Máster Universitario Ciberseguridad y Privacidad (MUCIP)

PRESENTACIÓN DEL PROYECTO

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

Trabajo Fin de Máster (TFM)

Natividad García Lacárcel

CONTENIDO

INTRODUCCIÓN

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

Importancia seguridad de la información

La información es uno de los principales activos que actualmente tienen las organizaciones. Por este motivo debe estar debidamente protegida y preservarse su confidencialidad, integridad y disponibilidad. Así como salvaguardar los sistemas y aplicaciones que la tratan.

La norma ISO/IEC 27001:2013

Es una herramienta, que mediante su aplicación pretende conseguir que la organización alcance un nivel adecuado de seguridad de la información. Ofrece una visión inicial del estado de la organización, sus deficiencias y las medidas necesarias para corregir dichos problemas y la situación final después de la aplicación de los proyectos emprendidos. Sienta las bases del proceso de mejora continua y plantea las acciones necesarias para minimizar el impacto de los riesgos potenciales.

FASES DEL PROYECTO

- **1. Situación actual**
- **2. Sistema Gestión documental**
- **3. Análisis de Riesgos**
- **4. Propuestas Proyectos**
- **5. Auditoría de cumplimiento**
- **6. Presentación de resultados y entrega de informes**

CONTEXTO DE LA ORGANIZACIÓN

MASIAG es una agencia de marketing digital. Su actividad consiste en diseñar estrategias de marketing online integral para los negocios y llevarlas a cabo.

Es compañía innovadora, creada en 2011 que ha tenido un rápido crecimiento y hoy día es líder en el sector del marketing.
La compañía analiza las particulares propias del sector del cliente, se ajusta a sus necesidades y estudia a la competencia. Su objetivo es promover marca, productos y servicios a través de internet.

Para poder aumentar la confianza de los clientes y seguir creciendo, la compañía necesita obtener la ISO 27001:2013.
Por tanto, se realizarán distintas acciones que favorezcan la mejora de la calidad y seguridad en los sistemas de información, así como la obtención de la certificación.

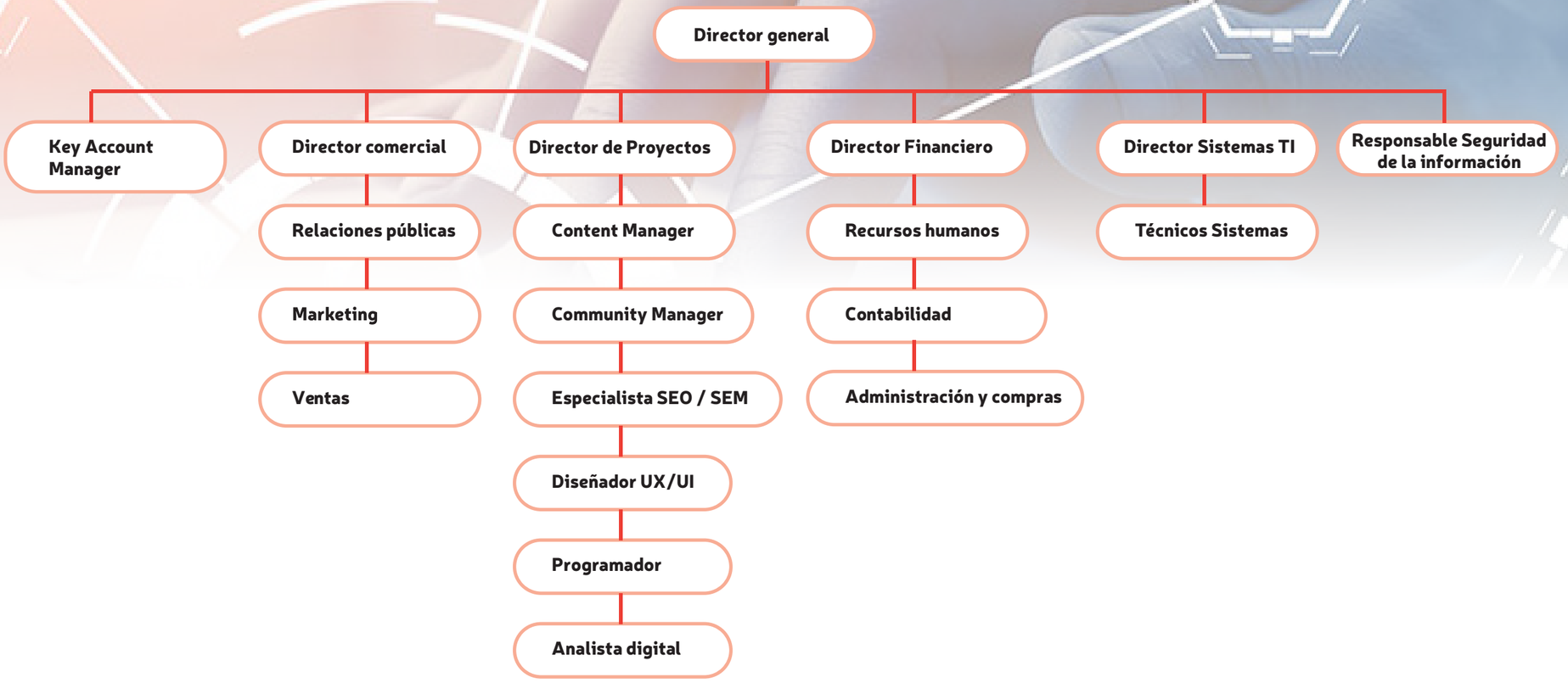
CONTEXTO DE LA ORGANIZACIÓN

Actividades

- Marketing digital
- Posicionamiento en buscadores
- Posicionamiento ASO
- Campañas de Email marketing
- Gestión redes sociales
- Marketing de contenidos
- Comercio electrónico
- Video marketing
- Formación a medida.

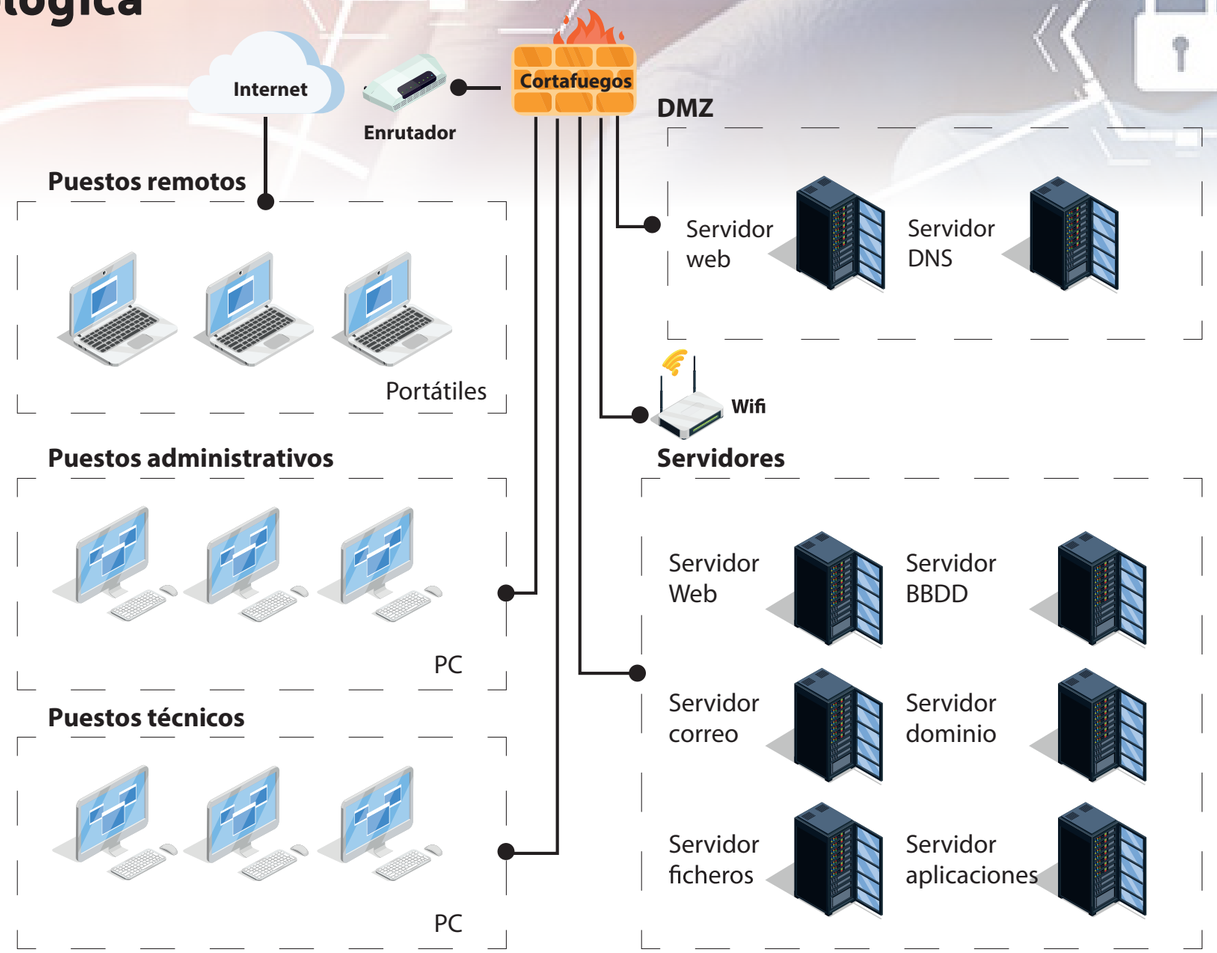
CONTEXTO DE LA ORGANIZACIÓN

Estructura organizativa



CONTEXTO DE LA ORGANIZACIÓN

Infraestructura tecnológica



ALCANCE

El alcance del proyecto incluye la totalidad de los procesos y tratamientos de la información que se efectúa en la empresa.
Afectará a todo el sistema, las instalaciones y el personal, así como a la información que pueda procesarse en la empresa, tanto si pertenece a ella como a terceros.

En el proceso de implementación del SGSI se procurará la gestión de la seguridad en todos los niveles y capas de la organización. Procurando alinear los objetivos de seguridad con el negocio. Implicando a la alta dirección y procurando la concienciación del personal para que efectuar un correcto tratamiento de la información. Incluyendo la gestión de la seguridad tanto de los soportes físicos como lógicos de la seguridad. Así como el acceso a la información de forma remota o localmente.

OBJETIVOS

- Involucrar a la alta dirección en el desarrollo e implantación del SGSI. Así como a toda la organización en conjunto para garantizar una correcta ejecución del SGSI.
- Establecer los canales adecuados para poder garantizar la seguridad de la información en todas las fases.
- Generar confianza a la dirección, trabajadores, empresas externas en los sistemas de información.
- Asegurar la confidencialidad, seguridad y correcto uso de los sistemas de la organización.
- Evaluar el nivel de cumplimiento, por medio del análisis diferencial respecto a las normas estándar ISO/IEC 27001 e ISO/IEC 27002.
- Detectar y valorar los riesgos; priorizándolos para implantar los controles que se consideren adecuados.
- Efectuar seguimiento sobre las propuestas y mejoras realizadas.
- Asegurar el cumplimiento de la legislación aplicable.

METODOLOGÍA

ISO/IEC 27001: marco de trabajo que define como ejecutar un SGSI, con una visión de mejora continua en el tiempo Plan, Do, Check, Act (PDCA). De estas fases, se obtienen unos objetivos, cuyo cumplimiento permitirá la certificación de la norma.

0. Introducción		
1. Alcance		
2. Referencias normativas		
3. Términos y definiciones		
4. Contexto de la organización	Conocimiento de la organización y de su contexto Comprensión de las necesidades y expectativas de las partes interesadas Determinación del alcance del SGSI	
5. Liderazgo	Liderazgo y compromiso Política Roles, responsabilidades y autoridades en la organización	
6. Planeación	Riesgos y oportunidades	
7. Soporte	Recursos Competencia Conciencia	Comunicación Información documentada
8. Operación	Evaluación de riesgos Tratamiento de riesgos	
9. Evaluación del desempeño	Procurar el seguimiento mediante el monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.	
	Seguimiento, medición, análisis y evaluación Auditoría interna Revisión por la dirección	
10. Mejora	No conformidades y acciones correctivas. Mejora continua.	

ISO/IEC 27002: guía de buenas prácticas, agrupadas en 14 dominios, para mejorar la seguridad de la información y que sirva como ayuda para alcanzar los objetivos marcados en la 27001.

- A5. Políticas de Seguridad
- A6. Organización de la Seguridad de la Información
- A7. Seguridad de los Recursos Humanos
- A8. Gestión de los Activos
- A9. 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 incidencias que afectan a la Seguridad de la Información
- A.17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad de Negocio
- A.18 Conformidad

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

Trabajo Fin de Máster (TFM)

Natividad García Lacárcel

ANÁLISIS DIFERENCIAL

Será el punto de partida para determinar la situación de la organización y poder valorar los avances que se realicen a lo largo del proyecto.

El análisis diferencial se realizará con respecto la norma ISO/IEC 27001 y las mejores prácticas descritas en ISO/IEC 27002, y nos permitirá evaluar la capacidad actual y realizar las recomendaciones y oportunidades de mejora.

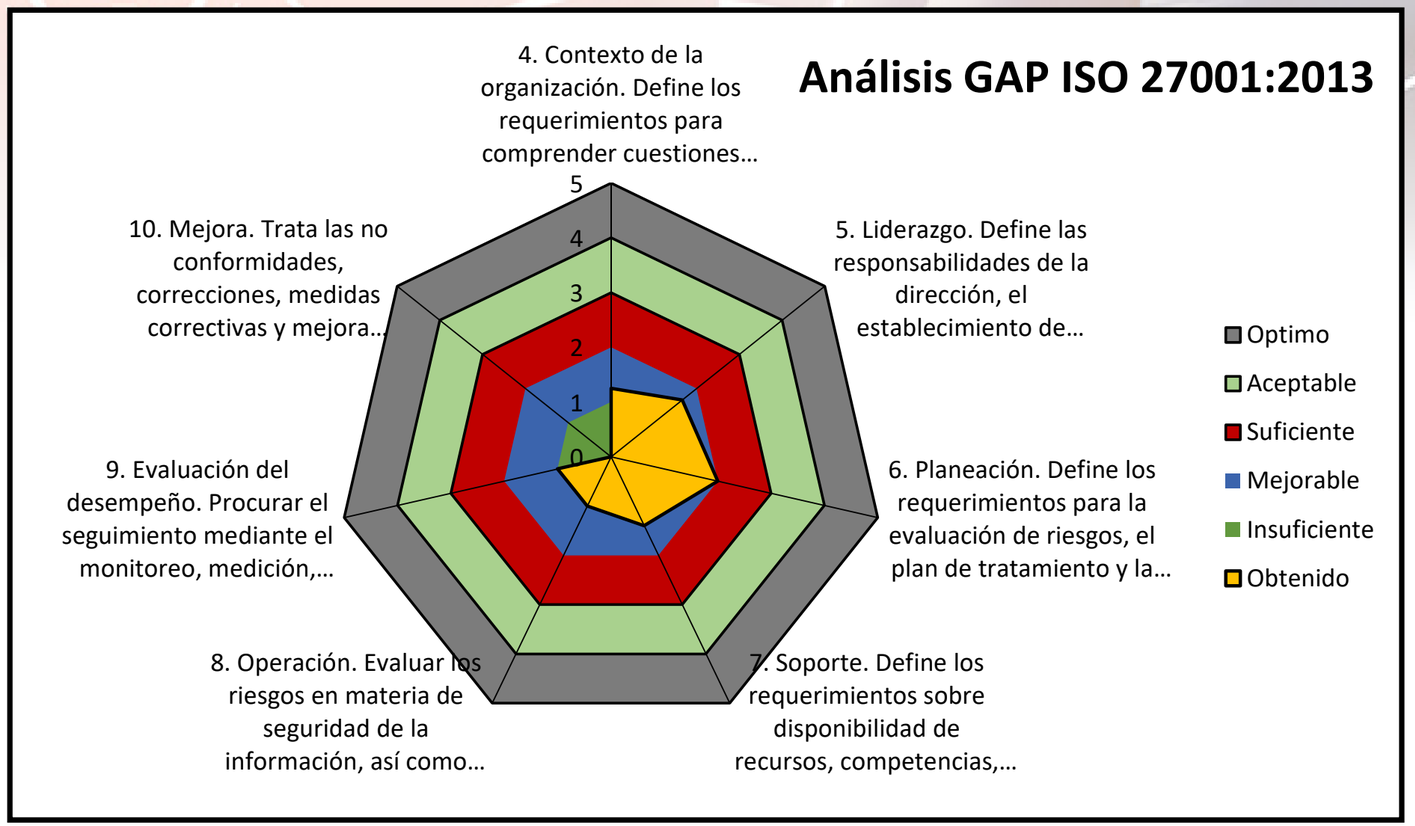
El análisis emplea para la valoración de los controles el modelo de madurez definido por COBIT y basado en el CMM.

	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de “best practice”, sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporciona mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos “ad hoc” que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

MENOR 1.65	NO CUMPLE
ENTRE 1.66 Y 3.25	CUMPLE PARCIALMENTE
MAYOR 3.26	CUMPLE REQUISITOS NORMA

ANÁLISIS DIFERENCIAL

Nivel de cumplimiento en los dominios de la ISO/IEC 27001:2013

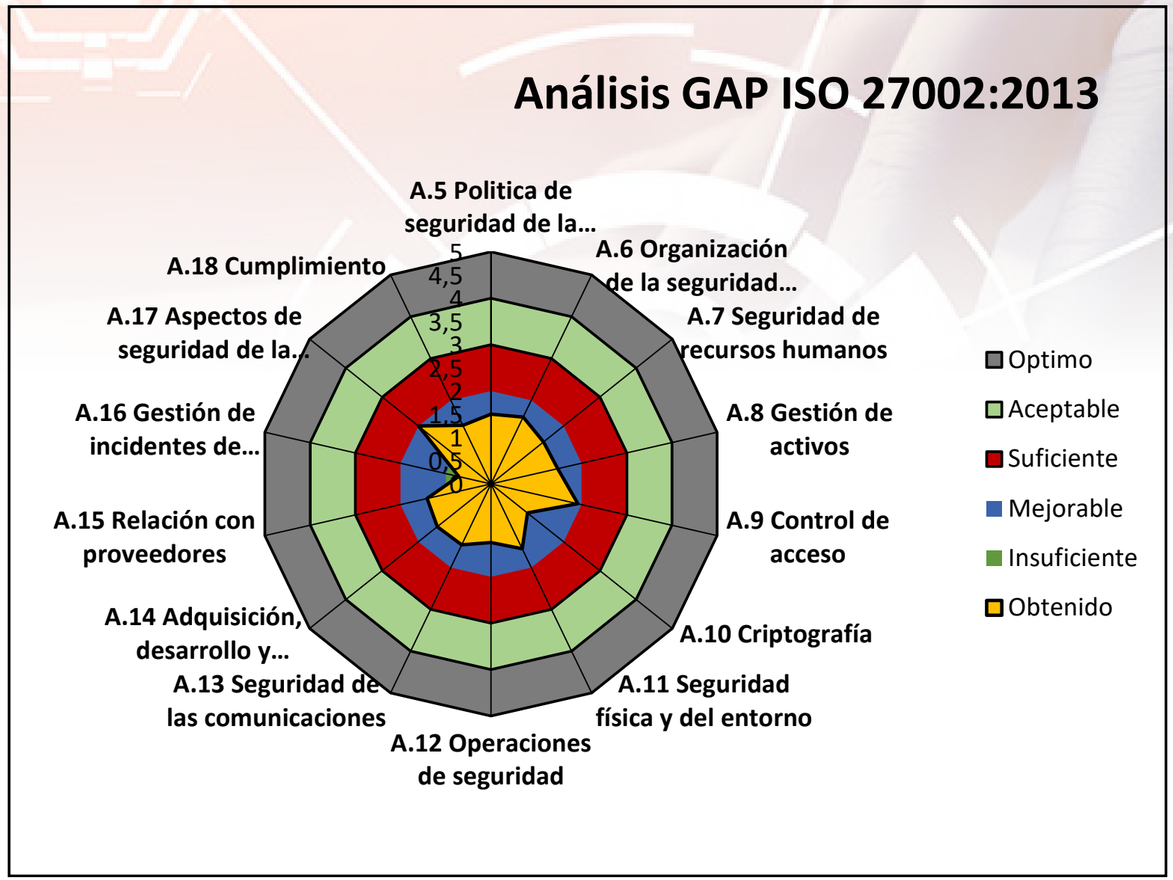


	VALOR	CUMPLIMIENTO
4. Contexto de la organización.	1,25	NO CUMPLE
5. Liderazgo.	1,666666667	CUMPLE PARCIALMENTE
6. Planeación.	2	CUMPLE PARCIALMENTE
7. Soporte	1,4	NO CUMPLE
8. Operación.	1	NO CUMPLE
9. Evaluación del desempeño.	1	NO CUMPLE
10. Mejora.	0	NO CUMPLE

0 - No existente	**3**
1 - Inicial	11
2 - Repetible	8
3 - Definido	0
4 - Gestionado	0
5 - Optimizado	0
TOTAL	22

ANÁLISIS DIFERENCIAL

Nivel de cumplimiento en los dominios de la ISO/IEC 27002:2013



CONTROL	VALOR	CUMPLIMIENTO
A.5 Política de seguridad de la información	1,5	NO CUMPLE
A.6 Organización de la seguridad de la información	1,6	NO CUMPLE
A.7 Seguridad de recursos humanos	1,44	NO CUMPLE
A.8 Gestión de activos	1,47	NO CUMPLE
A.9 Control de acceso	1,92	CUMPLE PARCIALMENTE
A.10 Criptografía	1	NO CUMPLE
A.11 Seguridad física y del entorno	1,56	NO CUMPLE
A.12 Operaciones de seguridad	1,26	NO CUMPLE
A.13 Seguridad de las comunicaciones	1,46	NO CUMPLE
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	1,48	NO CUMPLE
A.15 Relación con proveedores	1,42	NO CUMPLE
A.16 Gestión de incidentes de seguridad de la información	0,71	NO CUMPLE
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	2	CUMPLE PARCIALMENTE
A.18 Cumplimiento	1,4	NO CUMPLE

0 - No existente	14
1 - Inicial	35
2 - Repetible	62
3 - Definido	1
4 - Gestionado	2
5 - Optimizado	0
TOTAL	114

SISTEMA DE GESTIÓN DOCUMENTAL

- Política de seguridad
- Procedimiento de auditorías internas
- Gestión de indicadores
- Procedimiento de revisión por dirección
- Gestión de roles y responsabilidades
- Metodología de análisis de riesgos
- Declaración de aplicabilidad

ANÁLISIS DE RIESGOS

Metodología MAGERIT

Es un método formal para investigar los riesgos que soportan los Sistemas de Información y recomienda las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

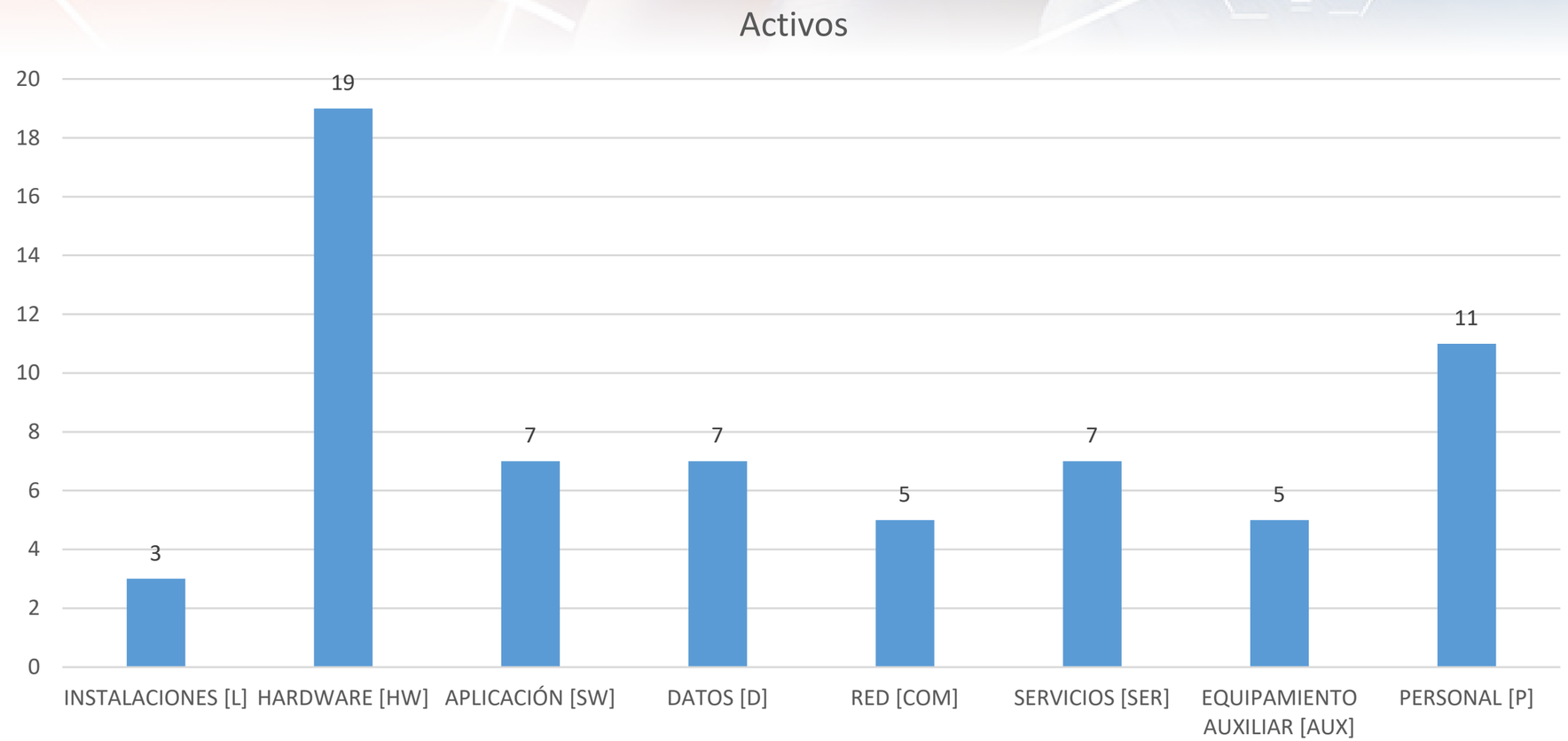
Procedimiento:

- Identificación de los activos y su valor asociado.
- Identificación de amenazas y vulnerabilidades cuya explotación puede permitir materializarlas.
- Gestión del riesgo en función del impacto potencial que supondría la materialización de las amenazas en los activos identificados.
- Calcular el nivel de riesgo aceptable y el riesgo residual.

ANÁLISIS DE RIESGOS

INVENTARIO DE ACTIVOS. POR CATEGORÍA

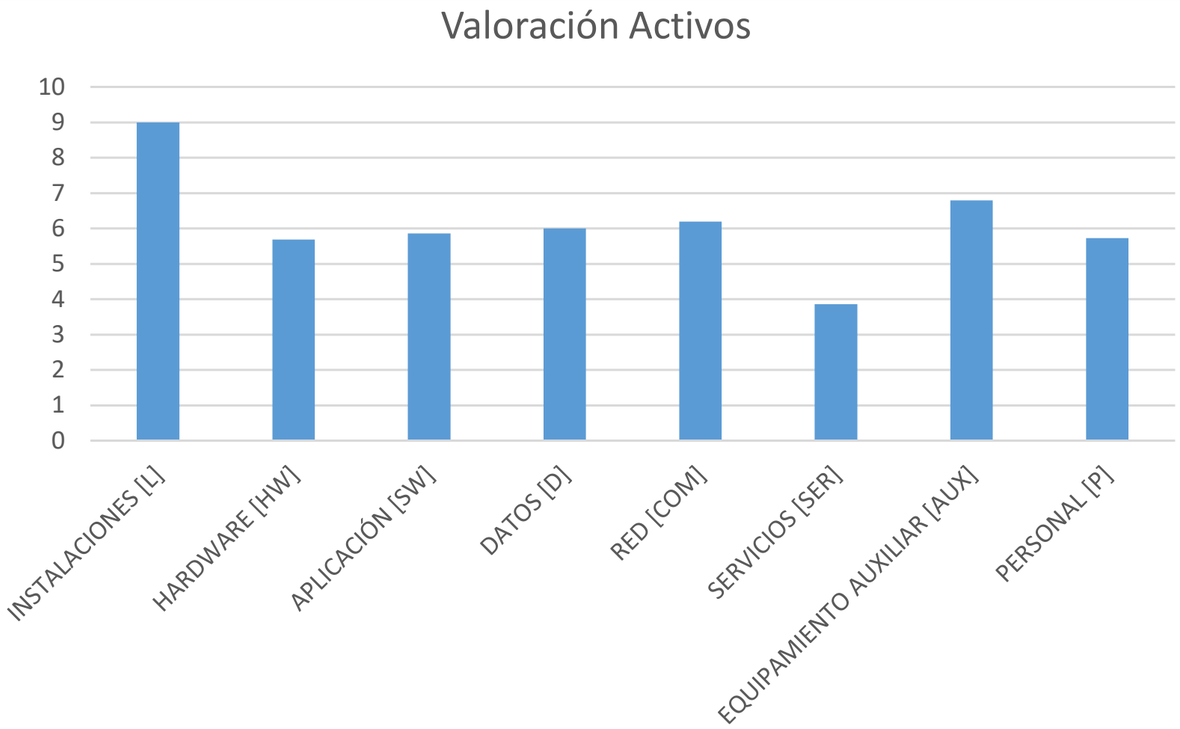
- 8 Categorías y 64 activos



ANÁLISIS DE RIESGOS

VALORACIÓN DE LOS ACTIVOS

La valoración de los activos, ha tenido en cuenta el valor de uso, de configuración y de sustitución de los activos.
Así como una representación cuantitativa en términos monetarios para la organización.



El rango de la valoración económica:	RANGO	VALOR
Muy alta	Valor>50.000€	100.000€
Alta	10.000€<valor>50.000€	25.000€
Media	5.000€<valor>10.000€	7.500€
Baja	1.000€<valor>5.000€	2.500€
Muy baja	Valor<1.000€	1.000€

ANÁLISIS DE RIESGOS

Autenticidad [A]
Confidencialidad [C]
Integridad [I]
Disponibilidad [D]
Trazabilidad [T]

Escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo)

Valor		Criterio
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

ANÁLISIS DE RIESGOS

INVENTARIO DE ACTIVOS. VALORACIÓN SEGÚN LAS DIMENSIONES DE SEGURIDAD

AMBITO	ACTIVO	A	C	I	D	T
INSTALACIONES [L]	Oficina	7	8	8	9	5
	CPD	9	9	9	9	9
	Recepción	5	5	1	1	1
HARDWARE [HW]	Servidor de aplicaciones	7	7	7	3	4
	Servidor de desarrollo y pruebas	7	3	3	3	4
	Servidor de Web	7	7	7	3	4
	Servidor BBDD	9	5	5	9	4
	Servidor DNS/Proxy/Dominio	7	1	3	3	4
	Servidor de ficheros	9	5	5	9	4
	Servidor de Email	9	5	5	9	4
	Equipamiento de respaldo	7	7	7	3	4
	Enrutador de Internet	5	5	5	5	5
	Switch	5	5	5	5	5
	Cortafuegos	9	9	9	9	9
	Punto de acceso inalámbrico	5	3	3	3	3
	Equipos escritorio pc	7	7	3	3	4
	Portátiles	7	7	3	3	4
	Impresoras y escáneres	3	3	1	1	4
	Centralita	3	3	3	1	3
	Teléfonos fijos	3	3	3	1	3
	Teléfonos móviles	3	3	3	1	3
	Cámaras de vigilancia	3	3	3	4	3
APLICACIÓN [SW]	Sistemas operativos	3	7	7	3	3
	Paquete ofimático	3	3	3	1	
	Antivirus	3	3	3	5	3
	Software de desarrollo	5	7	5	5	3
	Software de contabilidad	5	7	5	5	3
	Email	3	3	3	5	3
	Servidores	10	9	10	9	3
DATOS [D]	Bases de datos	10	9	10	9	10
	Datos de soporte y licencias	3	3	1	1	3
	Desarrollos propios	3	1	5	3	3
	Backups (copias de seguridad)	7	7	7	3	7
	Correo electrónico	3	1	5	3	3
	Logs de servidores y clientes	3	3	4	8	4
	Credenciales y datos de control de acceso.	3	3	4	8	4
RED [COM]	Internet	3	9	9	3	7
	Red inalámbrica	3	7	3	3	5
	Red cableada	3	9	9	3	7
	Telefonía fija	5	5	1	5	3
	Telefonía móvil	5	5	1	5	3
SERVICIOS [SER]	Acceso remoto	1	3	1	1	0
	Red de control e instrumentación	0	0	0	1	0
	Acceso a internet	3	3	0	1	0
	Correo electrónico	3	3	5	3	7
	Servicio web	5	5	5	5	5
	Servicio aplicaciones	0	7	0	7	0
	Servicio ficheros	0	7	0	7	0
EQUIPAMIENTO AUXILIAR [AUX]	Aire acondicionado	9	9	9	9	0
	Archivadores	3	1	1	3	0
	Consumibles varios	1	1	1	3	0
	SAI	7	7	7	7	0
	Corriente eléctrica	9	9	9	9	0
PERSONAL [P]	Director General	9	3	3	3	3
	Director comercial	9	3	3	3	3
	Director de proyectos	9	3	3	3	3
	Director financiero	9	3	3	3	3
	Director Sistemas TI	9		7	7	9
	Responsable seguridad de la información.	9	7	7	7	7
	Key Account Manager	9	0	0	3	3
	Técnicos de sistemas	9	0	0	3	9
	Personal del departamento comercial	3	0	0	3	3
	Personal del departamento de proyectos	3	0	0	3	3
	Personal del departamento financiero	3	0	0	1	3

ANÁLISIS DE RIESGOS

ANÁLISIS DE AMENAZAS. CLASIFICACIÓN

Desastres Naturales [N]
De origen Industrial [I]
Errores y fallos no intencionados [E]
Ataques Intencionados [A]

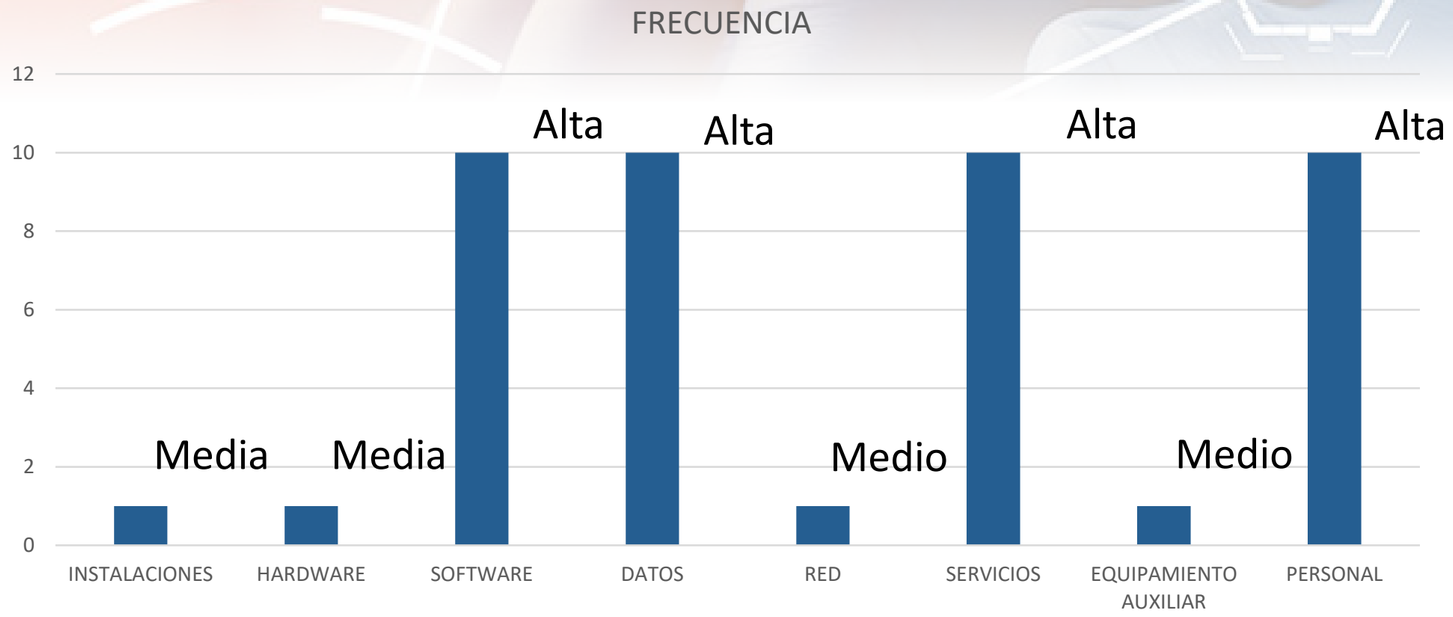
Probabilidad de ocurrencia: Representa la tasa anual de ocurrencia, es decir, cada cuanto se materializa una amenaza. La valoración se efectuará mediante la siguiente tabla:

Porcentaje de Degradación: Significa el daño causado por un incidente. El grado de degradación se detalla para cada activo relacionándolos con amenaza y dimensión, se mide entre 0% y el 100%.

VALOR		CRITERIO	
Muy Alta [MA]	100	Una vez al día	Muy frecuente
Alta [A]	10	Una vez al mes	Frecuente
Media [M]	1	Una vez al año	Normal
Baja [B]	1/10	Una vez cada varios años	Poco frecuente
Muy baja [MB]	1/100	Cada muchos años.	Muy poco frecuente

ANÁLISIS DE RIESGOS

ANÁLISIS DE AMENAZAS. FRECUENCIA.



ACTIVO	FRECUENCIA		A	C	I	D	T
		INSTALACIONES					
[L-01] – Oficina	Medio[M]	1	0%	100%	100%	100%	0%
[L-02] – CPD	Medio[M]	1	0%	100%	100%	100%	0%
[L-01] – Recepción	Medio[M]	1	0%	100%	100%	100%	0%

ANÁLISIS DE RIESGOS

CALCULO DEL IMPACTO

El cálculo del impacto potencial, se utiliza la siguiente fórmula:

Impacto potencial = valor del activo X valor del impacto

Entendido el valor del activo de cada dimensión y el impacto como la degradación en cada dimensión en la que se ve afectado el activo.

Según el método MAGERIT en su libro II apartado 2.1 se puede calcular el valor del impacto en base a la siguiente tabla sencilla.

La tabla para calcular el impacto:

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

ANÁLISIS DE RIESGOS

IMPACTO

ACTIVO	A	C	I	D	T
Oficina	0	8	8	9	0
CPD	0	9	9	9	0
Recepción	0	5	1	1	0
Servidor de aplicaciones	0	7	2,1	3	0
Servidor de desarrollo y pruebas	0	3	0,9	3	0
Servidor de Web	0	7	2,1	3	0
Servidor BBDD	0	5	1,5	9	0
Servidor DNS/Proxy/Dominio	0	1	0,9	3	0
Servidor de ficheros	0	5	1,5	9	0
Servidor de Email	0	5	1,5	9	0
Equipamiento de respaldo	0	7	2,1	3	0
Enrutador de Internet	0	5	1,5	5	0
Switch	0	5	1,5	5	0
Cortafuegos	0	9	2,7	9	0
Punto de acceso inalámbrico	0	3	1,5	3	0
Equipos escritorio pc	0	7	0,9	3	0
Portátiles	0	7	0,9	3	0
Impresoras y escáneres	0	3	0,3	1	0
Centralita	0	3	0,9	1	0
Teléfonos fijos	0	3	0,9	1	0
Teléfonos móviles	0	3	0,9	1	0
Cámaras de vigilancia	0	3	0,9	4	0
Sistemas operativos	3	7	7	3	0,9
Paquete ofimático	3	3	3	1	0
Antivirus	3	3	3	5	0,9
Software de desarrollo	5	7	5	5	0,9
Software de contabilidad	5	7	5	5	0,9
Email	3	3	3	5	0,9
Servidores	10	9	10	9	0,9
Bases de datos	10	9	3	9	0
Datos de soporte y licencias	3	3	0,3	1	0
Desarrollos propios	3	1	1,5	3	0
Backups (copias de seguridad)	7	7	2,1	3	0
Correo electrónico	3	1	1,5	3	0
Logs de servidores y clientes	3	3	1,2	8	0
Credenciales y datos de control de acceso.	3	3	1,2	8	0
Internet	1,5	4,5	2,7	1,5	0
Red inalámbrica	1,5	3,5	0,9	1,5	0
Red cableada	1,5	4,5	2,7	1,5	0
Telefonía fija	2,5	2,5	0,3	2,5	0
Telefonía móvil	2,5	2,5	0,3	2,5	0
Acceso remoto	1	3	0,5	1	0
Red de control e instrumentación	0	0	0	1	0
Acceso a internet	3	3	0	1	0
Correo electrónico	3	3	2,5	3	0
Servicio web	5	5	2,5	5	0
Servicio aplicaciones	0	7	0	7	0
Servicio ficheros	0	7	0	7	0
Aire acondicionado	0	4,5	2,7	9	0
Archivadores	0	0,5	0,3	3	0
Consumibles varios	0	0,5	0,3	3	0
SAI	0	3,5	2,1	7	0
Corriente eléctrica	0	4,5	2,7	9	0
Director General	0	0,6	0,9	3	0
Director comercial	0	0,6	0,9	3	0
Director de proyectos	0	0,6	0,9	3	0
Director financiero	0	0,6	0,9	3	0
Director Sistemas TI	0	0	2,1	7	0
Responsable seguridad de la información.	0	1,4	2,1	7	0
Key Account Manager	0	0	0	3	0
Técnicos de sistemas	0	0	0	3	0
Personal del departamento comercial	0	0	0	3	0
Personal del departamento de proyectos	0	0	0	3	0
Personal del departamento financiero	0	0	0	1	0

ANÁLISIS DE RIESGOS

CÁLCULO DE RIESGO
Riesgo = Impacto Potencial * Frecuencia

Según el método MAGERIT en su libro II apartado 2.1 se puede calcular el valor del impacto en base a la siguiente tabla sencilla.
Impacto, probabilidad y riesgo se modelan por medio de escalas cualitativas:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo.

ANÁLISIS DE RIESGOS

NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

TRATAMIENTO DEL RIESGO CRÍTICO	
[SW-07]	Servidores
[D-01]	Bases de datos

TRATAMIENTO DEL RIESGO IMPORTANTE	
[SW-01]	Sistemas operativos
[SW-04]	Software de desarrollo
[SW-05]	Software de contabilidad
[D-04]	Backups (copias de seguridad)
[D-06]	Logs de servidores y clientes
[D-7]	Credenciales y datos de control de acceso.
[SER-06]	Servicio aplicaciones
[SER-07]	Servicio ficheros
[P-05]	Director Sistemas TI
[P-06]	Responsable seguridad de la información.

TRATAMIENTO DEL RIESGO MODERADO	
[SW-03]	Antivirus
[SW-06]	Email
[SER-05]	Servicio web

PROPUESTA DE PROYECTOS

- **Proyecto 1 – Definir políticas de seguridad de la información**
- **Proyecto 2 – Mejora del CPD**
- **Proyecto 3 – Control de acceso**
- **Proyecto 4 – Plan de contingencia de datos – Backups y Restores**
- **Proyecto 5 – Monitoreo SGSI**
- **Proyecto 6 – Concienciación sobre la importancia de la información**
- **Proyecto 7 – Criptografía**
- **Proyecto 8 – Plan de clasificación de la información y tratamiento del mismo.**
- **Proyecto 9 – Mantenimiento, control y protección equipos informáticos**
- **Proyecto 10 – Proyecto Desarrollo de software**
- **Proyecto 11 – Plan de contingencia y continuidad de negocio**
- **Proyecto 12 – Procedimiento Gestión de incidentes**

PROPUESTA DE PROYECTOS

Planificación a 3 años

TAREA	INICIO	FIN
PROYECTOS		
Proyecto 1 – Política de seguridad	24-4-21	23-6-21
Proyecto 2 – Mejora del CPD	23-6-21	21-10-21
Proyecto 3 – Control de acceso	21-10-21	19-1-22
Proyecto 4 – Plan de contingencia de datos – Backups y Rest	19-1-22	19-4-22
Proyecto 5 – Monitoreo SGSI	19-4-22	18-7-22
Proyecto 6 – Concienciación sobre la importancia de la infor	18-7-22	15-11-22
Proyecto 7 – Criptografía	15-11-22	14-1-23
Proyecto 8 – Plan de clasificación de la información y tratam	14-1-23	14-4-23
Proyecto 9 – Mantenimiento, control y protección equipos ir	14-4-23	13-7-23
Proyecto 10 – Proyecto Desarrollo de software	13-7-23	11-10-23
Proyecto 11 – Plan de contingencia y continuidad de negocic	11-10-23	9-1-24
Proyecto 12 – Procedimiento Gestión de incidentes	9-1-24	8-4-24

PROPUESTA DE PROYECTOS

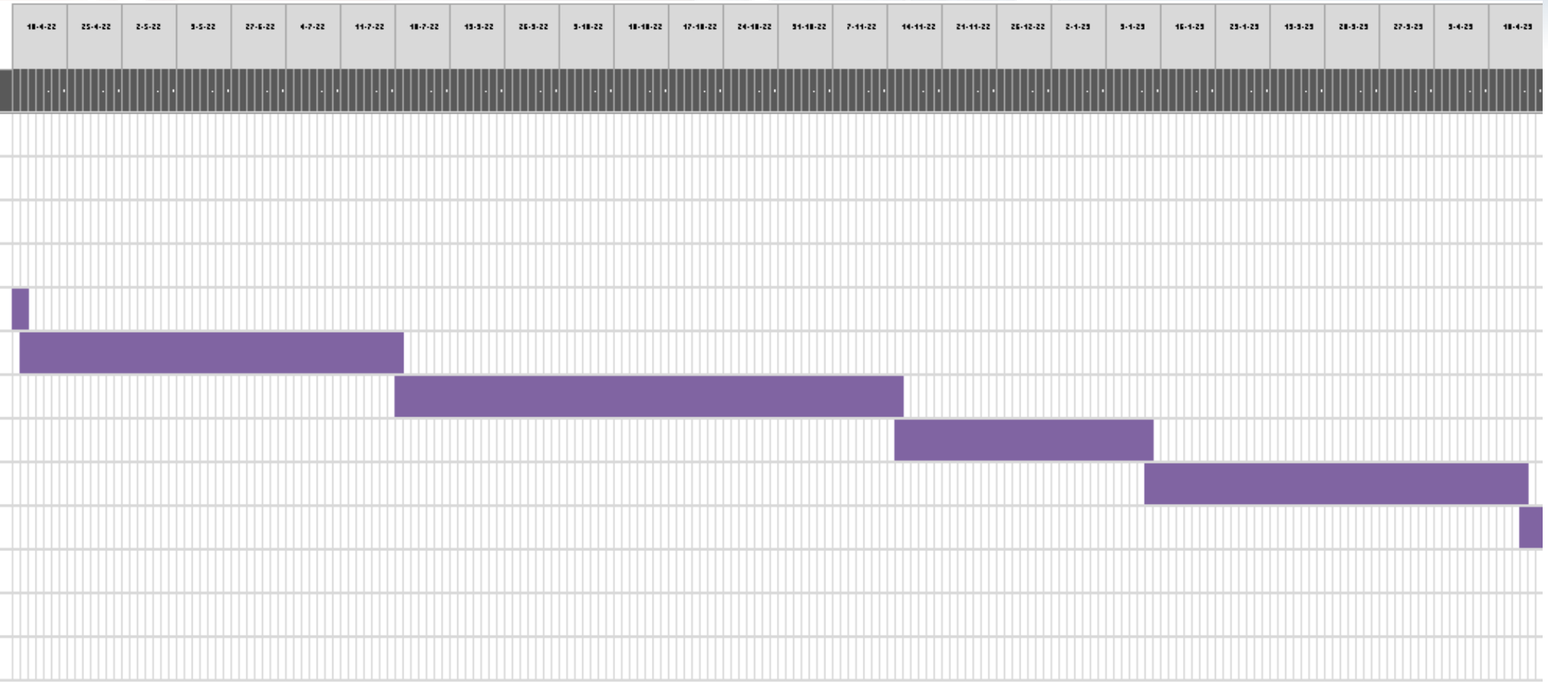
Planificación a 3 años

TAREA	INICIO	FIN
PROYECTOS		
Proyecto 1 – Política de seguridad	24-4-21	23-6-21
Proyecto 2 – Mejora del CPD	23-6-21	21-10-21
Proyecto 3 – Control de acceso	21-10-21	19-1-22
Proyecto 4 – Plan de contingencia de datos – Backups y Rest	19-1-22	19-4-22
Proyecto 5 – Monitoreo SGSI	19-4-22	18-7-22
Proyecto 6 – Concienciación sobre la importancia de la infor	18-7-22	15-11-22
Proyecto 7 – Criptografía	15-11-22	14-1-23
Proyecto 8 – Plan de clasificación de la información y tratam	14-1-23	14-4-23
Proyecto 9 – Mantenimiento, control y protección equipos ir	14-4-23	13-7-23
Proyecto 10 – Proyecto Desarrollo de software	13-7-23	11-10-23
Proyecto 11 – Plan de contingencia y continuidad de negocic	11-10-23	9-1-24
Proyecto 12 – Procedimiento Gestión de incidentes	9-1-24	8-4-24

PROPUESTA DE PROYECTOS

Planificación a 3 años

TAREA	INICIO	FIN
PROYECTOS		
Proyecto 1 – Política de seguridad	24-4-21	23-6-21
Proyecto 2 – Mejora del CPD	23-6-21	21-10-21
Proyecto 3 – Control de acceso	21-10-21	19-1-22
Proyecto 4 – Plan de contingencia de datos – Backups y Rest	19-1-22	19-4-22
Proyecto 5 – Monitoreo SGSI	19-4-22	18-7-22
Proyecto 6 – Concienciación sobre la importancia de la infor	18-7-22	15-11-22
Proyecto 7 – Criptografía	15-11-22	14-1-23
Proyecto 8 – Plan de clasificación de la información y tratam	14-1-23	14-4-23
Proyecto 9 – Mantenimiento, control y protección equipos ir	14-4-23	13-7-23
Proyecto 10 – Proyecto Desarrollo de software	13-7-23	11-10-23
Proyecto 11 – Plan de contingencia y continuidad de negocic	11-10-23	9-1-24
Proyecto 12 – Procedimiento Gestión de incidentes	9-1-24	8-4-24



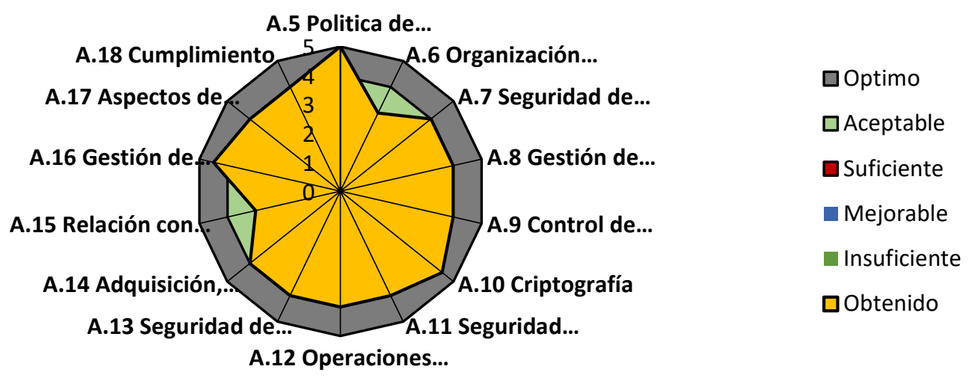
PROPUESTA DE PROYECTOS

Objetivo esperado con los proyectos

Los 12 proyectos planteados mejorarán prácticamente todos los dominios de la norma, subsanando aspectos graves y ante los cuales un eventual incidente podría ocasionar un gran perjuicio a la empresa.

ESTADO INICIAL ISO 27002:2013

CUMPLIMIENTO ESPERADO ISO 27002:2013



PROPUESTA DE PROYECTOS

Auditoría de Cumplimiento

Se evaluará la madurez de la seguridad en lo que respecta a los 14 dominios de control y los 114 controles planteados por la norma ISO/IEC 27002:2013 para cumplir con los diferentes objetivos de control.

La estimación se realizará según la tabla del Modelo de Madurez de la Capacidad (CMM).

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.

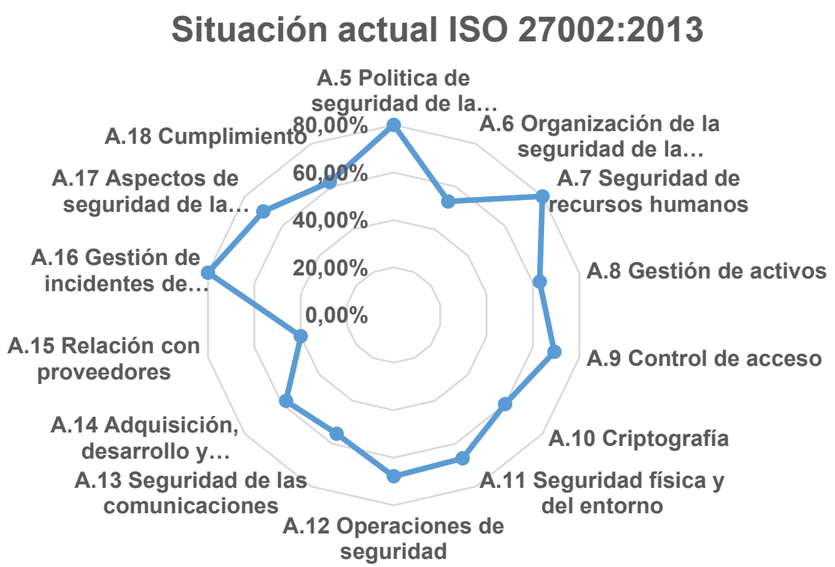
PROPUESTA DE PROYECTOS

ISO/IEC 27001:2013

SECCIÓN	DESCRIPCIÓN	ESTADO	OBSERVACIONES
4	Contexto de la organización	En cumplimiento	Se ha documentado el contexto de la organización, la identificación de necesidades, el alcance y el establecimiento del SGSI.
5	Liderazgo	En cumplimiento	La dirección se ha involucrado activamente en la creación, divulgación y documentación de las políticas de seguridad y la definición de roles y responsabilidades.
6	Planificación	En cumplimiento	Se evidencia la existencia de un plan de implementación del Sistema, objetivos de seguridad medibles y concretos.
7	Soporte	En cumplimiento	Se han determinado y proporcionado recursos para el establecimiento del SGSI. Además, se ha efectuado formación al personal para su sensibilización en relación, a la seguridad. Se mantiene información documentada de los temas de seguridad de la información.
8	Operación	En cumplimiento	Se ha evidenciado el funcionamiento del procedimiento de gestión de riesgos y la existencia de planes concretos de tratamiento de los riesgos identificados.
9	Evaluación del desempeño	En cumplimiento	Se evidencia la evaluación del desempeño del sistema mediante indicadores, monitorización, seguimiento del cumplimiento de los objetivos y la revisión de los objetivos en conjunto con la dirección para tomar las medidas adecuadas con respecto al desempeño.
10	Mejora	En cumplimiento	Existen procedimientos de revisión y mejora continua. Así como atención de las no conformidades y acciones correctivas.

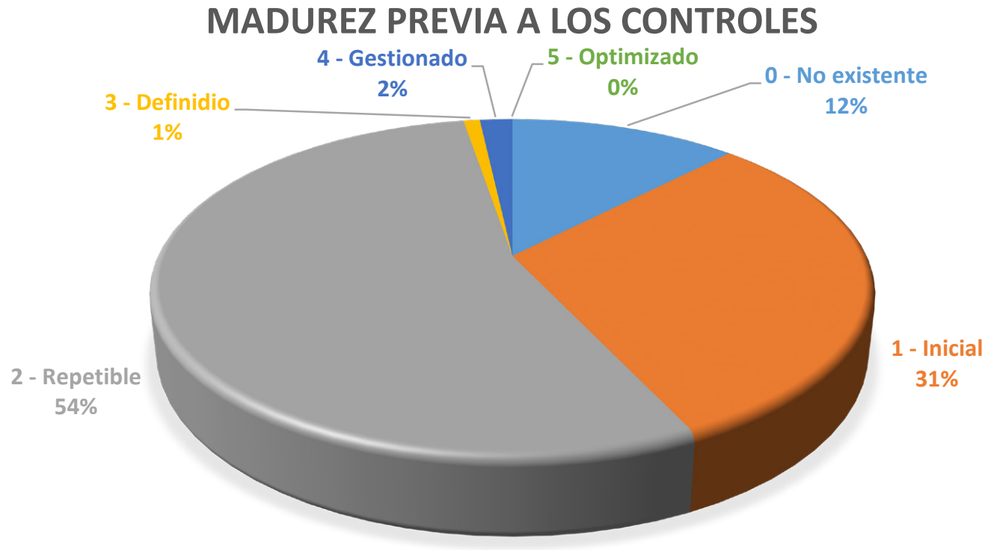
Auditoría. Resultados % madurez

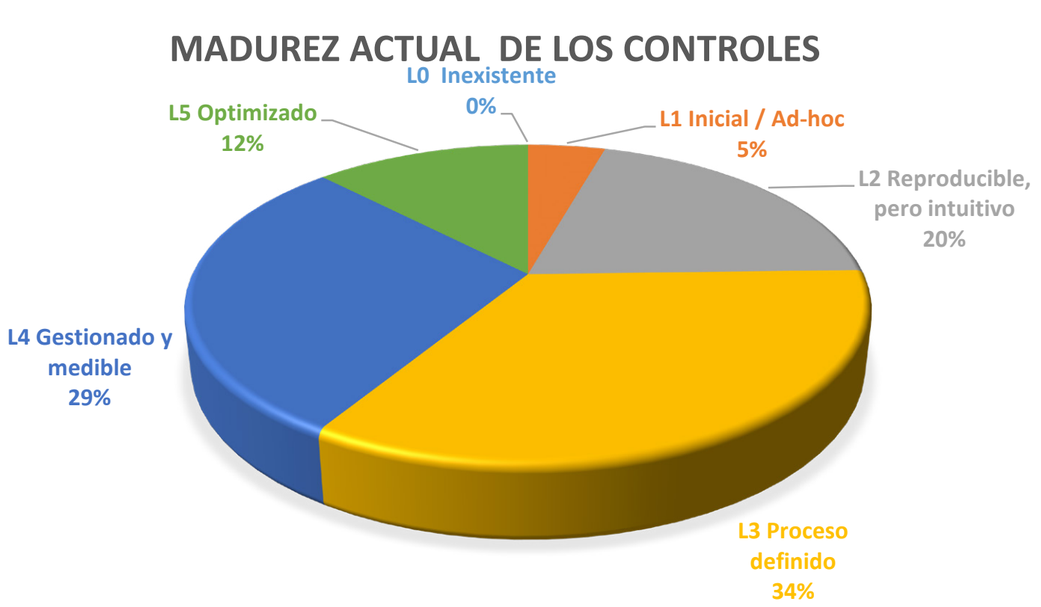
ISO/IEC 27001:2013



CONTROL	Situación actual	Objetivo	Óptimo
A.5 Política de seguridad de la información	80%	100%	100%
A.6 Organización de la seguridad de la información	53%	60%	100%
A.7 Seguridad de recursos humanos	80%	80%	100%
A.8 Gestión de activos	63%	80%	100%
A.9 Control de acceso	69,33%	80%	100%
A.10 Criptografía	60%	90%	100%
A.11 Seguridad física y del entorno	66,83%	80%	100%
A.12 Operaciones de seguridad	67,76%	80%	100%
A.13 Seguridad de las comunicaciones	55,33%	80%	100%
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	57,85%	80%	100%
A.15 Relación con proveedores	40%	60%	100%
A.16 Gestión de incidentes de seguridad de la información	80%	90%	100%
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	70%	80%	100%
A.18 Cumplimiento	62%	80%	100%

Auditoría. Comparativa madurez.





Conclusiones

La ejecución del presente proyecto supone una mejora en el nivel de madurez de seguridad de la información en la compañía. Se ha tomado conciencia sobre la importancia de los sistemas de gestión de la seguridad, para garantizar el tratamiento y seguridad de la información, hacer la empresa más competitiva tanto a nivel nacional como internacional, cumplir con la normativa legal y ofrecer una imagen de buenas prácticas a clientes y proveedores.

Se ha efectuado un análisis real de la empresa, en base a la norma ISO 27001:2013, identificando potenciales riesgos que afecten a la organización, estableciendo la estrategia a tomar para cada uno de ellos, ya sea asumir, traspasar a terceros o gestionar el riesgo. Así como una serie de proyectos para resolver los problemas de seguridad.

Mediante la mejora continua se seguirá trabajando para mantener el nivel de madurez en aquellos dominios que cumplen con los requisitos de la norma y alcanzar un nivel de madurez lo más óptimo posible del resto. Se seguirá trabajando en la toma de conciencia por parte de los empleados sobre la importancia de la seguridad, como elemento clave para la consecución de los objetivos de la compañía y permitir el crecimiento de esta acorde a las estrategias definidas por la dirección.

Máster Universitario Ciberseguridad y Privacidad (MUCIP)

¡MUCHAS GRACIAS!

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

Trabajo Fin de Máster (TFM)

Natividad García Lacárcel