Master Universitario Ciberseguridad y Privacidad

Presentación del Proyecto

Elaboración de un Plan de Implementación para ISO/IEC 27001:2013

Elena Sánchez Hernández

Contenido

1. Introducción

La seguridad de la información

Comprende la práctica de proteger la información valiosa dentro de los sistemas de información que constituyen un activo con el fin de preservar la confidencialidad, integridad y disponibilidad.

Norma ISO/IEC 27001:2013

La norma ofrece un marco internacional para la gestión de la seguridad de la información mediante requerimientos para la definición, implementación, matenimiento y mejora continua del Sistema de Gestión de la Seguridad de la información (SGSI).

2. Hitos del proyecto

1. Situación Actual
2. Sistema de Gestión documental
3. Análisis de Riesgos
4. Propuestas de Proyectos
5. Auditoría de cumplimiento
6. Presentación de resultados

3. Contextualización

La Organización

Grupo operador aviación comercial y transporte aéreo: 650 aeronaves

Opera servicios aeroportuarios para otras aerolíneas

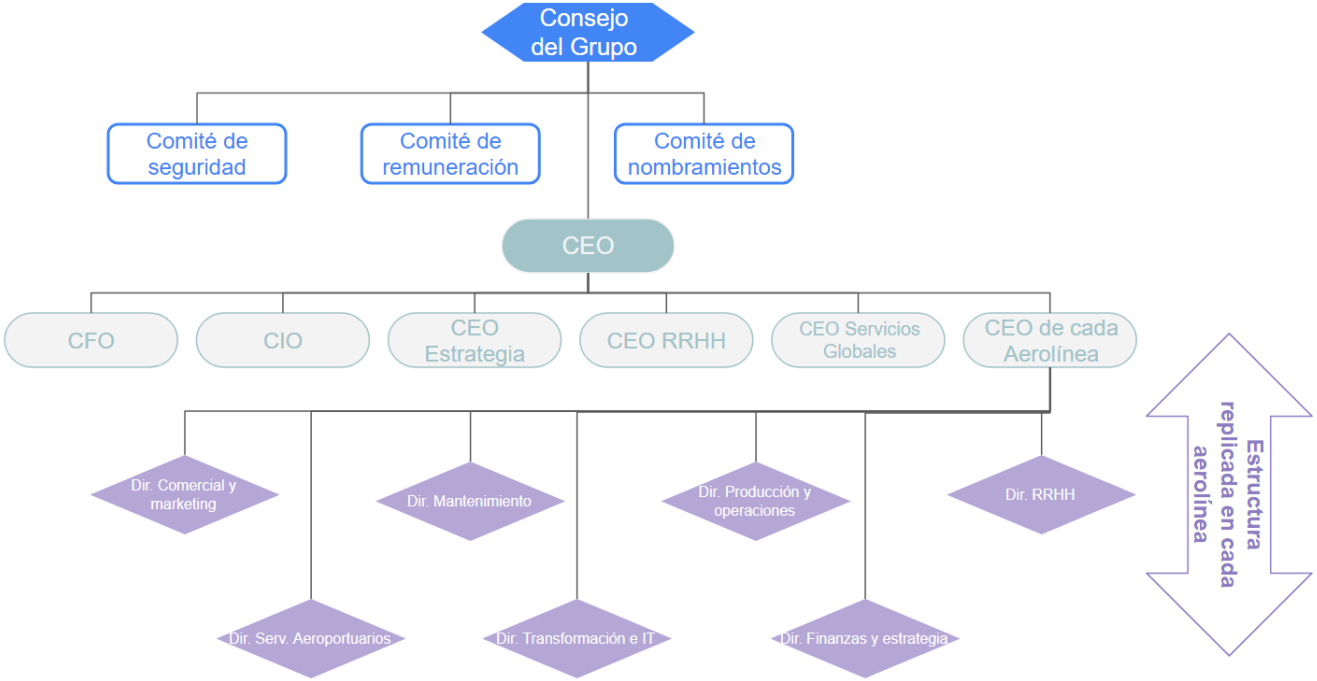
Volumen medio de pasajeros anuales 120.453.000. Ingresos anuales: 27m de Euros*

Opera en un total de 250 destinos

* Ingresos previos a la pandemia de la COVID

3. Contextualización

Organigrama Funcional



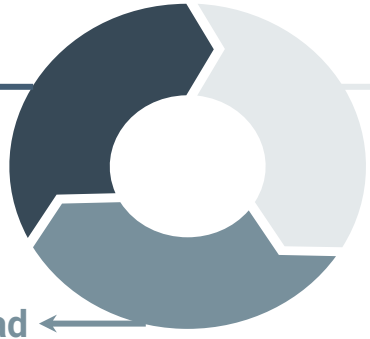
3. Contextualización

Proyecto GoOne

- **GoOne** surge como respuesta al mandato de integrar operaciones de todas las aerolíneas sobre un mismo sistema de manera que el proceso sea estándar para todas ellas y se asegure una alineación respecto a los principales objetivos estratégicos de la compañía.

- GoOne es el primer proyecto en nube pública dentro de la organización

Operaciones
Unificación proceso operaciones aéreas

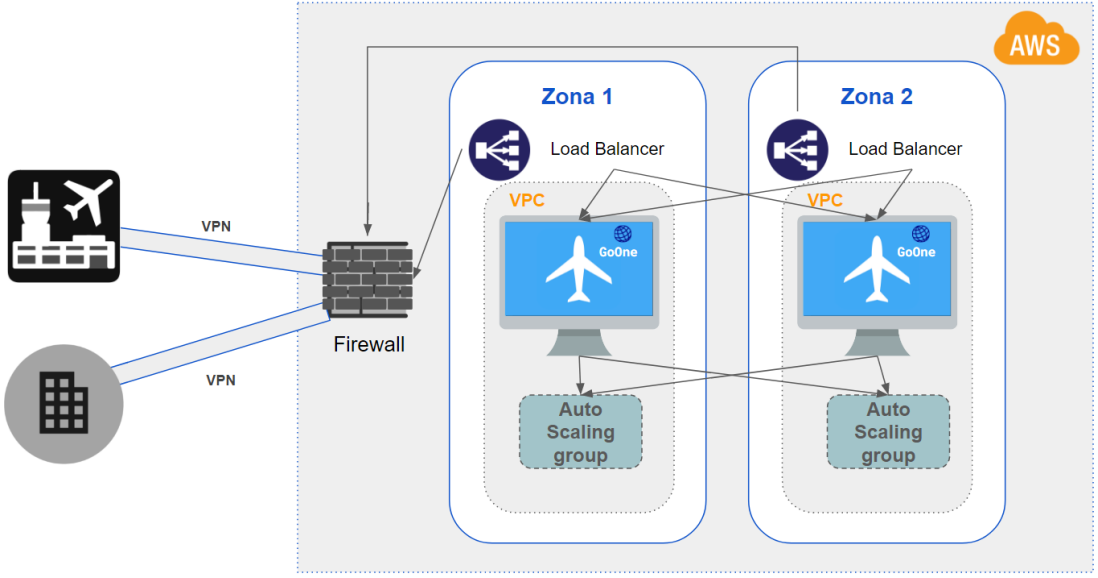


Aeronaves
Maximización de la eficiencia operativa ofrecida por las aeronaves

Sostenibilidad
Mejora de la eficiencia sostenible de las aeronaves

3. Contextualización

Arquitectura GoOne



Principales Características

- Infraestructura como servicio
- Infraestructura dinámica y escalable
- Arquitectura de alta disponibilidad y redundancia

4. Alcance y Objetivos

Proyecto GoOne

- El objetivo que se persigue es el de **implantar el Sistema de Gestión de la Seguridad de la Información (SGSI) GoOne** de manera 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.

- 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**.**

5. Metodología

ISO/IEC 27001

0. Introducción
1. Alcance
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Desempeño
10. Mejora

ISO/IEC 27002 + ISO/IEC 27017

A.5 Políticas de Seguridad
A.6 Organización de la Seguridad
A.7 Seguridad de los RRHH
A.8 Gestión de Activos
A.9 Control de Accesos
A.10 Criptografía
A.11 Seguridad física y ambiental
A.12 Seguridad de las Operaciones
A.13 Seguridad de las Comunicaciones
A.14 Adquisición de sistemas, desarrollo y mantenimiento
A.15 Relaciones con los 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

6. Análisis Diferencial

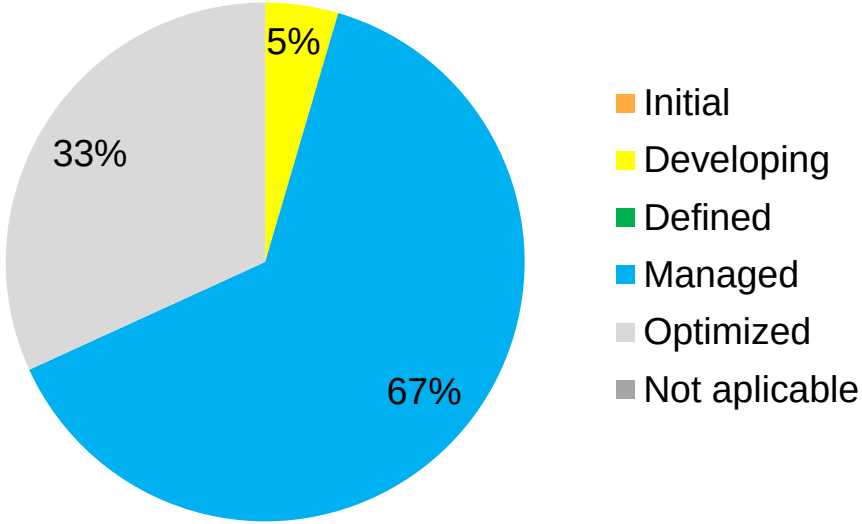
Método

- Con el fin de valorar el estado inicial del cumplimiento de GoOne y poder identificar las necesidades del SGSI se efectúa un análisis diferencial.
- Se toma como referencia la norma ISO/IEC 27001 y las mejores prácticas en ISO/IEC 27002 e ISO/IEC 27017 para valorar el estado del SGSI. Adicionalmente, se utiliza el modelo CMM para calibrar la valoración.

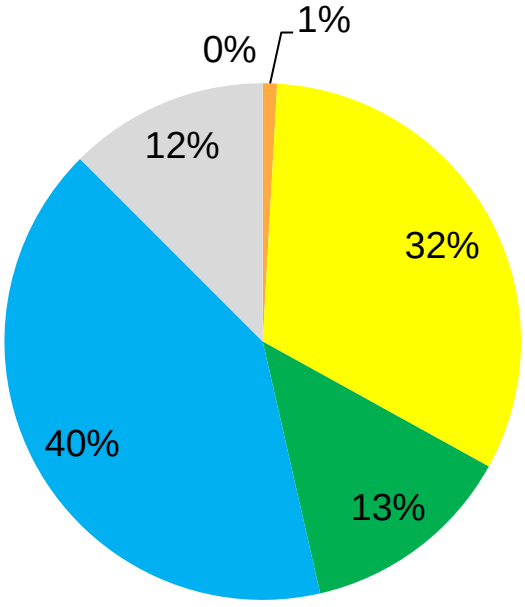
Nivel	Inicial	En desarrollo	Definido	Gestionado	Optimizado
Personas	Actividades sin personal o sin coordinación.	Liderazgo establecido, comunicación informal	Algunos controles en desarrollo con comunicación limitada	Mayores recursos y concienciación, funciones y responsabilidades claramente definidas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

6. Análisis Diferencial

Resultados



Nivel de cumplimiento ISO/IEC 27001:2013



Nivel de cumplimiento ISO/IEC 27002:2013

7. Sistema de Gestión Documental

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Gestión de roles y responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de aplicabilidad

8. Análisis de Riesgos

Metodología de Análisis

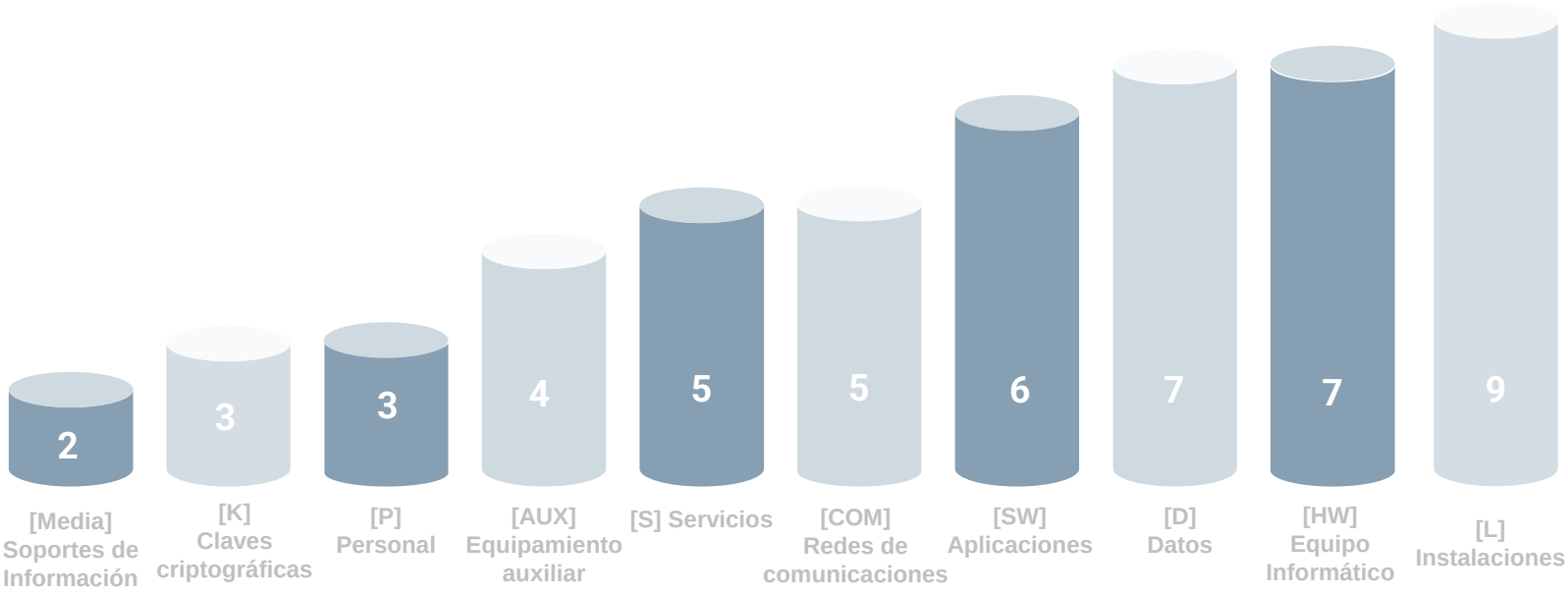
La metodología que se ustiliza en el proceso de análisis es **MAGERIT**: proceso estándar de análisis de riesgos asociados a Sistemas de Información.

Procedimiento

MAR.1 - Caracterización de activos	**MAR.2** - Caracterización de las amenazas	**MAR.3** - Caracterización de las salvaguardas	**MAR.4** - Estimación del estado de riesgo
MAR.11- Identificación de activos	**MAR.21**- Identificación de amenazas	**MAR.31**- Identificación de las salvaguardas	**MAR.41**- Estimación del impacto
MAR.12 - Dependencias entre activos	**MAR.22** -Valoración de las amenazas	**MAR.32** -Valoración de las salvaguardas	**MAR.42** -Estimación del riesgo
MAR.13 - Valoración de los activos			

8. Análisis de Riesgos

Inventario de Activos GoOne



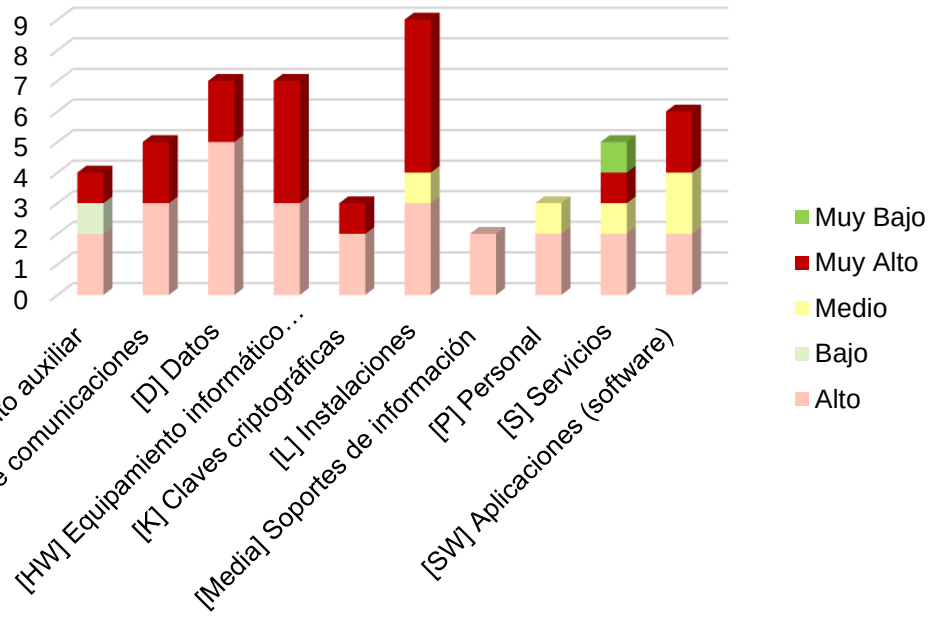
8. Análisis de Riesgos

Valoración activos GoOne

Tabla de referencia: Valoración económica

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

Resultado Valoración de activos



8. Análisis de Riesgos

Criterio valoración Impacto Activos GoOne

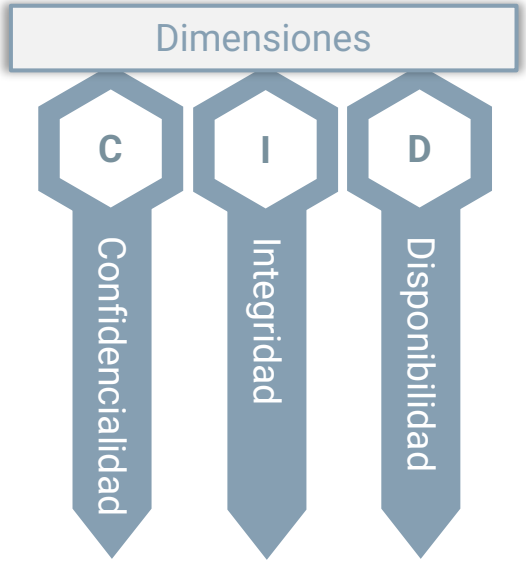


Tabla referencia Impacto

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

8. Análisis de Riesgos

Análisis de Impacto

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

Se realiza el análisis de impacto y valoración de dimesiones para cada activo del inventario

8. Análisis de Riesgos

Análisis de Amenazas: método

Tabla referencia probabilidades de ocurrencia

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

La probabilidad de ocurrencia se basa en la experiencia previa existente para la amenaza.

Categoría de amenazas aplicables a GoOne, extraído del catálogo de Magerit V.3 Libro II .

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

8. Análisis de Riesgos

Análisis de Amenazas: valoración frecuencia

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%	

Se realiza en función de las tablas anteriores el análisis de frecuencia de amenazas

8. Análisis de Riesgos

Calculo del Impacto Potencial de las amenazas

1

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

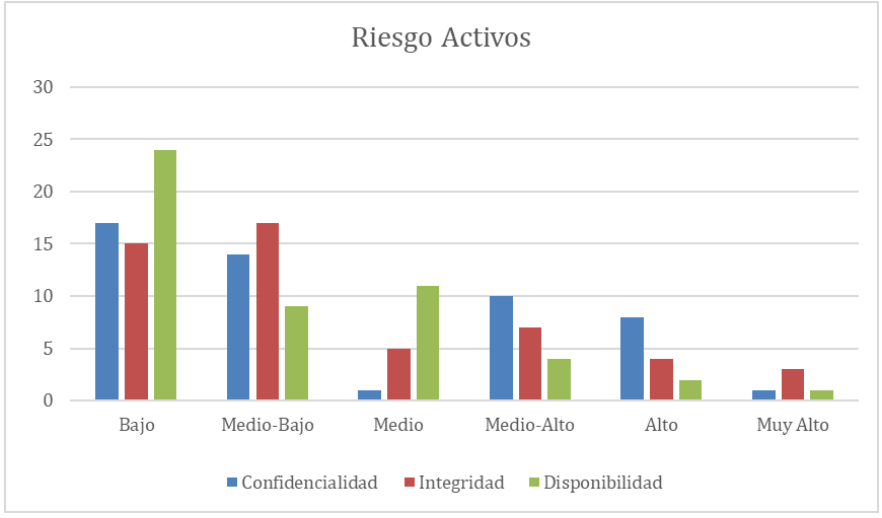
2

Cuandro de decisión para **niveles de riesgo** »

Frecuencia \ Impacto	Extremo	Muy Alto	Alto	Medio	Bajo
Alta	Muy Alto (9-10)		Alto (8-9)	Medio-Alto (8-7)	Medio (7-6)
Media	Alto (8-9)		Medio (7-6)	Medio (7-6)	Medio- Bajo (6-4)
Baja	Medio (7-6)	Medio- Bajo (6-4)	Medio- Bajo (6-4)	Medio- Bajo (6-4)	Bajo (<4)

8. Análisis de Riesgos

Resultado



Activos con riesgos Muy alto o Alto

Nombre activo	ID	Tipo Activo
Servicio AWS nube	*S4*	*[S] Servicios*
Servicios Globales	*S5*	*[S] Servicios*
Equipos de servicios aeroportuarios	*HW2*	*[HW] Equipamiento informático (hardware)*
Equipos en aeronaves	*HW3*	*[HW] Equipamiento informático (hardware)*
Servidor Interno para autenticación en AWS	*HW6*	*[HW] Equipamiento informático (hardware)*
Web Interfaz GoOne	*SW1*	*[SW] Aplicaciones (software)*
Software GoOne	*SW2*	*[SW] Aplicaciones (software)*
Sistema de ticketing	*SW5*	*[SW] Aplicaciones (software)*
Sistema Monitorización local	*SW6*	*[SW] Aplicaciones (software)*
Conexión con AWS	*COM1*	*[COM] Redes de comunicaciones*
Firewalls	*COM2*	*[COM] Redes de comunicaciones*

Como resultado del análisis de riesgos

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

9. Propuestas de proyectos

Selección y priorización

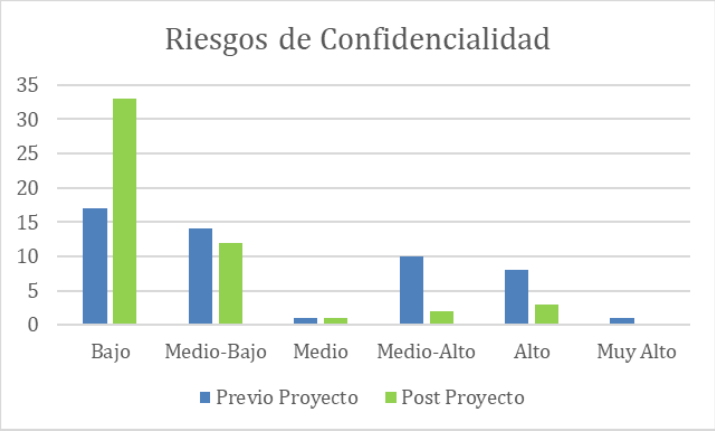
Marco de propuesta y priorización de proyectos

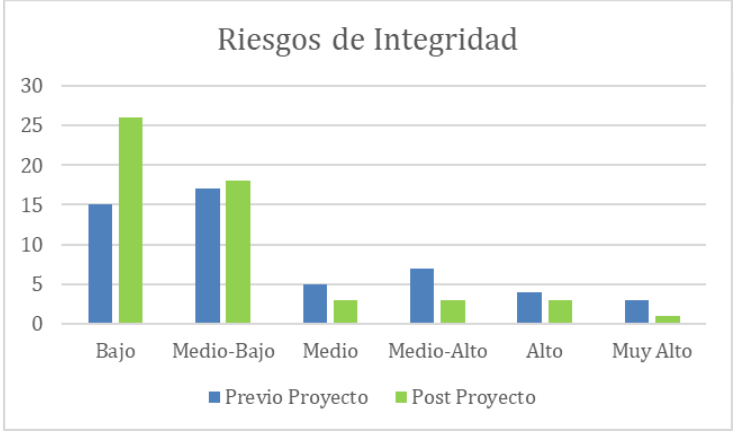
Activos con Riesgo “Muy Alto” o “Alto”

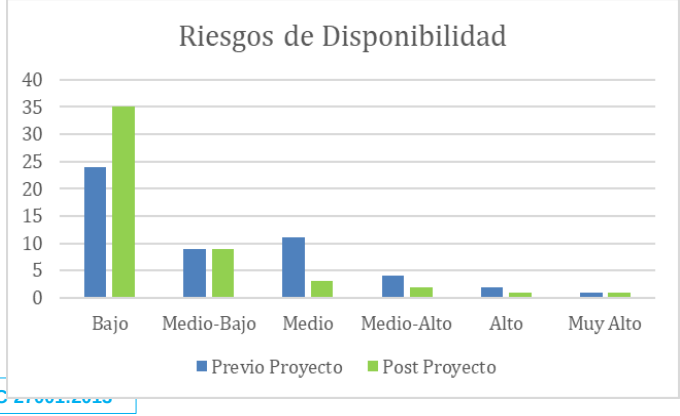
Análisis diferencial con resultado “inicial”, “en desarrollo” o “definido”

9. Propuestas de proyectos

Análisis riesgos tras implementación

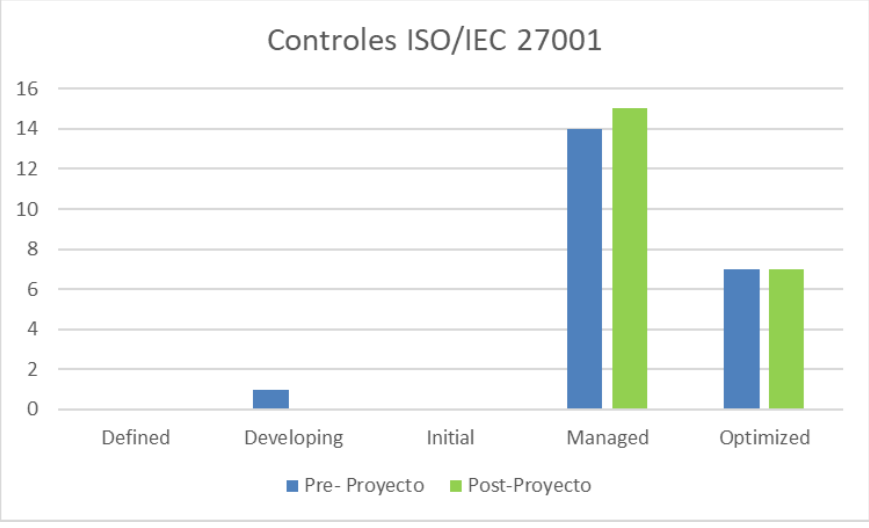


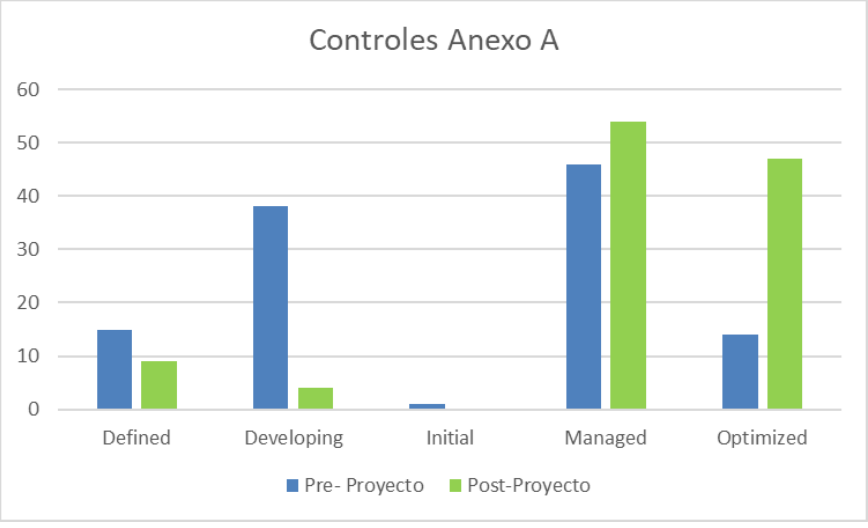




9. Propuestas de proyectos

Análisis Diferencial tras la implementación

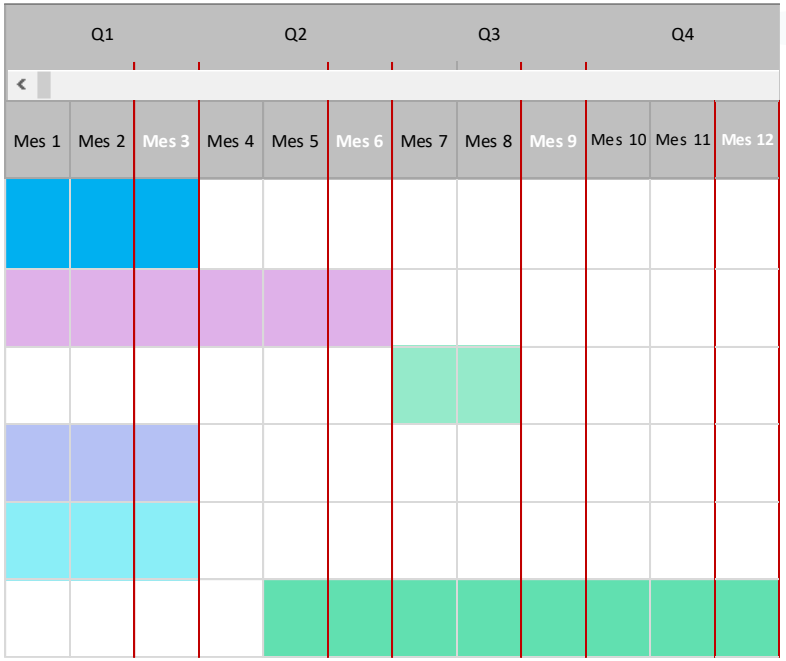




9. Propuestas de proyectos

Propuesta de planificación

Descripción del hito
Proyecto 1 - Definición e implantación de Política de desarrollo de Software Seguro en la nube
Proyecto 2- Integración del proceso de gestión de identidades y accesos de la nube en el sistema corporativo
Proyecto 3- Creación del modelo operacional para GoOne
Proyecto 4- Integración inventario de activos en CMDB corporativa
Proyecto 5- Control del servicio del proveedor de nube
Proyecto 6- Sistema de control sobre el cumplimiento de la política de seguridad de cloud



10. Auditoría de Cumplimiento

Criterio de Evaluación

Criterio/Base

Madurez: CMM

ISO/IEC 27001

0. Introducción
1. Alcance
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Desempeño
10. Mejora

➤ 14 Dominios de control

ISO/IEC 27002 + **ISO/IEC 27017**

A.5 Políticas de Seguridad
A.6 Organización de la Seguridad
A.7 Seguridad de los RRHH
A.8 Gestión de Activos
A.9 Control de Accesos
A.10 Criptografía
A.11 Seguridad física y ambiental
A.12 Seguridad de las Operaciones
A.13 Seguridad de las Comunicaciones
A.14 Adquisición de sistemas, desarrollo y mantenimiento
A.15 Relaciones con los 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

➤ 114 Controles

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.

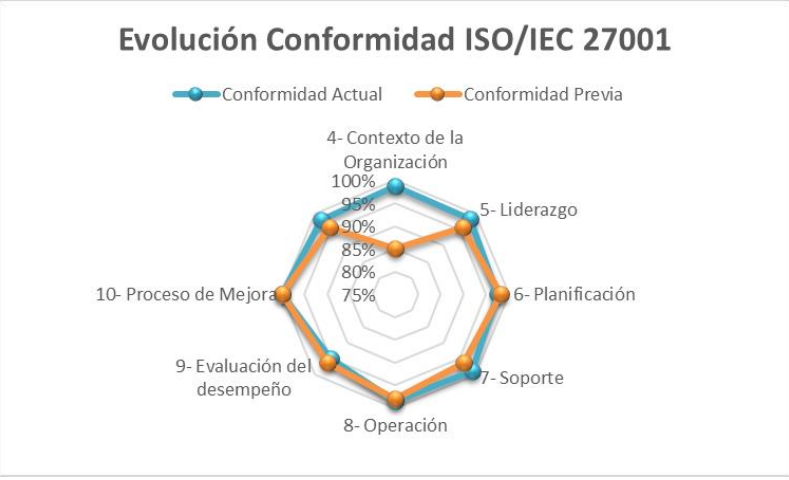
10. Auditoría de Cumplimiento

Resultados y Comparativa (I)

Resultado

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

Comparativa



Conformidad Previa 96%

Conformidad Auditoria 98%

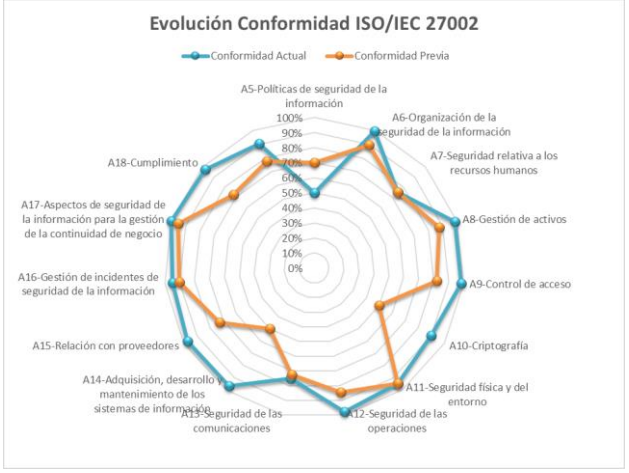
10. Auditoría de Cumplimiento

Resultados y Comparativa (II)

Resultado

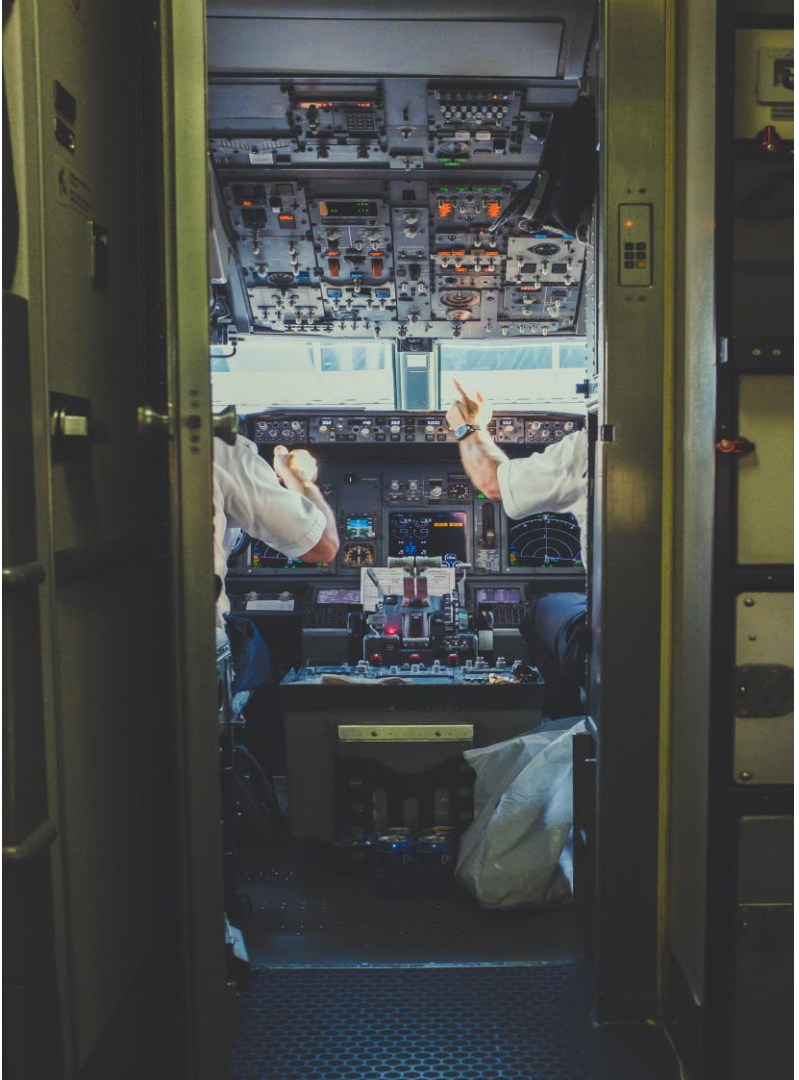
	No Conformidades Mayores (L0-L1)	No Conformidades Menores (L2-L3)	Oportunidades de Mejora (L4)	Cumplimiento (L5)
A5-Políticas de seguridad de la información	1	0	1	0
A6-Organización de la seguridad de la información	0	0	2	5
A7-Seguridad relativa a los recursos humanos	0	0	0	6
A8-Gestión de activos	0	0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

Comparativa



Conformidad Previa 78%

Conformidad Auditoria 90%



11. Conclusiones

- El proyecto ha mostrado tener un impacto positivo, especialmente en cuanto al cumplimiento de los controles del Anexo A.
- El análisis de riesgos y la posterior estrategia de plan de proyectos se ha comprobado tras la auditoría que tuvo el impacto esperado.
- El resultado ha sido positivo en parte gracias al elevado nivel de cumplimiento y experiencia de los controles corporativos respecto al estándar 27001.
- Se ha evidenciado, que pese al impacto positivo del plan de proyectos existe todavía un margen de acción y mejora continúa , especialmente en el área de controles de la nube.

12. Propuesta de Continuación

Propuestas siguientes pasos

Mejora	Cloud	Auditoría	Formación
Plan de remediación y mejora continua	Obtener asesoría técnica en cuanto a posibles proyectos de seguridad en la nube	Proyecto de auditoría SOC para GoOne	Estrategia de capacitación y formación en entorno cloud

¡Gracias!

Elaboración de un Plan de Implementación para ISO/IEC 27001:2013

Elena Sánchez Hernández