PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 EN LA EMPRESA GESPA

Master interuniversitario en seguridad de las TIC

Alumno: José Francisco Romano Herrera
Director: Antonio José Segovia Henares

Fecha de entrega: Junio 2019

CONTENIDO:

- *1. INTRODUCCIÓN*
- *2. FASES DEL TRABAJOS*

FASE 1 *- Situación inicial de la seguridad de Gespa: contextualización, objetivos y análisis diferencial*

FASE 2 *– Sistema de Gestión Documental*

FASE 3 *- Análisis de riesgos*

FASE 4 *– Propuesta de Proyectos*

FASE 5 *– Auditoría de cumplimiento*

- *3. CONCLUSIONES*

INTRODUCCIÓN:

- *La información es un activo importante de cualquier empresa.*
- *Aparece un nuevo concepto de protección de la información.*
- *La seguridad no se puede improvisar*
  - ✓ ***Implantación de un SGSI***
  - ✓ ***ISO 27001:2013 e ISO 27002***
- *Creación del Plan Director de Seguridad, una vez decidido el estándar.*

INTRODUCCIÓN:

- *Por parte de la dirección de Gespa se plantea la necesidad de **obtener la certificación** de la **ISO 27001** con el fin de:*
  - *Poder **acceder** a ciertos **concursos públicos** que requieren dicha certificación.*
  - ***Aumentar la seguridad de la información** que se genera, maneja, almacena y transmite en la empresa.*

- *Con la obtención de la certificación, se puede acceder a proyectos de instalación de sistemas de control en emplazamientos sujetos a requisitos legales de infraestructuras críticas.*

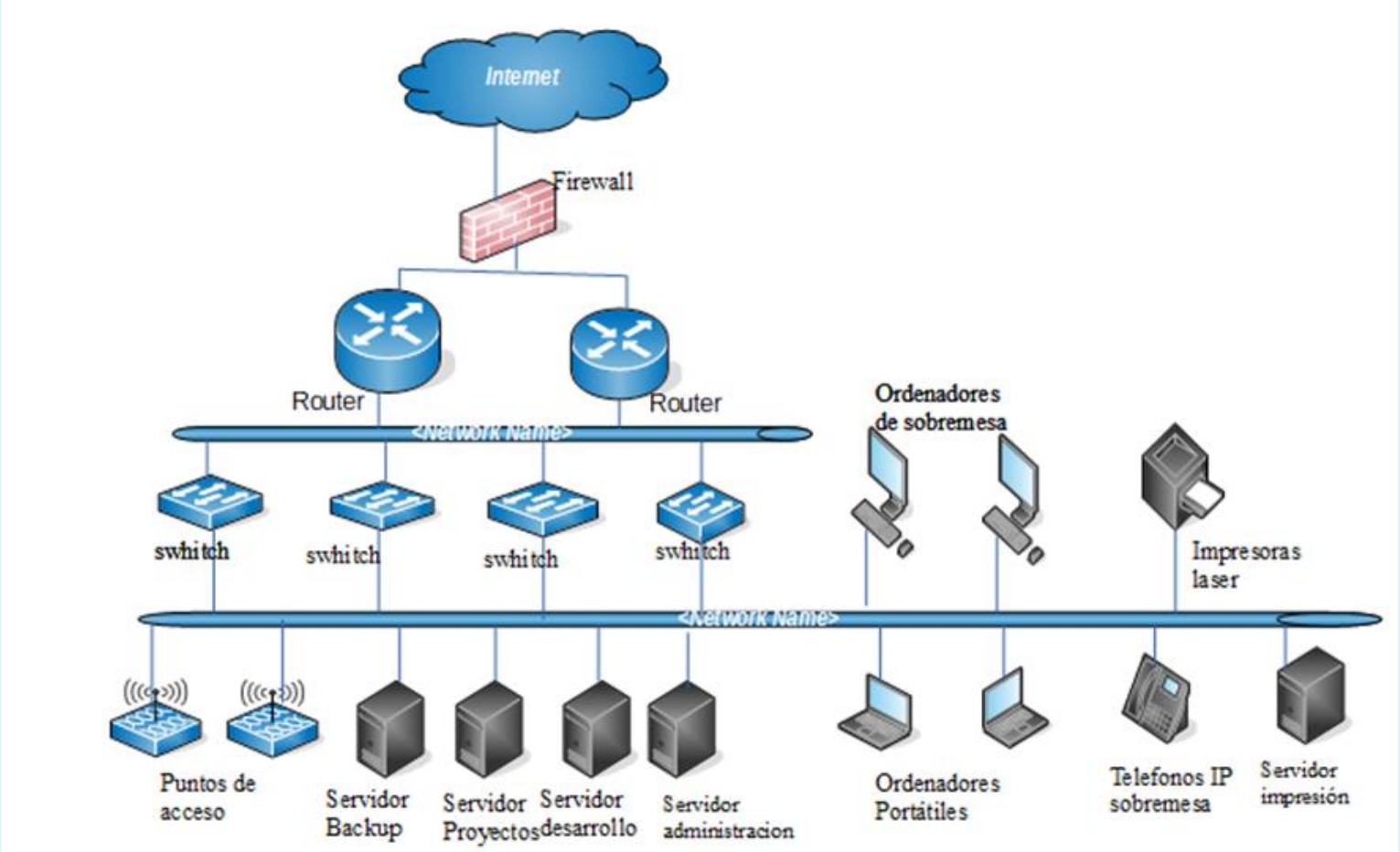
FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***1.1. Descripción contextual:***
  - *Empresa ubicada en Madrid*
  - *Dedicada a la fabricación, instalación, puesta en servicio y mantenimiento de sistema de control industrial*
  - *Tiene 115 empleados (70% ingenieros)*
  - *Dispone de seguridad física perimetral, control de accesos y vigilancia*
  - *Se accede al edificio por un solo punto.*
  - *Acceso restringido al CPD, que tiene control de accesos y elementos auxiliares.*
  - *En la planta baja se encuentra el departamento de montajes, fabricación y pruebas*

FASES DEL TRABAJOS – FASE 1

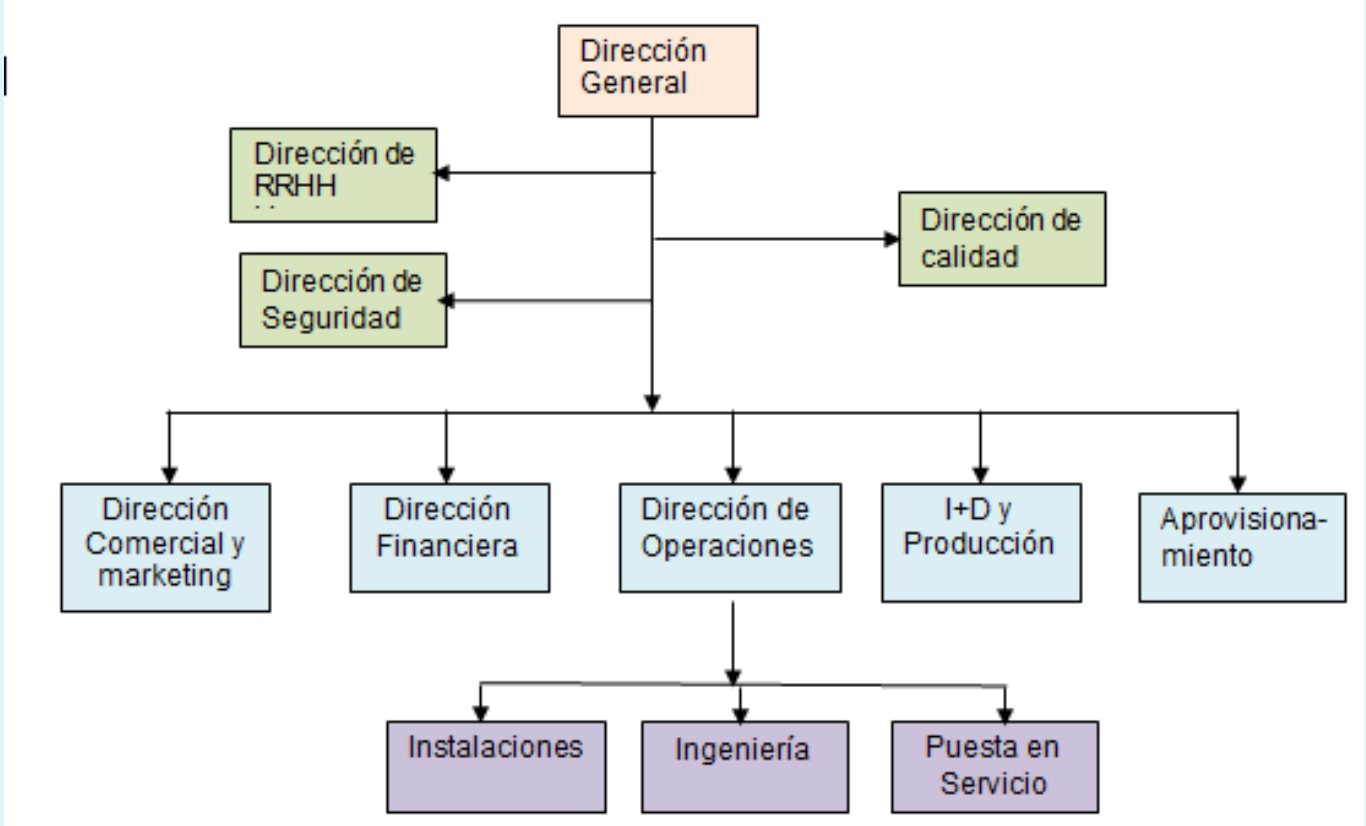
- ***1. Situación inicial de la seguridad de Gespa:***
- ***1.1. Descripción contextual:***
  - *Los empleados disponen de equipos de sobremesa o portátiles con Windows 7 o Windows 10 y las aplicaciones de ofimática, navegador Explorer y Firefox, antivirus Kaspersky, Acrobat reader y el software de gestión necesario.*
  - *No existe control sobre la conexión de dispositivos USB*
  -

FASES DEL TRABAJOS – FASE 1



FASES DEL TRABAJOS – FASE 1

- Organigrama de Gespa



FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***1.2. Objetivos:***
  - ***Generales:***

el aumento de la seguridad de los sistemas de información de la empresa

la obtención de la certificación de acuerdo a la norma ISO 27001:2013

Específicos:

- *Conseguir mayor conciencia de seguridad de los empleados.*
- *Aumento de los niveles de seguridad (confidencialidad, disponibilidad e integridad)*
- *Conseguir mayor nivel de confianza de los clientes en nuestro sistema TIC.*
- *Reducir los incidentes de seguridad como son el robo o pérdida, de información o dispositivos.*
- *Obtener la certificación de la ISO 27001 para poder optar a ciertos proyectos.*
- *Aumento de la seguridad la transmisión de información y de las comunicaciones*

FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***1.3. Análisis diferencial:***
  - *Nos permite conocer el grado de cumplimiento de nuestro sistema de seguridad de la información con relación a la ISO/IEC 27001:2013 y la ISO/IEC 27002*
  - *Representación gráfica de los resultados*

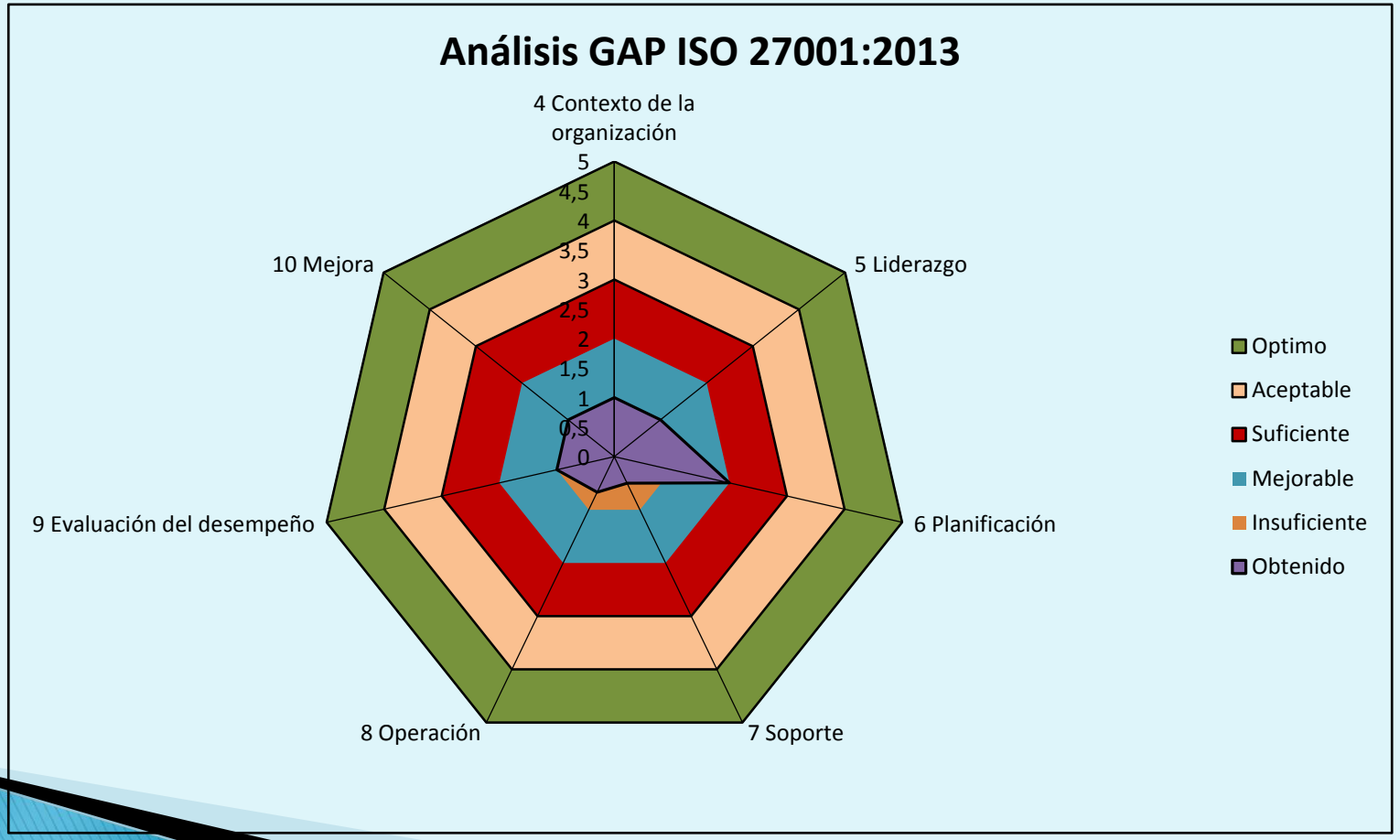
FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***Análisis diferencial con respecto a la ISO/IEC 27001:2003***

	Requerimientos ISO 27001	Evaluación	Valor	Total
4	**Contexto de la organización**			1
4.1	Comprensión de la organización y de su contexto	2 - Repetible	2	2
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	2 - Repetible	2	2
4.3	Determinación del alcance del SGSI	0 - No existente	0	0
4.4	SGSI	0 - No existente	0	0
5	**Liderazgo**			1
5.1	Liderazgo y compromiso	1 - Inicial	1	1
5.2	Política	0 - No existente	0	0
5.3	Roles, responsabilidades y autoridades en la organización	2 - Repetible	2	2
6	**Planificación**			2
6.1	Acciones para tratar los riesgos y oportunidades	2 - Repetible	2	2
6.2	Objetivos de seguridad de la información y planificación para su consecución	2 - Repetible	2	2
7	**Soporte**			0,5
7.1	Recursos	0 - No existente	0	0

FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***Análisis diferencial con respecto a la ISO/IEC 27001:2013***



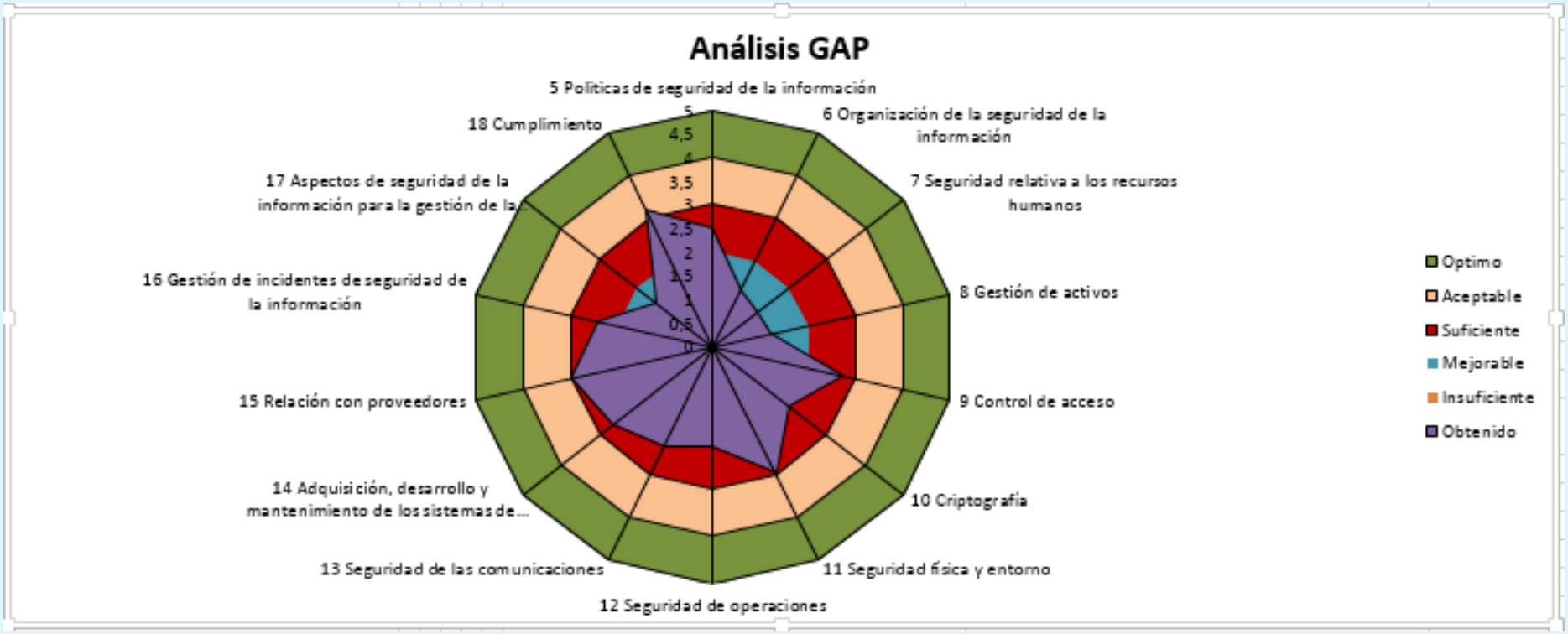
FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***Análisis diferencial con respecto a la ISO/IEC 27002***
  -

CONTROL			Evaluación	Valor	Total
liticas de seguridad de la información					2,5
5.1 Directrices de gestión de la seguridad de la información					2,5
	5.1.1	Políticas para la seguridad de la información	3 - Definido	3	
	5.1.2	Revisión de las políticas para la seguridad de la información	2 - Repetible	2	
ganización de la seguridad de la información					1,3
6.1 Organización interna					1,6
	6.1.1	Roles y responsabilidades en seguridad de la información	3 - Definido	3	
	6.1.2	Segregación de tareas	2 - Repetible	2	
	6.1.3	Contacto con las autoridades	2 - Repetible	2	
	6.1.4	Contacto con grupos de interés especial	1 - Inicial	1	
	6.1.5	Seguridad de la información en la gestión de proyectos	0 - No existente	0	
6.2 Dispositivos móviles y el teletrabajo					1
	6.2.1	Política de dispositivos móviles	1 - Inicial	1	
	6.2.2	Teletrabajo	1 - Inicial	1	
guridad relativa a los recursos humanos					1,16667
7.1 Antes del empleo					1,5

FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
- ***Análisis diferencial con respecto a la ISO/IEC 27002***
  -



FASES DEL TRABAJOS – FASE 1

- ***1. Situación inicial de la seguridad de Gespa:***
  - ***Conclusiones:***

  - *El sistema en líneas generales se encuentra en unos niveles relativamente aceptables de seguridad.*

FASES DEL TRABAJOS – FASE 2: Sistema de Gestión documental

- *Define el conjunto de documentos necesarios para cumplir con la norma ISO 27001.*
- ***Documentación generada en este trabajo***
  - *Política de Seguridad*
  - *Procedimiento de Auditorías Internas*
  - *Gestión de Indicadores.*
  - *Procedimiento Revisión por la Dirección.*
  - *Gestión de Roles y Responsabilidades.*
  - *Metodología de Análisis de Riesgos.*
  - *Declaración de Aplicabilidad*

FASES DEL TRABAJOS – FASE 2: Sistema de Gestión documental

- ***Política de Seguridad:*** *Documento breve de alto nivel que detalla el principal objetivo del SGSI*

- ***Procedimiento de Auditorías Internas:*** *Documento que sirve de base para llevar a cabo la auditoría de primera parte que la compañía.*

- ***Gestión de Indicadores****. Documento que recoge los indicadores que se usarán para realizar la medición, con fórmula utilizada, valor nominal, valor real obtenido y frecuencia con que se realizará la medición.*

- ***Procedimiento Revisión por la Dirección****. Documento que establece la forma en que la dirección revisará el SGSI*

FASES DEL TRABAJOS – FASE 2: Sistema de Gestión documental

- ***Gestión de Roles y Responsabilidades***. *Documento que recoge los roles y responsabilidades con respecto a la seguridad de la información.*

- ***Metodología de Análisis de Riesgos***. *Documento que recoge la metodología a seguir para el análisis de riesgos.*
  - *Magerit v 3*

- ***Declaración de Aplicabilidad*** *Documento clave dentro del Sistema de Gestión de la Seguridad de la Información que recogen los controles del Anexo A que son aplicables a nuestra empresa.*

FASES DEL TRABAJOS – FASE 3: Análisis de riesgos

- Para poder proteger cualquier activo, lo primero que hay que **determinar** son **los activos, su valor** y **las amenazas** a las que se encuentra expuesto.

- El análisis de riesgos se ha realizado desde las cinco dimensiones de seguridad que establece la metodología Magerit:
  - Disponibilidad
  - Autenticidad
  - Integridad
  - Confidencialidad
  - Trazabilidad

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Inventario de activos:***
- **Los activos esenciales de Gespa son la información y los servicios:**

  - El servicio de Desarrollo
  - El servicio de Instalación
  - El servicio de Puesta en servicio
  - El servicio de Mantenimiento

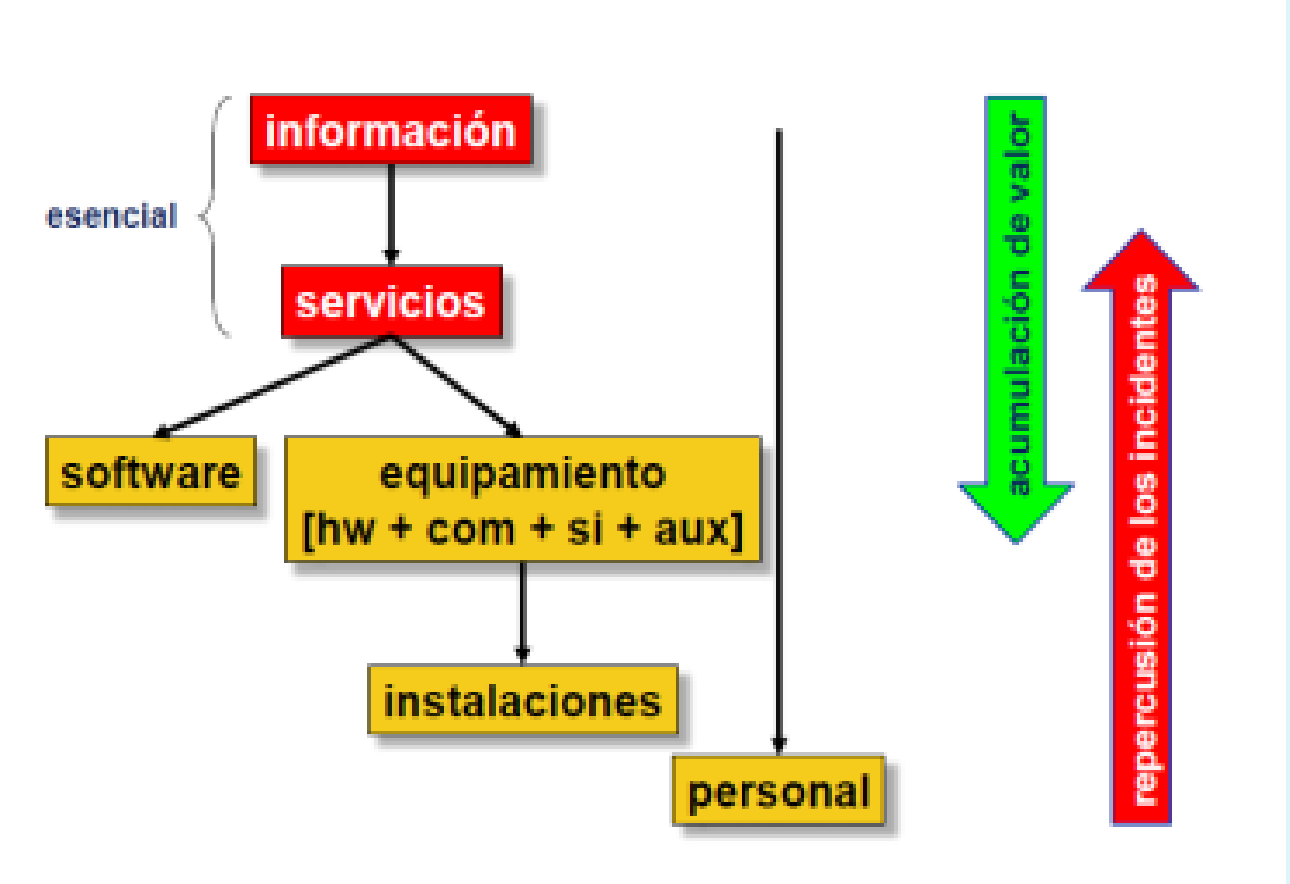
FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Inventario de activos:***
- **Los activos de soporte son los correspondiente a los siguientes ámbitos:**

Ambito
[L] Instalaciones
[HW] Equipamiento hardware
[SW] Aplicaciones
[D] Datos
[COM] Red de comunicaciones
[SS] Servicios subcontratados
[AUX] Equipamiento Auxiliar
[P] Personal

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Inventario de activos:***



FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Valoración de activos:***

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.

Escala de valoración

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Valoración de activos:***

Ámbito	Código	Activo	Valor	[A]	[C]	[I]	[D]	[T]
[L] Instalaciones								
	L.01	CPD	**MA**	7	7		9	
	L.02	Edificio	**A**				9	
[HW] Equipamiento hardware								
	HW.01	Pc portátiles	**B**	7	8	5	4	8
	HW.02	Pc de sobremesa	**B**	7	6	5	4	8
	HW.03	Servidor de proyectos	**A**	9	8	8	9	8
	HW.04	Servidor de desarrollo	**A**	7	8	8	8	8
	HW.05	Servidor de administración	**A**	7	8	8	8	8
	HW.06	Servidor de impresión	**B**				7	3
	HW.07	Teléfonos móviles	**B**	3	9	8	5	5
	HW.08	Teléfonos de sobremesa	**B**		5		3	
	HW.09	Routers	**A**	8	7	9	9	7
	HW.10	Switches	**M**	5	6	7	8	6

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Análisis de amenazas:***

- Las amenazas con la metodología Magerit se clasifican en los siguientes bloques:

-
- • Desastres naturales
- • De origen industrial
- • Errores y fallos no intencionados
- • Ataques intencionados

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Análisis de amenazas:***
- **Tabla de impacto**

Impacto	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

- **Tabla de frecuencia**

Valor	Nivel	Descripción
100	Muy frecuente	A diario
10	Frecuente	Una vez al mes
1	Normal	Una vez al año
0,1	Poco frecuente	Cada varios años

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Análisis de amenazas:***

- ***Impacto potencial = valor del activo x impacto***

- *En el cálculo del impacto potencial no se tiene en cuenta la aplicación de salvaguardas*

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Impacto potencial:***

			valoración					impacto					impacto potencial				
Ámbito	**Código**	**Activo**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones																	
	L.01	CPD	7	7		9			100%	100%	100%		7,0	7,0		9,0	
	L.02	Edificio				9					100%					9,0	
[HW] Equipamiento hardware																	
	HW.01	Pc portátiles	7	8	5	4	8	75%	100%	100%	100%		5,3	8,0	5,0	4,0	0,0
	HW.02	Pc de sobremesa	7	6	5	4	8	100%	100%	100%	100%		7,0	6,0	5,0	4,0	0,0
	HW.03	Servidor de proyectos	9	8	8	9	8	100%	100%	100%	100%		9,0	8,0	8,0	9,0	0,0
	HW.04	Servidor de desarrollo	7	8	8	8	8	100%	100%	100%	100%		7,0	8,0	8,0	8,0	0,0
	HW.05	Servidor de administración	7	8	8	8	8	100%	100%	100%	100%		7,0	8,0	8,0	8,0	0,0
	HW.06	Servidor de impresión				7	3	50%	75%	75%	75%		0,0	0,0	0,0	5,3	0,0
	HW.07	Routers	8	7	9	9	7		100%	100%	100%		0,0	7,0	9,0	9,0	0,0
	HW.10	Switches	5	6	7	8	6				100%		0,0	0,0	0,0	8,0	0,0

- ***Nivel de riesgo:***
- El nivel de riesgo de los activos se calcula mediante la siguiente fórmula:
  - ***Nivel de Riesgo*** = *Impacto Potencial x Frecuencia*

- Nuestro nivel máximo de riesgo es 90, por lo que nuestra escala de riesgos es:

NIVEL DE RIESGO	RANGO DE VALORES
Alto	75 =< Riesgo
Medio – alto	50<= Riesgo <75
Medio – bajo	25 =< Riesgo <50
Bajo	Riesgo <25

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- ***Nivel de riesgo aceptable:*** *Máximo nivel de riesgo aceptado por la empresa sin tener que aplicar salvaguardas*

- ***Nivel de riesgo residual:*** *Es el nivel de riesgo que queda tras aplicar las salvaguardas*

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- *Matriz de riesgos:*

f	100	100	200	300	400	500	600	700	800	900
r	10	10	20	30	40	50	60	70	80	90
e	9	9	18	27	36	45	54	63	72	81
c	8	8	16	24	32	40	48	56	64	72
u	7	7	14	21	28	35	42	49	56	63
e	6	6	12	18	24	30	36	42	48	54
n	5	5	10	15	20	25	30	35	40	45
c	4	4	8	12	16	20	24	28	32	36
i	3	3	6	9	12	15	18	21	24	27
a	2	2	4	6	8	10	12	14	16	18
	1	1	2	3	4	5	6	7	8	9
	0,1	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
		1	2	3	4	5	6	7	8	9
Impacto										

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- *Matriz de riesgos:*

				impacto potencial						Riesgo				
Ambito	Código	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]
[L] Instalaciones														
	L.01	CPD	**0,1**	7,0	7,0		9,0			0,7	0,7	0,0	0,9	0,0
	L.02	Edificio	**0,1**				9,0			0,0	0,0	0,0	0,9	0,0
[HW] Equipamiento hardware														
	HW.01	Pc portátiles	**10**	5,3	8,0	5,0	4,0	0,0		52,5	80,0	50,0	40,0	0,0
	HW.02	Pc de sobremesa	**10**	7,0	6,0	5,0	4,0	0,0		70,0	60,0	50,0	40,0	0,0
	HW.03	Servidor de proyectos	**10**	9,0	8,0	8,0	9,0	0,0		90,0	80,0	80,0	90,0	0,0
	HW.04	Servidor de desarrollo	**10**	7,0	8,0	8,0	8,0	0,0		70,0	80,0	80,0	80,0	0,0

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- *Activos con nivel alto de riesgo:*

Ambito	Código	Activo
[HW] Equipamiento hardware		
	HW.01	Pc portátiles
	HW.03	Servidor de proyectos
	HW.04	Servidor de desarrollo
	HW.05	Servidor de administración
[SW] Aplicaciones		
	SW.01	Sistemas operativos
	SW.03	Aplicaciones ofimáticas.
	SW.05	Software de gestión de proyectos
	SW.06	Software de desarrollo
	SW.07	Aplicación financiera
[D] Datos		
	D.01	Datos de clientes
	D.02	Datos de proyectos
	D.03	Datos de desarrollo
	D.04	Datos de emails
	D.05	Datos personales

FASES DEL TRABAJOS – FASE 3- Análisis de riesgos

- *Activos con nivel medio de riesgo:*

Ambito	Código	Activo
[HW] Equipamiento hardware		
	HW.02	Pc de sobremesa
	HW.06	Servidor de impresión

FASES DEL TRABAJOS – FASE 4– Propuesta de proyectos

- *- Es momento de decidir el plan de acción.*

- *- El objetivo es intentar reducir los niveles de riesgos a los que nos encontramos sometidos.*

- *Hay que mejorar en sectores como el equipamiento hardware, las aplicaciones y los datos, por lo que serán en esa dirección donde se encaminen los esfuerzos de mejora.*

- *Según el estudio realizado, los activos con un nivel alto o medio-alto de riego corresponden al grupo de [HW] Equipamiento hardware, [SW] Aplicaciones y [D] Datos.*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *Los proyectos propuestos son:*

PROYECTO	DESCRIPCIÓN
PRT01	Elaboración de la política de seguridad
PRT02	Revisión de los procedimientos operativos
PRT03	Plan de formación de empleados
PRT04	Implantación de un sistema de cifrado global
PRT05	Implantación de un sistema antimalware
PRT06	Procedimiento de uso de dispositivos móviles
PRT07	Procedimiento de copias de seguridad
PRT08	Elaboración del Inventario, clasificación y etiquetado de activos
PRT09	Elaboración de plantilla para contratos base con terceros
PRT10	Seguridad relativa a los recursos humanos
PRT11	Análisis de vulnerabilidades

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT01: Elaboración de la política de seguridad*
- ***Descripción:*** *Documento donde se recogen los principales objetivos del SGSI. Por regla general es un documento de alto nivel y relativamente breve en extensión.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[L] Instalaciones*
  - *[HW] Equipamiento hardware*
  - *[SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
  - *[SS] Servicios subcontratados*
  - *[AUX] Equipamiento Auxiliar*
  - *[P] Personal*
- ***Dominios y/o Controles afectados:***
  - *5.1.1 Políticas para la seguridad de la información*
  - *5.1.2 Revisión de las políticas para la seguridad de la información*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT02: Revisión de los procedimientos operativos*
- ***Descripción:*** *Revisar los procedimientos para reducir los errores durante la operación.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *SS] Servicios subcontratados*
  - *[P] Personal*
- ***Dominios y/o Controles afectados:***
  - *7.2.2 Concienciación, educación y capacitación en seguridad de la información.*
  - *12.1.1 Documentación de procedimientos de operación*
- ***Amenazas:***
  - *[E.1] Errores de los usuarios*
  - *[E.2] Errores del administrador.*
  - *[E.4] Errores de configuración*
  - *[E.21] Errores de mantenimiento / actualización de programas (software).*
  - *[E.23] Errores de mantenimiento / actualización de equipos (hardware).*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT03: Plan de formación de los empleados*
- ***Descripción:*** *Elaborar un plan de formación para paliar las deficiencias en materia de seguridad de la información.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *SS] Servicios subcontratados*
  - *[P] Personal*
- ***Dominios y/o Controles afectados:***
  - *7.2.2 Concienciación, educación y capacitación en seguridad de la información.*
- ***Amenazas:***
  - *[E.1] Errores de los usuarios*
  - *[E.2] Errores del administrador.*
  - *[E.4] Errores de configuración*
  - *[E.21] Errores de mantenimiento / actualización de programas (software).*
  - *[E.23] Errores de mantenimiento / actualización de equipos (hardware).*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT04: Implantación de un sistema de cifra global.*
- ***Descripción:*** *La finalidad última del proyecto es la de dotar al sistema de unas medidas de seguridad que garantice la integridad, confidencialidad, trazabilidad y autenticidad de la información.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
- ***Dominios y/o Controles afectados:***
  - *8.1.3 Uso aceptable de los activos*
  - *8.3.1 Gestión de soportes extraíbles*
  - *9.1.1 Política de control de acceso*
  - *9.1.2 Acceso a las redes y los servidores de red*
  - *10.1.1 Política de uso de los controles criptográficos*
  - *10.1.2 Gestión de claves*
  - *13.1.1 Controles de red*
  - *13.1.2 Seguridad de los servidores de red*
  - *18.1.3 Protección de los registros de la organización*
  - *18.1.4 Protección y privacidad de la información de carácter personal*
  - *18.1.5 Regulación de los controles criptográficos.*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT05: Implantación de un sistema antimalware.*
- ***Descripción:*** *La finalidad última del proyecto es la de investigar los posibles productos del mercado que se adapten a nuestra actividad, así como decidir el más adecuado*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[HW] Equipamiento hardware*
  - *[SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
- ***Dominios y/o Controles afectados:***
  - *9.4.1 Restricción del acceso no autorizado a los sistemas y aplicaciones*
  - *12.2.1 Controles contra el código malicioso*
  - *12.6.1 Gestión de las vulnerabilidades técnicas*
  - *13.1.2 Seguridad de los servidores de red*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT06: Procedimiento de uso de los dispositivos móviles.*
- ***Descripción:*** *La finalidad última del proyecto es procedimentar el uso que se puede hacer de los dispositivos móviles de la empresa, dado que es uno de los puntos débiles de la seguridad de la información.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[HW01] Ordenadores portátiles*
  - *[HW08] Teléfonos móviles*
  - *[SS.01] Correo electrónico*
  - *[SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
- ***Dominios y/o Controles afectados:***
  - *8.1.1 Inventario de activos*
  - *8.1.2 Propietario de los activos*
  - *6.2.1 Política de dispositivos móviles*
  - *6.2.2 Teletrabajo*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT07: Procedimiento de copias de seguridad.*
- ***Descripción:*** *Con el procedimiento de copias de seguridad se intenta marcar las pautas a seguir para la realización de las copias de la información de la compañía.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[SW] Aplicaciones*
  - *[D] Datos*
- ***Dominios y/o Controles afectados:***
  - *12.3.1 Copias de seguridad de la información*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT08: Elaboración del inventario, clasificación y etiquetado de activos*
- ***Descripción:*** *La finalidad del proyecto es la de solventar las deficiencias encontradas durante la auditoría.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[L] Instalaciones*
  - *[HW] Equipamiento hardware*
  - *[SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
  - *[SS] Servicios subcontratados*
  - *[AUX] Equipamiento Auxiliar*
- ***Dominios y/o Controles afectados:***
  - *8.1.1 Inventario de activos*
  - *8.1.2 Propietario de los activos*
  - *8.2.1 Clasificación de la información*
  - *8.2.2 Etiquetado de la información*
  - *8.2.3 Manipulación de la información*
  - *8.3.1 Gestión de soportes extraíbles*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT09: Elaboración la plantilla para los contratos base con terceros*
- ***Descripción:*** *El proyecto tiene como objetivo el preparar unas cláusulas con los requisitos generales que sean de aplicación a las distintas empresas subcontratistas y que formarán parte del clausulado general de todos los contratos*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[SS] Servicios subcontratados*
- ***Dominios y/o Controles afectados:***
  - *15.1.1 Política de seguridad de la información en las relaciones con los proveedores*
  - *15.1.2 Requisitos de seguridad en contratos con terceros*
  - *15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *PRT10: Seguridad relativa a los recursos humanos.*
- ***Descripción:*** *El proyecto tiene como objetivo la creación de un documento con las clausulas tipo que se incluirán en los contratos que se lleven a cabo para la incorporación de personal, independientemente de la modalidad de contrato (temporal, fijo, en prácticas etc.) y del personal subcontratado*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[P] Personal*
- ***Dominios y/o Controles afectados:***
  - *7.1.1 Investigación de antecedentes*
  - *7.1.2 Términos y condiciones del empleo*
  - *7.2.1 Responsabilidades de gestión*
  - *7.2.2 Concienciación, educación y capacitación en seguridad de la información*
  - *7.2.3 Proceso disciplinario*

FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

PRT11: Análisis de vulnerabilidades

- ***Descripción:*** *Dado que en la empresa no disponemos de los medios ni de los especialistas adecuados para llevar a cabo este análisis de vulnerabilidades (hacking ético), es necesario contratar estos servicios a través de un proveedor externo.*
- ***Tipo de activos involucrados****: Los activos afectados son:*
  - *[HW] Equipamiento hardware*
  - *[SW] Aplicaciones*
  - *[D] Datos*
  - *[COM] Red de comunicaciones*
  - *[SS] Servicios subcontratados*
- ***Dominios y/o Controles afectados:***
  - *12.6.1 Gestión de las vulnerabilidades técnicas*
  - *12.6.2 Restricción en la instalación del software*
  - *13.2.3 Mensajería electrónica*

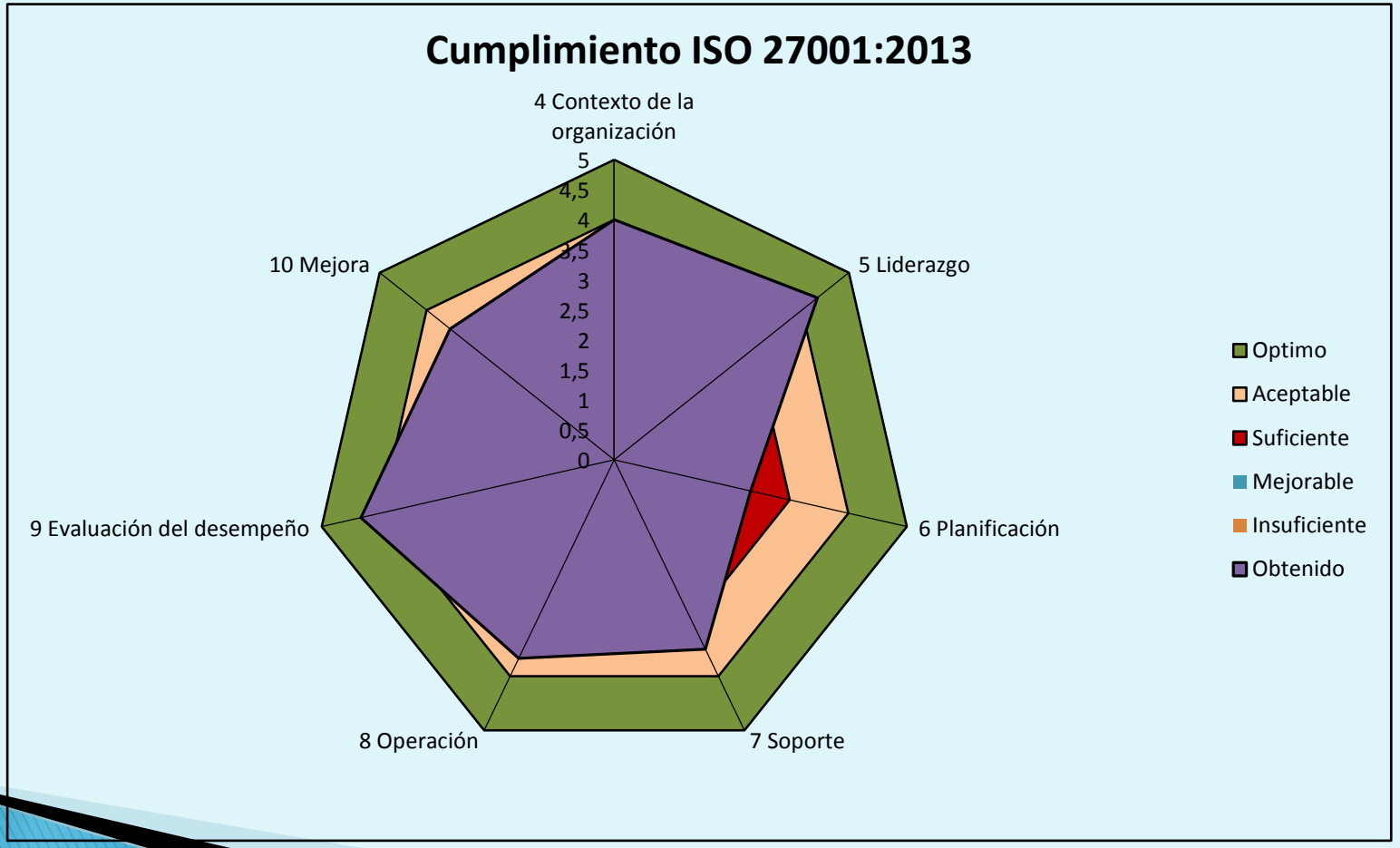
FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *Resultados:*
- *Se ha conseguido mejorar la seguridad de la compañía.*

- *Para ver la evolución sufrida, se presenta un nuevo análisis diferencial y un nuevo análisis de riesgos.*

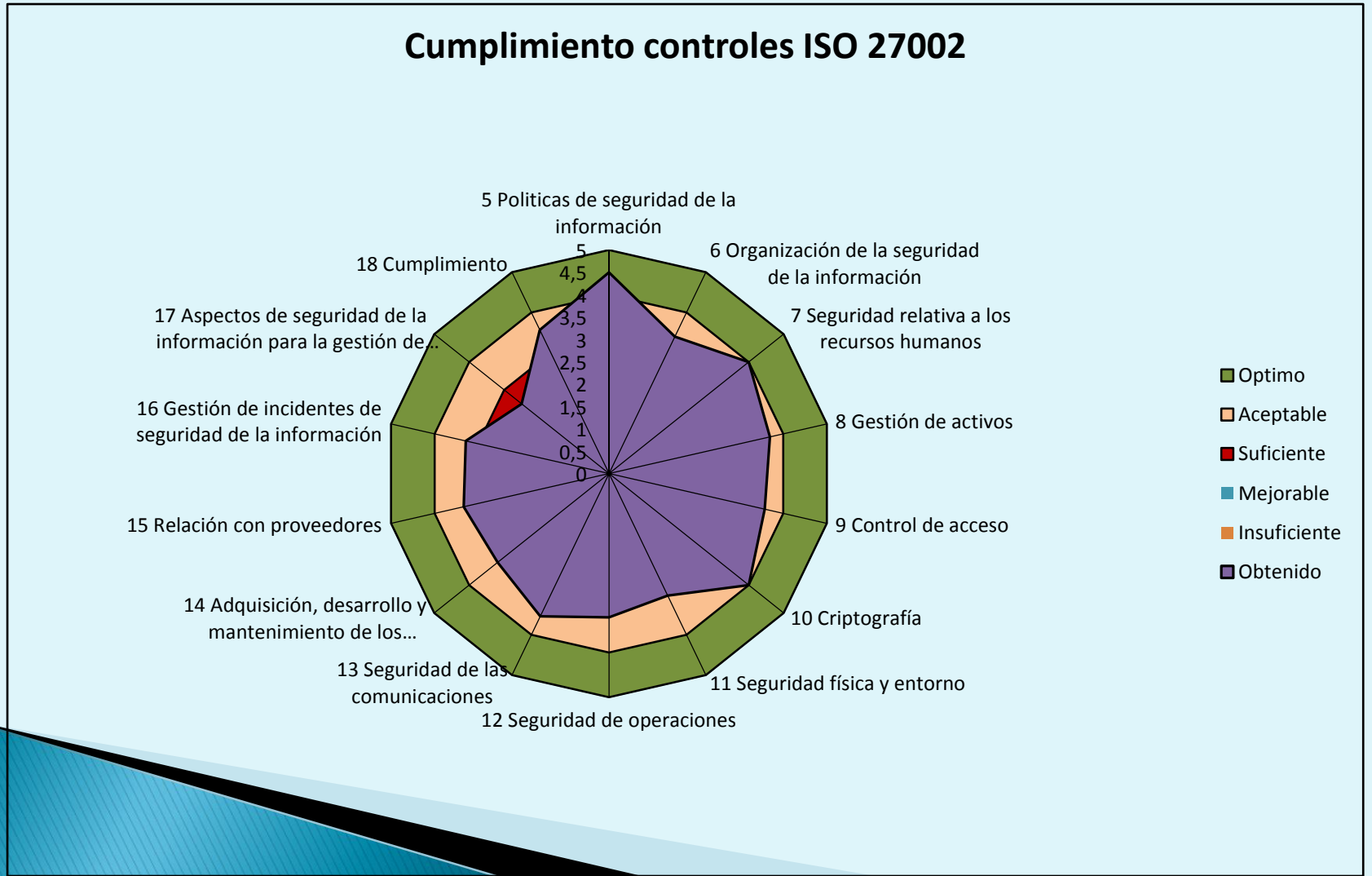
FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *Diagrama después de ejecutar los proyectos*



FASES DEL TRABAJOS – FASE4 – Propuesta de proyectos

- *Diagrama después de ejecutar los proyectos*



FASES DEL TRABAJOS – FASE5 – Auditoría de cumplimiento

- *Llegados a este punto es necesario realizar una auditoría cuyo objetivo es el de determinar el grado de cumplimiento de la compañía con respecto a las buenas prácticas en materia de seguridad*

- *Para ver el grado de cumplimiento de los 114 controles y 14 dominios recogidos en la ISO 27002, se determinará su nivel de madurez en base a los niveles definidos por CMM y que se recogen en la tabla siguiente.*

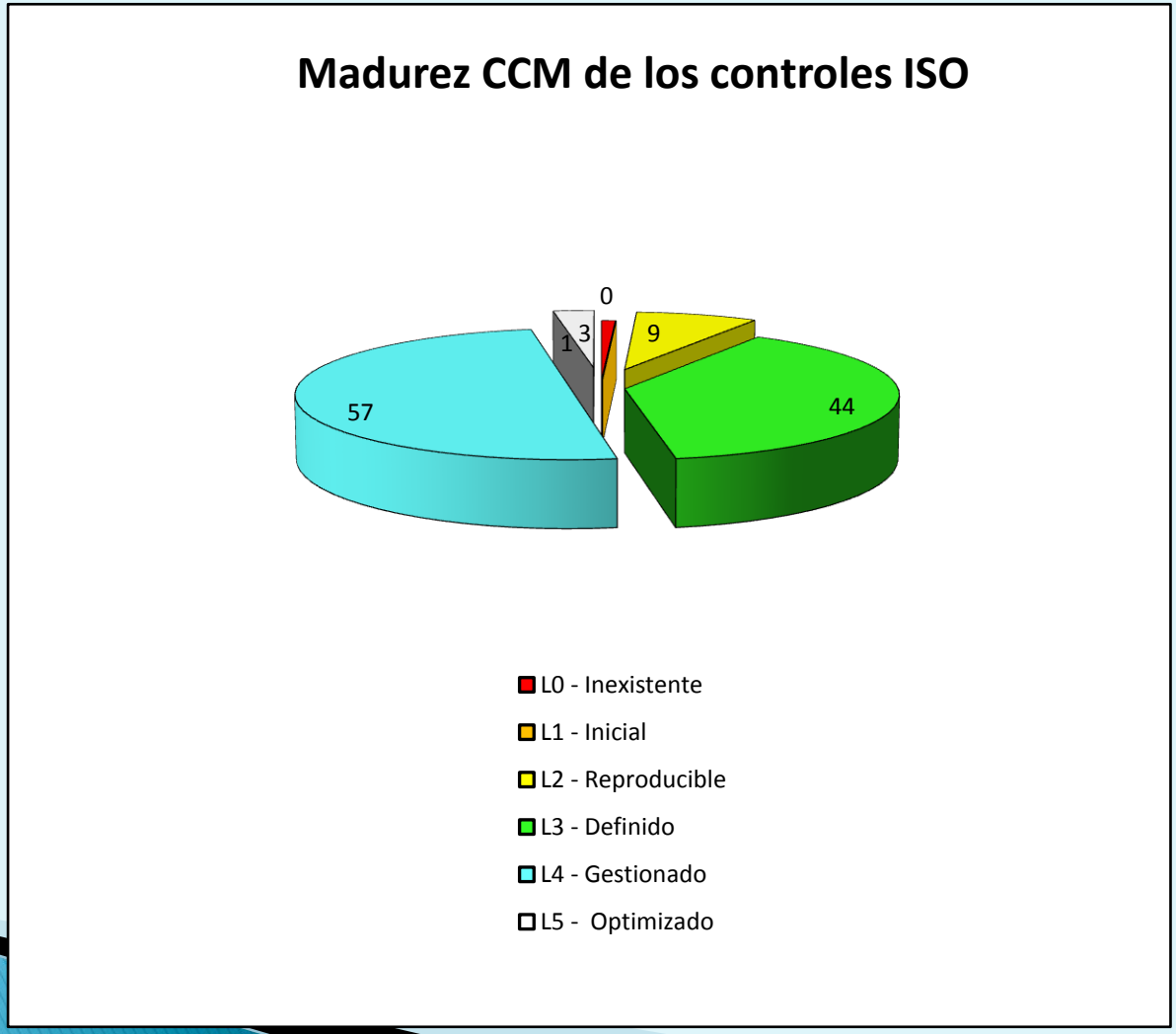
FASES DEL TRABAJOS – FASE5 – Auditoría de cumplimiento

- Criterios para la evaluación de los niveles de madurez

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 caca 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.

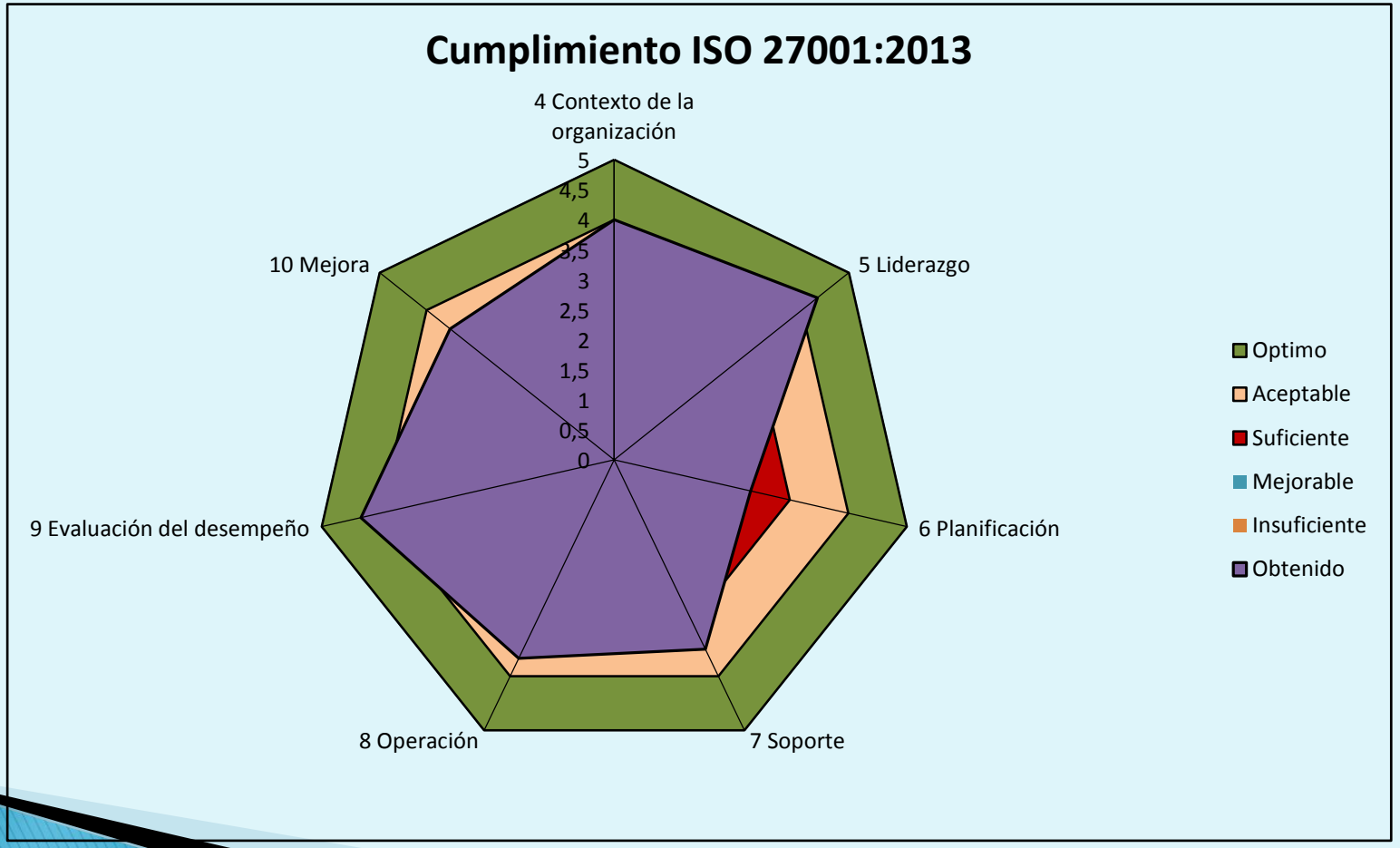
FASES DEL TRABAJOS – FASE5 – Auditoría de cumplimiento

- Representación de la madurez de los controles ISO una vez realizada la auditoría de cumplimiento



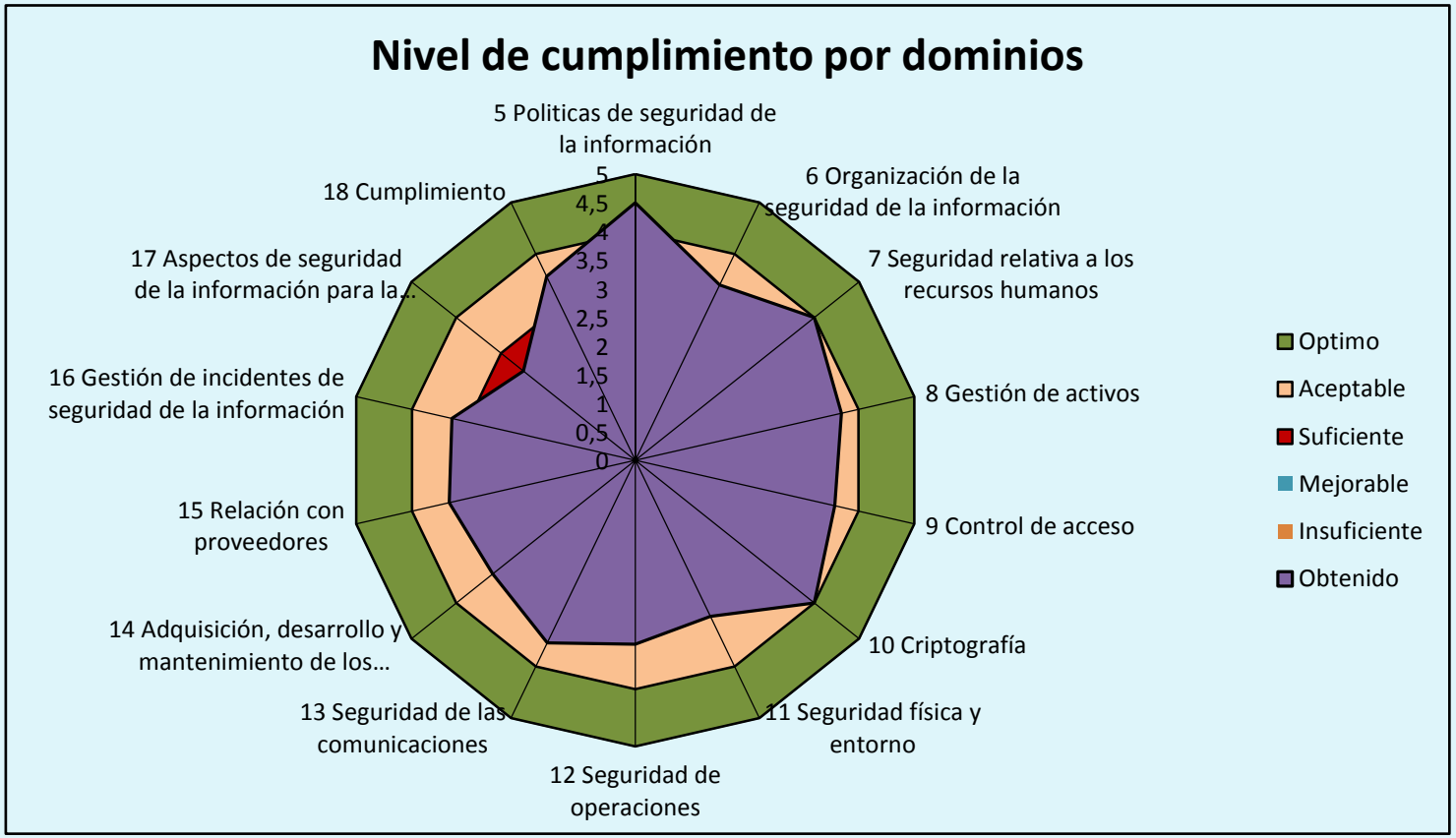
FASES DEL TRABAJOS – FASE5 – Auditoría de cumplimiento

- Diagrama de radar con la representación del grado de cumplimiento de a la ISO 27001:2013



FASES DEL TRABAJOS – FASE5 – Auditoría de cumplimiento

- Diagrama de radar con la representación del grado de cumplimiento de cada uno de los dominios de la ISO 27002



CONCLUSIONES

- Resumen de la auditoría:
- *En el informe de la auditoría se enumeran las no conformidades menores (m) que se han detectado en el transcurso de la auditoría, indicándose la descripción de la misma.*

- *Nº de NO conformidades Mayores: 0*
- *Nº de NO conformidades menores: 8*

- *El sistema cumple con los requisitos de la ISO 27001 y por lo tanto puede obtener la certificación.*

- ***Muchas Gracias*.**

UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013