina del CEO pues se busca dar respuesta a dos

[5] Jordi Piera Jiménez, Jose Ramón Rodriguez, “La confección del Plan director de sistemas de información del sistema sanitario integral de utilización pública de Cataluña” (Primera edición). Fundació Universitat Oberta de Catalunya (FUOC)

de los tres objetivos estratégicos del grupo, que ya resaltamos en el capítulo anterior. Estos objetivos van unidos intrínsecamente y de manera obligada a otro de los objetivos permanentes del grupo: ser referente en la industria en cuanto a prácticas de seguridad se refiere.

Es importante apuntar en este punto, que hablamos de un sistema que será categorizado como crítico, por lo tanto, no solo por lo comentado anteriormente habrá de cumplir con los requisitos de continuidad establecidos para estos sistemas (RTO, RPO, redundancy) Por esta última razón el sistema persigue como uno de sus objetivos que la arquitectura será redundante, disponiendo de dos zonas y dentro de estas con distintas zonas de disponibilidad para mayor disponibilidad y resiliencia.

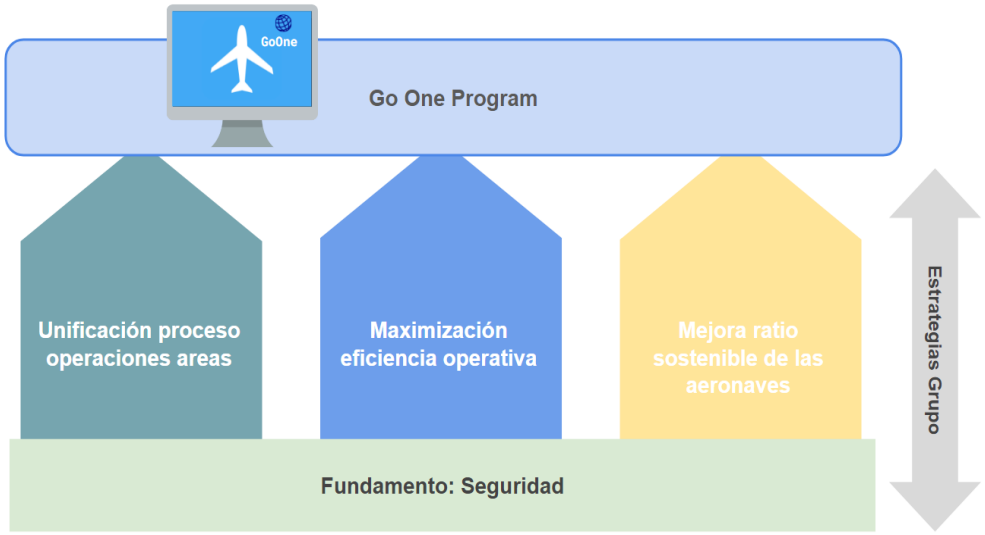

Ilustración 3 - GoOne Objetivos Estratégicos

2. 4 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 SOC6. No obstante, con el objetivo de

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

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 madurez7 de los procesos organizativos respecto a los estándares ISO/IEC 27001, 27002 y 27017:

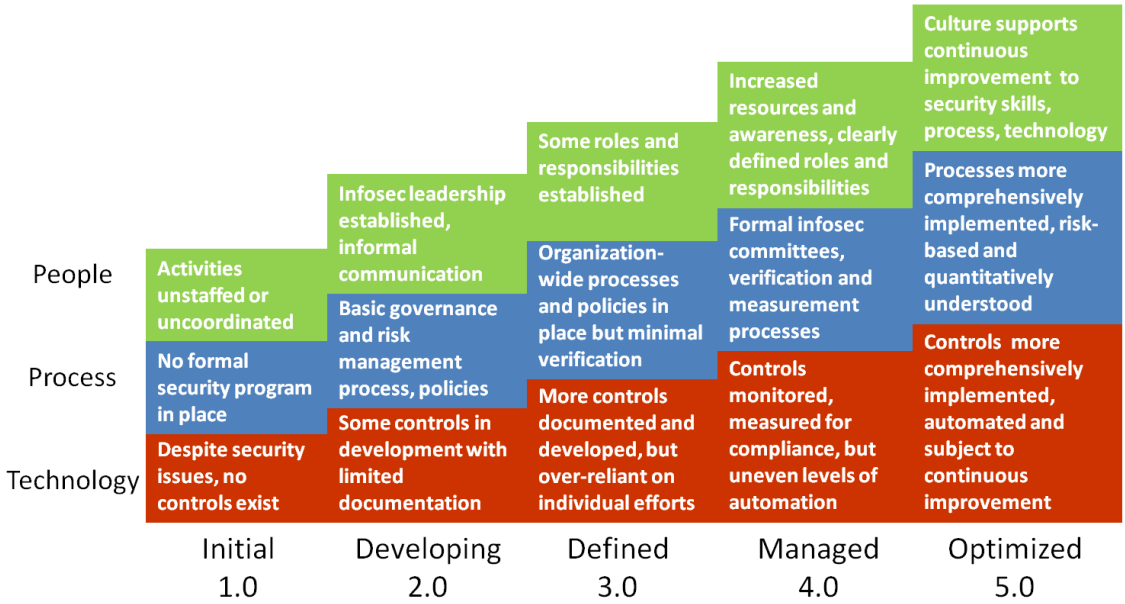

Figure 1 - Marco Referencia Niveles Madurez

El **análisis diferencial** (ver Anexo I: Análisis Diferencial) consta de un listado detallado de los controles incluidos en el estándar ISO/IEC 27001 junto con los controles complementarios del estándar ISO/IEC 27017, en aquellos casos en que exista un control o recomendación complementario para entornos en la nube:

[7] 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].

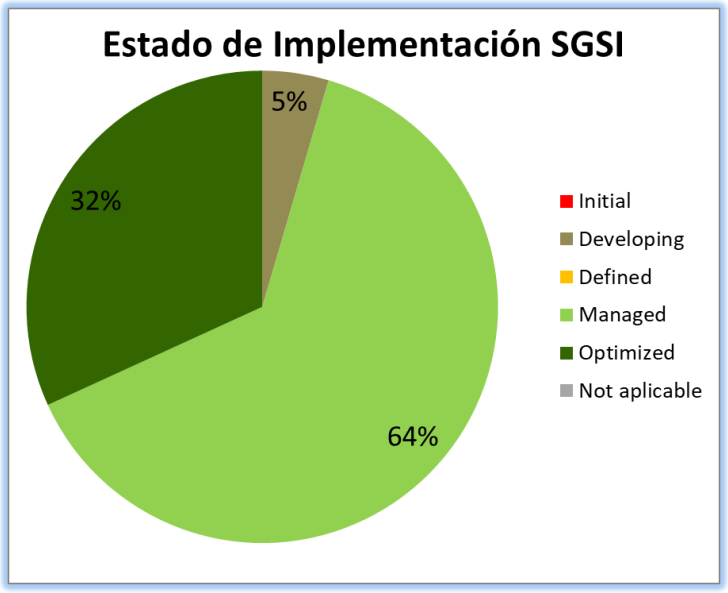

Ilustración 4 – Vista Estado Implementación SGSI

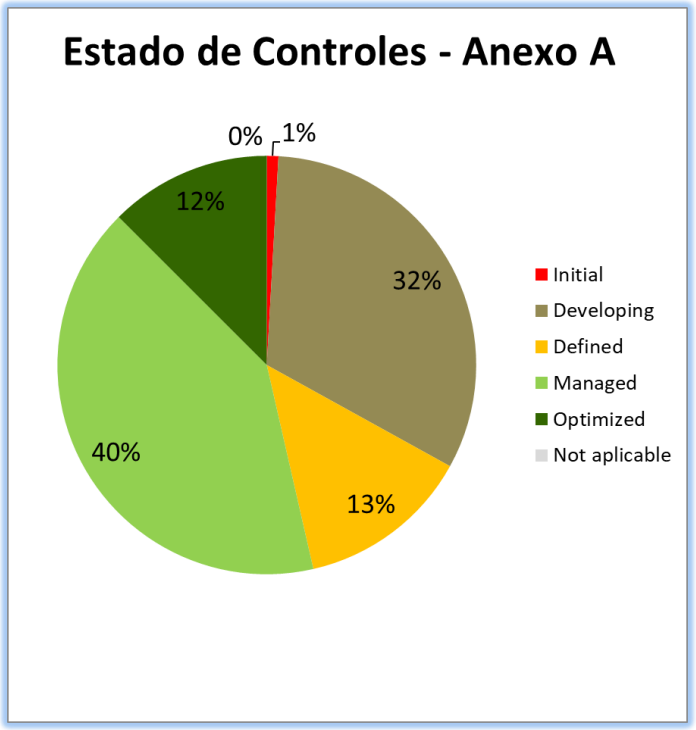

Ilustración 5 – Vista Estado Controles Anexo A

3. 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

3.1 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.

Ver Anexo: Anexo II: Política de Seguridad de la Información

3.2 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.

Ver Anexo: Anexo III: Procedimiento de Auditoría

3.3 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.

Ver Anexo: Anexo IV: Gestión de Indicadores

3.3 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:

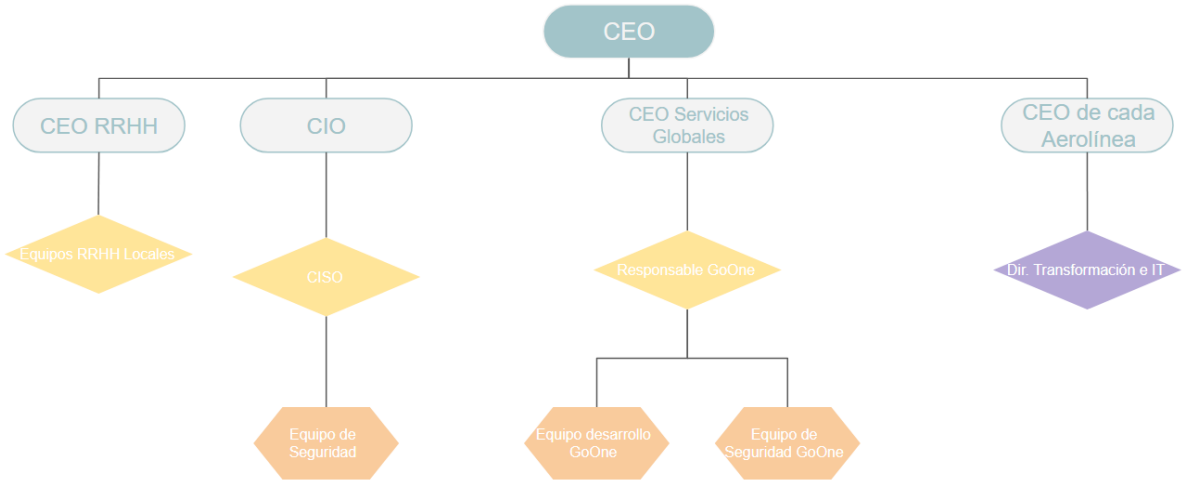

Ilustración 6 - Organigrama SGSI GoOne

Cabe destacar que el organigrama del SGSI de GoOne parte del organigrama funcional del grupo (Ilustración 1 - Organigrama Funcional), incluyendo detalle de aquellas áreas involucradas en el sistema GoOne.

El grupo que conforma el **comité ejecutivo de SGSI de GoOne** incluye a el CEO, CIO y el CISO del grupo, así como al CEO de Servicios Globales y el CEO de cada aerolínea. Las responsabilidades que ostenta este grupo son las de decidir sobre las estrategias, objetivos y sus relativas modificaciones respecto al sistema GoOne, así como realizar una supervisión no solo a nivel estratégico sino a nivel de los objetivos de seguridad y rendimiento del sistema.

- CEO
  - Espónsor del proyecto de GoOne, así como el proyecto de implantación del SGSI
  - Realizará a escala ejecutiva cierta labor de supervisión con el fin de asegurar que GoOne cumpla con los objetivos estratégicos establecidos dentro de la organización.
- CIO
  - Facilitador dentro de GoOne la adopción de las tecnologías adecuadas, así como de los recursos necesarios
  - Fijar las políticas en materia de Seguridad y SGSI
- CISO
  - Junto con el CIO establece la política global de SGSI y supervisa la política de SGSI para GoOne
  - Figura de supervisión sobre el cumplimiento y aplicación de los controles de seguridad establecidos en las políticas y estándares corporativos
  - Monitorizan las auditorías externas e internas

  - Supervisan y reportan aquellos eventos relevantes sobre la seguridad de la información

- CEO Servicios Globales
  - Espónsor junto con el CEO del proyecto de GoOne siendo principal responsable a nivel ejecutivo de su implementación
  - Reporta al comité ejecutivo de SGSI de GoOne sobre su progreso, nivel de implementación, seguridad y rendimiento
  - Colabora con el responsable de GoOne para facilitar los recursos necesarios en materia de desarrollo del sistema y seguridad
- CEO de cada aerolínea
  - Representan a cada a aerolínea ejerciendo como principal punto de conexión respecto a los objetivos estratégicos del grupo y los de cada aerolínea
  - Ejercen de figura responsable dentro de cara aerolínea sobre el correcto uso de GoOne, cumplimiento de controles operativos por los usuarios dentro de cada aerolínea y reporte de incidentes notables.

Fuera del comité ejecutivo existen otras funciones cuyas responsabilidades dentro del SGSI de GoOne se definen a continuación:

- Equipo de Seguridad Corporativo (del CISO):
  - Apoyan la figura y responsabilidades del CISO
- Responsable GoOne:
  - Es el responsable operativo de GoOne, asegurando que cumple con los objetivos definidos
  - Es responsable del correcto ciclo de vida del sistema, aprobando cualquier cambio relevante
  - Supervisa y monitoriza el cumplimiento de los controles de seguridad de la Información, así como de las políticas corporativas
- Equipo de desarrollo GoOne:
  - Realiza el desarrollo del sistema, asegurando que los requisitos funcionales y técnicos se cumplimentan adecuadamente
  - Asegura que los requisitos de seguridad del sistema se integren en el sistema de manera adecuada
- Equipo de seguridad GoOne:
  - Especifica los controles y configuraciones de seguridad dentro del sistema GoOne
  - Monitoriza el cumplimiento de los controles de seguridad
  - Monitoriza la confidencialidad, integridad y disponibilidad de la información del sistema, reportando incidentes de seguridad

- Colabora con los usuarios dentro de cada aerolínea para asegurar la transferencia de conocimiento y correcta operativa del sistema

- Dirección de Transformación en IT de cada aerolínea:
  - Aseguran que los usuarios del sistema GoOne lo operen de manera adecuada
  - Proporcionan la formación para los usuarios de GoOne
  - Monitorizan el correcto funcionamiento y operativa de GoOne, reportando incidencias e incidentes que se detecten (técnicos, de seguridad o de rendimiento).

3.4 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.

Así mismo, dentro de la gestión de riesgos existen distintas metodologías para el análisis de estos riesgos de manera que se asegure un correcto proceso de identificación, calibración y análisis de impacto. Para la implantación de un SGSI basado en estándar ISO/IEC 27001 es necesario definir una metodología de análisis de riesgos para los principales activos y procesos del SGSI.

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.[8]

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

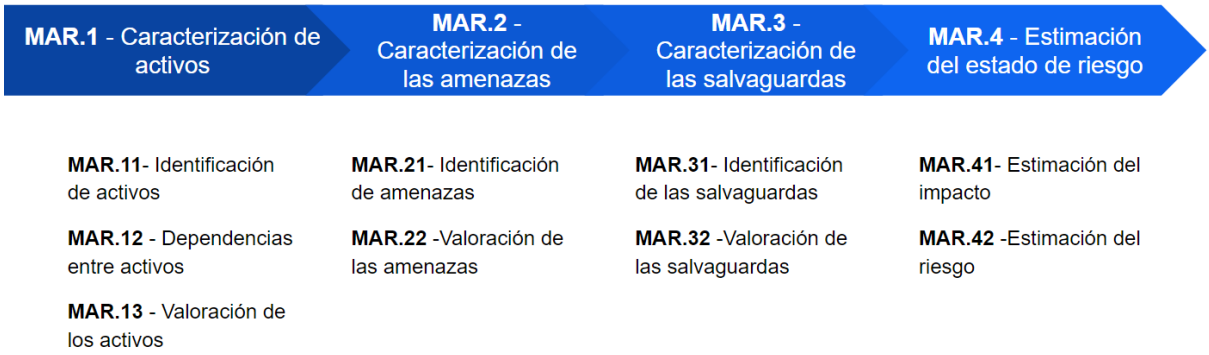

Ilustración 7 – Método de Análisis de Riesgos Magerit

1. **MAR.1 - Caracterización de los activos**

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

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado "**modelo de valor**".

2. **MAR.2** - **Caracterización de las amenazas**

   Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

   El resultado de esta actividad es el informe denominado "**mapa de riesgos**".

3. **MAR.3** - **Caracterización de las salvaguardas**

   Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

   El resultado de esta actividad se concreta en varios informes:

   I. Declaración de aplicabilidad
   II. Evaluación de salvaguardas
   III. Insuficiencias

4. **MAR.3** – **Estimación del estado de riesgo**

   Esta actividad procesa todos los datos recopilados en las actividades anteriores para:

   I. realizar un informe del estado de riesgo: estimación de impacto y riesgo
   II. realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

Como parte de la metodología de análisis de riesgos se habrán de identificar los activos principales MAR.1, para ello se usará como referencia el libro II de Magerit que contiene el catálogo de elementos principales[9]:

- Activos esenciales: información
- Arquitectura del sistema
- [D] Datos / Información
- [K] Claves criptográficas
- [S] Servicios
- [SW] Aplicaciones (software)
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar

[9] "*Magerit – Libro II- Catálogo de Elementos*" https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8ixx2gzaM-

- [L] Instalaciones
- [P] Personal

3.5 Declaración de Aplicabilidad

La existencia de todos estos documentos constituye evidencias palpables de que el Sistema de Gestión está funcionando. Ver Anexo V: Declaración de Aplicabilidad.

4. 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 (ver 3.4 Metodología de Análisis de Riesgos) donde ya presentamos las categorías de activos que proporciona Magerit y en las cuales nos íbamos a apoyar.

4.1 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 primer lugar, las **categorías de activos** que disponemos son las siguientes:

- Activos esenciales: información
- Arquitectura del sistema
- [D] Datos / Información
- [K] Claves criptográficas
- [S] Servicios
- [SW] Aplicaciones (software)
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

Una vez categorizado el activo, pasaremos a la **valoración del activo (MAR.13)** que ayudará a calibrar las medidas necesarias para protegerlo. Dicha valoración se habrá de realizar de manera que muestre cual sería el impacto en las personas derivado de una amenaza materializada en el activo. Es importante que dicha valoración se base en parte, en un posible resultado que afecte a la seguridad de las personas pues el negocio de la aviación civil exige un nivel de seguridad para sus usuarios muy elevado.

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

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 se extraen de las referencias proporcionadas también, por Magerit V3.0.

- **Disponibilidad (D)**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Integridad de los datos (I)**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Confidencialidad (C)**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

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 en el Anexo VI: Inventario Activos.

4.2 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 que incluye las siguientes categorías:

[N]	**Desastres naturales**
[N.1]	Fuego
[N.2]	Daños por agua
[N.*]	Desastres Naturales
[I]	**De 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 o lógico
[I.6]	Corte del suministro eléctrico
[I.7]	Condiciones inadecuadas de temperatura o humedad
[I.8]	Fallo de servicios de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales
[I.10]	Degradación de los soportes de almacenamiento de la información
[I.11]	Emanaciones electromagnéticas
[E]	**Errores y fallos no intencionados**
[E.1]	Errores de ellos usuarios
[E.2]	Errores del administrador
[E.3]	Errores de monitorización (log)
[E.4]	Errores de configuración
[E.7]	Deficiencias en la organización
[E.8]	Difusión de software dañino
[E.9]	Errores de [re-]encaminamiento
[E.10]	Errores de secuencia
[E.14]	Escapes de información
[E.15]	Alteración accidental de la información
[E.18]	Destrucción de información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)
[E.24]	Caída del sistema por agotamiento de recursos
[E.25]	Pérdida de equipos
[E.28]	Indisponibilidad del personal
[A]	**Ataques intencionados**
[A.3]	Manipulación de los registros de actividad (log)
[A.4]	Manipulación de la configuración
[A.5]	Suplantación de la identidad del usuario

[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.9]	[Re-]encaminamiento de mensajes
[A.10]	Alteración de secuencia
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.13]	Repudio
[A.14]	Interceptación de información (escucha)
[A.15]	Modificación deliberada de la información
[A.18]	Destrucción de información
[A.19]	Divulgación de información
[A.22]	Manipulación de programas
[A.23]	Manipulación de los equipos
[A.24]	Denegación de servicio
[A.25]	Robo
[A.26]	Ataque destructivo
[A.27]	Ocupación enemiga
[A.28]	Indisponibilidad del personal
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)

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

Cabe recordar que dentro de Magerit se define Probabilidad dentro de la metodología de gestión del riesgo como "(…*) la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente,*

cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática [tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado].”

Con todo lo anterior hemos procedido a analizar las amenazas respecto al inventario de activos. Ver Anexo VII: Identificación y Valoración de Amenazas.

4.3 Impacto Potencial

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.

Para ello vamos a calcular dicho impacto potencial como el resultado del porcentaje del impacto máximo del activo por el valor asignado al activo (ver Anexo VIII: Impacto Potencial de los Activos)

4.4 Nivel de Riesgo Aceptable y Residual

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.

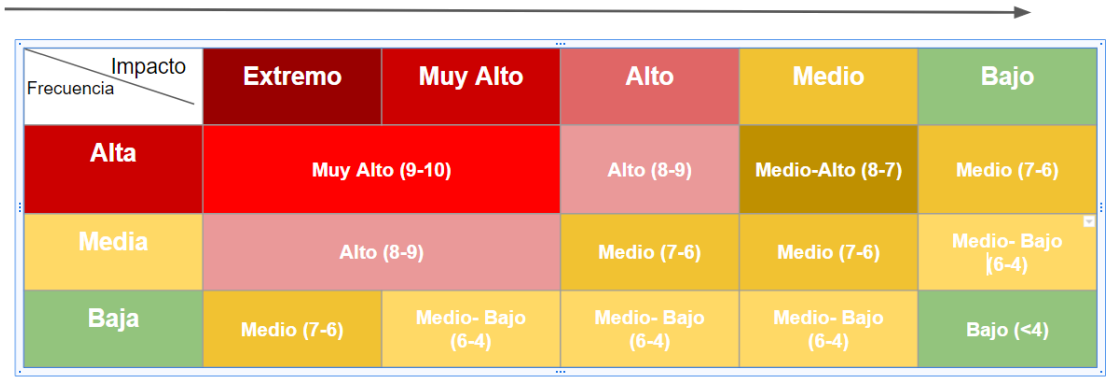

Ilustración 8 – Niveles de Riesgo Aceptable

Ver Niveles de riesgo calculados para el análisis de amenazas respecto a los activos en el Anexo IX: Análisis de Riesgo.

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.

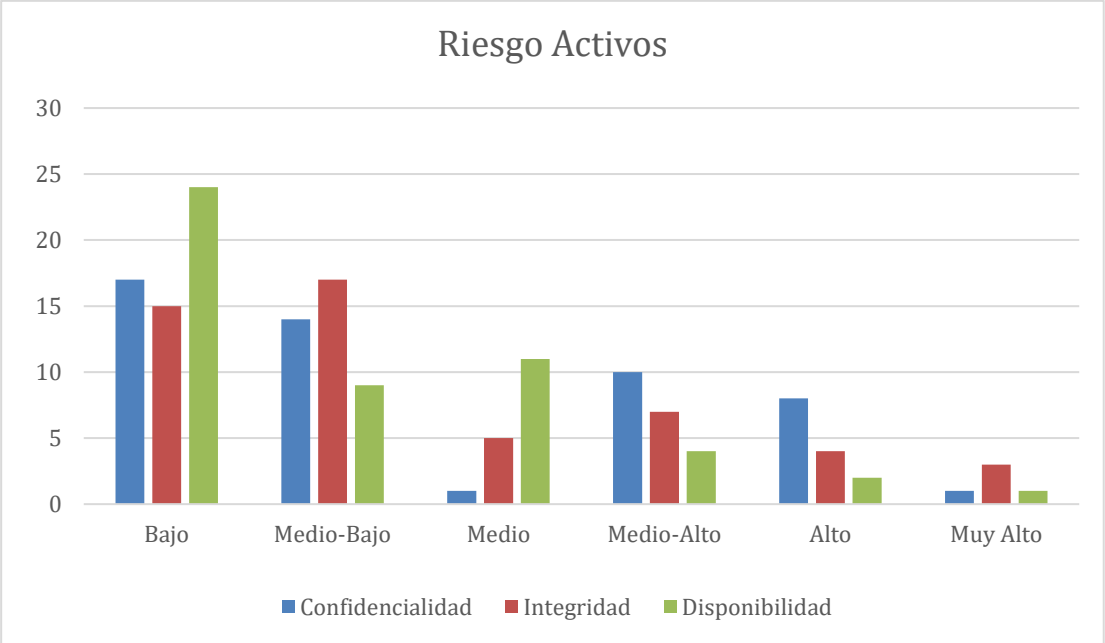

Ilustración 9 – Resultado Riesgos Activos

5. Propuestas de Proyectos

Tras haber analizado el estado/nivel de cumplimiento del sistema GoOne respecto a el estándar ISO/IEC 27001 y 27002 así como el análisis de riesgos de sus activos nos encontraríamos en el momento adecuado de analizar y proponer aquellos proyectos necesarios para mejorar el nivel de cumplimiento y tratar también, los riesgos más prioritarios detectados en nuestro análisis.

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.

5.1 Proyecto I- Definición e implantación de Política de desarrollo seguro de software en la nube

Objetivo	Establecer un sistema de desarrollo seguro de software adaptado al entorno de nube que garantice que el código se desarrolla y se mantiene asegurando un entorno estable y seguro.
Activos Impactados	• AUX3- Equipamiento a bordo • HW6- Servidor autenticación AWS • SW1-Web interfaz GoOne • SW2- SW GoOne • COM1- Conexión con AWS • COM2- Red de comunicación móvil • D1- Código Fuente GoOne • D2-Copias respaldo GoOne • K1- Claves sistemas en AWS • k2- Claves criptográficas en servidores • K3- Claves criptográficas copias de respaldo • Media 1- Sistemas de guardado Backup
Controles Impactados	• A.6.1 Organización interna • A.9.1 Requisitos de negocio para el control de acceso • A.10.1 Controles criptográficos • A.12.1 Procedimientos y responsabilidades operacionales • A.14.1 Requisitos de seguridad en los sistemas de información • A.14.2 Seguridad en el desarrollo y en los procesos de soporte • A.14.3 Datos de Prueba
Plazo Ejecución	3 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad
Coste Estimado	Se estima un coste aproximado de 12.000 euros de implantación junto con 3000 euros mensuales en licencias.

Responsable	CISO Equipo de Seguridad Corporativo
Resultado esperado	Se espera que todo desarrollo en GoOne cumpla con las reglas de desarrollo seguro y el código mantenga su ciclo de vida de acuerdo con esas condiciones. Además, se espera que gracias a este desarrollo seguro se reduzca el riesgo de amenazas relativas a los accesos no autorizados en distintos sistemas debido al almacenamiento de credenciales y puertas de atrás en el código.

5.2 Proyecto II- Integración del proceso de gestión de identidades y accesos de la nube en el sistema corporativo

Objetivo	Integrar la gestión de accesos e identidades basado en los roles definidos para la nube, integrando la trazabilidad para todo el proceso y ciclo de vida de gestión de identidades en la nube.
Activos Impactados	• S4- Servicio AWS nube • HW6- Servidor Interno para autenticación en AWS • SW1- Web Interfaz GoOne • SW2- Software GoOne • COM1- Conexión con AWS • D1- Código fuente GoOne • D2- Copias respaldo GoOne • D6- Credenciales AWS
Controles Impactados	• A.9.1 Requisitos de negocio para el control de acceso • A.9.2 Gestión de acceso de usuario • A.9.3 Responsabilidades del usuario • A.9.4 Control de acceso a sistemas y aplicaciones
Plazo Ejecución	6 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad [D]- Disponibilidad
Coste Estimado	Se estima un coste aproximado de 18.000 euros para el proceso de integración en la herramienta corporativa.
Responsable	Equipo de Seguridad GoOne Equipo de Seguridad Corporativo
Resultado esperado	Se espera que cualquier acceso para el entorno de GoOne en la nube se realice a través de la herramienta corporativa de manera que se registre apliquen los controles que esta herramienta provee (revisión de accesos periódica, borrado/bloqueo usuario automático, captura de evidencias, registros de cursos necesarios, etc).

5.3 Proyecto III- Creación del modelo operacional para GoOne

Objetivo	Definición e implantación del modelo operacional de GoOne de manera que asegure el funcionamiento seguro acorde a los

	objetivos del sistema y gestionando sus recursos adecuadamente. Este modelo operacional incluirá una definición de los roles y responsabilidades respecto a GoOne, incluyendo las de su seguridad de la información.
Activos Impactados	• S4- Servicio AWS nube • S5- Servicios Globales • HW2- Equipos de servicios aeroportuarios • HW3- Equipos en aeronaves • HW6- Servidor Interno para autenticación en AWS • SW1- Web Interfaz GoOne • SW2- Software GoOne • SW5- Servicio de ticketing • SW6- Servicio de monitorización local • COM1- Conexión con AWS • D1- Código fuente GoOne • D2- Copias respaldo GoOne • D6- Credenciales AWS • K1- Claves sistemas en AWS • K2- Claves criptográficas servidores • K3- Claves criptográficas copias de respaldo • Media1- Sistemas guardado Backup • AUX3- Equipamiento dispositivos a bordo para GoOne
Controles Impactados	• A.6.1 Organización interna • A.8 Gestión de Activos • A.9.2 Gestión de acceso de usuario • A.9.4 Control de acceso a sistemas y aplicaciones • A.15 Relación de Proveedores • A.16.1 Gestión de incidentes de seguridad de la información y mejoras
Plazo Ejecución	2 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad [D]- Disponibilidad
Coste Estimado	Se estima un coste aproximado de 20.000 euros para la definición del proceso, formación y fase de iniciación y puesta en marcha.
Responsable	Responsable GoOne Dirección de Transformación en IT de cada aerolínea
Resultado esperado	Se espera que una vez se establezca este proceso, el sistema GoOne se opere de manera ordenada, con todos los administradores y partes implicados sabiendo cuál es su función y rol en la operativa del sistema y que estos la operen adecuadamente.

5.4 Proyecto IV- Integración inventario de activos en CMDB corporativa

Objetivo	Definición del modelo de activos y componentes de hardware y software en la nube dentro de GoOne, así como su integración en la CMDB corporativa y mantenimiento del ciclo de vida en la misma.
Activos Impactados	• S4- Servicio AWS nube • SW1- Web Interfaz GoOne • SW2- Software GoOne • COM1- Conexión con AWS • D2- Copias respaldo GoOne
Controles Impactados	• A.8 Gestión de Activos
Plazo Ejecución	3 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad [D]- Disponibilidad
Coste Estimado	Se estima un coste aproximado de 6.000 euros para la definición del modelo de datos de activos y componentes que han de incluirse en la CMDB y el volcado de estos. Se incluirá la definición del proceso de ciclo de vida.
Responsable	Responsable GoOne Equipo de desarrollo GoOne
Resultado esperado	Se espera que una vez se establezca este proceso, todos los activos en la nube se encuentren inventariados en la CMDB corporativa con la información necesaria para cada uno. Adicionalmente, estos han de encontrarse al día respecto a su ciclo de vida.

5.5 Proyecto V- Control del servicio del proveedor de nube

Objetivo	Definir un proceso formal sobre la monitorización del servicio de AWS para GoOne, estableciendo las principales métricas a monitorizar y la periodicidad de chequeo, así como el proceso a seguir en caso de incidencia o desviación en el servicio.
Activos Impactados	• S4- Servicio AWS nube • SW1- Web Interfaz GoOne • SW2- Software GoOne • COM1- Conexión con AWS • D1- Código fuente GoOne • D2- Copias respaldo GoOne • D6- Credenciales AWS • K1- Claves sistemas en AWS
Controles Impactados	• A.6.1 Organización interna • A. 12. Seguridad de las Operaciones • A.13.2 Intercambio de información • A.15. Relación de proveedores

	• A.17. Aspectos de la seguridad de la información para la gestión de la continuidad del negocio • A.18. Cumplimiento
Plazo Ejecución	3 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad [D]- Disponibilidad
Coste Estimado	Se estima un coste aproximado de 18.000 euros para la definición del proceso de control, negociación con el proveedor sobre las medidas de control e implantación de las medidas oportunas internamente para ese control.
Responsable	Responsable GoOne Equipo de Seguridad GoOne
Resultado esperado	Una vez implantado el proceso se realizará un control periódico con el proveedor y se negociarán y solventarán posibles disputas e incidentes dentro del servicio. De la misma manera se identificarán riesgos y posibles medidas a tomar sobre los mismos.

5.6 Proyecto VI- Sistema de control sobre el cumplimiento de la política de seguridad de cloud

Objetivo	Establecer un proceso de control y monitorización del cumplimiento de la política de seguridad en cloud dentro de GoOne.
Activos Impactados	• S4- Servicio AWS nube • HW6- Servidor Interno para autenticación en AWS • SW1- Web Interfaz GoOne • SW2- Software GoOne • COM1- Conexión con AWS • D1- Código fuente GoOne • D2- Copias respaldo GoOne • D6- Credenciales AWS • AUX3- Equipamiento dispositivos a bordo para GoOne
Controles Impactados	• A.5.1 Directrices de gestión de la seguridad de la información • A.6.1 Organización interna • A.8 Gestión de Activos • A.9 Control de Acceso • A.10 Criptografía • 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 de Proveedores • A.16 Gestión de incidentes de seguridad de la información

	• A.17 Aspectos de la seguridad de la información para la gestión de la continuidad del negocio • A.18 Cumplimiento
Plazo Ejecución	8 meses
Dimensiones	[I]- Integridad [C]- Confidencialidad [D]- Disponibilidad
Coste Estimado	Se estima un coste aproximado de 40.000 euros para la definición del proceso y marco de control, periodicidad, equipo a cargo y herramienta usada.
Responsable	Responsable GoOne
Resultado esperado	Se espera que se establezca un proceso de monitorización manual y/o automática del cumplimiento respecto a la política de seguridad en cloud de manera periódica. Además, se espera que este proceso se coordine con el proceso de control del SGSI para evitar redundancias.

5.7 Estado de los Riesgos tras la implementación

Una vez realizada la propuesta de proyectos hemos vuelto a analizar el estado de los riesgos, así como la frecuencia con la que las amenazas se podrían materializar una vez implementadas las medidas que conllevan estos proyectos. El resultado es que una serie de activos experimentan una significativa mejora en sus riesgos:

Nombre activo	*ID*	*Tipo Activo*	Impacto (Max)			Impacto Potencial			Frecuencia Max	Riesgo		
			C	I	D	C	I	D				
Servicio AWS nube	*S4*	*[S] Servicios*	65%	55%	55%	4,55	4,95	5,5	Media	Bajo	Bajo	Bajo
Servicios Globales	*S5*	*[S] Servicios*	65%	75%	70%	3,9	3,75	4,2	Media	Bajo	Bajo	Bajo
Equipos de servicios aeroportuarios	*HW2*	*[HW] Equipamiento informático (hardware)*	65%	75%	70%	5,2	6,75	6,3	Media	Bajo	Medio-Bajo	Medio-Bajo
Equipos en aeronaves	*HW3*	*[HW] Equipamiento informático (hardware)*	65%	75%	80%	6,5	7,5	8	Alta	Medio	Medio-Alto	Alto
Servidor Interno para autenticación en AWS	*HW6*	*[HW] Equipamiento informático (hardware)*	75%	70%	90%	6,75	6,3	8,1	Media	Medio-Bajo	Medio-Bajo	Medio-Bajo
Web Interfaz GoOne	*SW1*	*[SW] Aplicaciones (software)*	65%	75%	60%	5,85	6	5,4	Media	Bajo	Medio-Bajo	Bajo
Software GoOne	*SW2*	*[SW] Aplicaciones (software)*	65%	60%	50%	6,5	6	4	Baja	Bajo	Bajo	Bajo
Sistema de ticketing	*SW5*	*[SW] Aplicaciones (software)*	65%	75%	60%	1,95	2,25	1,8	Media	Bajo	Bajo	Bajo
Sistema Monitorización local	*SW6*	*[SW] Aplicaciones (software)*	65%	75%	60%	3,9	6	1,8	Media	Bajo	Medio-Bajo	Bajo
Conexión con AWS	*COM1*	*[COM] Redes de comunicaciones*	60%	60%	50%	5,4	5,4	5	Media	Bajo	Bajo	Bajo
Firewalls	*COM2*	*[COM] Redes de comunicaciones*	60%	60%	70%	5,4	5,4	5,6	Media	Bajo	Bajo	Bajo

Código Fuente GoOne	*D1*	*[D] Datos*	50%	60%	65%	5	6	5,85	Media	Bajo	Medio-Bajo	Bajo
Copias Respaldo GoOne	*D2*	*[D] Datos*	40%	55%	55%	3,6	4,95	4,95	Media	Bajo	Bajo	Bajo
Credenciales AWS	*D6*	*[D] Datos*	40%	55%	55%	3,6	3,3	4,95	Media	Bajo	Bajo	Bajo
Claves sistemas en AWS	*K1*	*[K] Claves criptográficas*	60%	60%	60%	5,4	5,4	5,4	Media	Bajo	Bajo	Bajo
Claves criptográficas servidores	*K2*	*[K] Claves criptográficas*	60%	60%	60%	4,8	3,6	5,4	Media	Bajo	Bajo	Bajo
Claves criptográficas copias de respaldo	*K3*	*[K] Claves criptográficas*	60%	60%	60%	4,8	1,8	1,8	Media	Bajo	Bajo	Bajo
Sistemas guardado Backup	*Media1*	*[Media] Soportes de información*	60%	60%	70%	4,8	3,6	4,2	Media	Bajo	Bajo	Bajo
Equipamiento dispositivos a bordo para GoOne	*AUX3*	*[AUX] Equipamiento auxiliar*	40%	45%	80%	3,6	4,5	8	Media	Bajo	Bajo	Medio-Bajo

Sobre el listado completo de riesgos observamos que se han reducido significativamente los riesgos Medio-Alto, Alto y Muy Alto principalmente en las dimensiones de Confidencialidad e Integridad:

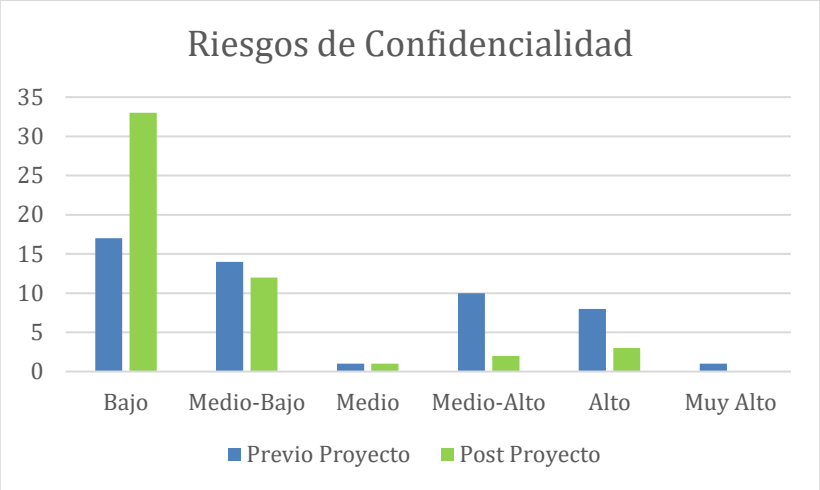

Ilustración 10 - Comparativa Riesgo Confidencialidad

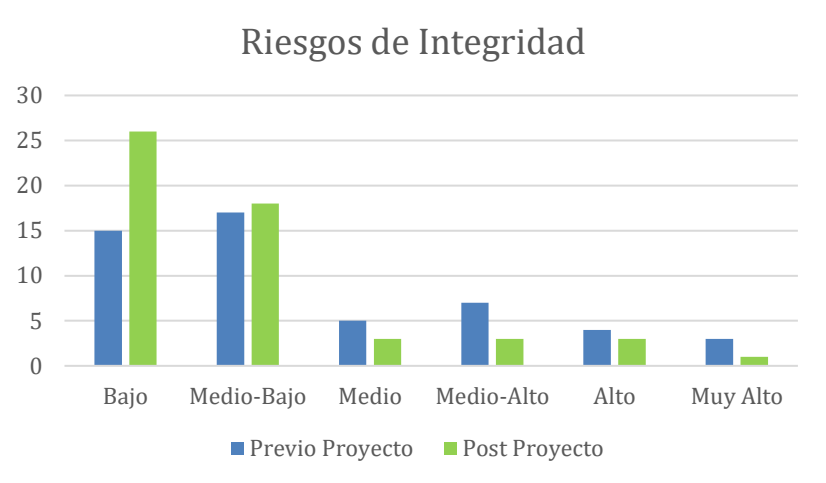

Ilustración 11- Comparativa Riesgo Integridad

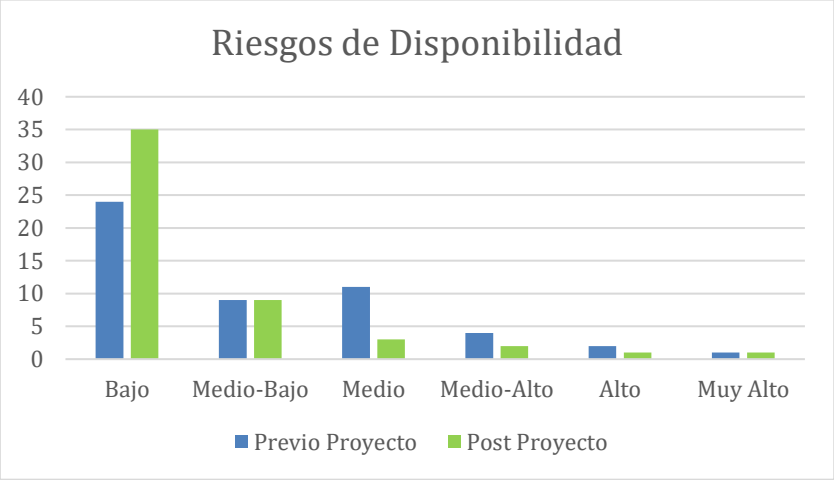

Ilustración 12- Comparativa Riesgo Disponibilidad

5.8 Planificación del plan de proyectos

El plan de proyectos presentado anteriormente se realizará en el plazo de un año y seguirá el orden que se presenta a continuación:

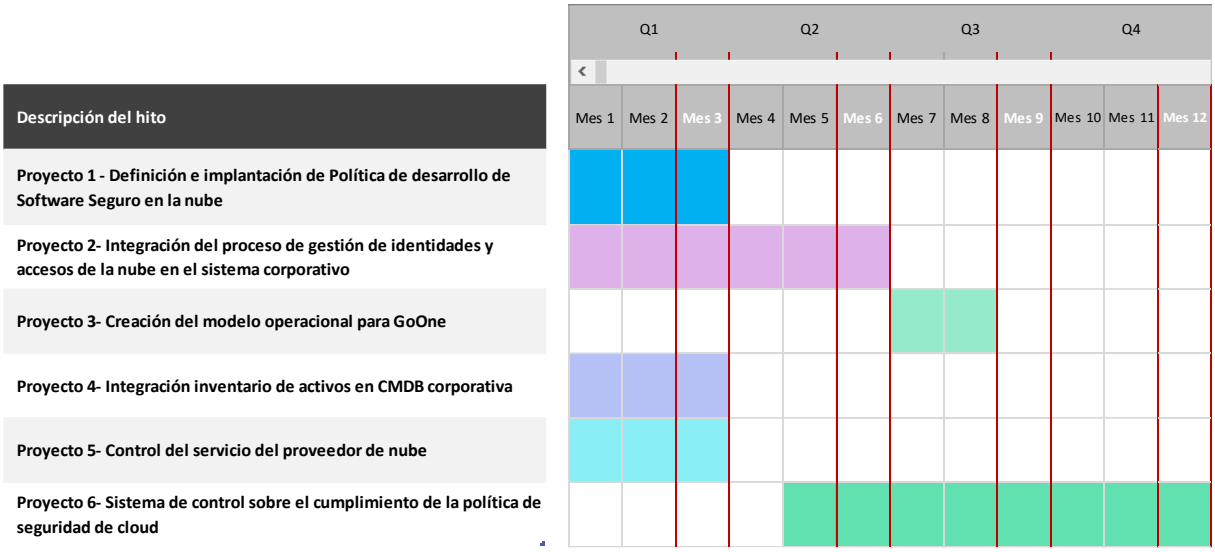

Ilustración 13 – Planificación del Plan de Proyectos

El proyecto número 3 no podrá ser acometido hasta que el proyecto 1, 2, 4 y 5 finalicen pues son piezas claves para la definición del modelo operacional de GoOne. Por otro lado, el proyecto número 6 se acometerá en último lugar pues se requerirá participación de todos los actores de GoOne y es preferible que este coincida con el menor número de proyectos. Además, acometer este proyecto en último lugar permitirá aprovecharse de las ventajas proporcionadas por los proyectos ya finalizados.

5.9 Estado del Análisis Diferencial tras la implementación

Una vez realizada la propuesta de proyectos hemos vuelto a analizar el estado de los controles tanto de la ISO/IEC 27001 como del Anexo A. (ver detalle en Anexo X: Detalle controles post-proyectos)

En el caso de los controles de la ISO/IEC 27001 vemos que la mejora no es muy significativa pues ya gozaba de un estado de madurez elevado debido a la experiencia y nivel de implementación del estándar a nivel del grupo:

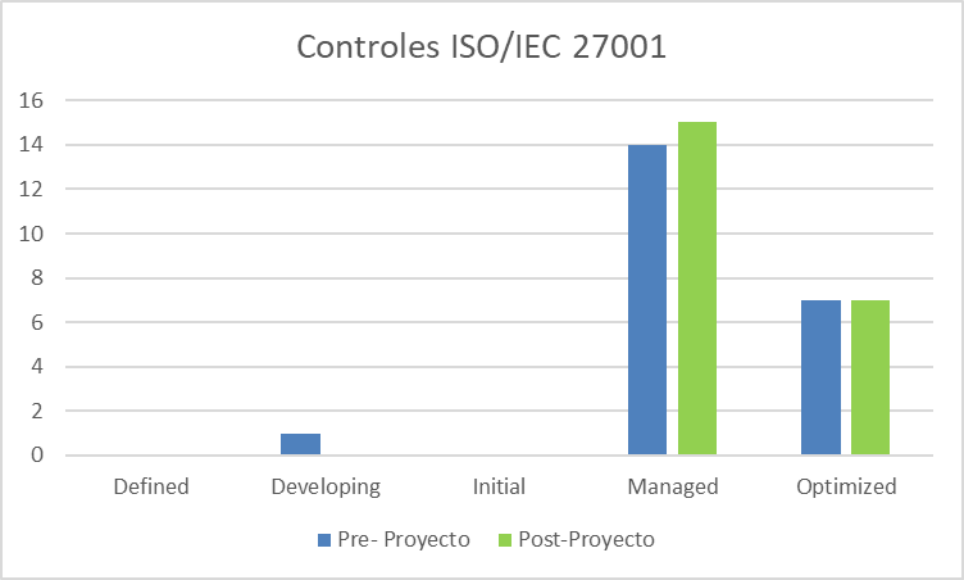

Ilustración 14 - Estado Controls ISO/IEC 27001

Para los controles del Anexo A, vemos que ya no hay controles en estado “Initial” y que los que estaban en estado “Developing” o “Defined” se han reducido significativamente:

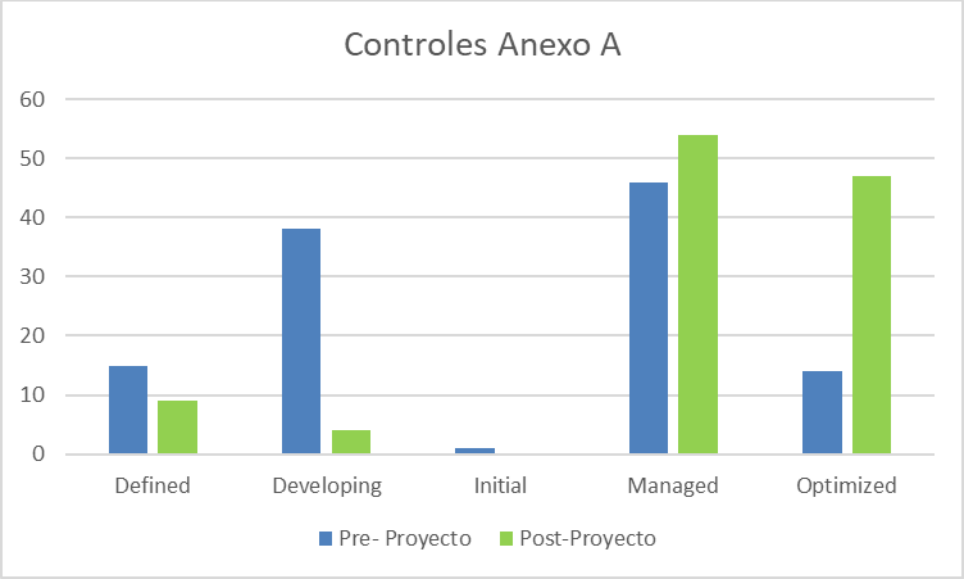

Ilustración 15 - Estado Controles Anexo A

6. Auditoría de Cumplimiento

6.1 Introducción

Habiendo concluido en las fases anteriores con el análisis de activos de la organización y los riesgos para la seguridad de la información de estos, así como los proyectos que la organización debía acometer con el fin de mitigar esos riesgos y mejorar el cumplimiento del SGSI.

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.

6.2 Metodología de Evaluación

El sistema SGSI de GoOne ha sido basado en la norma ISO/IEC 27001:2013, esta norma será utilizada como base para la evaluación y auditoría de GoOne con el fin de obtener un análisis del cumplimiento de la seguridad de la información respecto a ese estándar.

El estándar ISO/IEC 27002:2013 incluye un conjunto de 114 controles sobre buenas prácticas para la Gestión de la Seguridad de la Información, es ampliamente utilizado internacionalmente y reconocido por incluso organismos oficiales. Estos controles o salvaguardas constituyen en su conjunto una herramienta para la correcta gestión de la seguridad de la información y mitigación de los riesgos en los activos de información.

Los dominios que se analizarán son los siguientes:

- A5: Políticas de Seguridad de la Información
- A6: Organización de la Seguridad de la Información
- A7: Seguridad relativa a los Recursos Humanos
- A8: Gestión de activos
- A9: Control de acceso
- A10: Criptografía
- A11: Seguridad física y del entorno
- A12: Seguridad de las Operaciones
- A13: Seguridad de las Comunicaciones
- A14: Adquisición, desarrollo y mantenimiento de los sistemas de información
- A15: Relación de proveedores
- A16: Gestión de incidentes de seguridad de la información
- A17: Aspectos de la seguridad de la información para la gestión de la continuidad del negocio
- A18: Cumplimiento

6.3 Evaluación de la Madurez

Como parte de la auditoria del SGSI de GoOne se va a evaluar la madurez de la seguridad respecto a los diferentes dominios de control y controles del estándar ISO/IEC 27002:2013.

Este nivel de madurez se va a valorar de acuerdo con el siguiente criterio:

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

100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

6.4 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, Anexo XI: Informe Ejecutivo Auditoría Interna. (ver también Anexo XII: Detalle Resultados Auditoría):

6.4.1 Resultado ISO/IEC 27001/2013

	No Conformidades Mayores (L0-L1)	No Conformidades Menores (L2-L3)	Oportunidades de Mejora (L4)	Cumplimiento (L5)	Conformidad Actual	Conformidad Previa
4- Contexto de la Organización	0	0	1	3	99%	85%
5- Liderazgo	0	0	1	2	98%	96%
6- Planificación	0	0	1	1	98%	98%
7- Soporte	0	0	1	4	99%	96%
8- Operación	0	0	1	2	98%	98%
9- Evaluación del desempeño	0	0	2	0	95%	96%
10- Proceso de Mejora	0	0	0	2	100%	100%
	0	**0**	**7**	**14**	**98%**	**96%**

Ilustración 16 – Evolución Conformidad ISO/IEC 27001

- Podemos observar el estado de cumplimiento actual ha mejorado ligeramente (un 20%) respecto al análisis diferencial que se llevó a cabo al comienzo de la implantación del SGSI. Esto es debido a que el SGSI partía de un buen nivel de madurez debido a la experiencia de la organización respecto al estándar.
- No se han detectado No conformidades para los controles del estándar.
- Sí se destacan siete oportunidades de mejora para la mayoría de los controles del estándar.

6.4.2 Resultado ISO/IEC 27002 y ISO/IEC 27017

	No Conformidades Mayores (L0-L1)	No Conformidades Menores (L2-L3)	Oportunidades de Mejora (L4)	Cumplimiento (L5)	Conformidad Actual	Conformidad Previa
A5-Políticas de seguridad de la información	1	0	1	0	50%	70%
A6-Organización de la seguridad de la información	0	0	2	5	99%	89%
A7-Seguridad relativa a los recursos humanos	0	0	0	6	75%	75%
A8-Gestión de activos	0	0	3	7	99%	88%
A9-Control de acceso	0	1	4	9	99%	82%
A10-Criptografía	0	2	0	0	90%	50%
A11-Seguridad física y del entorno	0	0	15	0	95%	95%
A12-Seguridad de las operaciones	0	3	5	6	98%	85%
A13-Seguridad de las comunicaciones	0	3	0	4	75%	73%
A14-Adquisición, desarrollo y mantenimiento de los sistemas	0	0	10	3	97%	50%
A15-Relación con proveedores	0	0	2	3	98%	73%
A16-Gestión de incidentes de seguridad de la información	0	0	7	0	95%	90%
A17-Aspectos de seguridad de la información para la gestión	0	0	0	4	100%	95%
A18-Cumplimiento	0	0	5	4	98%	73%
	1	9	54	51	90%	78%

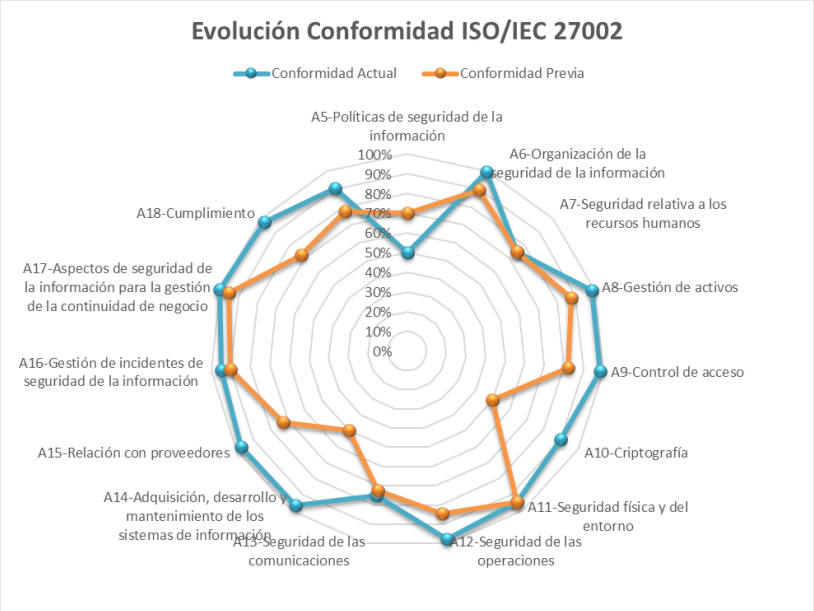

Ilustración 17 – Evolución Conformidad ISO/IEC 27002 y 27017

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. (5. Propuestas de Proyectos).

- 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- Procedimientos seguros de inicio de sesión	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.
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.

6.5 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.

7. Presentación de Resultados y Conclusiones

7.1 Introducción

Tras completar la fase de auditoría interna como último hito en el proceso de desarrollo e implantación del SGSI de GoOne, vamos a concluir el presente proyecto.

7.2 Presentación de resultados

La siguiente documentación se incluirá como parte de la implementación del presente proyecto:

- **Resumen ejecutivo**, incluyendo una descripción breve sobre la motivación, metodología y enfoque del proyecto, así como las conclusiones.
- **Memoria del proyecto** (este documento), incluyendo de manera detallada el proceso de definición del proyecto, contextualización, análisis de riesgos, análisis de cumplimiento, plan de proyectos e informe de auditoría.
- **Presentación del proyecto,** incluyendo los principales hitos del proyecto, resultados, plan de acción y conclusiones.
- **Video de presentación** del proyecto, cuyo destinatario será el tribunal del Trabajo de Fin de Master.

7.3 Conclusiones

El objetivo que perseguía este proyecto era la implantación de un SGSI para GoOne, el podríamos concluir que ha sido conseguido de manera efectiva. Este resultado ha sido conseguido en parte y como se ha mencionado en varias ocasiones, gracias a la amplia experiencia y madurez del SGSI corporativo. Todo esto por mandato de la oficina del CISO que como ya indicábamos, exigía que todos los sistemas tuviesen su propio SGSI por definición. Adicionalmente, la metodología de trabajo seguida ha permitido que las fases se desarrollaran con un objetivo claro enfocado a obtener resultados concretos.

Si bien, este resultado positivo no queda ajeno de un amplio margen de mejora en el entorno de la nube. Se ha podido observar que al ser el primer proyecto que la organización lleva a cabo en nube pública, existen una serie de aspectos que si bien cumplen de manera eficaz con el estándar pueden y deben mejorar. Para ello, se propone a la organización establecer un marco colaborativo con una consultoría externa especializada en este entorno, así como contratar y/o capacitar al equipo de manera adecuada para poder desarrollar sus funciones y mantener el SGSI de GoOone de manera adecuada.

La anterior propuesta, permitirá acometer las acciones correctivas necesarias para solventar las no conformidades identificadas en la auditoría, así como a priorizar y enforcar las oportunidades de mejora en forma de posibles proyectos para el SGSI y seguridad de GoOne.

8. Glosario

Activo – Suelen ser dispositivos para usuarios finales y componentes de infraestructura que sean propiedad de la empresa: Ordenadores de escritorio, monitores, impresoras, teléfonos, servidores, bases de datos, etc.
Auditoria – Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.
AWS – Amazon Web Services es una colección de servicios de computación en la nube pública (también llamados servicios web) que en conjunto forman una plataforma de computación en la nube, ofrecidas a través de Internet por Amazon.com
Confidencialidad – Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
Control Correctivo – Control que se realiza posteriormente a la finalización de un proceso.
Control Detectivo – Control que se realiza durante la ejecución de un proceso.
Control Preventivo – Control que se anticipa a un evento no deseado y aplica medidas para prevenirlo.
Computación en la nube o Cloud – Modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de internet a un conjunto de recursos compartidos y configurables de modo escalable (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios, etc.) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de internet.
Disponibilidad – Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
Impacto – Efecto producido por las consecuencias originados por un riesgo materializado.
Infraestructura como Servicio (IaaS- Infrastructure as a Service) - se refiere a los servicios en línea que proporcionan un alto-nivel de aplicaciones utilizadas para indireccionar detalles a bajo nivel de infraestructura como recursos de informática física, ubicación, dato, seguridad, copia de seguridad etc.
Integridad - Propiedad o característica consistente en que el activo de
MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: está 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, enfocada a las Administraciones Públicas.
Marco Referencia Niveles Madurez de Capacidades (CMM) - es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el Software Engineering Institute (SEI).

Pandemia de la COVID – conocida también como pandemia de coronavirus, es una pandemia actualmente en curso derivada de la enfermedad causada por el virus SARS-CoV-2

Riesgo Residual – Es aquel Riesgo que permanece tras la aplicación de controles y medidas destinadas a minimizar el riesgo.

Recovery Time Objective (RTO) - El tiempo objetivo de recuperación o RTO por sus siglas en inglés es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre o pérdida para así evitar consecuencias debido a la ruptura de continuidad de servicio.

Redundancia – La redundancia en datos es la duplicación o re-escritura de información con la intención de aumentar la confiabilidad del sistema, generalmente en forma de respaldo de almacenamiento o prueba de fallas.

Recovery Point Objective (RPO) - El objetivo de punto de recuperación (RPO) generalmente se refiere a la cantidad de datos que se pueden perder dentro del período más relevante para una empresa, antes de que ocurra un daño significativo, desde el punto de un evento crítico hasta la copia de seguridad con mayor precedencia.

9. Bibliografía

[1] "*ISO/IEC 27001*" https://www.iso.org/isoiec-27001-information-security.html [Fecha de consulta: 27 de febrero del 2022].

[2] ESTÁNDAR ISO/IEC INTERNACIONAL 17799, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

[3] Silvia Garre Gui, Antonio José Segovia Henares, Arsenio Tortajada Gallego (septiembre 2020). "*Implantación de un sistema de gestión de la seguridad de la información (SGSI)*" (Tercera edición). Fundació Universitat Oberta de Catalunya (FUOC)

[4] "*Impacto en la aviación de la pandemia de COVID-19*" https://es.wikipedia.org/wiki/Impacto_en_la_aviaci%C3%B3n_de_la_pandemia_de_COVID-19 [Fecha de consulta: 27 de febrero del 2022].

[5] Jordi Piera Jiménez, José Ramón Rodríguez, "*La confección del Plan director de sistemas de información del sistema sanitario integral de utilización pública de Cataluña*" (Primera edición). Fundació Universitat Oberta de Catalunya (FUOC)

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

[7] 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].

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

[9] "*Magerit – Libro II- Catálogo de Elementos*" https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8ixx2gzaM-

10. Anexos

Anexo I: Análisis Diferencial

Análisis Diferencial Controles ISO/IEC 27001:2017

Capítulo	Requerimientos ISO 27001	Estado
4	Contexto de la organización	
4,1	Comprensión de la organización y de su contexto	Optimized
4,2	Comprensión de las necesidades y expectativas de las partes interesadas	Managed
4,3	Determinación del alcance del SGSI	Managed
4,4	SGSI	Developing
5	Liderazgo	
5,1	Liderazgo y compromiso	Managed
5,2	Política	Managed
5,3	Roles, responsabilidades y autoridades en la organización	Managed
6	Planificación	
6,1	Acciones para tratar los riesgos y oportunidades	Managed
6,2	Objetivos de seguridad de la información y planificación para su consecución	Managed
7	Soporte	
7,1	Recursos	Optimized
7,2	Competencia	Managed
7,3	Concienciación	Managed
7,4	Comunicación	Managed

7,5	**Información documentada**	Optimized
8	**Operación**	
8,1	**Planificación y control operacional**	Managed
8,2	**Apreciación de los riesgos de seguridad de la información**	Optimized
8,3	**Tratamiento de los riesgos de seguridad de la información**	Optimized
9	**Evaluación del desempeño**	
9,1	**Seguimiento, medición, análisis y evaluación**	Managed
9,2	**Auditoría interna**	Managed
9,3	**Revisión por la dirección**	Managed
10	**Mejora**	
10,1	**No conformidad y acciones correctivas**	Optimized
10,2	**Mejora continua**	Optimized

Análisis Diferencial Controles Anexo A

Capítulo	Objetivo	Control	Descripción	Requisito en ISO/IEC27017	Estado de madurez
5. Políticas de Seguridad de la Información	**A.5.1 Directrices de gestión de la seguridad de la información:** Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.	**A.5.1.1 Políticas para la seguridad de la información**	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.	Existencia de política para la gestión de la seguridad de la información en la nube	**Defined**
		A.5.1.1 Revisión de las políticas para la seguridad de la información	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.	Sin requisito adicional.	**Developing**

6. Organización de la Seguridad de la Información	**A.6.1 Organización interna:** Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización	**A.6.1.1 Roles y responsabilidades en seguridad de la información**	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	El cliente de servicios en la nube debe acordar con el proveedor en la nube una asignación adecuada de funciones y responsabilidades en materia de seguridad de la información, y confirmar que puede cumplir las funciones y responsabilidades asignadas.	**Developing**
		A.6.1.2 Segregación de tareas	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.	Sin requisito adicional.	**Developing**
		A.6.1.3 Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes	El cliente de servicios en la nube debe identificar a las autoridades pertinentes para la operación combinada del cliente de servicios en la nube y el proveedor de servicios en la nube.	**Managed**
		A.6.1.4 Contacto con grupos de interés especial	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	Sin requisito adicional.	**Managed**
		A.6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	Sin requisito adicional.	**Managed**
	A.6.2 Los dispositivos móviles y el teletrabajo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.	**A.6.2.1 Política de dispositivos móviles**	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	Sin requisito adicional.	**Managed**
		A.6.2.2 Teletrabajo	Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	Sin requisito adicional.	**Managed**

7. Seguridad relativa a los Recursos Humanos	**A.7.1 Antes del empleo:** Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.	**A.7.1.1 Investigación de antecedentes**	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa 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	Sin requisito adicional.	**Optimized**
		A.7.1.2 Términos y condiciones del empleo	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	Sin requisito adicional.	**Optimized**
	A.7.2 Durante el empleo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.	**A.7.2.1 Responsabilidades de gestión**	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.	Sin requisito adicional.	**Optimized**
		A.7.2.2 Concienciación, educación y capacitación en seguridad de la información	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.	El personal involucrado en entornos de cloud deberá recibir formación sobre los estándares y procedimientos a usar dichos entornos, los riesgos relativos a esos entornos, así como consideraciones legales o regulatorias.	**Optimized**
		A.7.2.3 Proceso disciplinario	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.	Sin requisito adicional.	**Optimized**
	A.7.3 Finalización del empleo o cambio en el puesto de trabajo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.	**A.7.3.1 Responsabilidades ante la finalización o cambio**	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	Sin requisito adicional.	**Optimized**

8. Gestión de activos	**A.8.1 Responsabilidad sobre los activos:** Identificar los activos de la organización y definir las responsabilidades de protección adecuadas	**A.8.1.1 Inventario de activos**	La información y otros 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.	El inventario de activos del cliente de servicios en la nube debe dar cuenta de la información y los activos asociados almacenados en el entorno de nube. Los registros del inventario deben indicar dónde se mantienen los activos.	**Developing**
		A.8.1.2 Propiedad de los activos	Todos los activos que figuran en el inventario deben tener un propietario.	Sin requisito adicional.	**Developing**
		A.8.1.3 Uso aceptable de los activos	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.	Sin requisito adicional.	**Developing**
		A.8.1.4 Devolución de activos	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	Sin requisito adicional.	**Optimized**
	A.8.2 Clasificación de la información: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.	**A.8.2.1 Clasificación de la información**	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.	Sin requisito adicional.	**Optimized**
		A.8.2.2 Etiquetado de la información	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	El cliente debe etiquetar la información y los activos asociados que se mantienen en el entorno de la nube de acuerdo con sus procedimientos.	**Optimized**
		A.8.2.3 Manipulado de la información	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.	Sin requisito adicional.	**Optimized**
	A.8.3 Manipulación de los soportes: Evitar la revelación, modificación, eliminación o	**A.8.3.1 Gestión de soportes extraíbles**	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema	Sin requisito adicional.	**Optimized**

	destrucción no autorizadas de la información almacenada en soportes		de clasificación adoptado por la organización.		
		A.8.3.2 Eliminación de soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	Sin requisito adicional.	**Optimized**
		A.8.3.3 Soportes físicos en tránsito	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.	Sin requisito adicional.	**Optimized**
9. Control de acceso	**A.9.1 Requisitos de negocio para el control de acceso:** Limitar el acceso a los recursos de tratamiento de la información y a la información.	**A.9.1.1 Política de control de acceso**	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	Sin requisito adicional.	**Developing**
		A.9.1.2 Acceso a las redes y a los servicios de red	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	La política de control de acceso del cliente de servicios en la nube para el uso de los servicios de red debe especificar los requisitos para el acceso de los usuarios a cada uno de los servicios en la nube que se utilicen.	**Developing**
	A.9.2 Gestión de acceso de usuario: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.	**A.9.2.1 Registro y baja de usuario**	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	Sin requisito adicional.	**Defined**
		A.9.2.2 Provisión de acceso de usuario	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.	Sin requisito adicional.	**Defined**
		A.9.2.3 Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	El cliente de servicios en la nube debe utilizar técnicas de autenticación suficientes para autenticar a los administradores de servicios en la nube del cliente de servicios en la nube en las capacidades administrativas de un servicio en la	**Defined**

				nube de acuerdo con el riesgo identificado.	
		A.9.2.4 Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	El cliente de servicios en la nube debe verificar que el procedimiento de gestión del proveedor de servicios en la nube para la asignación de información secreta de autenticación, como las contraseñas, cumple con los requisitos del cliente de servicios en la nube.	**Managed**
		A.9.2.5 Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	Sin requisito adicional.	**Managed**
		A.9.2.6 Retirada o reasignación de los derechos de acceso	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.	Sin requisito adicional.	**Managed**
	A.9.3 Responsabilidades del usuario: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación	**A.9.3.1 Uso de la información secreta de autenticación**	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	Sin requisito adicional.	**Managed**
	A.9.4 Control de acceso a sistemas y aplicaciones: Prevenir el acceso no autorizado a los sistemas y aplicaciones	**A.9.4.1 Restricción del acceso a la información**	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.	El cliente del servicio en la nube debe garantizar que el acceso a la información en el servicio en la nube pueda restringirse de acuerdo con su política de control de acceso y que dichas restricciones se realicen.	**Defined**
		A.9.4.2 Procedimientos seguros de inicio de sesión	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.	Sin requisito adicional.	**Defined**
		A.9.4.3 Sistema de gestión de	Los sistemas para la gestión de contraseñas deben ser interactivos y	Sin requisito adicional.	**Managed**

		contraseñas	establecer contraseñas seguras y robustas.		
		A.9.4.4 Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	Cuando se permita el uso de programas de utilidad, el cliente del servicio en la nube debe identificar los programas de utilidad que se utilizarán en su entorno de computación en la nube, y asegurarse de que no interfieren con los controles del servicio en la nube.	**Defined**
		A.9.4.5 Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas	Sin requisito adicional.	**Defined**
10. Criptografía	**A.10.1 Controles criptográficos:** Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información	**A.10.1.1 Política de uso de los controles criptográficos**	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	El cliente de servicios en la nube debe implementar controles criptográficos para su uso de los servicios en la nube si lo justifica el análisis de riesgos. Los controles deben ser lo suficientemente fuertes como para mitigar los riesgos identificados.	**Developing**
		A.10.1.2 Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	El cliente de servicios en la nube debe identificar las claves criptográficas para cada servicio en la nube, e implementar procedimientos para la gestión de claves.	**Developing**
11. Seguridad física y del entorno	**A.11.1 Áreas seguras:** Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.	**A.11.1.1 Perímetro de seguridad física**	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.	Sin requisito adicional.	**Managed**
		A.11.1.2 Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	Sin requisito adicional.	**Managed**
		A.11.1.3 Seguridad de oficinas, despachos y	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad	Sin requisito adicional.	**Managed**

		recursos	física.		
		A.11.1.4 Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	Sin requisito adicional.	**Managed**
		A.11.1.5 El trabajo en áreas seguras	Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	Sin requisito adicional.	**Managed**
		A.11.1.6 Áreas de carga y descarga	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.	Sin requisito adicional.	**Managed**
	A.11.2 Seguridad de los equipos: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.	**A.11.2.1 Emplazamiento y protección de equipos**	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	Sin requisito adicional.	**Managed**
		A.11.2.2 Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Sin requisito adicional.	**Managed**
		A.11.2.3 Seguridad del cableado	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.	Sin requisito adicional.	**Managed**
		A.11.2.4 Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas	Sin requisito adicional.	**Managed**
		A.11.2.5 Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	Sin requisito adicional.	**Managed**

		A.11.2.6 Seguridad de los equipos fuera de las instalaciones	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.	Sin requisito adicional.	**Managed**
		A.11.2.7 Reutilización o eliminación segura de equipos	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.	El cliente de servicios en la nube debe solicitar la confirmación de que el proveedor de servicios en la nube dispone de políticas y procedimientos para la eliminación o reutilización segura de los recursos.	**Managed**
		A.11.2.8 Equipo de usuario desatendido	Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	Sin requisito adicional.	**Managed**
		A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia	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.	Sin requisito adicional.	**Managed**
12. Seguridad de las Operaciones	**A.12.1 Procedimientos y responsabilidades operacionales:** Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información	**A.12.1.1 Documentación de procedimientos operacionales**	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.	Sin requisito adicional.	**Developing**
		A.12.1.2 Gestión de cambios	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados	El cliente de servicios en la nube deberá tener en cuenta dentro de su proceso de gestión de cambios el impacto de cualquier cambio realizado por el proveedor de nube.	**Managed**
		A.12.1.3 Gestión de capacidades	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.	El cliente de servicios en la nube deberá asegurar que la capacidad acordada con el proveedor se corresponde con los requerimientos, así como monitorizarla.	**Initial**
		A.12.1.4 Separación de los recursos de desarrollo, prueba y	Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no	Sin requisito adicional.	**Developing**

		operación	autorizado o los cambios del sistema en producción.		
	A.12.2 Protección contra el software malicioso (malware): Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware	**A.12.2.1 Controles contra el código malicioso**	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	Sin requisito adicional.	**Managed**
	A.12.3 Copias de seguridad: Evitar la pérdida de datos	**A.12.3.1 Copias de seguridad de la información**	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada	Cuando el proveedor de servicios en la nube proporcione capacidad de copia de seguridad como parte del servicio en la nube, el cliente de servicios en la nube debe solicitar las especificaciones de la capacidad de copia de seguridad al proveedor de servicios en la nube. El cliente de servicios en la nube también debe verificar que cumplen sus requisitos de copia de seguridad.	**Managed**
	A.12.4 Registros y supervisión: Registrar eventos y generar evidencias	**A.12.4.1 Registro de eventos**	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información	El cliente de servicios en la nube debe definir sus requerimientos para el registro de eventos y verificar que el servicio de cloud cumple con ellos.	**Developing**
		A.12.4.2 Protección de la información del registro	Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	Sin requisito adicional.	**Developing**
		A.12.4.3 Registros de administración y operación	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	Si la operación privilegiada es delegada al cliente del servicio, la operación y rendimiento de esas operaciones debe ser registrada.	**Developing**
		A.12.4.4 Sincronización del reloj	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.	El cliente del servicio deberá solicitar al proveedor de la nube la sincronización de reloj usada por los sistemas en la nube.	**Managed**
	A.12.5 Control del software en	**A.12.5.1 Instalación del**	Se deben implementar procedimientos	Sin requisito adicional.	**Managed**

	explotación: Asegurar la integridad del software en explotación.	**software en explotación**	para controlar la instalación del software en explotación.		
	A.12.6 Gestión de la vulnerabilidad técnica: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.	**A.12.6.1 Gestión de las vulnerabilidades técnicas**	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.	El cliente del servicio de nube deberá solicitar al proveedor sobre su proceso de gestión de vulnerabilidades técnicas.	**Managed**
		A.12.6.2 Restricción en la instalación de software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	Sin requisito adicional.	**Managed**
	A.12.7 Consideraciones sobre la auditoria de sistemas de información: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.	**A.12.7.1 Controles de auditoría de sistemas de información**	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	Sin requisito adicional.	**Optimized**
13. Seguridad de las Comunicaciones	**A.13.1 Gestión de la seguridad de las redes**: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.	**A.13.1.1 Controles de red**	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	Sin requisito adicional.	**Developing**
		A.13.1.2 Seguridad de los servicios de red	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.	Sin requisito adicional.	**Developing**
		A.13.1.3 Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	El cliente de servicio en la nube deberá definir sus requisitos para la segregación de redes con el fin de alcanzar el aislamiento necesario en el entorno compartido.	**Developing**
	A.13.2 Intercambio de información: Mantener la	**A.13.2.1 Políticas y procedimientos de**	Deben establecerse políticas, procedimientos y controles formales que	Sin requisito adicional.	**Managed**

	seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa	**intercambio de información**	protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.		
		A.13.2.2 Acuerdos de intercambio de información	Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	Sin requisito adicional.	**Managed**
		A.13.2.3 Mensajería electrónica	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	Sin requisito adicional.	**Managed**
		A.13.2.4 Acuerdos de confidencialidad o no revelación	Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación	Sin requisito adicional.	**Managed**
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.1 Requisitos de seguridad en los sistemas de información:** Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.	**A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información**	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.	El cliente de servicio en la nube deberá determinar los requisitos de seguridad para su información en la nube y evaluar si los servicios ofrecidos por el proveedor cumplen con ellos.	**Developing**
		A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas	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.	Sin requisito adicional.	**Developing**
		A.14.1.3 Protección de las transacciones de servicios de aplicaciones	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.	Sin requisito adicional.	**Developing**
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte: Garantizar la seguridad de la información que se ha	**A.14.2.1 Política de desarrollo seguro**	Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los	Sin requisito adicional.	**Developing**

	diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.		sistemas de información.		
		A.14.2.2 Procedimiento de control de cambios en sistemas	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.	Sin requisito adicional.	**Developing**
		A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	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.	Sin requisito adicional.	**Developing**
		A.14.2.4 Restricciones a los cambios en los paquetes de software	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	Sin requisito adicional.	**Developing**
		A.14.2.5 Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	Sin requisito adicional.	**Developing**
		A.14.2.6 Entorno de desarrollo seguro	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.	Sin requisito adicional.	**Developing**
		A.14.2.7 Externalización del desarrollo de software	El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	Sin requisito adicional.	**Developing**
		A.14.2.8 Pruebas funcionales de seguridad de sistemas	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	Sin requisito adicional.	**Developing**
		A.14.2.9 Pruebas de aceptación de sistemas	Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de	Sin requisito adicional.	**Developing**

			información, actualizaciones y nuevas versiones.		
	A.14.3 Datos de prueba: Asegurar la protección de los datos de prueba	**A.14.3.1 Protección de los datos de prueba**	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	Sin requisito adicional.	**Developing**
15. Relación de proveedores	**A.15.1 Seguridad en las relaciones con proveedores:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores	**A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores**	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.	El cliente de servicios de nube deberá incluir al proveedor de servicio de nube dentro de su proceso de gestión de proveedores.	**Managed**
		A.15.1.2 Requisitos de seguridad en contratos con terceros	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 de Tecnología de la Información.	El cliente de servicios de nube deberá confirmar que los roles de seguridad y las responsabilidades relacionadas con el servicio de nube son definidas en el acuerdo a firmar.	**Managed**
		A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	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.	Sin requisito adicional.	**Managed**
	A.15.2 Gestión de la provisión de servicios del proveedor: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores	**A.15.2.1 Control y revisión de la provisión de servicios del proveedor**	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	Sin requisito adicional.	**Managed**
		A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.	Sin requisito adicional.	**Managed**

16. Gestión de incidentes de seguridad de la información	**A.16.1 Gestión de incidentes de seguridad de la información y mejoras:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.	**A.16.1.1 Responsabilidades y procedimientos**	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.	El cliente de servicio en la nube deberá verificar las responsabilidades en materia de gestión de incidentes de la seguridad de la información y asegurar que el proveedor cumple con ellas.	**Defined**
		A.16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible	El cliente de servicio en la nube deberá solicitar la información a proveedor sobre los mecanismos para reportar sobre los eventos de seguridad.	**Defined**
		A.16.1.3 Notificación de puntos débiles de la seguridad	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.	Sin requisito adicional.	**Defined**
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	Sin requisito adicional.	**Defined**
		A.16.1.5 Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Sin requisito adicional.	**Defined**
		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro	Sin requisito adicional.	**Defined**
		A.16.1.7 Recopilación de evidencias	La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.	El cliente de servicio en la nube y el proveedor deberán acordar los procedimientos para recopilar las evidencias sobre incidentes de seguridad.	**Defined**
17. Aspectos de la seguridad de	**A.17.1 Continuidad de la seguridad de la información:** La	**A.17.1.1 Planificación de la continuidad de la**	La organización debe determinar sus necesidades de seguridad de la	Sin requisito adicional.	**Managed**

la información para la gestión de la continuidad del negocio	continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.	**seguridad de la información**	información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		
		A.17.1.2 Implementar la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	Sin requisito adicional.	**Managed**
		A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	Sin requisito adicional.	**Managed**
	A.17.2 Redundancias: Asegurar la disponibilidad de los recursos de tratamiento de la información.	**A.17.2.1 Disponibilidad de los recursos de tratamiento de la información**	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	Sin requisito adicional.	**Managed**
18. Cumplimiento	**A.18.1 Cumplimiento de los requisitos legales y contractuales:** Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.	**A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales**	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.	El cliente del servicio en cloud debería considerar y verificar las leyes y regulaciones aplicables para el proveedor de servicio en la nube.	**Developing**
		A.18.1.2 Derechos de Propiedad Intelectual (DPI)	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.	El cliente del servicio en cloud debería tener un procedimiento para identificar los requerimientos de licencias específicas de cloud antes de permitir instalar ningún software en el servicio de nube.	**Developing**

		A.18.1.3 Protección de los registros de la organización	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.	El cliente del servicio en cloud debería solicitar información al proveedor sobre la protección de registros.	**Developing**
		A.18.1.4 Protección y privacidad de la información de carácter persona	Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	Sin requisito adicional.	**Developing**
		A.18.1.5 Regulación de los controles criptográficos	Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	El cliente del servicio en cloud debería verificar los controles criptográficos que aplican para el uso del servicio de nube.	**Developing**
	A.18.2 Revisiones de la seguridad de la información: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.	**A.18.2.1 Revisión independiente de la seguridad de la información**	El enfoque de la organización para la gestión de la 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.	El cliente del servicio en cloud debería solicitar evidencia documentada sobre la implementación de controles sobre la seguridad de la información.	**Managed**
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad	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	Sin requisito adicional.	**Managed**
		A.18.2.3 Comprobación del cumplimiento técnico	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	Sin requisito adicional.	**Managed**

Anexo II: Política de Seguridad de la Información

1. Alcance

La presente Política de Seguridad de la Información establece las directrices respecto a la gestión de la seguridad de la información dentro del ámbito de los sistemas informáticos de las empresas que conforman el grupo.
Es de aplicación para todo el personal de las empresas del grupo, tanto interno como personal externo, así como proveedores y colaboradores. Es por ello, que todo el personal mencionado anteriormente debe conocer esta política y cumplirla.

Esta política supone un elemento clave para la estrategia de la compañía pues asegura los principios básicos para asegurar y mantener la integridad, disponibilidad y confidencialidad de la información.

2. Gestión de la seguridad en procesos de Recursos Humanos

2.1 Antes de la contratación

- Se debe asegurar que los empleados y personal subcontratado entiende sus responsabilidades y los roles para los que han sido asignados.
- El departamento de Recursos Humanos debe asegurar que se realizan los chequeos previos adecuados respecto a los candidatos dependiendo de la función, así como de los reglamentos locales aplicables.
- Los contratos han de incluir dentro de sus cláusulas la responsabilidad de los empleados respecto a la seguridad de la información.

2.2 Durante la contratación

- Se debe asegurar que los empleados y personal subcontratado antes de acceder a los sistemas de información han entendido los requerimientos y procedimientos de seguridad de la organización.
- Los roles de gestión deberán asegurar que sus empleados entienden y son conscientes de la necesidad de aplicar la seguridad a la información como procedimiento habitual.

2.3 Durante la terminación del empleo

- Las responsabilidades respecto a la seguridad de la información que se mantengan tras la finalización del empleo han de ser comunicadas.
- Los accesos a los sistemas de información, así como accesos físicos han de eliminarse tras la terminación del empleo.

3. Gestión de los activos

3.1 Responsabilidades en la gestión de activos

- Se deben identificar los activos organizativos y tecnológicos asignando un responsable a cada uno de ellos.

3.2 Gestión del inventario de activos

- La información, los activos que incluyan información y las instalaciones en las que se procese información han de identificarse e inventariarse, incluyendo un dueño y responsable para cada una de ellas.
- El cambio de responsabilidad respecto a un activo ha de identificarse y actualizarse en el inventario.
- El personal ha de conocer los procedimientos para gestión de información.

3.3 Devolución de activos

- Los activos que contengan información habrán de devolverse cuando se finalice el contrato o colaboración con la organización.

3.4 Gestión de los medios informáticos

- Deben seguirse los procedimientos definidos para la gestión de dispositivos informáticos con el fin de que no se llegue a una pérdida de información.
- Se deben implementar medidas para deshabilitar el uso de medios informáticos en caso de necesitar prevenir un acceso no autorizado.
- El desecho de medios informáticos ha de realizarse de manera segura y con proveedores que acrediten su correcta destrucción.

4. Clasificación de la información

- Se debe asegurar que toda información recibe un nivel de protección adecuado de acuerdo con su importancia dentro de la organización.
- Se deberá clasificar la información en función de los requerimientos legales, el valor que tenga para la organización, la criticidad e impacto que provocaría su filtración.
- En función de lo anterior se han definido cuatro niveles para clasificar la información:
    - Información Pública
    - Información Interna
    - Información Confidencial
    - Información Secreta

5. Control de Accesos

5.1 Política de Control de accesos

- Deben implementarse medidas para asegurar que los accesos a los sistemas de información son los adecuados y se basan en la información y sus requisitos de seguridad.
- Los usuarios han de tener acceso específico a aquellos entornos de la red y sistemas operativos para los que estén autorizados.
- Deben existir procedimientos de log-on seguros donde se cumplan las siguientes condiciones:
    - La contraseña no se muestre en pantalla
    - La contraseña no se transmita sin cifrar en los sistemas
    - Se limite el número de intentos de acceso fallidos
    - La contraseña ha de contener al menos:
        - 8 caracteres
        - Un numero
        - Una mayúscula
        - Una minúscula
        - Un carácter especial

5.2 Gestión de accesos

- Los accesos a los sistemas han de ser siempre autorizados por personal interno de la compañía o autorizados.
- Las credenciales de acceso han de ser únicos, personales y proporcionados de manera segura.
- El registro de usuarios debe hacerse de manera formal quedando siempre documentado, incluyendo la razón y las aprobaciones proporcionadas.
- Los accesos se deben revisar de manera periódica con el fin de confirmar que se mantienen aplicables, así como registrar formalmente dicha revisión.
- Cuando la relación contractual termina se deberá asegurar que el usuario es eliminado de los sistemas de información, de manera que se deshabilite cualquier método de acceso.

6. Control Criptográficos

6.1 Gestión de claves

- Se deben implementar controles criptográficos proporcionales y de acuerdo con la información que resida en los sistemas con el fin de asegurar su confidencialidad, integridad y disponibilidad.
- Los controles criptográficos deben gestionarse bajo una política de uso, protección y gestión del ciclo de vida.

7. Seguridad Física y Medioambiental

7.1 Áreas seguras

- Con el fin de prevenir accesos físicos no autorizados o que se dañe información se deben implementar una serie de controles físicos.
- Se deben establecer unos perímetros de seguridad que aseguren la protección de aquellas áreas donde se encuentren instalaciones de procesamiento de información o que contengan información.
- El acceso a las instalaciones ha de realizarse mediante autenticación personal.
- Todos los visitantes han de identificarse y registrarse antes de acceder a instalaciones de la organización. Adicionalmente, deberán ir siempre acompañados por personal interno.

7.2 Protección de los equipos

- El equipamiento físico debe estar correctamente protegido con el fin de reducir los riesgos de pérdida de información.
- El equipamiento que necesite especial protección se deberá aislar con el fin de aplicar medidas específicas.
- Los dispositivos deben estar protegidos contra fallos energéticos y con ello su correcta detección.
- Los sistemas que contienen cableado deben estar correctamente aislados y protegidos para evitar intercepciones o daños.
- El equipamiento ha de mantenerse de manera regular con el fin de asegurar que se mantienen íntegros y disponibles. Dichos mantenimientos han de monitorizarse y registrarse.
- Aquel equipamiento que haya de desecharse deberá asegurarse que cualquier dato que contenga ha sido correctamente eliminado antes de su transporte y/o destrucción.
- El personal deberá asegurar que su equipamiento siempre se mantiene protegido.
- El personal deberá asegurar que sus puestos de trabajo se mantienen libres de material físico que contenga información, así como tener sus pantallas bloqueadas cuando no atiendan su equipo informático.

8. Gestión de la seguridad de la operativa

8.1 Gestión de cambios

- Se debe asegurar que los cambios en la organización, sistemas de información e instalaciones de procesamiento de información se realizan de manera segura, son aprobados y registrados.
- Los entornos de desarrollo, test y producción deben estar segregados correctamente para reducir los riesgos de acceso no autorizado o los cambios no autorizados.

8.2 Manteniendo la seguridad de la información

- Debe existir una protección adecuada contra código malicioso, para ello se deben utilizar sistemas de escaneo y detección sobre los sistemas.
- Debe existir un proceso de protección contra perdida de datos, que asegure que se realicen copias de respaldo de manera periódica en función de la criticidad de la información contenida en el sistema.
- Las copias de respaldo se deben encriptar y realizar en otro sistema de procesamiento de información, es decir, en otra localización.
- Se deben registrar los eventos que ocurran en el sistema sobre excepciones, actividades de usuario, fallos, eventos de seguridad. Estos han de ser capturados, transmitidos y revisados de manera periódica.
- Los eventos registrados han de mantenerse protegidos.
- Los sistemas deben tener sus sistemas horarios sincronizados con una única referencia horaria, sobre un mismo servidor.

9. Gestión de la seguridad de las comunicaciones

9.1 Gestión de la seguridad de la red

- Los sistemas de red deben tener un nivel de protección adecuado que aseguren la información que circula a través de ellos.
- El acceso remoto ha de ser enrutado exclusivamente por gateways corporativos que implementen los controles de autenticación para la red corporativa.
- La red ha de estar segregada en función de grupos de servicios de información, usuarios y sistemas de información. Estos dominios de red deben implementar controles adecuados y acordes a su función.

9.2 Transferencia segura de información

- Se deben establecer protocolos seguros de transferencia de información.
- La información debe transferirse encriptada en aquellos casos que se trate de información confidencial o secreta.

Anexo III: Procedimiento de Auditoría

El procedimiento que se detalla a continuación ha de ser aplicado dentro de la organización en aquellas actividades que se engloben dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

1.1 El deber de Monitorizar

Dentro de las obligaciones que conlleva el SGSI está la de monitorizar y medir su cumplimiento donde se determine:

- Qué se debe monitorizar y medir, incluyendo procesos e información.
- Los métodos de monitorización, medición y análisis del cumplimiento que aseguren resultados fiables.
- Cuando ha de monitorizarse y como.
- Quién ha de monitorizar y evaluar esos resultados.

1.2 Auditoría Interna

Con el fin de monitorizar el cumplimiento del SGIS se establece un proceso de auditoría interna como método válido. Dicha auditoría interna debe asegurar:

- Conformar con los requerimientos del SGSI internos y con los del estándar ISO/IEC 27001
- Que el SGSI se haya implementado y mantenido correctamente
- Se planifique y establezca de manera adecuada el programa de auditoria (este documento) incluyendo responsabilidades y requerimientos.
- Definir el criterio y alcance para cada auditoria
- Seleccionar a los auditores de manera que sean objetivos e imparciales
- Que los resultados de la auditoria sean reportados a los grupos relevantes
- Que la documentación se mantiene como evidencia

1.2.1 Requisitos para el Equipo Auditor

Habilidades técnicas	-Grado universitario en Ingeniería Informática o de Telecomunicaciones O - Seis años de experiencia equivalente en funciones de gestión de sistemas informáticos
Certificaciones	Certificación de Implementador de ISO/IEC 27001
Habilidades profesionales	-Capacidad de gestión de capacidad y planificación de recursos -Capacidad analítica y crítica -Rol de liderazgo en equipo y gestión de personas -Capacidades de comunicación a nivel técnico, financiero, organizativo, etc.

	-Habilidad oral y escrita avanzada en inglés y Castellano -Conocimiento del negocio de la aviación

El equipo auditor constará con los siguientes roles:

- Un Auditor líder: deberá proceder de la oficina del CISO pues aseguraremos que tiene los conocimientos respecto a las políticas internas necesario, así como la experiencia en seguridad de la información necesaria.
- 3 auditores: procederán del equipo de auditoría del grupo y tendrán conocimientos de auditoria pero también sobre distintas áreas del grupo
- Expertos de las áreas técnicas: habrá uno procedente de los servicios globales y otro de cada área de servicios de IT y transformación de cada marca de aerolínea.

1.3 Requisitos del Plan de Auditoria

El plan de auditoría tendrá la siguiente forma de manera estándar:

PLAN DE AUDITORIA INTERNA DE SGSI	
Requisito Plan de Auditoria	**Descripción**
Alcance y objetivos	Establecer y definir todos los objetivos que persigue la auditoría, estos deben ser medibles, realistas, alcanzables y limitados. Se deben indicar las áreas, unidades, centros de trabajo impactados.
Requerimientos especiales	Si existe algún requisito o exclusión especial sobre la auditoria se debe detallar.
Calendario de auditoría	Se especificarán los hitos de la auditoria dentro de un calendario que incluya los resultados esperados en cada hito.
Recursos necesarios	Se detallarán los recursos necesarios para llevar a cabo la auditoría, se identificarán recursos externos si fuesen necesarios.
Listado de auditores	El equipo de auditoría se debe presentar en el plan incluyendo una descripción de su perfil y rol dentro de la auditoria.
Documentación proporcionada	Se incluirá la información y distado de documentos con los que se ha partido y basado el plan de auditoría.
Controles a auditar	Se detallarán los controles que se espera auditar en el ejercicio.
Agenda de reuniones	Se incluirá un calendario de reuniones específico, incluyendo área involucrada y controles objeto de la reunión.
Informes y reportes que presentar	Se incluirá un listado con los informes y documentos que se entregarán para apoyar el ejercicio de auditoría y los resultados/análisis realizado por parte del equipo auditor.

1.4 Plantilla de informe de auditoría

El informe de auditoría deberá seguir el siguiente formato establecido:

Informe de Auditoria											
1. Información sobre la auditoria											
Referencia auditoria											
Norma/s usadas											
Fecha auditoria											
Lugar auditoría											
2. Objetivo											
3. Alcance											
4. Equipo Auditor					**5. Invitados**						
6. Debilidades					**7. Puntos Fuertes**						
8. Resultados											
Oportunidades de mejora ____					**No conformidades____**						
Oportunidades de mejora											
ID	Proceso/función				Descripción					Responsable	Auditor
No Conformidades											
ID	Proceso/función				Descripción					Responsable	Auditor
9. Conclusiones											

1.5 Calendario de auditoría

Trimestre	Áreas Auditadas
Primer trimestre	- 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
Segundo Trimestre	- A.8 Gestión de Activos - A.9 Control de Acceso - A.10 Criptografía - A.11 Seguridad física y del entorno
Tercer Trimestre	- A.12 Seguridad de las Operaciones - A.12 Seguridad de las Comunicaciones - A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información
Cuarto Trimestre	- A.15 Relación de proveedores - A.16 Gestión de incidentes de seguridad de la información - A. 17 Aspectos de la seguridad de la información para la gestión de la continuidad del negocio - A. Cumplimiento

Anexo IV: Gestión de Indicadores

Sección	Áreas de control+ Métrica	Medición	Valor Aceptable	Valor Objetivo
A5	**Políticas de seguridad de la información**			
M5.1	Revisiones Anuales de la Política de Seguridad	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
A6	**Organización de la seguridad de la información**			
M6.1	Revisión de los Roles y responsabilidades en seguridad de la información	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M6.2	Revisión matriz RACI	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M6.3	Revisiones Lista de Contactos de autoridades reguladoras	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M6.4	Revisión Riesgos registrados sobre los proyectos y su seguridad	(Número total de Revisiones Anuales /Número Mínimo de revisiones=4) *100	75%	100%
M6.5	Revisión política de dispositivos móviles	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M6.6	Reporte estado seguridad dispositivos móviles	(Número total de Reportes /Número Mínimo de reportes=4) *100	75%	100%
A7	**Seguridad relativa a los recursos humanos**			
M7.1	Investigación de antecedentes empleados previo contrato	Tomando una muestra nuevos contratos Investigaciones realizadas en los contratos tomados/Muestra de contratos tomada) *100	80%	100%
M7.2	Reporte completitud curso sobre seguridad de la información	(Número de cursos completos/número de empleados) *100	90%	100%
M7.3	Revisión programa formación sobre seguridad de la información	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%

A8	**Gestión de activos**			
M8.1	Revisión Aleatoria de activos para completitud	Tomando una muestra aleatoria de activos (revisiones satisfactorias de activos/Muestra tomada) *100	80%	100%
M8.2	Revisión procedimiento satisfactorio de devolución dispositivos para abandonos	(Número de bajas con procedimiento satisfactorio/número total de bajas) *100	90%	100%
M8.3	Revisión Proceso satisfactorio de eliminación medios físicos	Tomando una muestra aleatoria de activos eliminados (revisiones satisfactorias de activos/Muestra tomada) *100	95%	100%
A9	**Control de acceso**			
M9.1	Revisión Política de accesos	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M9.2	Revisión reportes accesos no autorizados + investigación derivada	Tomando una muestra de reportes de accesos no autorizados (Número de investigaciones satisfactorias/Muestra tomada) *100	85%	100%
M9.3	Revisión procedimiento altas de usuarios aprobadas y registradas	Tomando una muestra de altas en la compañía (Número de altas satisfactorias/Muestra tomada) *100	80%	100%
M9.4	Revisión procedimiento bajas de usuarios aprobadas y registradas	Tomando una muestra de bajas en la compañía (Número de bajas satisfactorias/Muestra tomada) *100	80%	100%
M9.5	Revisión de los derechos de acceso de usuario	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M9.6	Revisión de los derechos de acceso de usuarios privilegiados	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M9.7	Revisión política gestión de contraseñas	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
A10	**Criptografía**			
M10.1	Revisión proceso actualización de claves	(Número total de actualización /Número Mínimo =1) *100	100%	100%
M10.2	Revisión protocolo de gestión de claves	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%

A11	**Seguridad física y del entorno**			
M11.1	Inspección hojas de registro accesos visitantes	Tomando una muestra aleatoria de hojas de registro de acceso (Número de hojas satisfactorias/Muestra tomada) *100	85%	100%
M11.2	Hojas de Registro Mantenimiento sistema contra incendios	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M11.3	Hojas de Registro Mantenimiento sistema cableado	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
M11.4	Inspección visual sobre posibles equipos de usuario desatendido	(Número de equipos desatendidos/Máximo 3) *100	50%	0%
A12	**Seguridad de las operaciones**			
M12.1	Revisión cambios realizados y registrados	Selección de muestra aleatoria de cambios (Numero de cambios correctamente documentados, aprobados y revisados dentro de la muestra seleccionada/muestra aleatoria de cambios) *100	80%	100%
M12.2	Revisión escáneres de antivirus funcionando en dispositivos	Selección de muestra aleatoria de dispositivos (portátiles y servidores) (Número de escáneres de antivirus funcionando dentro de la muestra seleccionada/muestra aleatoria de dispositivos) *100	90%	100%
M12.3	Revisión copias de seguridad de la información	Selección de muestra aleatoria de dispositivos (portátiles y servidores) (Número de dispositivos con copias de respaldo satisfactoria/muestra aleatoria de dispositivos) *100	80%	100%
M12.4	Comprobación sincronización del reloj	Selección de muestra aleatoria de dispositivos (portátiles y servidores) (Número de sincronizaciones correctas dentro de la muestra seleccionada/muestra aleatoria de dispositivos) *100	90%	100%
M12.5	Software preventivo de instalación de software no autorizado	Selección de muestra aleatoria de dispositivos (portátiles y servidores) (Número de dispositivos con software preventivo dentro de la muestra seleccionada/muestra aleatoria de dispositivos) *100	90%	100%
A13	**Seguridad de las comunicaciones**			
M13.1	Existe un Mapa de segmentación de la red	Existe=100% No existe=0%	100%	100%
M13.2	Reportes de sistemas IDS/IPS	(Número total de Reportes realizados /Número Mínimo de reportes=12) *100	83%	100%

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
M14.1	Informes de revisión y análisis de impacto de parches previos a aplicación	Selección de 5 parches aplicados durante el año (Numero de parches correctamente analizados*100) /5	85%	100%
M14.2	Revisión política SDLC	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
A15	**Relación con proveedores**			
M15.1	Revisiones mensuales del servicio de cloud	(Número total de Revisiones /Número Mínimo de revisiones=4) *100	75%	100%
M15.2	Revisión alineación controles corporativos de seguridad respecto al servicio de cloud	(Número total de Revisiones /Número Mínimo de revisiones=12) *100	83%	100%
M15.3	Chequeo certificación anual ISO 27001 del proveedor de cloud y test de recuperación de desastres	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%
A16	**Gestión de incidentes de seguridad de la información**			
M16.1	Registro de incidentes en GoOne	Existe=100% No existe=0%	100%	100%
M16.2	Registro de incidentes reportados por el proveedor de cloud	Existe=100% No existe=0%	100%	100%
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
M17.1	Ejecución test de recuperación de desastres de GoOne	(Número total de ejecuciones /Número Mínimo de ejecuciones=2) *100	50%	100%
M17.2	Revisión plan de continuidad de GoOne	(Número total de Revisiones Anuales /Número Mínimo de revisiones=2) *100	50%	100%

A18	Cumplimiento			
M18.1	Revisión Independiente de la seguridad de la información	(Número total de revisiones /Número Mínimo =1) *100	100%	100%
M18.2	Notificaciones confirmadas de pérdidas de datos de GoOne	(Número de notificaciones/Máximo 2) *100	50%	0%

Anexo V: Declaración de Aplicabilidad

Capítulo	Control	Aplica	Estado	Indicador
A.5	**Políticas de Seguridad de la Información**			
A.5.1	**Directrices de gestión de la seguridad de la información**			
A.5.1.1	Políticas para la seguridad de la información	**Sí**	Sabemos que la oficina del CISO publicó hace menos de un año la Directiva de Seguridad de Cloud y en este proyecto se va a introducir en los requisitos técnicos y funcionales.	
A.5.1.2	Revisión de las políticas para la seguridad de la información	**Sí**	Aunque la Directiva de Seguridad de Cloud existe el proceso de revisión periódica está definiéndose pues pese a que la definieron los roles principales se ha de revisar si han de añadirse roles nuevos dentro del proceso de revisión.	M5.1
A.6	**Organización de la Seguridad de la Información**			
A.6.1	**Organización interna**			
A.6.1.1	Roles y responsabilidades en seguridad de la información	**Sí**	Dentro de la organización los roles y responsabilidades respecto a la seguridad de la información y los procesos asociados están definidos. Sin embargo, dentro de la particularidad del proyecto se tendrán que revisitar y detallar estos procesos respecto al modelo de responsabilidad compartida con el proveedor de cloud.	M6.1
A.6.1.2	Segregación de tareas	**Sí**	Pese a que los roles con el proveedor de cloud han sido definidos dentro del contrato, internamente la segregación de tareas está definiéndose y los controles son muy limitados pues la tecnología es emergente dentro de la compañía.	M6.2
A.6.1.3	Contacto con las autoridades	**Sí**	Los contactos con las autoridades pertinentes están definidos, las funciones necesarias saben su rol. No es un proceso nuevo tan solo se han añadido los contactos necesarios del proveedor de cloud.	M6.3
A.6.1.4	Contacto con grupos de interés especial	**Sí**	La organización ya formaba parte de grupos de interés como pueden ser ISACA, ENISA, CSIRT. Recientemente se ha unido al grupo de trabajo de CSA para obtener mayor visión de los entornos cloud.	
A.6.1.5	Seguridad de la información en la gestión de proyectos	**Sí**	La metodología estándar definida dentro de la organización para la gestión de proyectos establece las herramientas y procesos para la correcta gestión de riesgos de los proyectos y como monitorizarlos.	M6.4

A.6.2	**Los dispositivos móviles y el teletrabajo**			
A.6.2.1	Política de dispositivos móviles	**Sí**	Existe una política de uso de dispositivos móviles corporativos y una serie de medidas de monitorización y seguridad para asegurar la información.	M6.5
A.6.2.2	Teletrabajo	**Sí**	Existe una política de teletrabajo, recientemente actualizada. Dentro de ella se establecen las medidas a desarrollar por el empleado mientras realiza teletrabajo, así como los controles implantados por la compañía.	M6.6
A.7	**Seguridad relativa a los Recursos Humanos**			
A.7.1	**Antes del empleo**			
A.7.1.1	Investigación de antecedentes	**Sí**	Los procesos de RRHH tienen un nivel de implementación muy elevado avalado por las diversas revisiones/certificaciones a las que se someten anualmente.	M7.1
A.7.1.2	Términos y condiciones del empleo	**Sí**	Los procesos de RRHH tienen un nivel de implementación muy elevado avalado por las diversas revisiones/certificaciones a las que se someten anualmente.	
A.7.2	**Durante el empleo**			
A.7.2.1	Responsabilidades de gestión	**Sí**	Dentro de las responsabilidades de empleados, así como personal subcontratado se encuentran aquellas que implican cumplir con las políticas de seguridad.	
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	**Sí**	De manera periódica todos los empleados y personal con acceso a los sistemas de información realizan una serie de cursos destinados a la concienciación y preparación en materia de seguridad de la información. Se monitoriza la realización de estos cursos. Adicionalmente, se ha añadido un nuevo portfolio de cursos específicos para el personal que está involucrado en el proyecto GoOne.	M7.2 M7.3
A.7.2.3	Proceso disciplinario	**Sí**	Existe un proceso definido y publicado en la intranet de la empresa sobre medidas disciplinarias para aquellos casos en que se provoque una brecha de seguridad.	
A.7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A.7.3.1	Responsabilidades ante la finalización o cambio	**Sí**	Los procesos de RRHH comparten dentro de los procesos de bienvenida de empleados las condiciones en caso de finalización del contrato y las responsabilidades del empleado en materia de seguridad de la información.	

A.8	**Gestión de activos**			
A.8.1	**Responsabilidad sobre los activos**			
A.8.1.1	Inventario de activos	**Sí**	El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.	M8.1
A.8.1.2	Propiedad de los activos	**Sí**	El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.	M8.1
A.8.1.3	Uso aceptable de los activos	**Sí**	El proceso para la infraestructura interna está definido, sin embargo, este proceso ha de perfilarse para el entorno de cloud pues de momento no se han inventariado de manera formal.	M8.1
A.8.1.4	Devolución de activos	**Sí**	Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado.	M8.2
A.8.2	**Clasificación de la información**			
A.8.2.1	Clasificación de la información	**Sí**	Existe un proceso definido para la clasificación de toda la información con la que se trabaja dentro de la compañía y esta es por supuesto, aplicable al entorno de nube.	M8.1
A.8.2.2	Etiquetado de la información	**Sí**	Dentro del proyecto se identificaron los tipos de datos que se iban a alojar en la nube y que requisitos de seguridad y controles habrían de tener.	M8.1
A.8.2.3	Manipulado de la información	**Sí**		M8.1
A.8.3	**Manipulación de los soportes**			
A.8.3.1	Gestión de soportes extraíbles	**Sí**	Este control aplicaría a aquellos componentes físicos para los cuales existe un proceso bien definido, operado e incluso ya auditado donde se asegura la gestión de estos y su ciclo de vida.	M8.3
A.8.3.2	Eliminación de soportes	**Sí**		M8.3

A.8.3.3	Soportes físicos en tránsito	**Sí**		M8.3
A.9	**Control de acceso**			
A.9.1	**Requisitos de negocio para el control de acceso**			
A.9.1.1	Política de control de acceso	**Sí**	El proceso de control de accesos a entornos internos es definido, pero para aquellos accesos en cloud se deberán definir detalladamente, sobre todo para el personal externo.	M9.1
A.9.1.2	Acceso a las redes y a los servicios de red	**Sí**		M9.1
A.9.2	**Gestión de acceso de usuario**			
A.9.2.1	Registro y baja de usuario	**Sí**	Se ha definido un procedimiento de altas y bajas que está en proceso de formalización.	M9.3
A.9.2.2	Provisión de acceso de usuario	**Sí**	Dentro de proceso de altas, se ha definido cual es el procedimiento para asignar roles y que privilegios estos conceden, así como los aprobadores necesarios y el sistema de autenticación e inicio de sesión (multifactor).	M9.3
A.9.2.3	Gestión de privilegios de acceso	**Sí**		M9.3
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	**Sí**	Dentro del proyecto se ha asegurado que la gestión de información de autenticación se realizada por parte del proveedor de cloud de manera adecuada y alineada con las políticas internas de seguridad relacionadas.	M9.3 M9.7
A.9.2.5	Revisión de los derechos de acceso de usuario	**Sí**	El proceso de revisión de usuarios es el establecido dentro de la compañía y este entorno se adhiere al de manera que se cumple y se registra de manera trimestral la revisión de usuarios y accesos en los entornos de GoOne.	M9.5
A.9.2.6	Retirada o reasignación de los derechos de acceso	**Sí**	Dentro del proceso de baja de un empleado o colaborador se encuentra el borrado de sus credenciales por parte de su jefe directo. En el caso del personal que trabaja en el entorno de nube se sigue el mismo proceso.	M9.4
A.9.3	**Responsabilidades del usuario**			
A.9.3.1	Uso de la información secreta de autenticación	**Sí**	Dentro de las formaciones en materia de seguridad de la información se forma a los usuarios sobre métodos y herramientas corporativas para la correcta gestión de sus	

			credenciales, aplicable al entorno de nube.	
A.9.4	**Control de acceso a sistemas y aplicaciones**			
A.9.4.1	Restricción del acceso a la información	**Sí**	Se ha definido dentro de los roles definidos el tipo de información y al que se tiene acceso, así como las funcionalidades disponibles según la clasificación de la información.	M9.6
A.9.4.2	Procedimientos seguros de inicio de sesión	**Sí**	Dentro de proceso de altas, se ha definido cual es el procedimiento para asignar roles y que privilegios estos conceden, así como los aprobadores necesarios y el sistema de autenticación e inicio de sesión (multifactor).	M9.2
A.9.4.3	Sistema de gestión de contraseñas	**Sí**	Dentro de las formaciones en materia de seguridad de la información se forma a los usuarios sobre métodos y herramientas corporativas para la correcta gestión de sus credenciales, aplicable al entorno de nube.	M9.7
A.9.4.4	Uso de utilidades con privilegios del sistema	**Sí**	Se ha definido dentro de los roles definidos las funcionalidades disponibles para los tipos de usuarios, así como los procesos permitidos dentro de la nube y para cuales se requiere aprobación.	M9.6
A.9.4.5	Control de acceso al código fuente de los programas	**Sí**		M9.6
A.10	**Criptografía**			
A.10.1	**Controles criptográficos**			
A.10.1.1	Política de uso de los controles criptográficos	**Sí**	Dentro de la organización existen controles criptográficos pero la Directiva de Seguridad en la nube establece ciertas particularidades que se están analizando respecto a los controles aplicados por el proveedor y su cumplimiento con la política interna. Adicionalmente, se está definiendo como conservar estas claves y manejar su ciclo de vida.	M10.1
A.10.1.2	Gestión de claves	**Sí**		M10.2
A.11	**Seguridad física y del entorno**			
A.11.1	**Áreas seguras**			
A.11.1.1	Perímetro de seguridad física	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las oficinas de la organización están protegidas por cámaras de seguridad y sistemas de detección de presencia.	
A.11.1.2	Controles físicos de entrada	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría	M11.1

A.11.1.3	Seguridad de oficinas, despachos y recursos	**Sí**	ISO 27001 y el cloud provider también cuenta con ella. El acceso a las oficinas de realiza a través de un torno con una tarjeta identificativa. En caso de visitantes siempre acceden acompañados con un empleado previo registro en la entrada del edificio.	M11.1
A.11.1.4	Protección contra las amenazas externas y ambientales	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las instalaciones se encuentran protegidas con sistemas de detección y prevención de incendios, fuga de gas o fallo eléctrico, entre otros.	
A.11.1.5	El trabajo en áreas seguras	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Existen una serie de medidas de seguridad adicionales para las zonas de trabajo en las que existe información física confidencial.	
A.11.1.6	Áreas de carga y descarga	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las zonas de carga y descarga solo se encuentran en el centro de datos, que no da soporte a GoOne.	
A.11.2	**Seguridad de los equipos**			
A.11.2.1	Emplazamiento y protección de equipos	**Sí**	Dentro de la organización la seguridad física se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las medidas de seguridad de los equipos de concentran en el centro de datos, que no da soporte a GoOne.	
A.11.2.2	Instalaciones de suministro	**Sí**		
A.11.2.3	Seguridad del cableado	**Sí**		M11.3
A.11.2.4	Mantenimiento de los equipos	**Sí**		M11.2 M11.3
A.11.2.5	Retirada de materiales propiedad de la empresa	**Sí**		
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	**Sí**		
A.11.2.7	Reutilización o eliminación segura de equipos	**Sí**	El cloud provider también cuenta con la certificación ISO 27001 que asegura este proceso.	
A.11.2.8	Equipo de usuario desatendido	**Sí**	Los equipos de los usuarios disponen de cierre de sesión tras 5 minutos de inactividad.	M11.4

A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	**Sí**	Adicionalmente, los usuarios son formados de manera que conocen su deber respecto a la atención de sus dispositivos y la política y manejo de material físico en el puesto de trabajo.	M11.4
A.12	**Seguridad de las Operaciones**			
A.12.1	**Procedimientos y responsabilidades operacionales**			
A.12.1.1	Documentación de procedimientos operacionales	**Sí**	El paradigma al que se enfrenta la organización con esta aplicación es nuevo, esto conlleva que las operaciones en el entorno de cloud han de definirse partiendo de las directivas y políticas ya existentes, por tanto, el procedimiento operacional de cloud se está definiendo.	
A.12.1.2	Gestión de cambios	**Sí**	El proveedor de cloud ha definido y compartido su proceso formal de notificación de cambios para los clientes de manera que estos puedan anticiparse y analizarlos.	M12.1
A.12.1.3	Gestión de capacidades	**Sí**	El proceso de monitorización de las capacidades se realiza de manera informal y se planea comenzar a definirlo a través de un procedimiento operacional.	
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	**Sí**	Se han provisto de momento un entorno de pruebas y otro de operación, se ha planificado la instalación de un entorno de desarrollo separado del de pruebas. Los movimientos al entorno de operación han de ser aprobados por 2 roles definidos.	
A.12.2	**Protección contra el software malicioso (malware)**			
A.12.2.1	Controles contra el código malicioso	**Sí**	Todo el código para GoOne se desarrolla dentro del proceso de desarrollo seguro de software donde se incluyen test de detección de código malicioso.	M12.2
A.12.3	**Copias de seguridad**			
A.12.3.1	Copias de seguridad de la información	**Sí**	Dentro de las necesidades de la arquitectura se han definido los requisitos de copias de seguridad y configurado en el entorno de nube.	M12.3
A.12.4	**Registros y supervisión**			
A.12.4.1	Registro de eventos	**Sí**	Se están definiendo los requisitos de monitorización del entorno de cloud para asegurar que cubran el entorno respecto a los riesgos identificados, aun así, el proveedor establece una configuración mínima de registros.	
A.12.4.2	Protección de la información del registro	**Sí**	El proveedor de cloud asegura que los registros se mantienen encriptados y accesibles solo por los administradores del cliente.	

A.12.4.3	Registros de administración y operación	**Sí**	Se están definiendo los requisitos de monitorización del entorno de cloud para asegurar que cubran el entorno respecto a los riesgos identificados, aun así, el proveedor establece una configuración mínima de registros.	
A.12.4.4	Sincronización del reloj	**Sí**	Dicha información es publicada y accesible por los clientes del servicio de nube.	M12.4
A.12.5	**Control del software en explotación**			
A.12.5.1	Instalación del software en explotación	**Sí**	No está permitido la instalación de software de explotación y el proveedor de cloud asegura los controles para ello.	
A.12.6	**Gestión de la vulnerabilidad técnica**			
A.12.6.1	Gestión de las vulnerabilidades técnicas	**Sí**	El proveedor de nube notifica a sus clientes de las vulnerabilidades que afectan a sus sistemas y de las medidas a tomar por parte del cliente.	
A.12.6.2	Restricción en la instalación de software	**Sí**	No está permitido la instalación de software de explotación y el proveedor de cloud asegura los controles para ello.	M12.5
A.12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A.12.7.1	Controles de auditoría de sistemas de información	**Sí**	El plan de auditorías interno y externo es notificado con antelación para prever posibles impactos sobre los recursos de personal y los entornos.	
A.13	**Seguridad de las Comunicaciones**			
A.13.1	**Gestión de la seguridad de las redes**			
A.13.1.1	Controles de red	**Sí**	Dentro de la organización los procesos de redes están bien definidos. Sin embargo, dentro de la particularidad del proyecto se están revisitando y detallando estos procesos respecto al modelo de responsabilidad compartida con el proveedor de cloud.	M13.2
A.13.1.2	Seguridad de los servicios de red	**Sí**	Se han establecido unas medidas mínimas sobre la seguridad de los servicios de red, que suelen ser propuestas por el baseline del proveedor de cloud. Sin embargo, se están revisando para GoOne las necesidades en materia de seguridad de red y segregación de esta.	M13.1
A.13.1.3	Segregación en redes	**Sí**		M13.1
A.13.2	**Intercambio de información**			
A.13.2.1	Políticas y procedimientos de	**Sí**	Se han establecido unos protocolos de transferencia segura de información (https, http)	

	intercambio de información		de manera que pueda transferirse la información segura. Adicionalmente, toda la información se transfiere encriptada.	
A.13.2.2	Acuerdos de intercambio de información	**Sí**		
A.13.2.3	Mensajería electrónica	**Sí**		
A.13.2.4	Acuerdos de confidencialidad o no revelación	**Sí**	Existe un acuerdo de confidencialidad firmado con el proveedor de servicio en la nube, así como un acuerdo de transferencia segura de información.	
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A.14.1	**Requisitos de seguridad en los sistemas de información**			
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	**Sí**	Dentro de la fase inicial del proyecto se realizó un análisis de los servicios de seguridad ofrecidos por el proveedor y como estos cumplían con los requisitos funcionales y de seguridad de la aplicación GoOne. Dicho análisis se ha mantenido vivo y se va a actualizando en función de necesidades o actualizaciones.	
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	**Sí**		
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	**Sí**		
A.14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A.14.2.1	Política de desarrollo seguro	**Sí**	Existen procesos de desarrollo de software, sin embargo, este proyecto trae consigo la Infraestructura como código lo que obligará a adoptar controles de desarrollo seguro de software.	M14.2
A.14.2.2	Procedimiento de control de cambios en sistemas	**Sí**		M14.1
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**Sí**		M14.2
A.14.2.4	Restricciones a los cambios en los paquetes de software	**Sí**		M14.2
A.14.2.5	Principios de ingeniería de sistemas seguros	**Sí**		M14.2
A.14.2.6	Entorno de desarrollo seguro	**Sí**		M14.2
A.14.2.7	Externalización del desarrollo de software	**Sí**		M14.2

A.14.2.8	Pruebas funcionales de seguridad de sistemas	**Sí**		M14.1
A.14.2.9	Pruebas de aceptación de sistemas	**Sí**		M14.1
A.14.3	**Datos de prueba**			
A.14.3.1	Protección de los datos de prueba	**Sí**		M14.1
A.15	**Relación de proveedores**			
A.15.1	**Seguridad en las relaciones con proveedores**			
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	**Sí**	El equipo de compras y el equipo de gestión de proveedores implementan una serie de controles y verificaciones manuales, sin embargo, dentro del entorno de cloud es muy posible que se necesite añadir algunos controles automáticos para una mayor optimización.	M15.1
A.15.1.2	Requisitos de seguridad en contratos con terceros	**Sí**	El equipo de compras y el equipo de gestión de proveedores dentro de su proceso de negociación de contrato con el proveedor han definido de manera adecuada los roles a incluir.	M15.2
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	**Sí**	El contrato con el proveedor de nube incluye clausulas para la correcta gestión de la información, así como la transferencia y procesamiento de datos segura.	M15.2
A.15.2	**Gestión de la provisión de servicios del proveedor**			
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	**Sí**	Existe un proceso de revisión periódica del servicio donde se hace un seguimiento de incidentes, se comprueba el cumplimiento del servicio, SLA, cambios en el servicio, en los controles y procedimientos, así como posibles riesgos que afecten al servicio.	M15.1 M15.3
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	**Sí**		M15.1
A.16.	**Gestión de incidentes de seguridad de la información**			
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
A.16.1.1	Responsabilidades y procedimientos	**Sí**	El proceso de gestión de incidentes es definido y conocido por los actores involucrados, será necesario ampliarlo para cubrir los incidentes en entornos de cloud.	

A.16.1.2	Notificación de los eventos de seguridad de la información	**Sí**	El proveedor de servicio en la nube ha proporcionado un proceso de notificación de incidentes y eventos de seguridad para los administradores de GoOne.	M16.1 M16.2
A.16.1.3	Notificación de puntos débiles de la seguridad	**Sí**		M16.1 M16.2
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	**Sí**	El proceso de gestión de incidentes es definido y conocido por los actores involucrados, sin embargo, los procesos de decisión para el entorno de cloud no son conocidos y aplicados de manera extensa.	M16.1 M16.2
A.16.1.5	Respuesta a incidentes de seguridad de la información	**Sí**		M16.1 M16.2
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	**Sí**		M16.1 M16.2
A.16.1.7	Recopilación de evidencias	**Sí**		M16.1 M16.2
A.17	**Aspectos de la seguridad de la información para la gestión de la continuidad del negocio**			
A.17.1	**Continuidad de la seguridad de la información**			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**Sí**	Dentro de la organización se monitorizan y redundan los sistemas críticos de manera estricta, en este caso se han adaptado las monitorizaciones sobre controles clave de continuidad de negocio para que incluyan GoOne su entorno de cloud.	M17.2
A.17.1.2	Implementar la continuidad de la seguridad de la información	**Sí**	Existe una política definida de continuidad de negocio y dentro del sistema GoOne se ha definido un procedimiento de recuperación de desastres para alinearlo con la política de continuidad de negocio.	M17.2
A.17.1.2	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Sí**	Existe un procedo anual en el que se revisa y se prueba la estrategia de recuperación de desastres, además se coordina con el proveedor de cloud. Adicionalmente, se hace un seguimiento al proveedor de cloud sobre su política de continuidad de negocio y la gestión de ella.	M17.1
A.17.2	**Redundancias**			

A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	**Sí**		M17.2
A.18	**Cumplimiento**			
A.18.1	**Cumplimiento de los requisitos legales y contractuales**			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	**Sí**	Para GoOne el estado de cumplimiento inicial respecto a la seguridad de la información es el derivado de los procesos heredados de la organización y del proveedor de cloud, sin embargo, este cumplimiento se debe definir de manera detallada para el producto.	
A.18.1.2	Derechos de Propiedad Intelectual (DPI)	**Sí**		
A.18.1.3	Protección de los registros de la organización	**Sí**		M18.2
A.18.1.4	Protección y privacidad de la información de carácter persona	**Sí**		M18.2
A.18.1.5	Regulación de los controles criptográficos	**Sí**		M18.2
A.18.2	**Revisiones de la seguridad de la información**			
A.18.2.1	Revisión independiente de la seguridad de la información	**Sí**	La organización dentro de su proceso de seguimiento del servicio se asegura que el proveedor del servicio de cloud proporcione de manera anual su certificación ISO/IEC 27001.	M18.1
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	**Sí**		M18.1
A.18.2.3	Comprobación del cumplimiento técnico	**Sí**		M18.1

Anexo VI: Inventario Activos

Nombre	ID	Tipo de activo	Valoración del activo	Dimensiones		
				C	I	D
Suministro Eléctrico	*S1*	*[S] Servicios*	*Medio*	*3*	*3*	*0*
Servicio Limpieza	*S2*	*[S] Servicios*	*Muy Bajo*	*0*	*0*	*0*
Servicio Internet	*S3*	*[S] Servicios*	*Alto*	*2*	*3*	*6*
Servicio AWS nube	*S4*	*[S] Servicios*	*Muy Alto*	*7*	*9*	*10*
Servicios Globales	*S5*	*[S] Servicios*	*Alto*	*6*	*5*	*6*
Personal (staff)	*P1*	*[P] Personal*	*Alto*	*3*	*3*	*6*
Personal tierra y operaciones aeroportuarias	*P2*	*[P] Personal*	*Alto*	*3*	*3*	*6*
Personal Dirección	*P3*	*[P] Personal*	*Medio*	*3*	*2*	*3*
Equipos de Usuario oficinas	*HW1*	*[HW] Equipamiento informático (hardware)*	*Alto*	*6*	*5*	*6*
Equipos de servicios aeroportuarios	*HW2*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*8*	*9*	*9*

Equipos en aeronaves	*HW3*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*10*	*10*	*10*
Servidor VPN	*HW4*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*7*	*9*	*9*
Servidor Correo	*HW5*	*[HW] Equipamiento informático (hardware)*	*Alto*	*5*	*6*	*3*
Servidor Interno para autenticación en AWS	*HW6*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*9*	*9*	*9*
Routers instalaciones locales	*HW7*	*[HW] Equipamiento informático (hardware)*	*Alto*	*5*	*6*	*3*
Web Interfaz GoOne	*SW1*	*[SW] Aplicaciones (software)*	*Muy Alto*	*9*	*8*	*9*
Software GoOne	*SW2*	*[SW] Aplicaciones (software)*	*Muy Alto*	*10*	*10*	*8*
Antivirus equipos usuario	*SW3*	*[SW] Aplicaciones (software)*	*Alto*	*8*	*3*	*0*
Sistema Operativo equipos usuario	*SW4*	*[SW] Aplicaciones (software)*	*Medio*	*6*	*3*	*3*
Sistema de ticketing	*SW5*	*[SW] Aplicaciones (software)*	*Medio*	*3*	*3*	*3*
Sistema Monitorización local	*SW6*	*[SW] Aplicaciones (software)*	*Alto*	*6*	*8*	*3*
Conexión con AWS	*COM1*	*[COM] Redes de comunicaciones*	*Muy Alto*	*9*	*9*	*10*
Firewalls	*COM2*	*[COM] Redes de comunicaciones*	*Muy Alto*	*9*	*9*	*8*
Red de comunicación móvil	*COM3*	*[COM] Redes de comunicaciones*	*Alto*	*4*	*8*	*6*
Red de comunicación oficinas	*COM4*	*[COM] Redes de comunicaciones*	*Alto*	*5*	*8*	*6*

Conexión a Datacenters corporativos	*COM5*	*[COM] Redes de comunicaciones*	*Alto*	*6*	*8*	*8*
Sede Grupo	*L1*	*[L] Instalaciones*	*Medio*	*6*	*0*	*3*
Sede de cada Aerolínea	*L2*	*[L] Instalaciones*	*Muy Alto*	*6*	*8*	*8*
Datacenter Europa	*L3*	*[L] Instalaciones*	*Muy Alto*	*8*	*9*	*8*
Datacenter América	*L4*	*[L] Instalaciones*	*Muy Alto*	*8*	*9*	*8*
Servicios Aeroportuarios Asia-Pacífico	*L5*	*[L] Instalaciones*	*Muy Alto*	*5*	*8*	*8*
Servicios Aeroportuarios EMEA	*L6*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*
Servicios Aeroportuarios América Norte	*L7*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*
Servicios Aeroportuarios América Sur	*L8*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*
Aeronaves	*L9*	*[L] Instalaciones*	*Muy Alto*	*9*	*10*	*10*
Código Fuente GoOne	*D1*	*[D] Datos*	*Muy Alto*	*10*	*10*	*9*
Copias Respaldo GoOne	*D2*	*[D] Datos*	*Muy Alto*	*9*	*9*	*9*
Datos Financieros/Contables	*D3*	*[D] Datos*	*Alto*	*9*	*10*	*8*
Datos Personal	*D4*	*[D] Datos*	*Alto*	*9*	*5*	*2*
Credenciales corporativas	*D5*	*[D] Datos*	*Alto*	*9*	*6*	*9*
Credenciales AWS	*D6*	*[D] Datos*	*Alto*	*9*	*6*	*9*

Datos en papel físico	*D7*	*[D] Datos*	*Alto*	*7*	*2*	*0*
Claves sistemas en AWS	*K1*	*[K] Claves criptográficas*	*Muy Alto*	*9*	*9*	*9*
Claves criptográficas servidores	*K2*	*[K] Claves criptográficas*	*Alto*	*8*	*6*	*9*
Claves criptográficas copias de respaldo	*K3*	*[K] Claves criptográficas*	*Alto*	*8*	*3*	*3*
Sistemas guardado Backus	*Media1*	*[Media] Soportes de información*	*Alto*	*8*	*6*	*6*
Dispositivos portátiles de almacenamiento	*Media2*	*[Media] Soportes de información*	*Alto*	*8*	*2*	*3*
Equipamiento prevención incendios	*AUX1*	*[AUX] Equipamiento auxiliar*	*Alto*	*2*	*9*	*8*
Equipamiento cableado	*AUX2*	*[AUX] Equipamiento auxiliar*	*Alto*	*2*	*3*	*8*
Equipamientos dispositivos a bordo para GoOne	*AUX3*	*[AUX] Equipamiento auxiliar*	*Muy Alto*	*9*	*10*	*10*
Impresoras	*AUX4*	*[AUX] Equipamiento auxiliar*	*Bajo*	*2*	*0*	*0*

Anexo VII: Identificación y Valoración de Amenazas

Nombre	ID	Tipo de activo	Valoración del activo	Frecuencia	Impacto Amenaza C	I	D
Suministro Eléctrico	S1	[S] Servicios	Medio		3	3	0
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.24] Caída del sistema por agotamiento de recursos				2			70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicio Limpieza	S2	[S] Servicios	Muy Bajo		0	0	0
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicio Internet	S3	[S] Servicios	Alto		2	3	6
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.24] Caída del sistema por agotamiento de recursos				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicio AWS nube	S4	[S] Servicios	Muy Alto		7	9	10
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.24] Caída del sistema por agotamiento de recursos				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicios Globales	S5	[S] Servicios	Alto		6	5	6
[E.2] Errores del administrador				3	85%	80%	70%
[E.24] Caída del sistema por agotamiento de recursos				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Personal (staff)	P1	[P] Personal	Alto		3	3	6
[E.7] Deficiencias en la organización				3			40%
[E.28] Indisponibilidad del personal				3			40%
Personal tierra y operaciones aeroportuarias	P2	[P] Personal	Alto		3	3	6
[E.7] Deficiencias en la organización				3			40%
[E.28] Indisponibilidad del personal				3			60%
Personal Dirección	P3	[P] Personal	Medio		3	2	3
[E.7] Deficiencias en la organización				3			40%
[E.28] Indisponibilidad del personal				3			60%

Equipos de Usuario oficinas	**HW1**	**[HW] Equipamiento informático (hardware)**	**Alto**		**6**	**5**	**6**
[N.1] Fuego				2			50%
[N.2] Daños por agua				2			50%
[I.4] Contaminación electromagnética				1			50%
[I.5] Avería de origen físico o lógico				2			50%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
Equipos de servicios aeroportuarios	**HW2**	**[HW] Equipamiento informático (hardware)**	**Muy Alto**		**8**	**9**	**9**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[I.4] Contaminación electromagnética				2			70%
[I.5] Avería de origen físico o lógico				2			70%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Equipos en aeronaves	**HW3**	**[HW] Equipamiento informático (hardware)**	**Muy Alto**		**10**	**10**	**10**
[N.1] Fuego				3			80%
[N.2] Daños por agua				3			80%
[I.3] Contaminación mecánica				1			80%
[I.4] Contaminación electromagnética				1			80%
[I.5] Avería de origen físico o lógico				3			80%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servidor VPN	**HW4**	**[HW] Equipamiento informático (hardware)**	**Muy Alto**		**7**	**9**	**9**
[N.1] Fuego				2			75%
[N.2] Daños por agua				2			75%
[I.4] Contaminación electromagnética				1			80%
[I.5] Avería de origen físico o lógico				3			80%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Servidor Correo	**HW5**	**[HW] Equipamiento informático (hardware)**	**Alto**		**5**	**6**	**3**
[N.1] Fuego				2			50%
[N.2] Daños por agua				2			50%
[I.4] Contaminación electromagnética				1			80%
[I.5] Avería de origen físico o lógico				3			80%
[E.2] Errores del administrador				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servidor Interno para autenticación en AWS	**HW6**	**[HW] Equipamiento informático (hardware)**	**Muy Alto**		**9**	**9**	**9**
[N.1] Fuego				2			90%
[N.2] Daños por agua				2			90%
[I.4] Contaminación electromagnética				1			80%
[I.5] Avería de origen físico o lógico				3			80%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Routers instalaciones locales	**HW7**	**[HW] Equipamiento informático (hardware)**	**Alto**		**5**	**6**	**3**
[N.1] Fuego				2			60%
[N.2] Daños por agua				2			60%
[I.4] Contaminación electromagnética				1			80%
[I.5] Avería de origen físico o lógico				3			80%
[I.6] Corte del suministro eléctrico				2			60%
[E.2] Errores del administrador				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Web Interfaz GoOne	**SW1**	**[SW] Aplicaciones (software)**	**Muy Alto**		**9**	**8**	**9**
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Software GoOne	**SW2**	**[SW] Aplicaciones (software)**	**Muy Alto**		**10**	**10**	**8**
[E.1] Errores de ellos usuarios				2	70%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Antivirus equipos usuario	**SW3**	**[SW] Aplicaciones (software)**	**Alto**		**8**	**3**	**0**
[I.5] Avería de origen físico o lógico				3			30%
[E.1] Errores de ellos usuarios				2	88%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Sistema Operativo equipos usuario	**SW4**	**[SW] Aplicaciones (software)**	**Medio**		**6**	**3**	**3**
[I.5] Avería de origen físico o lógico				3			80%
[E.1] Errores de ellos usuarios				2	75%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Sitema de ticketing	**SW5**	**[SW] Aplicaciones (software)**	**Medio**		**3**	**3**	**3**
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Sistema Monitorización local	**SW6**	**[SW] Aplicaciones (software)**	**Alto**		6	8	3
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.8] Difusión de software dañino				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.8] Difusión de software dañino				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Conexión con AWS	**COM1**	**[COM] Redes de comunicaciones**	**Muy Alto**		9	9	10
[E.2] Errores del administrador				3	85%	80%	70%
[E.9] Errores de [re-]encaminamiento				3	85%		
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Firewalls	**COM2**	**[COM] Redes de comunicaciones**	**Muy Alto**		9	9	8
[I.5] Avería de origen físico o lógico				3			80%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Red de comunicación móvil	**COM3**	**[COM] Redes de comunicaciones**	**Alto**		4	8	6
[I.5] Avería de origen físico o lógico				3			80%
[E.2] Errores del administrador				3	85%	80%	70%
[E.9] Errores de [re-]encaminamiento				3	85%		
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Red de comunicación oficinas	**COM4**	**[COM] Redes de comunicaciones**	**Alto**		5	8	6
[I.5] Avería de origen físico o lógico				3			80%
[E.2] Errores del administrador				3	85%	80%	70%
[E.9] Errores de [re-]encaminamiento				3	85%		
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Conexión a Datacenters corporativos	**COM5**	**[COM] Redes de comunicaciones**	**Alto**		6	8	8
[E.2] Errores del administrador				3	85%	80%	70%
[E.9] Errores de [re-]encaminamiento				3	85%		
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Sede Grupo	**L1**	**[L] Instalaciones**	**Medio**		6	0	3
[N.1] Fuego				2			40%
[N.2] Daños por agua				2			40%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Sede de cada Aerolinea	**L2**	**[L] Instalaciones**	**Muy Alto**		**6**	**8**	**8**
[N.1] Fuego				2			40%
[N.2] Daños por agua				2			40%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Datacenter Europa	**L3**	**[L] Instalaciones**	**Muy Alto**		**8**	**9**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Datacenter America	**L4**	**[L] Instalaciones**	**Muy Alto**		**8**	**9**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Servicios Aeroportuarios Asia-Pacífico	**L5**	**[L] Instalaciones**	**Muy Alto**		**5**	**8**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicios Aeroportuarios EMEA	**L6**	**[L] Instalaciones**	**Alto**		**5**	**8**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicios Aeroportuarios América Norte	**L7**	**[L] Instalaciones**	**Alto**		**5**	**8**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Servicios Aeroportuarios América Sur	**L8**	**[L] Instalaciones**	**Alto**		**5**	**8**	**8**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Aeronaves	**L9**	**[L] Instalaciones**	**Muy Alto**		**9**	**10**	**10**
[N.1] Fuego				2			70%
[N.2] Daños por agua				2			70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Código Fuente GoOne	**D1**	**[D] Datos**	**Muy Alto**		**10**	**10**	**9**
[E.1] Errores de ellos usuarios				2	85%	80%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Copias Respaldo GoOne	**D2**	**[D] Datos**	**Muy Alto**		**9**	**9**	**9**
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Datos Financieros/Contables	**D3**	**[D] Datos**	**Alto**		**9**	**10**	**8**
[E.1] Errores de ellos usuarios				3	95%	95%	90%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Datos Personal	**D4**	**[D] Datos**	**Alto**		**9**	**5**	**2**
[E.1] Errores de ellos usuarios				3	95%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Credenciales corporativos	**D5**	**[D] Datos**	**Alto**		9	6	9
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Credenciales AWS	**D6**	**[D] Datos**	**Alto**		9	6	9
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Datos en papel fisico	**D7**	**[D] Datos**	**Alto**		7	2	0
[E.1] Errores de ellos usuarios				3	70%	20%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Claves sistemas en AWS	**K1**	**[K] Claves criptográficas**	**Muy Alto**		9	9	9
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Claves criptográficas servidores	**K2**	**[K] Claves criptográficas**	**Alto**		8	6	9
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Claves criptográficas copias de respaldo	**K3**	**[K] Claves criptográficas**	**Alto**		8	3	3
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
[A.11] Acceso no autorizado				2	85%	80%	

Sistemas guardado Backup	**Media 1**	**[Media] Soportes de información**	**Alto**		**8**	**6**	**6**
[N.1] Fuego				2			60%
[N.2] Daños por agua				2			60%
[I.4] Contaminación electromagnética				1			60%
[I.5] Avería de origen físico o lógico				2			70%
[I.6] Corte del suministro eléctrico				2			70%
[I.10] Degradación de los soportes de almacenamiento de la información				2			70%
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.4] Errores de configuración				3		80%	
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Dispositivos portátiles de almacenamiento	**Media 2**	**[Media] Soportes de información**	**Alto**		**8**	**2**	**3**
[N.1] Fuego				2			30%
[N.2] Daños por agua				2			30%
[I.3] Contaminación mecánica				2			30%
[I.4] Contaminación electromagnética				1			30%
[I.5] Avería de origen físico o lógico				2			50%
[I.6] Corte del suministro eléctrico				2			50%
[I.10] Degradación de los soportes de almacenamiento de la información				2			50%
[E.1] Errores de ellos usuarios				3	90%	95%	70%
[E.2] Errores del administrador				3	85%	80%	70%
[E.4] Errores de configuración				3		80%	
[A.5] Suplantación de la identidad del usuario				2	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	

Equipamiento prevención incendios	**AUX1**	**[AUX] Equipamiento auxiliar**	**Alto**		**2**	**9**	**8**
[N.1] Fuego				2			80%
[N.2] Daños por agua				2			80%
[I.3] Contaminación mecánica				2			80%
[I.5] Avería de origen físico o lógico				2			80%
[I.6] Corte del suministro eléctrico				2			80%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Equipamiento cableado	**AUX2**	**[AUX] Equipamiento auxiliar**	**Alto**		**2**	**3**	**8**
[N.1] Fuego				2			80%
[N.2] Daños por agua				2			80%
[I.3] Contaminación mecánica				2			80%
[I.4] Contaminación electromagnética				2			80%
[I.5] Avería de origen físico o lógico				2			80%
[I.6] Corte del suministro eléctrico				2			80%
[E.2] Errores del administrador				3	85%	80%	70%
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Equipamiento dispositivos a bordo para GoOne	**AUX3**	**[AUX] Equipamiento auxiliar**	**Muy Alto**		**9**	**10**	**10**
[N.1] Fuego				3			95%
[N.2] Daños por agua				3			95%
[I.3] Contaminación mecánica				3			95%
[I.4] Contaminación electromagnética				3			95%
[I.5] Avería de origen físico o lógico				3			95%
[I.6] Corte del suministro eléctrico				2			80%
[E.2] Errores del administrador				3	85%	80%	70%
[E.4] Errores de configuración				3		95%	
[A.7] Uso no previsto				2	85%	80%	70%
[A.11] Acceso no autorizado				2	85%	80%	
Impresoras	**AUX4**	**[AUX] Equipamiento auxiliar**	**Bajo**		**2**	**0**	**0**
[N.1] Fuego				2			60%
[N.2] Daños por agua				2			60%
[I.4] Contaminación electromagnética				2			60%
[I.5] Avería de origen físico o lógico				2			60%
[I.6] Corte del suministro eléctrico				2			60%

Anexo VIII: Impacto Potencial de los Activos

Nombre	ID	Tipo de activo	Valoración del activo	Dimensiones			Impacto (Max)			Impacto Potencial		
				C	I	D	C	I	D	C	I	D
Suministro Eléctrico	S1	[S] Servicios	Medio	3	3	0	85%	80%	70%	2,55	2,4	0
Servicio Limpieza	S2	[S] Servicios	Muy Bajo	0	0	0	85%	80%	70%	0	0	0
Servicio Internet	S3	[S] Servicios	Alto	2	3	6	85%	80%	70%	1,7	2,4	4,2
Servicio AWS nube	S4	[S] Servicios	Muy Alto	7	9	10	85%	80%	70%	5,95	7,2	7
Servicios Globales	S5	[S] Servicios	Alto	6	5	6	85%	80%	70%	5,1	4	4,2
Personal (staff)	P1	[P] Personal	Alto	3	3	6	0	0	40%	0	0	2,4
Personal tierra y operaciones aeroportuarias	P2	[P] Personal	Alto	3	3	6	0	0	60%	0	0	3,6
Personal Dirección	P3	[P] Personal	Medio	3	2	3	0	0	60%	0	0	1,8
Equipos de Usuario oficinas	HW1	[HW] Equipamiento informático (hardware)	Alto	6	5	6	85%	80%	70%	5,1	4	4,2
Equipos de servicios aeroportuarios	HW2	[HW] Equipamiento informático (hardware)	Muy Alto	8	9	9	85%	80%	70%	6,8	7,2	6,3

Equipos en aeronaves	*HW3*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*10*	*10*	*10*	85%	80%	80%	8,5	8	8
Servidor VPN	*HW4*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*7*	*9*	*9*	85%	80%	80%	5,95	7,2	7,2
Servidor Correo	*HW5*	*[HW] Equipamiento informático (hardware)*	*Alto*	*5*	*6*	*3*	85%	80%	80%	4,25	4,8	2,4
Servidor Interno para autenticación en AWS	*HW6*	*[HW] Equipamiento informático (hardware)*	*Muy Alto*	*9*	*9*	*9*	85%	80%	90%	7,65	7,2	8,1
Routers instalaciones locales	*HW7*	*[HW] Equipamiento informático (hardware)*	*Alto*	*5*	*6*	*3*	85%	80%	80%	4,25	4,8	2,4
Web Interfaz GoOne	*SW1*	*[SW] Aplicaciones (software)*	*Muy Alto*	*9*	*8*	*9*	85%	80%	70%	7,65	6,4	6,3
Software GoOne	*SW2*	*[SW] Aplicaciones (software)*	*Muy Alto*	*10*	*10*	*8*	85%	80%	70%	8,5	8	5,6
Antivirus equipos usuario	*SW3*	*[SW] Aplicaciones (software)*	*Alto*	*8*	*3*	*0*	88%	80%	70%	7,04	2,4	0
Sistema Operativo equipos usuario	*SW4*	*[SW] Aplicaciones (software)*	*Medio*	*6*	*3*	*3*	85%	80%	80%	5,1	2,4	2,4
Sistema de ticketing	*SW5*	*[SW] Aplicaciones (software)*	*Medio*	*3*	*3*	*3*	85%	80%	70%	2,55	2,4	2,1
Sistema Monitorización local	*SW6*	*[SW] Aplicaciones (software)*	*Alto*	*6*	*8*	*3*	85%	80%	70%	5,1	6,4	2,1
Conexión con AWS	*COM1*	*[COM] Redes de comunicaciones*	*Muy Alto*	*9*	*9*	*10*	85%	80%	70%	7,65	7,2	7
Firewalls	*COM2*	*[COM] Redes de comunicaciones*	*Muy Alto*	*9*	*9*	*8*	85%	80%	80%	7,65	7,2	6,4
Red de comunicación móvil	*COM3*	*[COM] Redes de comunicaciones*	*Alto*	*4*	*8*	*6*	85%	80%	80%	3,4	6,4	4,8

Red de comunicación oficinas	*COM4*	*[COM] Redes de comunicaciones*	*Alto*	*5*	*8*	*6*	85%	80%	80%	4,25	6,4	4,8
Conexión a Datacenters corporativos	*COM5*	*[COM] Redes de comunicaciones*	*Alto*	*6*	*8*	*8*	85%	80%	70%	5,1	6,4	5,6
Sede Grupo	*L1*	*[L] Instalaciones*	*Medio*	*6*	*0*	*3*	85%	80%	70%	5,1	0	2,1
Sede de cada Aerolínea	*L2*	*[L] Instalaciones*	*Muy Alto*	*6*	*8*	*8*	85%	80%	70%	5,1	6,4	5,6
Datacenter Europa	*L3*	*[L] Instalaciones*	*Muy Alto*	*8*	*9*	*8*	85%	80%	70%	6,8	7,2	5,6
Datacenter América	*L4*	*[L] Instalaciones*	*Muy Alto*	*8*	*9*	*8*	85%	80%	70%	6,8	7,2	5,6
Servicios Aeroportuarios Asia-Pacífico	*L5*	*[L] Instalaciones*	*Muy Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6
Servicios Aeroportuarios EMEA	*L6*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6
Servicios Aeroportuarios América Norte	*L7*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6
Servicios Aeroportuarios América Sur	*L8*	*[L] Instalaciones*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6
Aeronaves	*L9*	*[L] Instalaciones*	*Muy Alto*	*9*	*10*	*10*	85%	80%	70%	7,65	8	7
Código Fuente GoOne	*D1*	*[D] Datos*	*Muy Alto*	*10*	*10*	*9*	90%	95%	70%	9	9,5	6,3
Copias Respaldo GoOne	*D2*	*[D] Datos*	*Muy Alto*	*9*	*9*	*9*	90%	95%	70%	8,1	8,55	6,3
Datos Financieros/Contables	*D3*	*[D] Datos*	*Alto*	*9*	*10*	*8*	95%	95%	90%	8,55	9,5	7,2
Datos Personal	*D4*	*[D] Datos*	*Alto*	*9*	*5*	*2*	95%	95%	70%	8,55	4,75	1,4

Credenciales corporativas	*D5*	*[D] Datos*	*Alto*	*9*	*6*	*9*	90%	95%	70%	8,1	5,7	6,3
Credenciales AWS	*D6*	*[D] Datos*	*Alto*	*9*	*6*	*9*	90%	95%	70%	8,1	5,7	6,3
Datos en papel físico	*D7*	*[D] Datos*	*Alto*	*7*	*2*	*0*	85%	80%	70%	5,95	1,6	0
Claves sistemas en AWS	*K1*	*[K] Claves criptográficas*	*Muy Alto*	*9*	*9*	*9*	90%	95%	70%	8,1	8,55	6,3
Claves criptográficas servidores	*K2*	*[K] Claves criptográficas*	*Alto*	*8*	*6*	*9*	90%	95%	70%	7,2	5,7	6,3
Claves criptográficas copias de respaldo	*K3*	*[K] Claves criptográficas*	*Alto*	*8*	*3*	*3*	90%	95%	70%	7,2	2,85	2,1
Sistemas guardado Backup	*Media 1*	*[Media] Soportes de información*	*Alto*	*8*	*6*	*6*	90%	95%	70%	7,2	5,7	4,2
Dispositivos portátiles de almacenamiento	*Media 2*	*[Media] Soportes de información*	*Alto*	*8*	*2*	*3*	90%	95%	70%	7,2	1,9	2,1
Equipamiento prevención incendios	*AUX1*	*[AUX] Equipamiento auxiliar*	*Alto*	*2*	*9*	*8*	85%	80%	80%	1,7	7,2	6,4
Equipamiento cableado	*AUX2*	*[AUX] Equipamiento auxiliar*	*Alto*	*2*	*3*	*8*	85%	80%	80%	1,7	2,4	6,4
Equipamiento dispositivos a bordo para GoOne	*AUX3*	*[AUX] Equipamiento auxiliar*	*Muy Alto*	*9*	*10*	*10*	85%	95%	95%	7,65	9,5	9,5
Impresoras	*AUX4*	*[AUX] Equipamiento auxiliar*	*Bajo*	*2*	*0*	*0*	0%	0%	60%	0	0	0

Anexo IX: Análisis de Riesgo

Nombre	ID	Valoración del activo	Dimensiones			Impacto (Max)			Impacto Potencial			Frecuencia MAX	Riesgo			Riesgo		
			C	I	D	C	I	D	C	I	D		C	I	D	C	I	D
Suministro Eléctrico	S1	Medio	3	3	0	85%	80%	70%	2,55	2,4	0	Alta	2,55	2,4	0	Bajo	Bajo	Bajo
Servicio Limpieza	S2	Muy Bajo	0	0	0	85%	80%	70%	0	0	0	Media	0	0	0	Bajo	Bajo	Bajo
Servicio Internet	S3	Alto	2	3	6	85%	80%	70%	1,7	2,4	4,2	Alta	1,7	2,4	4,2	Bajo	Bajo	Medio-Bajo
Servicio AWS nube	S4	Muy Alto	7	9	10	85%	80%	70%	5,95	7,2	7	Alta	5,95	7,2	7	Medio-Bajo	Medio-Alto	Medio-Alto
Servicios Globales	S5	Alto	6	5	6	85%	80%	70%	5,1	4	4,2	Alta	5,1	4	4,2	Medio-Bajo	Medio-Bajo	Medio-Bajo
Personal (staff)	P1	Alto	3	3	6	0	0	40%	0	0	2,4	Alta	0	0	2,4	Bajo	Bajo	Bajo
Personal tierra y operaciones aeroportuarias	P2	Alto	3	3	6	0	0	60%	0	0	3,6	Alta	0	0	3,6	Bajo	Bajo	Bajo
Personal Dirección	P3	Medio	3	2	3	0	0	60%	0	0	1,8	Alta	0	0	1,8	Bajo	Bajo	Bajo
Equipos de Usuario oficinas	HW1	Alto	6	5	6	85%	80%	70%	5,1	4	4,2	Alta	5,1	4	4,2	Medio-Bajo	Medio-Bajo	Medio-Bajo
Equipos de servicios aeroportuarios	HW2	Muy Alto	8	9	9	85%	80%	70%	6,8	7,2	6,3	Alta	6,8	7,2	6,3	Medio	Medio-Alto	Medio

Equipos en aeronaves	*HW3*	*Muy Alto*	*10*	*10*	*10*	85%	80%	80%	8,5	8	8	Alta	8,5	8	8	Alto	Alto	Alto
Servidor VPN	*HW4*	*Muy Alto*	*7*	*9*	*9*	85%	80%	80%	5,95	7,2	7,2	Alta	5,95	7,2	7,2	Medio-Bajo	Medio-Alto	Medio-Alto
Servidor Correo	*HW5*	*Alto*	*5*	*6*	*3*	85%	80%	80%	4,25	4,8	2,4	Alta	4,25	4,8	2,4	Medio-Bajo	Medio-Bajo	Bajo
Servidor Interno para autenticación en AWS	*HW6*	*Muy Alto*	*9*	*9*	*9*	85%	80%	90%	7,65	7,2	8,1	Alta	7,65	7,2	8,1	Medio-Alto	Medio-Alto	Alto
Routers instalaciones locales	*HW7*	*Alto*	*5*	*6*	*3*	85%	80%	80%	4,25	4,8	2,4	Alta	4,25	4,8	2,4	Medio-Bajo	Medio-Bajo	Bajo
Web Interfaz GoOne	*SW1*	*Muy Alto*	*9*	*8*	*9*	85%	80%	70%	7,65	6,4	6,3	Alta	7,65	6,4	6,3	Medio-Alto	Medio	Medio
Software GoOne	*SW2*	*Muy Alto*	*10*	*10*	*8*	85%	80%	70%	8,5	8	5,6	Alta	8,5	8	5,6	Alto	Alto	Medio-Bajo
Antivirus equipos usuario	*SW3*	*Alto*	*8*	*3*	*0*	88%	80%	70%	7,04	2,4	0	Alta	7,04	2,4	0	Medio-Alto	Bajo	Bajo
Sistema Operativo equipos usuario	*SW4*	*Medio*	*6*	*3*	*3*	85%	80%	80%	5,1	2,4	2,4	Alta	5,1	2,4	2,4	Medio-Bajo	Bajo	Bajo
Sistema de ticketing	*SW5*	*Medio*	*3*	*3*	*3*	85%	80%	70%	2,55	2,4	2,1	Alta	2,55	2,4	2,1	Bajo	Bajo	Bajo
Sistema Monitorización local	*SW6*	*Alto*	*6*	*8*	*3*	85%	80%	70%	5,1	6,4	2,1	Alta	5,1	6,4	2,1	Medio-Bajo	Medio	Bajo
Conexión con AWS	*COM1*	*Muy Alto*	*9*	*9*	*10*	85%	80%	70%	7,65	7,2	7	Alta	7,65	7,2	7	Medio-Alto	Medio-Alto	Medio-Alto
Firewalls	*COM2*	*Muy Alto*	*9*	*9*	*8*	85%	80%	80%	7,65	7,2	6,4	Alta	7,65	7,2	6,4	Medio-Alto	Medio-Alto	Medio

Red de comunicación móvil	*COM3*	*Alto*	*4*	*8*	*6*	85%	80%	80%	3,4	6,4	4,8	Alta	3,4	6,4	4,8	Bajo	Medio	Medio-Bajo
Red de comunicación oficinas	*COM4*	*Alto*	*5*	*8*	*6*	85%	80%	80%	4,25	6,4	4,8	Alta	4,25	6,4	4,8	Medio-Bajo	Medio	Medio-Bajo
Conexión a Datacenters corporativos	*COM5*	*Alto*	*6*	*8*	*8*	85%	80%	70%	5,1	6,4	5,6	Alta	5,1	6,4	5,6	Medio-Bajo	Medio	Medio-Bajo
Sede Grupo	*L1*	*Medio*	*6*	*0*	*3*	85%	80%	70%	5,1	0	2,1	Media	3,4	0	1,4	Bajo	Bajo	Bajo
Sede de cada Aerolínea	*L2*	*Muy Alto*	*6*	*8*	*8*	85%	80%	70%	5,1	6,4	5,6	Media	3,4	4,267	3,73	Bajo	Medio-Bajo	Bajo
Datacenter Europa	*L3*	*Muy Alto*	*8*	*9*	*8*	85%	80%	70%	6,8	7,2	5,6	Media	4,533	4,8	3,73	Medio-Bajo	Medio-Bajo	Bajo
Datacenter América	*L4*	*Muy Alto*	*8*	*9*	*8*	85%	80%	70%	6,8	7,2	5,6	Media	4,533	4,8	3,73	Medio-Bajo	Medio-Bajo	Bajo
Servicios Aeroportuarios Asia-Pacífico	*L5*	*Muy Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6	Media	2,833	4,267	3,73	Bajo	Medio-Bajo	Bajo
Servicios Aeroportuarios EMEA	*L6*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6	Media	2,833	4,267	3,73	Bajo	Medio-Bajo	Bajo
Servicios Aeroportuarios América Norte	*L7*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6	Media	2,833	4,267	3,73	Bajo	Medio-Bajo	Bajo
Servicios Aeroportuarios América Sur	*L8*	*Alto*	*5*	*8*	*8*	85%	80%	70%	4,25	6,4	5,6	Media	2,833	4,267	3,73	Bajo	Medio-Bajo	Bajo

Aeronaves	*L9*	*Muy Alto*	*9*	*10*	*10*	85%	80%	70%	7,65	8	7	Media	5,1	5,333	4,67	Medio-Bajo	Medio-Bajo	Medio-Bajo
Código Fuente GoOne	*D1*	*Muy Alto*	*10*	*10*	*9*	90%	95%	70%	9	9,5	6,3	Alta	9	9,5	6,3	Muy Alto	Muy Alto	Medio
Copias Respaldo GoOne	*D2*	*Muy Alto*	*9*	*9*	*9*	90%	95%	70%	8,1	8,55	6,3	Alta	8,1	8,55	6,3	Alto	Alto	Medio
Datos Financieros/Contables	*D3*	*Alto*	*9*	*10*	*8*	95%	95%	90%	8,55	9,5	7,2	Alta	8,55	9,5	7,2	Alto	Muy Alto	Medio-Alto
Datos Personal	*D4*	*Alto*	*9*	*5*	*2*	95%	95%	70%	8,55	4,75	1,4	Alta	8,55	4,75	1,4	Alto	Medio-Bajo	Bajo
Credenciales corporativos	*D5*	*Alto*	*9*	*6*	*9*	90%	95%	70%	8,1	5,7	6,3	Alta	8,1	5,7	6,3	Alto	Medio-Bajo	Medio
Credenciales AWS	*D6*	*Alto*	*9*	*6*	*9*	90%	95%	70%	8,1	5,7	6,3	Alta	8,1	5,7	6,3	Alto	Medio-Bajo	Medio
Datos en papel físico	*D7*	*Alto*	*7*	*2*	*0*	85%	80%	70%	5,95	1,6	0	Alta	5,95	1,6	0	Medio-Bajo	Bajo	Bajo
Claves sistemas en AWS	*K1*	*Muy Alto*	*9*	*9*	*9*	90%	95%	70%	8,1	8,55	6,3	Alta	8,1	8,55	6,3	Alto	Alto	Medio
Claves criptográficas servidores	*K2*	*Alto*	*8*	*6*	*9*	90%	95%	70%	7,2	5,7	6,3	Alta	7,2	5,7	6,3	Medio-Alto	Medio-Bajo	Medio
Claves criptográficas copias de respaldo	*K3*	*Alto*	*8*	*3*	*3*	90%	95%	70%	7,2	2,85	2,1	Alta	7,2	2,85	2,1	Medio-Alto	Bajo	Bajo
Sistemas guardado Backup	*Media 1*	*Alto*	*8*	*6*	*6*	90%	95%	70%	7,2	5,7	4,2	Alta	7,2	5,7	4,2	Medio-Alto	Medio-Bajo	Medio-Bajo
Dispositivos portátiles de almacenamiento	*Media 2*	*Alto*	*8*	*2*	*3*	90%	95%	70%	7,2	1,9	2,1	Alta	7,2	1,9	2,1	Medio-Alto	Bajo	Bajo

Equipamiento prevención incendios	*AUX1*	*Alto*	*2*	*9*	*8*	85%	80%	80%	1,7	7,2	6,4	Alta	1,7	7,2	6,4	Bajo	Medio -Alto	Medio
Equipamiento cableado	*AUX2*	*Alto*	*2*	*3*	*8*	85%	80%	80%	1,7	2,4	6,4	Alta	1,7	2,4	6,4	Bajo	Bajo	Medio
Equipamiento dispositivos a bordo para GoOne	*AUX3*	*Muy Alto*	*9*	*10*	*10*	85%	95%	95%	7,65	9,5	9,5	Alta	7,65	9,5	9,5	Medio -Alto	Muy Alto	Muy Alto
Impresoras	*AUX4*	*Bajo*	*2*	*0*	*0*	0%	0%	60%	0	0	0	Media	0	0	0	Bajo	Bajo	Bajo

Anexo X: Detalle controles post-proyectos

ISO/IEC 27001:

Capítulo	Requerimientos ISO 27001	Estado Pre-proyecto	Estado post-Proyecto
4	Contexto de la organización		
4,1	Comprensión de la organización y de su contexto	Optimized	Optimized
4,2	Comprensión de las necesidades y expectativas de las partes interesadas	Managed	Managed
4,3	Determinación del alcance del SGSI	Managed	Managed
4,4	SGSI	Developing	Managed
5	Liderazgo		
5,1	Liderazgo y compromiso	Managed	Managed
5,2	Política	Managed	Managed
5,3	Roles, responsabilidades y autoridades en la organización	Managed	Managed
6	Planificación		
6,1	Acciones para tratar los riesgos y oportunidades	Managed	Managed
6,2	Objetivos de seguridad de la información y planificación para su consecución	Managed	Managed
7	Soporte		
7,1	Recursos	Optimized	Optimized
7,2	Competencia	Managed	Managed
7,3	Concienciación	Managed	Managed
7,4	Comunicación	Managed	Managed
7,5	Información documentada	Optimized	Optimized

8	**Operación**		
8,1	**Planificación y control operacional**	Managed	Managed
8,2	**Apreciación de los riesgos de seguridad de la información**	Optimized	Optimized
8,3	**Tratamiento de los riesgos de seguridad de la información**	Optimized	Optimized
9	**Evaluación del desempeño**		
9,1	**Seguimiento, medición, análisis y evaluación**	Managed	Managed
9,2	**Auditoría interna**	Managed	Managed
9,3	**Revisión por la dirección**	Managed	Managed
10	**Mejora**		
10,1	**No conformidad y acciones correctivas**	Optimized	Optimized
10,2	**Mejora continua**	Optimized	Optimized

Anexo A:

Sección	Controles de Seguridad de la Información	Estado Pre-proyecto	Estado Post -proyecto
A6.1.1	Roles y responsabilidades en seguridad de la información	Developing	Managed
A6.1.2	Segregación de tareas	Developing	Managed
A6.1.3	Contacto con las autoridades	Managed	Optimized
A6.1.4	Contacto con grupos de interés especial	Managed	Optimized
A6.1.5	Seguridad de la información en la gestión de proyectos	Managed	Optimized
A6.2.1	Política de dispositivos móviles	Managed	Optimized
A6.2.2	Teletrabajo	Managed	Optimized
A8.1.1	Inventario de activos	Developing	Managed
A8.1.2	Propiedad de los activos	Developing	Managed

A8.1.3	Uso aceptable de los activos	Developing	Managed
A9.1.1	Política de control de acceso	Developing	Optimized
A9.1.2	Acceso a las redes y a los servicios de red	Developing	Optimized
A9.2.1	Registro y baja de usuario	Defined	Optimized
A9.2.2	Provisión de acceso de usuario	Defined	Optimized
A9.2.3	Gestión de privilegios de acceso	Defined	Optimized
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Managed	Optimized
A9.2.5	Revisión de los derechos de acceso de usuario	Managed	Optimized
A9.2.6	Retirada o reasignación de los derechos de acceso	Managed	Optimized
A9.3.1	Uso de la información secreta de autenticación	Managed	Optimized
A9.4.1	Restricción del acceso a la información	Defined	Managed
A9.4.2	Procedimientos seguros de inicio de sesión	Defined	Managed
A9.4.4	Uso de utilidades con privilegios del sistema	Defined	Managed
A9.4.5	Control de acceso al código fuente de los programas	Defined	Managed
A10.1.1	Política de uso de los controles criptográficos	Developing	Defined
A10.1.2	Gestión de claves	Developing	Defined
A12.1.1	Documentación de procedimientos operacionales	Developing	Managed
A12.1.2	Gestión de cambios	Managed	Managed
A12.1.3	Gestión de capacidades	Initial	Managed
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Developing	Managed
A12.2.1	Controles contra el código malicioso	Managed	Optimized
A12.4.1	Registro de eventos	Developing	Defined
A12.4.2	Protección de la información del registro	Developing	Defined
A12.4.3	Registros de administración y operación	Developing	Defined
A12.4.4	Sincronización del reloj	Managed	Optimized
A12.5.1	Instalación del software en explotación	Managed	Optimized

A12.6.1	Gestión de las vulnerabilidades técnicas	Managed	Optimized
A12.6.2	Restricción en la instalación de software	Managed	Optimized
A13.2.1	Políticas y procedimientos de intercambio de información	Managed	Optimized
A13.2.2	Acuerdos de intercambio de información	Managed	Optimized
A13.2.3	Mensajería electrónica	Managed	Optimized
A13.2.4	Acuerdos de confidencialidad o no revelación	Managed	Optimized
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Developing	Defined
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Developing	Defined
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Developing	Defined
A14.2.1	Política de desarrollo seguro	Developing	Managed
A14.2.2	Procedimiento de control de cambios en sistemas	Developing	Managed
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Developing	Managed
A14.2.4	Restricciones a los cambios en los paquetes de software	Developing	Managed
A14.2.5	Principios de ingeniería de sistemas seguros	Developing	Managed
A14.2.6	Entorno de desarrollo seguro	Developing	Managed
A14.2.7	Externalización del desarrollo de software	Developing	Managed
A14.2.8	Pruebas funcionales de seguridad de sistemas	Developing	Managed
A14.2.9	Pruebas de aceptación de sistemas	Developing	Managed
A14.3.1	Protección de los datos de prueba	Developing	Managed
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Managed	Optimized
A15.1.2	Requisitos de seguridad en contratos con terceros	Managed	Optimized
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Managed	Optimized
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Developing	Managed
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Developing	Managed
A16.1.1	Responsabilidades y procedimientos	Defined	Managed
A16.1.2	Notificación de los eventos de seguridad de la información	Defined	Managed

A16.1.3	Notificación de puntos débiles de la seguridad	Defined	Managed
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Defined	Managed
A16.1.5	Respuesta a incidentes de seguridad de la información	Defined	Managed
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Defined	Managed
A16.1.7	Recopilación de evidencias	Defined	Managed
A17.1.1	Planificación de la continuidad de la seguridad de la información	Managed	Optimized
A17.1.2	Implementar la continuidad de la seguridad de la información	Managed	Optimized
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Managed	Optimized
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Managed	Optimized
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Developing	Managed
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Developing	Managed
A18.1.3	Protección de los registros de la organización	Developing	Managed
A18.1.4	Protección y privacidad de la información de carácter personal	Developing	Managed
A18.1.5	Regulación de los controles criptográficos	Developing	Managed
A18.2.1	Revisión independiente de la seguridad de la información	Managed	Optimized
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Managed	Optimized
A18.2.3	Comprobación del cumplimiento técnico	Managed	Optimized

Anexo XI: Informe Ejecutivo Auditoría Interna

Informe de Auditoria	
1. Información sobre la auditoria	
Referencia auditoria	Auditoría Interna sobre el Sistema de Gestión de Seguridad de la Información de GoOne
Norma/s usadas	ISO/IEC 27001:2013 ISO/IEC 27002:2013 ISO/IEC 27017:2015
Fecha auditoria	may-22
Lugar auditoría	Sede corporativa
2. Objetivo	
El objetivo de la presente auditoría interna pretende analizar y determinar el estado y nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información del sistema corporativo GoOne con la norma ISO/IEC 27001:2013.	
3. Alcance	
Esta auditoría se centra en GoOne y todos los sistemas que intervienen en sus procesos operativos y técnicos y que deben asegurar la seguridad de la información. La evaluación se realiza sobre todos los dominios y controles de las normas mencionadas.	
4. Equipo Auditor	**5. Invitados**
Auditor Líder	Responsable GoOne
Auditor oficina del CISO	Responsable desarrollo GoOne
Auditor área transformación IT aerolínea Cargo	Responsable seguridad GoOne
Auditor área auditoría interna Servicios Globales	
6. Debilidades	**7. Puntos Fuertes**

Control sobre la seguridad de la información en la nube tiene un nivel de madurez aceptable, pero se recomienda elevarlo de manera que se optimice el control sobre esta seguridad.	Los controles del SGSI cuya ejecución recae sobre procesos corporativos, cuentan con un nivel de madurez y optimización muy positivo, en parte gracias a la experiencia de la organización en el marco del SGSI.
La implementación de controles de seguridad de red en el ámbito de la nube cuenta con una implementación básica proporcionada por el proveedor, lo cual puede derivar en que estos no se adapten a las necesidades de GoOne.	La reciente implementación e integración de ciertos sistemas de GoOne con los servicios generales de la compañía, se ha comprobado que ha repercutido muy positivamente en el estado de control sobre la seguridad de la información.

8. Resultados ISO/IEC 27001:2013	
Oportunidades de mejora: 7	**No conformidades: 0**

Oportunidades de mejora

ID	Proceso/función	Descripción	Responsable	Auditor
4.3	Determinación del alcance del SGSI	El alcance del SGSI está definido de manera adecuada, sin embargo, se recomienda implementar medidas de ajuste periódicas que facilitarán su adaptación acorde al dinamismo y volatilidad de los activos y recursos en la nube.	Responsable GoOne	Auditor Oficina del CISO
5.1	Liderazgo y compromiso	Si bien el SGSI asegura el liderazgo y compromiso, dentro de estas atribuciones se aconseja optimizar los procesos de mejora continua para el SGSI de GoOne de manera que apalanquen en los ya exitosos procesos equivalentes de mejora en la compañía.	Responsable GoOne	Auditor Oficina del CISO
6.2	Objetivos de seguridad de la información y planificación para su consecución	Se ha observado que, si bien existe un proceso de evaluación de riesgos para la seguridad de la información, se aconseja que estas se optimicen de manera que sigan un patrón de frecuencia, consistencia y con resultados comparables.	Responsable GoOne	Auditor Oficina del CISO

7.2	Competencia	Se aconseja llevar a cabo campañas de recapacitación y de análisis del estado de la misma, con el fin de poder medir el estado y poder aplicar medidas correctivas de manera temprana.	Responsable GoOne	Auditor Oficina del CISO
8.1	Planificación y control operacional	Se ha observado que, si bien existe un proceso de evaluación de riesgos para la seguridad de la información, se aconseja que estas se optimicen de manera que sigan un patrón de frecuencia, consistencia y con resultados comparables.	Responsable GoOne	Auditor Oficina del CISO
9.1	Seguimiento. medición. análisis y evaluación	Se ha comprobado que se realizan seguimientos y mediciones sobre los indicadores de auditoría de manera periódica, se aconseja optimizar el proceso mediante la implantación del SGSI en la herramienta de gobierno corporativa.	Responsable GoOne	Auditor Oficina del CISO
9.2	Auditoría interna	El ejercicio de auditoría ha tenido lugar y se aconseja que se optimice el proceso de planificación anual y especialmente el proceso de reporte y mantenimiento a través de los procesos estándares que se siguen en la compañía para su SGSI.	Responsable GoOne	Auditor Oficina del CISO

8. Resultados ISO/IEC 27002:2013 e ISO/IEC 27017:2015	
Oportunidades de mejora: 54	**No conformidades: 10**

Oportunidades de mejora

ID	Proceso/función	Descripción	Responsable	Auditor
A5.1.1	Políticas para la seguridad de la información	Se ha observado que la política de seguridad en la nube se ha definido e implementado correctamente, pero se aconseja realizar labores de concienciación y conocimiento periódicos.	Responsable GoOne	Auditor Oficina del CISO
A6.1.1	Roles y responsabilidades en seguridad de la información	Si bien se ha llevado a cabo una definición reciente de los roles y responsabilidades para la información en la nube, se recomienda que estos se revisiten de manera periódica respecto al modelo de responsabilidad compartida con el proveedor de cloud.	Responsable GoOne	Auditor Oficina del CISO

A6.1.2	Segregación de tareas	Se ha observado que existe una segregación de tareas en GoOne y que se encuentra definida. Se aconseja que se contraste esta segregación de tareas respecto al modelo de responsabilidad compartida y que se comunique de manera periódica.	Responsable GoOne	Auditor Oficina del CISO
A8.1.1	Inventario de activos	Se ha observado que tras la implementación del reciente proyecto de integración de los activos de la nube en la CMDB corporativa los activos de la nube se encuentran correctamente inventariados en dicha CMDB. Se recomienda establecer un sistema automático de barrido, creación y comprobación de activos para GoOne.	Responsable GoOne	Auditor Oficina del CISO
A8.1.2	Propiedad de los activos	Se ha observado que tras la implementación del reciente proyecto de integración de los activos de la nube en la CMDB corporativa los activos de la nube se encuentran correctamente inventariados en dicha CMDB. Se recomienda establecer un sistema automático de barrido, creación y comprobación de activos para GoOne.	Responsable GoOne	Auditor Oficina del CISO
A8.1.3	Uso aceptable de los activos	Se ha observado que tras la implementación del reciente proyecto de integración de los activos de la nube en la CMDB corporativa los activos de la nube se encuentran correctamente inventariados en dicha CMDB. Se recomienda establecer un sistema automático de barrido, creación y comprobación de activos para GoOne.	Responsable GoOne	Auditor Oficina del CISO
A9.4.1	Restricción del acceso a la información	Se ha observado que dentro de los roles definidos se detalla el tipo de información al que se tiene acceso, así como las funcionalidades disponibles según la clasificación de la información. Esto ha quedado integrado en el sistema de gestión de identidades recientemente implantado si bien se aconseja revisar los roles y el acceso a la información en la nube de manera periódica y automática.	Responsable seguridad GoOne	Auditor Oficina del CISO
A9.4.3	Sistema de gestión de contraseñas	Se ha observado que existe un sistema de gestión de contraseñas seguras integrado en el sistema de gestión de accesos e identidades para usuarios personales y compartidos. Se aconseja que este sistema chequee de manera automática las rotaciones de contraseñas con el fin de detectar contraseñas antiguas y/o débiles.	Responsable seguridad GoOne	Auditor Oficina del CISO

A9.4.4	Uso de utilidades con privilegios del sistema	Se ha comprobado que existe una definición de los roles definidos las funcionalidades disponibles para los tipos de usuarios, así como los procesos permitidos dentro de la nube. Además, se ha comprobado que existe un proceso de aprobación para acciones privilegiadas. Se recomienda que para que este proceso sea óptimo se automatice el proceso de aprobación junto con un proceso de monitorización y chequeo de las acciones privilegiadas.	Responsable seguridad GoOne	Auditor Oficina del CISO
A9.4.5	Control de acceso al código fuente de los programas	Se ha verificado que el código fuente se encuentra en el repositorio de la herramienta destinada a desarrollo y que el acceso se realiza a través del sistema de gestión de identidades y accesos. Se aconseja implementar un sistema de alertas de acceso y/o modificaciones del código fuente.	Responsable desarrollo GoOne	Auditor Oficina del CISO
A11.1.1	Perímetro de seguridad física	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las oficinas de la organización están protegidas por cámaras de seguridad y sistemas de detección de presencia.	Responsable GoOne	Auditor Líder
A11.1.2	Controles físicos de entrada	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. El acceso a las oficinas de realiza a través de un torno con una tarjeta identificativa. En caso de visitantes siempre acceden acompañados con un empleado previo registro en la entrada del edificio. Se recomienda optimizar el sistema de registro de visitantes con el fin de que este se automatice.	Responsable GoOne	Auditor Líder
A11.1.3	Seguridad de oficinas, despachos y recursos	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. El acceso a las oficinas de realiza a través de un torno con una tarjeta identificativa. En caso de visitantes siempre acceden acompañados con un empleado previo registro en la entrada del edificio. Se recomienda optimizar el sistema de registro de visitantes con el fin de que este se automatice.	Responsable GoOne	Auditor Líder

A11.1.4	Protección contra las amenazas externas y ambientales	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las instalaciones se encuentran protegidas con sistemas de detección y prevención de incendios, fuga de gas o fallo eléctrico, entre otros.	Responsable GoOne	Auditor Líder
A11.1.5	El trabajo en áreas seguras	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Existen una serie de medidas de seguridad adicionales para las zonas de trabajo en las que existe información física confidencial.	Responsable GoOne	Auditor Líder
A11.1.6	Áreas de carga y descarga	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las zonas de carga y descarga solo se encuentran en el centro de datos, que no da soporte a GoOne.	Responsable GoOne	Auditor Líder
A11.2.1	Emplazamiento y protección de equipos	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella.	Responsable GoOne	Auditor Líder
A11.2.2	Instalaciones de suministro		Responsable GoOne	Auditor Líder
A11.2.3	Seguridad del cableado		Responsable GoOne	Auditor Líder
A11.2.4	Mantenimiento de los equipos		Responsable GoOne	Auditor Líder
A11.2.5	Retirada de materiales propiedad de la empresa		Responsable GoOne	Auditor Líder
A11.2.6	Seguridad de los equipos fuera de las instalaciones		Responsable GoOne	Auditor Líder
A11.2.7	Reutilización o eliminación segura de equipos		Responsable GoOne	Auditor Líder

A11.2.8	Equipo de usuario desatendido		Responsable GoOne	Auditor Líder
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia		Responsable GoOne	Auditor Líder
A12.1.1	Documentación de procedimientos operacionales	Se ha comprobado que existe un proceso operacional recientemente definido para GoOne que el equipo ya pone en práctica. Se aconseja llevar a cabo una monitorización de los objetivos definidos en dicho documento.	Responsable GoOne	Auditor área auditoría interna Servicios Globales
A12.1.2	Gestión de cambios	Se ha comprobado que el equipo de GoOne sigue un procedimiento formal de gestión de cambios. Se recomienda realizar un ejercicio de revisión de cambios periódica para analizar posibles acciones de mejora.	Responsable GoOne	Auditor área auditoría interna Servicios Globales
A12.1.3	Gestión de capacidades	Como parte de los controles implementados en el entorno de GoOne, se ha observado que se monitorizan las capacidades mediante un procedimiento periódico. Se recomienda, optimizar este procedimiento con el fin de poder realizarlo de manera automática a tiempo real.	Responsable GoOne	Auditor área auditoría interna Servicios Globales
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Se ha verificado que existe un entorno de pruebas y otro de operación. Adicionalmente, se ha verificado que existe entorno de desarrollo separado del de pruebas y que los cambios de entornos se aprueban por dos roles definidos.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A12.3.1	Copias de seguridad de la información	Se ha verificado que existe un proceso de realización de copias de seguridad en la nube que se realiza de manera periódica. Se recomienda que los resultados de dicho procedimiento se monitoricen para detectar posibles fallos de manera automática.	Responsable seguridad GoOne	Auditor área auditoría interna Servicios Globales

A14.2.1	Política de desarrollo seguro	Se ha verificado que GoOne tiene una política de desarrollo seguro implantada hace unos meses y que opera de manera adecuada. Se aconseja revisar esta política de manera periódica.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.2	Procedimiento de control de cambios en sistemas	Se ha comprobado que los cambios en el sistema exigen un análisis de impacto previo a su autorización e implementación. Se recomienda analizar aquellos patrones de cambios cuya aprobación puede ser automatizada para permitir mayor agilidad.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Se ha verificado que los cambios requieren un plan de vuelta atrás para poder ser aprobados. Adicionalmente, se ha comprobado que las copias de respaldo permiten este procedimiento.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.4	Restricciones a los cambios en los paquetes de software	Si bien se ha verificado que las normas para la restricción a los cambios en paquetes de software han sido definidas y se usan, se recomienda revisarlas de manera periódica por los responsables de las áreas aplicables.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.5	Principios de ingeniería de sistemas seguros	Se ha comprobado que GoOne sigue los principios de ingeniera corporativos para arquitectura en la nube y de desarrollo seguro.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.6	Entorno de desarrollo seguro	Se ha verificado que GoOne tiene una política de desarrollo seguro implantada hace unos meses y que opera de manera adecuada. Se aconseja revisar esta política de manera periódica.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales

A14.2.7	Externalización del desarrollo de software	Se ha verificado que el servicio gestionado que participa en el equipo de GoOne sigue los procedimientos corporativos para el desarrollo. Se recomienda asegurar la correcta documentación y formación para los nuevos miembros del servicio gestionado.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.8	Pruebas funcionales de seguridad de sistemas	Se ha comprobado que existe un proceso de verificación de requisitos funcionales para GoOne. Se recomienda, en la medida de lo posible, aplicar métodos de automatización que permitan realizar el proceso de manera ágil.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.2.9	Pruebas de aceptación de sistemas	Se ha comprobado que existe un proceso de pruebas de aceptación para GoOne. Se recomienda, en la medida de lo posible, aplicar métodos de automatización que permitan realizar el proceso de manera ágil.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A14.3.1	Protección de los datos de prueba	Se ha verificado que existe un proceso de protección estándar para los datos de prueba seleccionados, se recomienda revisitar este proceso para el entorno de nube y aplicar posibles mejoras sobre el mismo.	Responsable desarrollo GoOne	Auditor área auditoría interna Servicios Globales
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Se ha verificado que existe un proceso gestionado de proveedor de servicios con AWS con el que se verifica y revisa de manera periódica el servicio proporcionado. Se recomienda que el proceso se optimice con el fin de evolucionar las revisiones.	Responsable desarrollo GoOne	Auditor área transformación IT aerolínea Cargo
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Se ha verificado que existe un proceso gestionado de proveedor de servicios con AWS con el que se verifica y revisa de manera periódica el servicio proporcionado identificando los cambios con antelación, verificando posibles acciones en el lado de GoOne y gestionando las comunicaciones con el proveedor durante el proceso.	Responsable desarrollo GoOne	Auditor área transformación IT aerolínea Cargo

A16.1.1	Responsabilidades y procedimientos	Se ha comprobado que GoOne cuenta con un procedimiento de gestión de incidentes basado en el modelo de responsabilidad compartida.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.2	Notificación de los eventos de seguridad de la información	Se ha verificado que existe dentro del proceso mencionado un listado de contactos y notificaciones en caso de incidentes de seguridad. Se recomienda, que este listado se revise de manera periódica.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.3	Notificación de puntos débiles de la seguridad	Se ha comprobado que el procedimiento de monitorización de puntos débiles se opera de manera adecuada, si bien se aconseja que se adopten medidas telemáticas que faciliten la comunicación y escalación.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Se ha comprobado que el procedimiento de gestión de eventos cuenta con una guía para el análisis y decisión respecto a las acciones a tomar. Se aconseja involucrar medidas de automatización que permitan apoyar la toma de decisiones ágil.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.5	Respuesta a incidentes de seguridad de la información	Se ha verificado que, para los incidentes de seguridad revisados, se realizó una correcta aplicación del proceso de respuesta de incidentes.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se ha verificado que, para los incidentes de seguridad revisados, se realizó un ejercicio posterior de aprendizaje si bien se aconseja, que este ejercicio se realice con todas las partes interesadas.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo
A16.1.7	Recopilación de evidencias	Se ha comprobado que el procedimiento de gestión de incidentes establece las medidas y evidencias a tomar dentro de cada paso requerido.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo

A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se ha comprobado que se realiza una revisión de las regulaciones aplicables para GoOne. Se recomienda que esta revisión se apoye en las organizaciones locales con el fin de asegurar que se capturan los requisitos a nivel local.	Responsable GoOne	Auditor área transformación IT aerolínea Cargo
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Se ha verificado que existe un departamento especializado en auditar las licencias de software de servicios globales, incluyendo GoOne, para el que se ha comprobado la auditoría cubrió las licencias en el entorno de la nube. Se recomienda monitorizar las licencias en el entorno de la nube de manera periódica para no incurrir en sobrecostes.	Responsable GoOne	Auditor área transformación IT aerolínea Cargo
A18.1.3	Protección de los registros de la organización	Se ha verificado que este control se audita de manera periódica tanto en la organización como en el proveedor de servicios en la Nube.	Responsable GoOne	Auditor área transformación IT aerolínea Cargo
A18.1.4	Protección y privacidad de la información de carácter personal	Se ha verificado que el dueño de los datos contenidos en GoOne, revisa dentro de sus tareas de manera periódica el cumplimiento de las leyes de protección de datos aplicables.	Responsable GoOne	Auditor área transformación IT aerolínea Cargo
A18.1.5	Regulación de los controles criptográficos	Se ha comprobado que los dispositivos de cifrado de la organización son auditados de manera anual dentro de la auditoría del SGSI corporativo.	Responsable seguridad GoOne	Auditor área transformación IT aerolínea Cargo

No Conformidades Menores				
ID	Proceso/función	Descripción	Responsable	Auditor

A9.4.2	Procedimientos seguros de inicio de sesión	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.	Responsable seguridad GoOne	Auditor Oficina del CISO
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.	Responsable seguridad GoOne	Auditor Oficina del CISO
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.	Responsable seguridad GoOne	Auditor Oficina del CISO
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.	Responsable seguridad GoOne	Auditor Líder
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.	Responsable seguridad GoOne	Auditor Líder
A12.4.3	Registros de administración y operación		Responsable seguridad GoOne	Auditor Líder
A13.1.1	Controles de red	Se ha identificado que existe una configuración de controles de red, pero no se alinea con los controles definidos por las políticas de seguridad.	Responsable seguridad GoOne	Auditor área auditoría interna Servicios Globales
A13.1.2	Seguridad de los servicios 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.	Responsable seguridad GoOne	Auditor área auditoría interna

				Servicios Globales
A13.1.3	Segregación en redes	Se ha verificado que el equipo de GoOne ha establecido una segregación de redes, pero esta no se ajusta a un proceso formal documentado.	Responsable seguridad GoOne	Auditor área auditoría interna Servicios Globales
No Conformidades Mayores				
ID	Proceso/función	Descripción	Responsable	Auditor
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.	Responsable GoOne	Auditor Oficina del CISO

9. 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.

Anexo XII: Detalle Resultados Auditoría

Resultados ISO/IEC 27001:2013

Capítulo	Requerimientos ISO 27001	Valoración	Efectividad	CMM	Observaciones
4	**Contexto de la organización**		**99%**		
4.1	**Comprensión de la organización y de su contexto**	Optimizado	100%	L5	
4.2	**Comprensión de las necesidades y expectativas de las partes interesadas**	Optimizado	100%	L5	
4.3	**Determinación del alcance del SGSI**	Gestionado y Medible	95%	L4	El alcance del SGSI esta definido de manera adecuada, sin embargo, se recomienda implementar medidas de ajuste periódicas que facilitarán su adaptación acorde al dinamismo y volatilidad de los activos y recursos en la nube.
4.4	**SGSI**	Optimizado	100%	L5	
5	**Liderazgo**		**98%**		
5.1	**Liderazgo y compromiso**	Gestionado y Medible	95%	L4	Si bien el SGSI asegura el liderazgo y compromiso, dentro de estas atribuciones se aconseja optimizar los procesos de mejora continua para el SGSI de GoOne de manera que apalanquen en los ya existosos procesos equivalentes de mejora en la compañía.
5.2	**Política**	Optimizado	100%	L5	
5.3	**Roles. responsabilidades y autoridades en la organización**	Optimizado	100%	L5	
6	**Planificación**		**98%**		
6.1	**Acciones para tratar los riesgos y oportunidades**	Optimizado	100%	L5	
6.2	**Objetivos de seguridad de la información y planificación para su consecución**	Gestionado y Medible	95%	L4	Se ha observado que si bien existe un proceso de evaluación de riesgos para la seguridad de la información, se aconseja que estas se optimicen de manera que sigan un patrón de frecuencia, consistencia y con resultados comparables.

7	**Soporte**		**99%**		
7.1	**Recursos**	Optimizado	100%	L5	
7.2	**Competencia**	Gestionado y Medible	95%	L4	Se aconseja llevar a cabo campañas de recapacitación y de análsis del estado de la misma, con el fin de poder medir el estado y poder aplicar medidas correctivas de manera temprana.
7.3	**Concienciación**	Optimizado	100%	L5	
7.4	**Comunicación**	Optimizado	100%	L5	
7.5	**Información documentada**	Optimizado	100%	L5	
8	**Operación**		**98%**		
8.1	**Planificación y control operacional**	Gestionado y Medible	95%	L4	Se ha observado que si bien existe un proceso de evaluación de riesgos para la seguridad de la información, se aconseja que estas se optimicen de manera que sigan un patrón de frecuencia, consistencia y con resultados comparables.
8.2	**Apreciación de los riesgos de seguridad de la información**	Optimizado	100%	L5	
8.3	**Tratamiento de los riesgos de seguridad de la información**	Optimizado	100%	L5	
9	**Evaluación del desempeño**		**95%**		
9.1	**Seguimiento. medición. análisis y evaluación**	Gestionado y Medible	95%	L4	Se ha comprobado que se realizan seguimientos y mediciones sobre los indicadores de auditoría de manera periódica, se aconseja optimizar el proceso mediante la implentación del SGSI en la herramienta de gobierno corporativa.
9.2	**Auditoría interna**	Gestionado y Medible	95%	L4	El ejercicio de auditoría ha tenido lugar y se aconseja que se optimice el proceso de planificación anual y especialmente el proceso de reporte y mantenimiento a través de los procesos estándares que se siguen en la compañía para su SGSI.
9.3	**Revisión por la dirección**	No aplica			No ha podido valorarse pues el presente documento constituye la primera revisión por lo que habrá de evaluarse en el futuro.
10	**Mejora**		**100%**		
10.1	**No conformidad y acciones correctivas**	Optimizado	100%	L5	
10.2	**Mejora continua**	Optimizado	100%	L5	

Resultado ISO/IEC 27002 y ISO/IEC 27017

Sección	Controles de Seguridad de la Información	Valoración	Efectividad	CMM	Observaciones
A5	**Políticas de seguridad de la información**		**50%**		
A5.1	**Directrices de gestión de la seguridad de la información**		**50%**		
A5.1.1	Políticas para la seguridad de la información	Gestionado y Medible	90%	L4	Se ha observado que la política de seguridad en la nube se ha definido e implamantado correctamente pero se aconseja realizar labores de concienciación y conocimiento periódicos.
A5.1.2	Revisión de las políticas para la seguridad de la información	Inicial/Ad-hoc	10%	L1	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.
A6	**Organización de la seguridad de la información**		**99%**		
A6.1	**Organización interna**		**99%**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Gestionado y Medible	95%	L4	Si bien se ha llevado a cabo una definición reciente de los roles y responsabilidades para la información en la nube, se recomienda que estos se revisiten de manera periódica respecto al modelo de responsabilidad compartida con el proveedor de cloud.
A6.1.2	Segregación de tareas	Gestionado y Medible	95%	L4	Se ha observado que existe una segregación de tareas en GoOne y que se encuentra definida. Se aconseja que se contraste esta segregación de tareas respecto al modelo de responsabilidad compartida y que se comunique de manera periócia.
A6.1.3	Contacto con las autoridades	Optimizado	100%	L5	
A6.1.4	Contacto con grupos de interés especial	Optimizado	100%	L5	
A6.1.5	Seguridad de la información en la gestión de proyectos	Optimizado	100%	L5	
A6.2	**Los dispositivos móviles y el teletrabajo**		**100%**		
A6.2.1	Política de dispositivos móviles	Optimizado	100%	L5	
A6.2.2	Teletrabajo	Optimizado	100%	L5	
A7	**Seguridad relativa a los recursos humanos**		**75%**		
A7.1	**Antes del empleo**		**100%**		
A7.1.1	Investigación de antecedentes	Optimizado	100%	L5	
A7.1.2	Términos y condiciones del empleo	Optimizado	100%	L5	
A7.2	**Durante el empleo**		**100%**		
A7.2.1	Responsabilidades de gestión	Optimizado	100%	L5	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Optimizado	100%	L5	
A7.2.3	Proceso disciplinario	Optimizado	100%	L5	
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		**100%**		
A7.3.1	Responsabilidades ante la finalización o cambio	Optimizado	100%	L5	

A8	**Gestión de activos**		**99%**		
A8.1	**Responsabilidad sobre los activos**		**96%**		
A8.1.1	Inventario de activos	Gestionado y Medible	95%	L4	Se ha observado que tras la implementación del reciente proyecto de integración de los activos de la nube en la CMDB corporativa los activos de la nube se encuentran correctamente inventariados en dicha CMDB. Se recomienda establecer un sistema automático de barrido, creación y comprobación de activos para GoOne.
A8.1.2	Propiedad de los activos	Gestionado y Medible	95%	L4	
A8.1.3	Uso aceptable de los activos	Gestionado y Medible	95%	L4	
A8.1.4	Devolución de activos	Optimizado	100%	L5	
A8.2	**Clasificación de la información**		**100%**		
A8.2.1	Clasificación de la información	Optimizado	100%	L5	
A8.2.2	Etiquetado de la información	Optimizado	100%	L5	
A8.2.3	Manipulado de la información	Optimizado	100%	L5	
A8.3	**Manipulación de los soportes**		**100%**		
A8.3.1	Gestión de soportes extraíbles	Optimizado	100%	L5	
A8.3.2	Eliminación de soportes	Optimizado	100%	L5	
A8.3.3	Soportes físicos en tránsito	Optimizado	100%	L5	
A9	**Control de acceso**		**99%**		
A9.1	**Requisitos de negocio para el control de acceso**		**100%**		
A9.1.1	Política de control de acceso	Optimizado	100%	L5	
A9.1.2	Acceso a las redes y a los servicios de red	Optimizado	100%	L5	
A9.2	**Gestión de acceso de usuario**		**100%**		
A9.2.1	Registro y baja de usuario	Optimizado	100%	L5	
A9.2.2	Provisión de acceso de usuario	Optimizado	100%	L5	
A9.2.3	Gestión de privilegios de acceso	Optimizado	100%	L5	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Optimizado	100%	L5	
A9.2.5	Revisión de los derechos de acceso de usuario	Optimizado	100%	L5	
A9.2.6	Retirada o reasignación de los derechos de acceso	Optimizado	100%	L5	
A9.3	**Responsabilidades del usuario**		**100%**		
A9.3.1	Uso de la información secreta de autenticación	Optimizado	100%	L5	

A9.4	**Control de acceso a sistemas y aplicaciones**		**94%**		
A9.4.1	Restricción del acceso a la información	Gestionado y Medible	95%	L4	Se ha observado que dentro de los roles definidos se detalla el tipo de información al que se tiene acceso, así como las funcionalidades disponibles según la clasificación de la información. Esto ha quedado integrado en el sistema de gestión de identidades recientemente implantado si bien se aconseja revisar los roles y el acceso a la información en la nube de manera periódica y automática.
A9.4.2	Procedimientos seguros de inicio de sesión	Proceso Definido	90%	L3	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.
A9.4.3	Sistema de gestión de contraseñas	Gestionado y Medible	95%	L4	Se ha observado que existe un sistema de gestión de contraseñas seguras integrado en el sistema de gestión de accesos e identidades para usuarios personales y compartidos. Se aconseja que este sistema chequee de manera automática las rotaciones de contraseñas con el fin de detectar contraseñas antiguas y/o débiles.
A9.4.4	Uso de utilidades con privilegios del sistema	Gestionado y Medible	95%	L4	Se ha comprobado que existe uan definición de los roles definidos las funcionalidades disponibles para los tipos de usuarios, así como los procesos permitidos dentro de la nube. Además se ha comprobado que existe un proceso de aprobación para acciones privilegiadas. Se recomienda que para que este proceso sea óptimo se automatice el proceso de aprobación junto con un proceso de monitorización y chequeo de las acciones privilegiadas.
A9.4.5	Control de acceso al código fuente de los programas	Gestionado y Medible	95%	L4	Se ha verificado que el código fuente se encuentra en el repositorio de la herramienta destinadada a desarrollo y que el acceso se realiza a través del sistema de gestión de identidades y accesos. Se aconseja implementar un sistema de alertas de acceso y/o modificaciones del código fuente.
A10	**Criptografía**		**90%**		
A10.1	**Controles criptográficos**		**90%**		
A10.1.1	Política de uso de los controles criptográficos	Proceso Definido	90%	L3	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	Proceso Definido	90%	L3	Se ha comprobado que a consecuencia de encontrar limitaciones técnicas para la implementacion del control de claves en la nube no se esta gestionando de manera adecuada, si bien existe un plan para su corrección.

A11	**Seguridad física y del entorno**		**95%**		
A11.1	**Áreas seguras**		**95%**		
A11.1.1	Perímetro de seguridad física	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las oficinas de la organización están protegidas por cámaras de seguridad y sistemas de detección de presencia.
A11.1.2	Controles físicos de entrada	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. El acceso a las oficinas de realiza a través de un torno con una tarjeta identificativa. En caso de visitantes siempre acceden acompañados con un empleado previo registro en la entrada del edificio. Se recomienda optimizar el sistema de registro de visitantes con el fin de que este se automatice.
A11.1.3	Seguridad de oficinas, despachos y recursos	Gestionado y Medible	95%	L4	
A11.1.4	Protección contra las amenazas externas y ambientales	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las instalaciones se encuentran protegidas con sistemas de detección y prevención de incendios, fuga de gas o fallo eléctrico, entre otros.
A11.1.5	El trabajo en áreas seguras	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Existen una serie de medidas de seguridad adicionales para las zonas de trabajo en las que existe información física confidencial.
A11.1.6	Áreas de carga y descarga	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella. Las zonas de carga y descarga solo se encuentran en el centro de datos, que no da soporte a GoOne.
A11.2	**Seguridad de los equipos**		**95%**		
A11.2.1	Emplazamiento y protección de equipos	Gestionado y Medible	95%	L4	Se ha verificado que la organización se certifica anualmente con una auditoría ISO 27001 y el cloud provider también cuenta con ella.
A11.2.2	Instalaciones de suministro	Gestionado y Medible	95%	L4	
A11.2.3	Seguridad del cableado	Gestionado y Medible	95%	L4	
A11.2.4	Mantenimiento de los equipos	Gestionado y Medible	95%	L4	
A11.2.5	Retirada de materiales propiedad de la empresa	Gestionado y Medible	95%	L4	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Gestionado y Medible	95%	L4	
A11.2.7	Reutilización o eliminación segura de equipos	Gestionado y Medible	95%	L4	
A11.2.8	Equipo de usuario desatendido	Gestionado y Medible	95%	L4	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Gestionado y Medible	95%	L4	

A12	**Seguridad de las operaciones**		**98%**		
A12.1	**Procedimientos y responsabilidades operacionales**		**95%**		
A12.1.1	Documentación de procedimientos operacionales	Gestionado y Medible	95%	L4	Se ha comprobado que existe un proceso operacional recientemente definido para GoOne que el equipo ya pone en práctica. Se aconseja llevar a cabo una monitorización de los objetivos definidos en dicho documento.
A12.1.2	Gestión de cambios	Gestionado y Medible	95%	L4	Se ha comprobado que el equipo de GoOne sigue un procedimiento formal de gestión de cambios. Se recomienda realizar un ejercicio de revisión de cambios periódica para analizar posibles acciones de mejora.
A12.1.3	Gestión de capacidades	Gestionado y Medible	95%	L4	Como parte de los controles implementados en el entorno de GoOne, se ha observado que se monitorizan las capacidades mediante un procedimiento periódico. Se recomienda, optimizar este procedimiento con el fin de poder realizarlo de manera automática a tiempo real.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Gestionado y Medible	95%	L4	Se ha verificado que existe un entorno de pruebas y otro de operación. Adicionalmente, se ha verificado que existe entorno de desarrollo separado del de pruebas y que los cambios de entornos se aprueba por dos roles definidos.
A12.2	**Protección contra el software malicioso (malware)**		**100%**		
A12.2.1	Controles contra el código malicioso	Optimizado	100%	L5	
A12.3	**Copias de seguridad**		**95%**		
A12.3.1	Copias de seguridad de la información	Gestionado y Medible	95%	L4	Se ha verificado que existe un proceso de realización de copias de seguridad en la nube que se realiza de manera periódica. Se recomienda que los resultados de dicho procedimiento se monitoricen para detectar posibles fallos de manera automática.
A12.4	**Registros y supervisión**		**93%**		
A12.4.1	Registro de eventos	Proceso Definido	90%	L3	Se ha verificado que se ha definido recientemente el proceso de monitorización de registro de eventos pero esta pendiente de implementar.
A12.4.2	Protección de la información del registro	Proceso Definido	90%	L3	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	Proceso Definido	90%	L3	
A12.4.4	Sincronización del reloj	Optimizado	100%	L5	
A12.5	**Control del software en explotación**		**100%**		
A12.5.1	Instalación del software en explotación	Optimizado	100%	L5	
A12.6	**Gestión de la vulnerabilidad técnica**		**100%**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Optimizado	100%	L5	
A12.6.2	Restricción en la instalación de software	Optimizado	100%	L5	
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		**100%**		
A12.7.1	Controles de auditoría de sistemas de información	Optimizado	100%	L5	

A13	**Seguridad de las comunicaciones**		**75%**		
A13.1	**Gestión de la seguridad de las redes**		**50%**		
A13.1.1	Controles de red	Reproducible pero Intuitivo	50%	L2	Se ha identificado que existe una configuración de controles de red pero no se alinea con los controles definidos por las políticas de seguridad.
A13.1.2	Seguridad de los servicios de red	Reproducible pero Intuitivo	50%	L2	Se ha verificado que el equipo de GoOne esta 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.
A13.1.3	Segregación en redes	Reproducible pero Intuitivo	50%	L2	Se ha verificado que el equipo de GoOne ha establecido una segregación de redes pero esta no se ajusta a un proceso formal documentado.
A13.2	**Intercambio de información**		**100%**		
A13.2.1	Políticas y procedimientos de intercambio de información	Optimizado	100%	L5	
A13.2.2	Acuerdos de intercambio de información	Optimizado	100%	L5	
A13.2.3	Mensajería electrónica	Optimizado	100%	L5	
A13.2.4	Acuerdos de confidencialidad o no revelación	Optimizado	100%	L5	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		**97%**		
A14.1	**Requisitos de seguridad en los sistemas de información**		**100%**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Optimizado	100%	L5	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Optimizado	100%	L5	
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Optimizado	100%	L5	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		**95%**		
A14.2.1	Política de desarrollo seguro	Gestionado y Medible	95%	L4	Se ha verificado que GoOne tiene una política de desarrollo seguro implantada hace unos meses y que opera de manera adecuada. Se aconseja revisar esta política de manera periódica.
A14.2.2	Procedimiento de control de cambios en sistemas	Gestionado y Medible	95%	L4	Se ha comprobado que los cambios en el sistema exigen un análisis de impacto previo a su autorización e implementación. Se recomienda análiza aquellos patrones de cambios cuya aprobación puede ser automatizada para pemitir mayor agilidad.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Gestionado y Medible	95%	L4	Se ha verificado que los cambios requieren un plan de vuelta atrás para poder ser aprobados. Adicionalmente, se ha comprobado que las copias de respaldo permiten este procedimiento.
A14.2.4	Restricciones a los cambios en los paquetes de software	Gestionado y Medible	95%	L4	
A14.2.5	Principios de ingeniería de sistemas seguros	Gestionado y Medible	95%	L4	Se ha comprobado que GoOne sigue los principios de ingeniera corporativos para arquitectura en la nube y de desarrollo seguro.
A14.2.6	Entorno de desarrollo seguro	Gestionado y Medible	95%	L4	Se ha verificado que GoOne tiene una política de desarrollo seguro implantada hace unos meses y que opera de manera adecuada. Se aconseja revisar esta política de manera periódica.
A14.2.7	Externalización del desarrollo de software	Gestionado y Medible	95%	L4	Se ha verificado que el servicio gestionado que participa en el equipo de GoOne sigue los procedimientos corporativos para el desarrollo. Se recomienda asegurar la correcta documentación y formación para los nuevos miembros del servicio gestionado.
A14.2.8	Pruebas funcionales de seguridad de sistemas	Gestionado y Medible	95%	L4	Se ha comprobado que existe un proceso de verificación de requisitos funcionales para GoOne. Se recomienda, en la medida de lo posible, aplicar métodos de automatización que permitan realizar el proceso de manera ágil.
A14.2.9	Pruebas de aceptación de sistemas	Gestionado y Medible	95%	L4	Se ha comprobado que existe un proceso de pruebas de aceptación para GoOne. Se recomienda, en la medida de lo posible, aplicar métodos de automatización que permitan realizar el proceso de manera ágil.
A14.3	**Datos de prueba**		**95%**		
A14.3.1	Protección de los datos de prueba	Gestionado y Medible	95%	L4	

A15	**Relación con proveedores**		**98%**		
A15.1	**Seguridad en las relaciones con proveedores**		**100%**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Optimizado	100%	L5	
A15.1.2	Requisitos de seguridad en contratos con terceros	Optimizado	100%	L5	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Optimizado	100%	L5	
A15.2	**Gestión de la provisión de servicios del proveedor**		**95%**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Gestionado y Medible	95%	L4	Se ha verificado que existe un proceso gestionado de proveedor de servicios con AWS con el que se verifica y revisa de manera periódica el servicio proporcionado. Se recomienda que el proceso se optimice con el fin de evolucionar las revisiones.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Gestionado y Medible	95%	L4	Se ha verificado que existe un proceso gestionado de proveedor de servicios con AWS con el que se verifica y revisa de manera periódica el servicio proporcionado identificando los cambios con antelación, verificando posibles acciones en el lado de GoOne y gestionando las comunicaciones con el proveedor durante el proceso.
A16	**Gestión de incidentes de seguridad de la información**		**95%**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		**95%**		
A16.1.1	Responsabilidades y procedimientos	Gestionado y Medible	95%	L4	Se ha comprobado que GoOne cuenta con un procedimiento de gestión de incidentes basado en el modelo de responsabilidad compartida.
A16.1.2	Notificación de los eventos de seguridad de la información	Gestionado y Medible	95%	L4	Se ha verificado que existe dentro del proceso mencionado un listado de contactos y notificaciones en caso de incidentes de seguridad. Se recomienda, que este listado se revise de manera periódica.
A16.1.3	Notificación de puntos débiles de la seguridad	Gestionado y Medible	95%	L4	Se ha comprobado que el procedimiento de monitorización de puntos débiles se opera de manera adecuada, si bien se aconseja que se adopten medidas telemáticas que faciliten la comunicación y escalación.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Gestionado y Medible	95%	L4	Se ha comprobado que el procedimiento de gestión de eventos cuenta con una guía para el análisis y decisión respecto a las acciones a tomar. Se aconseja involucrar medidas de automatización que permitan apoyar la toma de decisiones ágil.
A16.1.5	Respuesta a incidentes de seguridad de la información	Gestionado y Medible	95%	L4	Se ha verificado que para los incidentes de seguridad revisados, se realizó una correcta aplicación del proceso de respuesta de incidentes.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Gestionado y Medible	95%	L4	Se ha verificado que para los incidentes de seguridad revisados, se realizó un ejercicio posterior de aprendizaje si bien se aconseja, que este ejercicio se realice con todas las partes interesadas.
A16.1.7	Recopilación de evidencias	Gestionado y Medible	95%	L4	Se ha comprobado que el procedimiento de gestión de incidentes, establece las medidas y evidencias a tomar dentro de cada paso requerido.

A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		**100%**		
A17.1	**Continuidad de la seguridad de la información**		**100%**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Optimizado	100%	L5	
A17.1.2	Implementar la continuidad de la seguridad de la información	Optimizado	100%	L5	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Optimizado	100%	L5	
A17.2	**Redundancias**		**100%**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Optimizado	100%	L5	
A18	**Cumplimiento**		**98%**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		**95%**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Gestionado y Medible	95%	L4	Se ha comprobado que se realiza una revisión de las regulaciones aplicables para GoOne. Se recomienda que esta revisión se apoye en las organizaciones locales con el fin de asegurar que se capturan los requsitos a nivel local.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Gestionado y Medible	95%	L4	Se ha verificado que existe un departamento especializado en auditar las licencias de software de servicios globales, incluyendo GoOne, para el que se ha comprobado la auditoría cubrió las licencias en el entorno de la nube. Se recomienda monitorizar las licencias en el entorno de la nube de manera periódica para no incurrir en sobrecostes.
A18.1.3	Protección de los registros de la organización	Gestionado y Medible	95%	L4	Se ha verificado que este control se audita de manera periódica tanto en la organización como en el proveedor de servicios en la Nube.
A18.1.4	Protección y privacidad de la información de carácter personal	Gestionado y Medible	95%	L4	Se ha verificado que el dueño de los datos contenidos en GoOne, revisa dentro de sus tareas de manera periódica el cumplimiento de las leyes de protección de datos aplicables.
A18.1.5	Regulación de los controles criptográficos	Gestionado y Medible	95%	L4	Se ha comprobado que los dispositivos de cifrado de la organización son auditados de manera anual dentro de la auditoría del SGSI corporativo.
A18.2	**Revisiones de la seguridad de la información**		**100%**		
A18.2.1	Revisión independiente de la seguridad de la información	Optimizado	100%	L5	
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Optimizado	100%	L5	
A18.2.3	Comprobación del cumplimiento técnico	Optimizado	100%	L5	