Trabajo Final De Máster

Plan de Implantación de SGSI según norma ISO/IEC 27001:2013

Índice de Contenidos

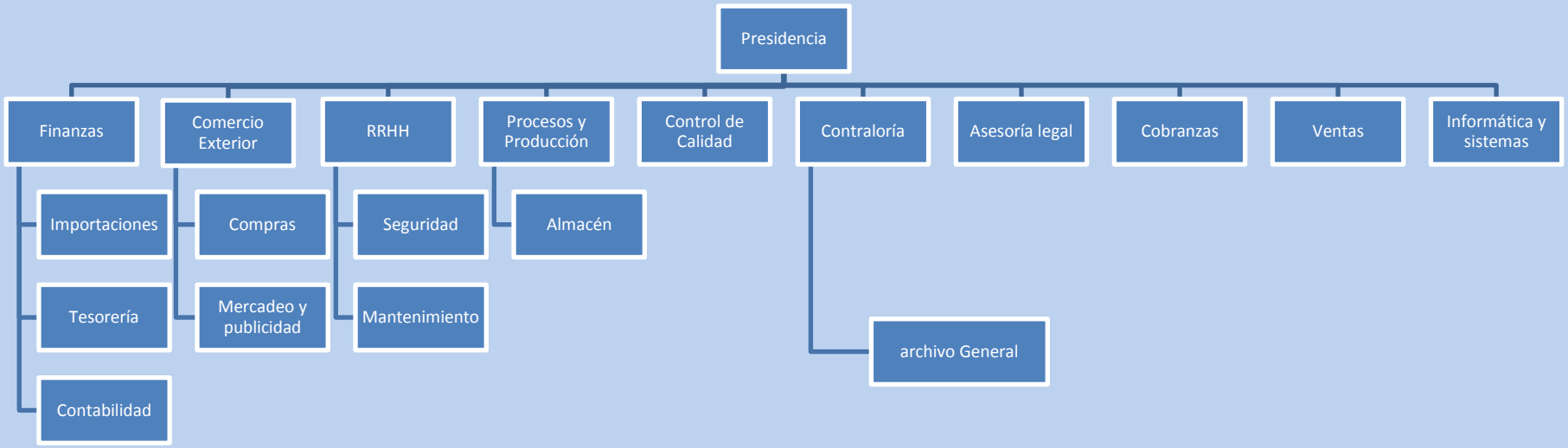
Introducción

Seguridad de la información:
•Concepto.
•Importancia.
•SGSI.
•ISO/IEC 27001:2013.

Tomado de 123RF.com

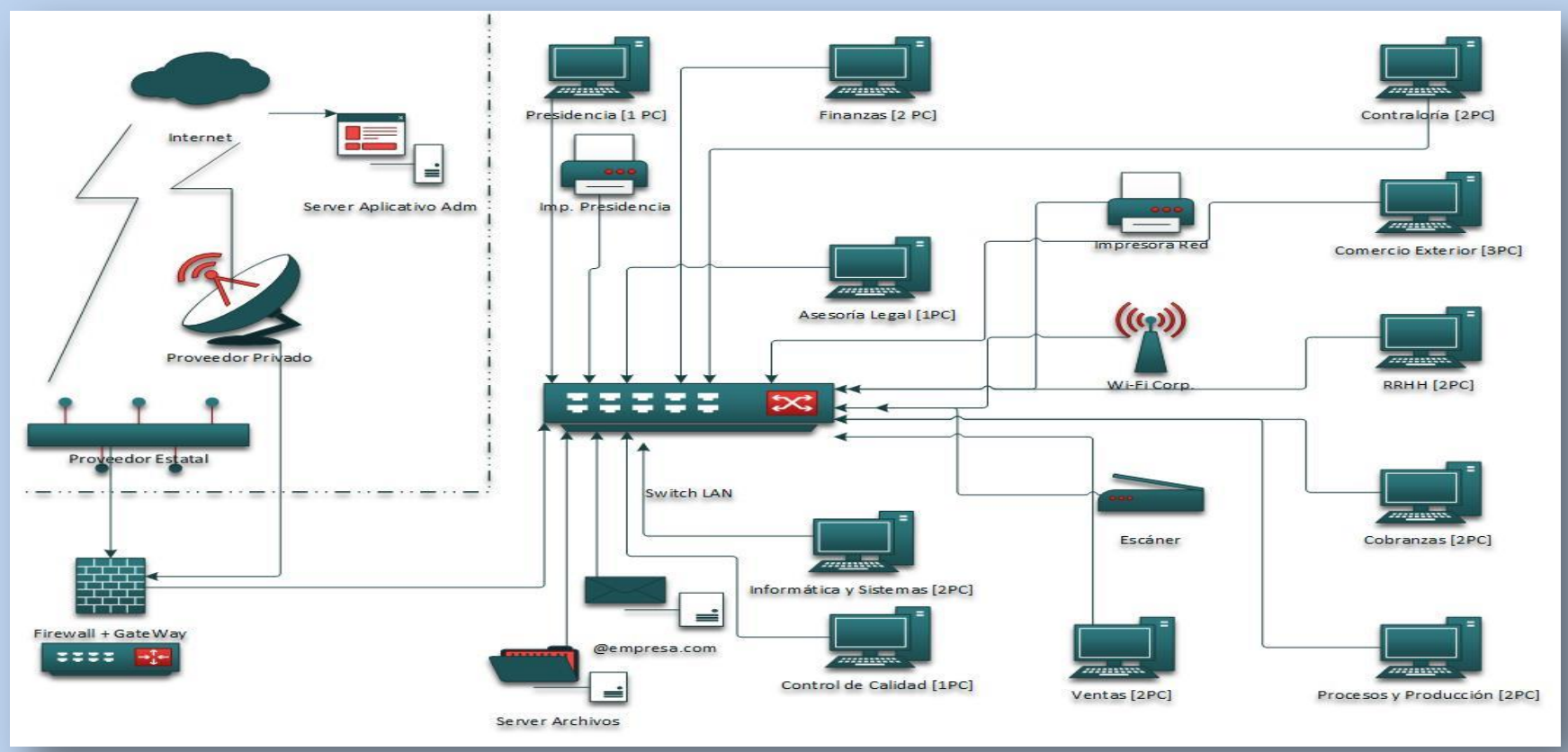
Situación Actual

- Objetivos del proyecto.
- Situación actual de la empresa.



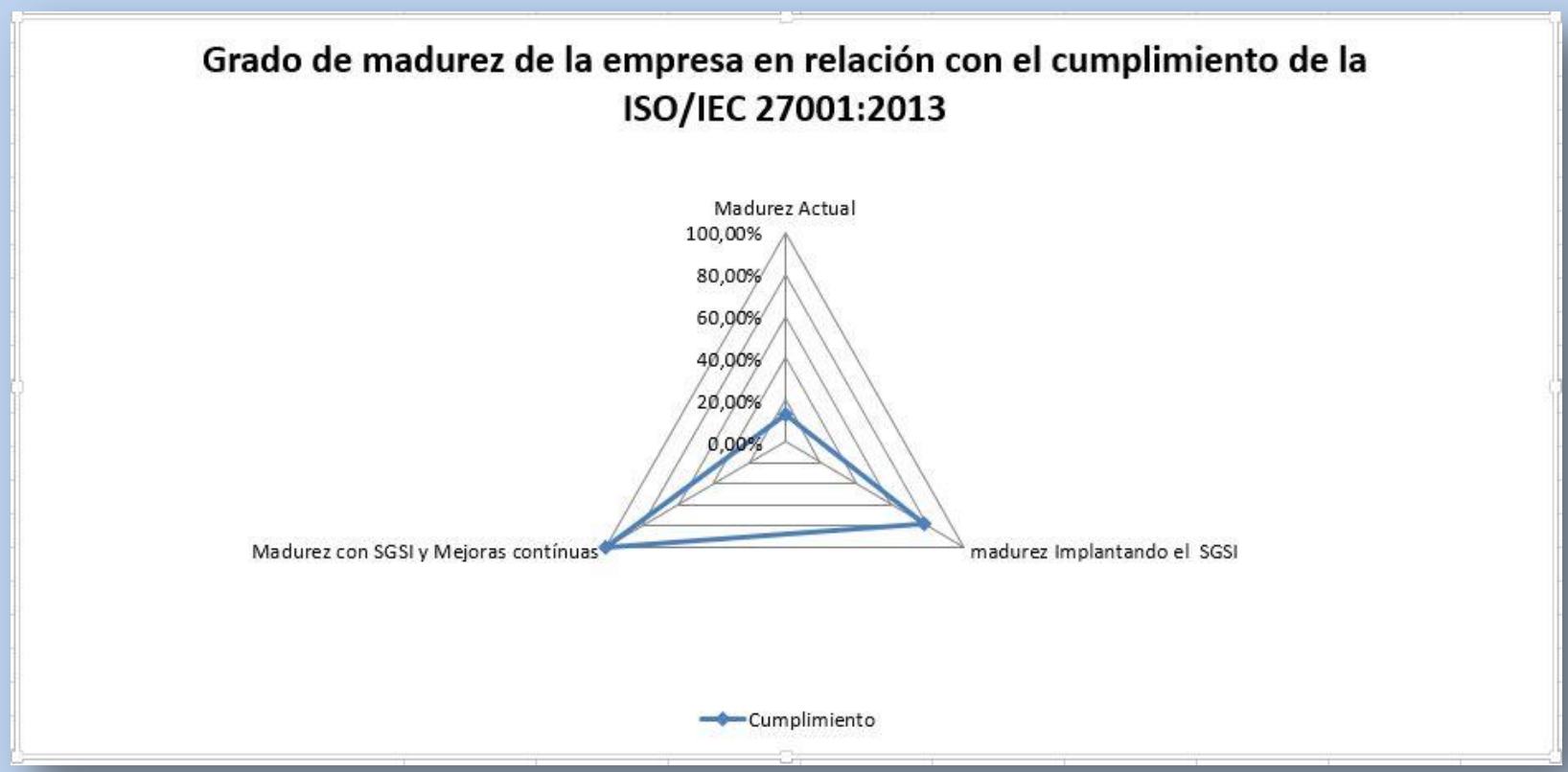
Alcance del Proyecto

•Alcance: Sistemas de información (Automatizado y Manual) y sus activos relacionados.



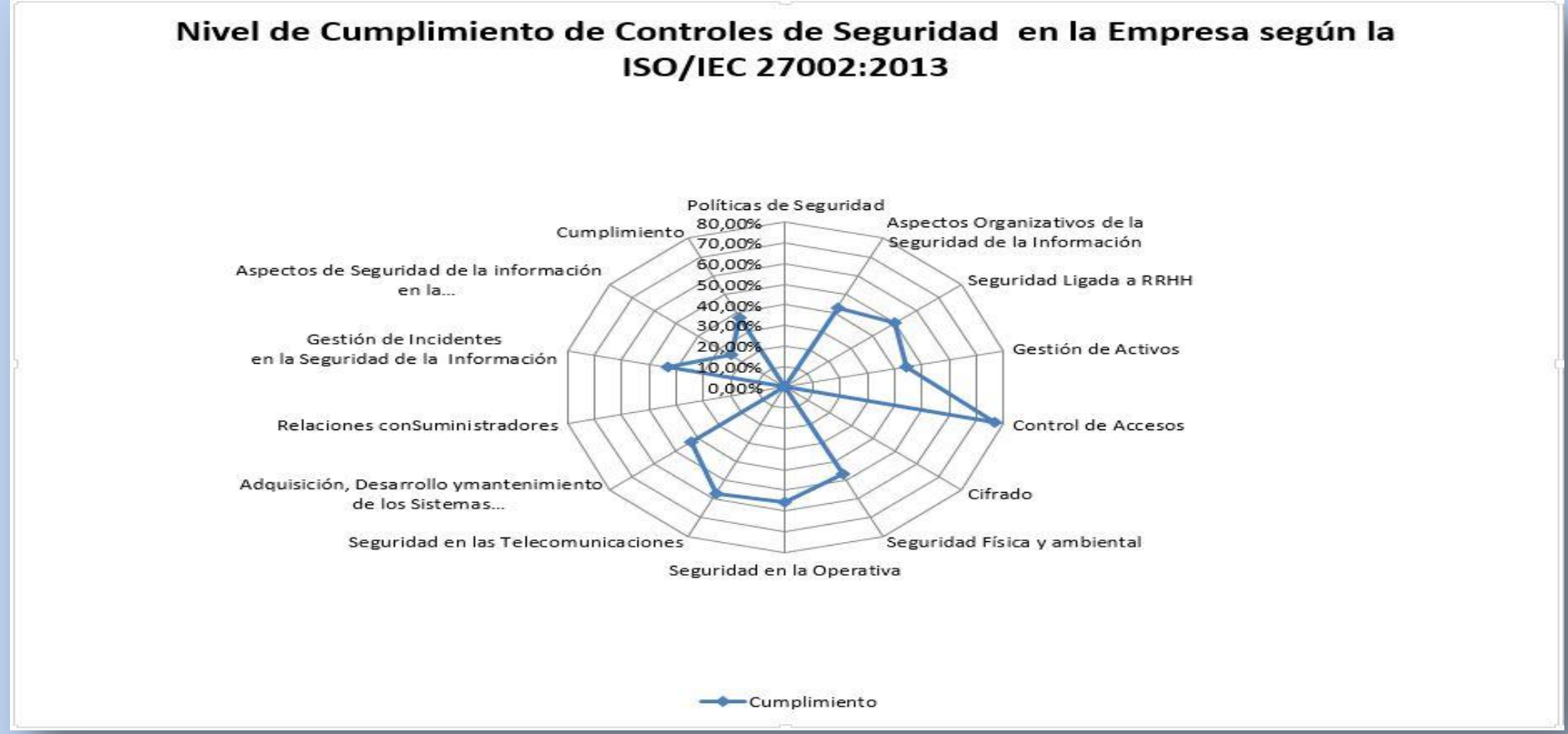
Fase I: Análisis Diferencial

•Análisis diferencial ISO/IEC 27001:2013-27002:2013: Grado de madurez de la empresa (13,04%).



Fase I: Análisis Diferencial

•Nivel de cumplimiento según ISO/IEC 27002:2013: De 114 controles se aplican 103 y se cumplen 46 (44,66%).

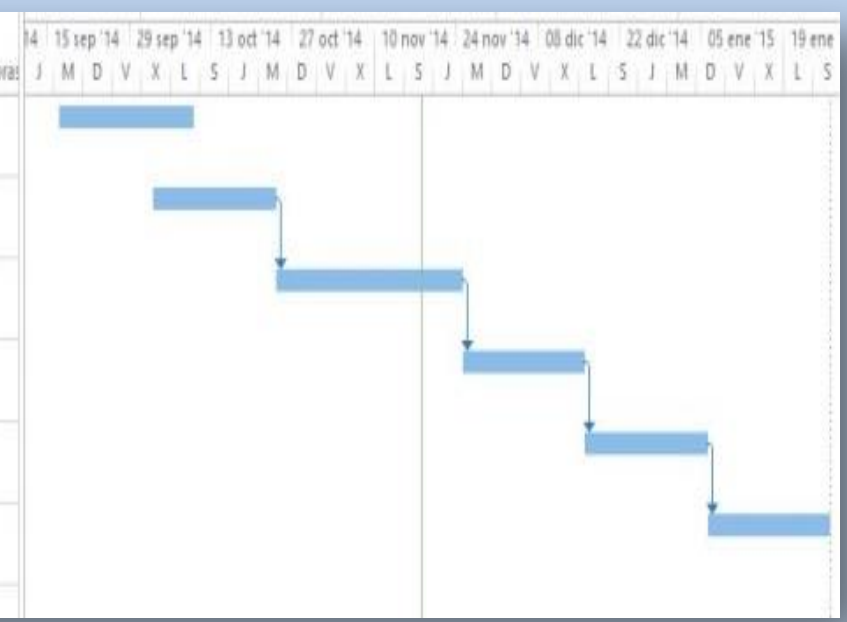


Fase I: Análisis Diferencial

•Plan director de seguridad: Conformado por Seis fases para implantar un SGSI según ISO/IEC 27001:2013.

DIAGRAMA DE GANTT

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	Fase I: Contextualización, Objetivos y Análisis diferencial	17 días	mié 17/09/14	jue 09/10/14	
2	Fase II: Sistema Gestión Documental	15 días	vie 03/10/14	jue 23/10/14	
3	Fase III: Análisis de Riesgos	22 días	vie 24/10/14	lun 24/11/14	2
4	Fase IV: Propuestas de Proyectos	15 días	mar 25/11/14	lun 15/12/14	3
5	Fase V: Auditoría de Cumplimiento	15 días	mar 16/12/14	lun 05/01/15	4
6	Fase VI: Presentación de Resultados y	15 días	mar 06/01/15	lun 26/01/15	5



Fase II: Esquema Documental

- Declaración de aplicabilidad.
- Gestión de Indicadores
- Gestión de roles y responsabilidades.
- Metodología para el análisis de riesgos.
- Política de seguridad.
- Procedimiento auditorías internas.
- Programa de auditorías.
- Procedimiento revisión por dirección.

Fase III: Análisis de Riesgos

- Catálogo de Activos.
- Valoración de Activos.

			Valor por Dimensión					Dependencia		Categoria de Activos						
ID	Activo	Criticidad	C	I	D	A	T	Activo del que Depende	Grado de Dependencia	Hardware	Software	Interfaces	Datos	Personal	Servicio	Misión
C	Credibilidad	10	8	10	10	8	8	A. Información	0,9							X

Fase III: Análisis de Riesgos

- Valoración amenazas y vulnerabilidades.
- Impacto potencial.

	Credibilidad	
	Frecuencia	Impacto
N-1. Desastre Natural	D	0,5
I-1. Falla Infraestructura	MPF	0,5
I-2. Ataque Físico	PF	0,75
A-1. Ciberataque	F	0,75
A-2. Espionaje Industrial	MPF	0,9
A-3. Falla Recursos software	PF	0,75
A-4. Falla Equipos Informáticos	PF	0,75
A-5. Robo	PF	0,75
A-6. Hurto	F	0,9
E-1. Falla Servicios	F	0,75

Fase III: Análisis de Riesgos

- Riesgo potencial calculado para el activo esencial 'Credibilidad'.

	Credibilidad		
	Valor	Frecuencia	Impacto
N-1. Desastre Natural	500.000,00 €	0,002740	0,5
			684,93 €
I-1. Falla en Infraestructura	500.000,00 €	0,005479	0,5
			1.369,86 €
I-2. Ataque Físico	500.000,00 €	0,010959	0,75
			4.109,59 €
A-1. ciberataque	500.000,00 €	0,032877	0,75
			12.328,77 €
A-2. Espionaje Industrial	500.000,00 €	0,005479	0,9
			2.465,75 €
A-3. Falla en Recursos Software	500.000,00 €	0,010959	0,75
			4.109,59 €
A-4. Falla en Equipos Informáticos	500.000,00 €	0,010959	0,75
			4.109,59 €
A-5. Robo	500.000,00 €	0,010959	0,75
			4.109,59 €
A-6. Hurto	500.000,00 €	0,032877	0,9
			14.794,52 €
E-1. Falla en Servicios	500.000,00 €	0,032877	0,75
			12.328,77 €

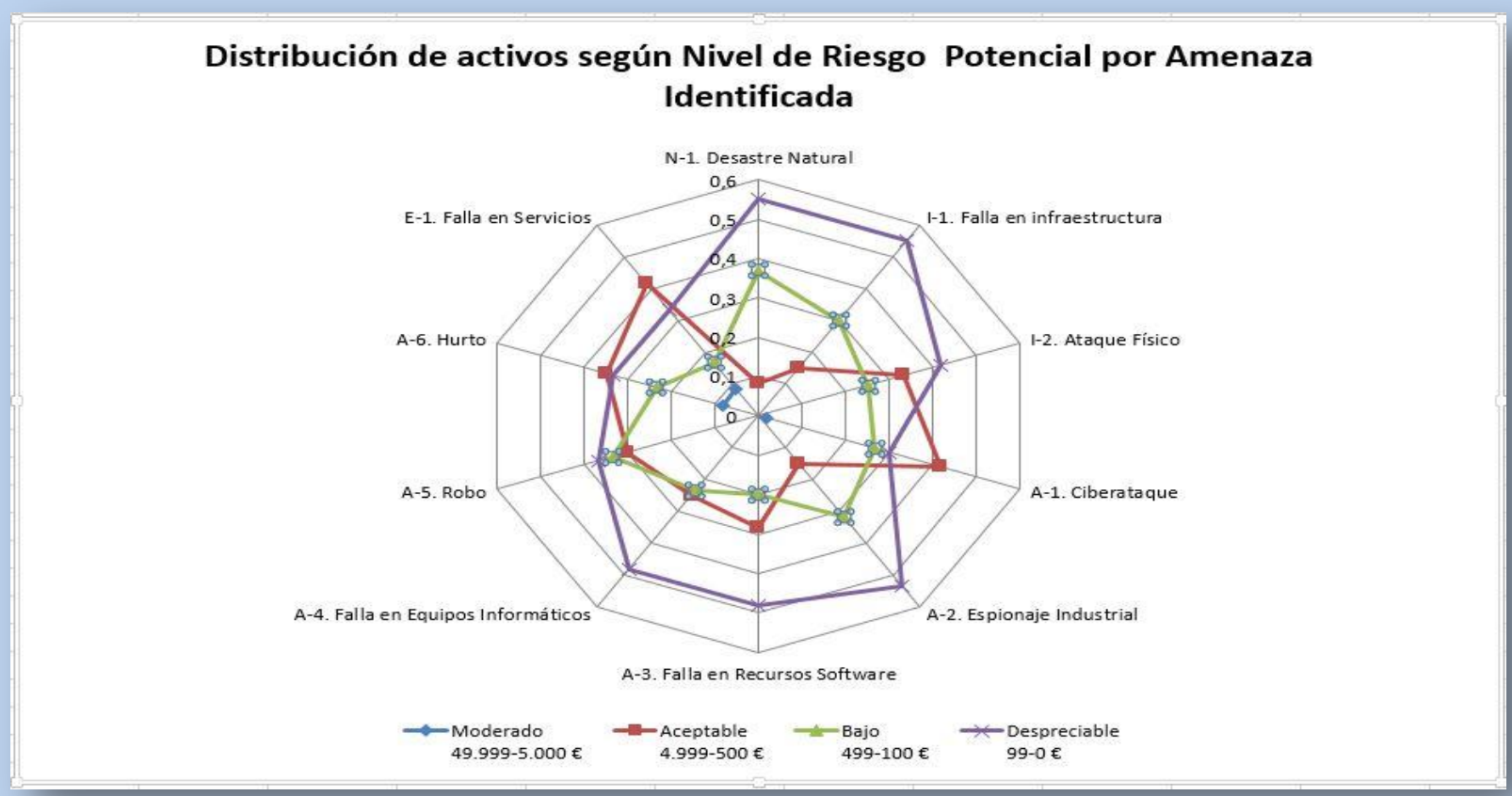
Fase III: Análisis de Riesgos

- Riesgo residual calculado para el activo esencial 'Credibilidad'.

	Credibilidad		
	Valor	Frecuencia R	Impacto Resi
N-1. Desastre Natural	500.000,00 €	0,002740	0,38 513,70 €
I-1. Falla en Infraestructura	500.000,00 €	0,005479	0,38 1.027,40 €
I-2. Ataque Físico	500.000,00 €	0,010959	0,56 3.082,19 €
A-1. ciberataque	500.000,00 €	0,024658	0,75 9.246,58 €
A-2. Espionaje Industrial	500.000,00 €	0,005479	0,68 1.849,32 €
A-3. Falla en Recursos Software	500.000,00 €	0,010959	0,56 3.082,19 €
A-4. Falla en Equipos Informáticos	500.000,00 €	0,010959	0,56 3.082,19 €
A-5. Robo	500.000,00 €	0,010959	0,56 3.082,19 €
A-6. Hurto	500.000,00 €	0,032877	0,68 11.095,89 €
E-1. Falla en Servicios	500.000,00 €	0,032877	0,56 9.246,58 €

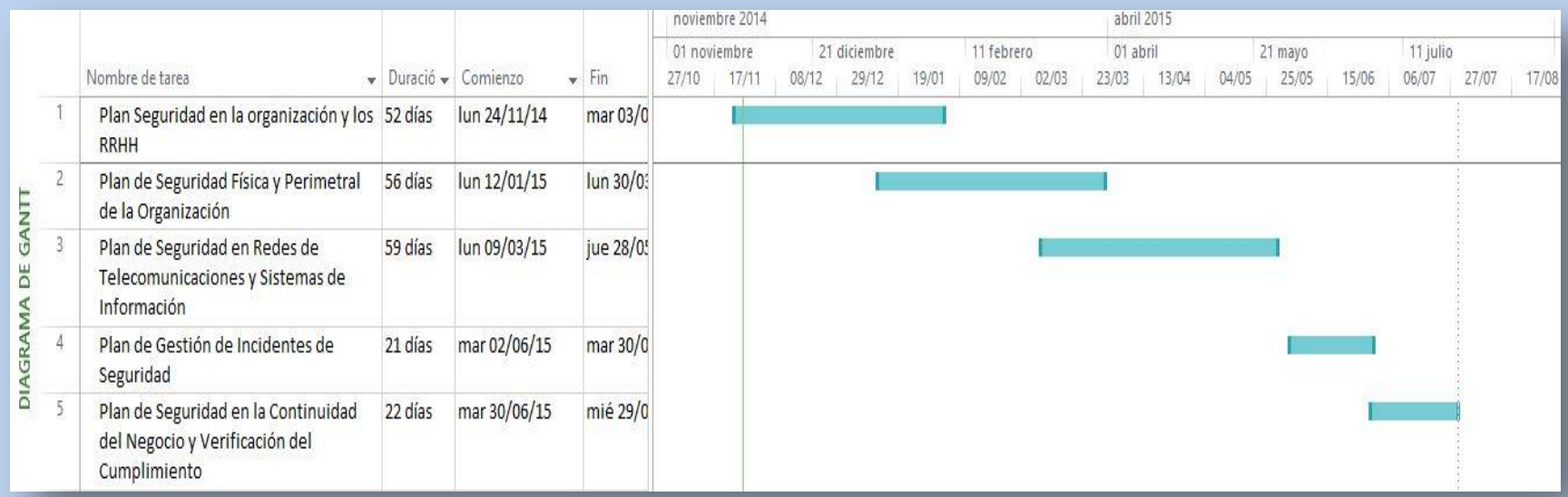
Fase IV: Plan de Acción

•Análisis de la distribución de activos según el riesgo potencial por amenaza identificada



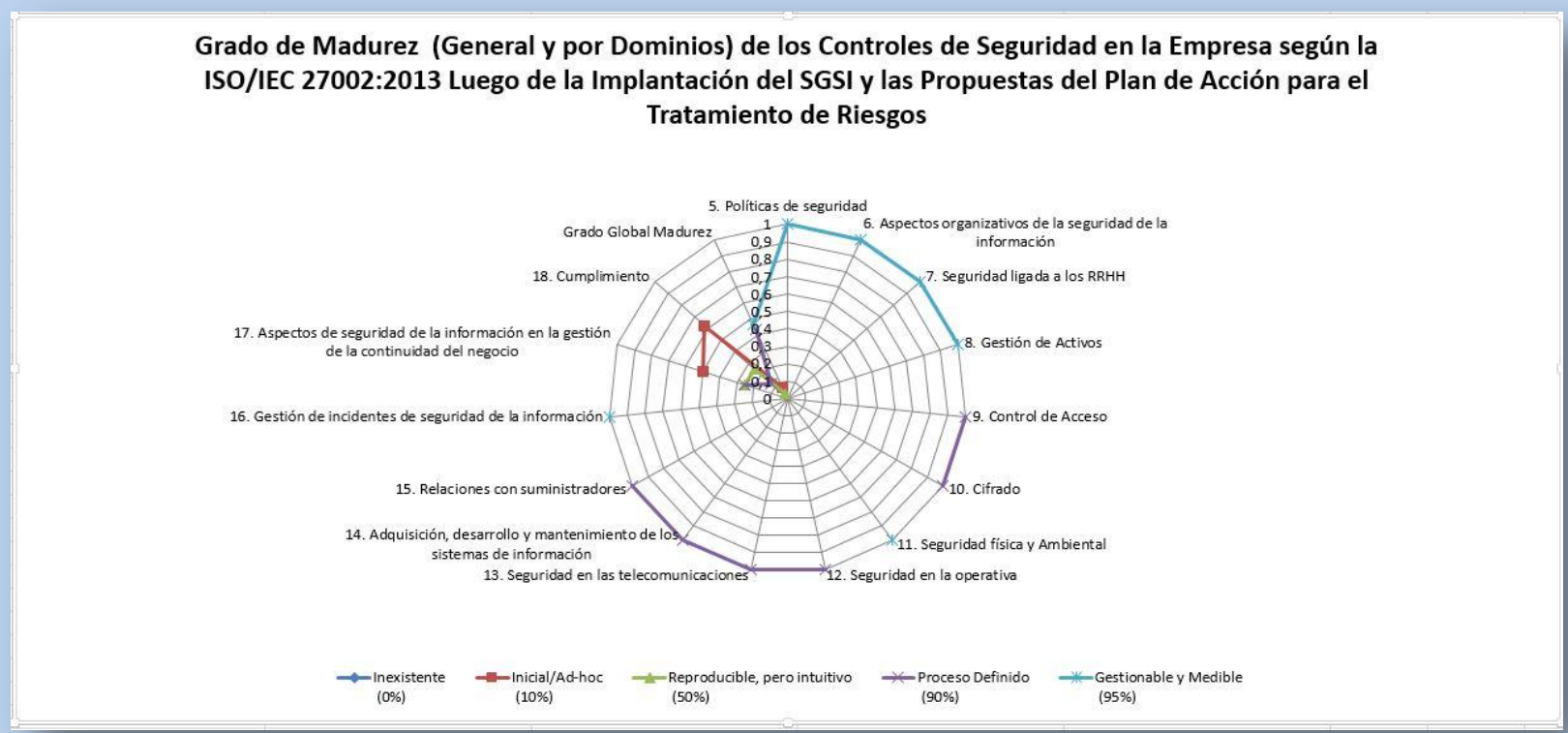
Fase IV: Plan de Acción

•Plan seguridad en la organización y los RRHH.
•Plan seguridad física y perimetral.
•Plan seguridad en redes de telecomunicaciones y sistemas de información.
•Plan de gestión de incidentes de seguridad.
•Plan seguridad en la continuidad del negocio y verificación del cumplimiento.



Fase V: Auditoría de Cumplimiento

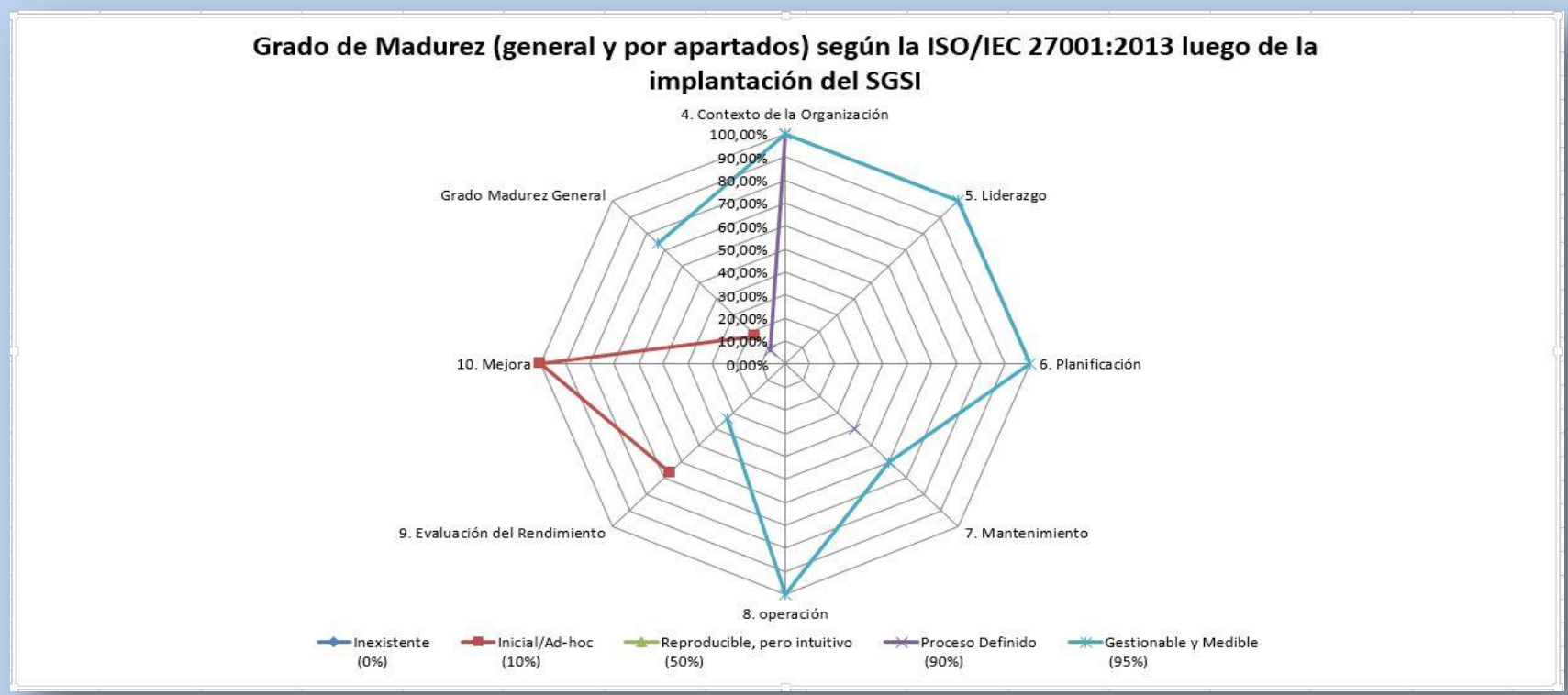
- Verificación de la existencia documentación y controles físicos de seguridad.
- Grado de madurez y cumplimiento según ISO/IEC 27002:2013.



Fase V: Auditoría de Cumplimiento

•Revisión ejecución del plan de acción para el tratamiento de riesgos.

•Grado de madurez y cumplimiento según ISO/IEC 27001:2013.



Fase VI: Entrega de Resultados

- Entrega de Informes.
- Presentación de resultados a la directiva de la empresa.

Tomado de 123RF.com

Conclusiones

Conclusiones más importantes :

•Notable mejora en el estado de la seguridad de la información de la empresa.

• Mejora en la madurez de controles y medidas de seguridad.

•Alto compromiso de la empresa (directiva y personal en general).

•Rápida adopción del plan de acción para el tratamiento de riesgos.

•Plena intención de establecer una cultura general de seguridad en la información de la empresa.

•Mejora en la efectividad y productividad en áreas y procesos de la empresa, luego de la implementación del plan de acción.

Referencias

•Cao Avellaneda, J. (jul 31, 2008). Políticas, normas, procedimientos de seguridad y otros documentos de un SGSI. En línea. Consultado el 11/12/2014. Disponible en: http://sgsi-iso27001.blogspot.com/2008/07/como-resumen-al-documento-que-ya-indiqu.html

•Díaz, A.; Collazos, G.; Cortez Lozano, H.; Ortiz, L. y Herazo Pérez, G. (2011). Sistema para el control de gestión de seguridad de la información. [PDF]. Consultado el 01/10/2014. Disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

•Garre Gui, S. (2011) Introducción a la seguridad de la información. [PDF]. Material didáctico de la asignatura sistemas de gestión de la seguridad, máster MISTIC. FUOC. pág. 7. .

•Gutiérrez Amaya, S. (dic 12, 2013). ISO/IEC 27002:2013 y los cambios en los dominios de control. En línea. Consultado el 30/09/2014. Disponible en: http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

•ISACA. (2014). PO4.6 Establishment of roles and responsibilities overview. En línea. Consultado el 8/10/2014. Disponible en: http://www.isaca.org/GROUPS/PROFESSIONAL-ENGLISH/PO4-6-ESTABLISHMENT-OF-ROLES-AND-RESPONSIBILITIES/Pages/overview.aspx

•iso27000.es. (2012). Gestión de Seguridad de la Información. En línea. Consultada el 30/09/2014. Disponible en: http://www.iso27000.es/sgsi.html

Referencias

•ISO27000.es. (2013). Nueva guía IsO/IEC 27002:2013. [PDF]. Disponible en: http:// www.iso27000.es/download/ControlesISO27002-2013.pdf

•ISO27001Security.com. (2014). ISO/IEC 27004 metrics standard. En línea. Consultado el 6/10/2014. Disponible en: http://www.iso27001security.com/html/27004.html

•IT360.es. (2014). ISO 27001 infografías y esquemas gráficos. En líneea. Disponible en: http://www.it360.es/infografia-iso27001-5-politica-seguridad-de-la-informacion.

•Mendoza López, M. y Lorenzana Gutiérrez, P. (mar 1, 2013). Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I. Revista .Seguridad. Vol. 16. UNAM, México. En línea. Consultada el 30/09/2014. Disponible en: http://revista.seguridad.unam.mx/numero-16/normatividad-en-las-organizaciones-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n-parte-i

•Pallavicini, C. (2011). Norma ISO 27004. [PDF]. Consultado el 9/10/2014. Disponible en: http:// www.pallavicini.cl/sites/default/files/iso_27004.pdf

•Esteban de Quesada, R. (2009). Auditoría técnica de seguridad. [PDF]. FUOC, Barcelona, España.

Gracias por su atención

"La Seguridad no es solo un proceso Tecnológico… Es un proceso Organizacional"

Kenneth Amaditz