Máster Universitario Ciberseguridad y Privacidad (MUCIP)

UOC
www.uoc.edu

RESULTADOS ANÁLISIS DE RIESGOS Y PROYECTOS

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

Trabajo Fin de Máster (TFM)

Natividad García Lacárcel

CONTENIDO

Metodología empleada

Análisis de riesgos

Propuesta de proyectos

Conclusiones y recomendaciones

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.

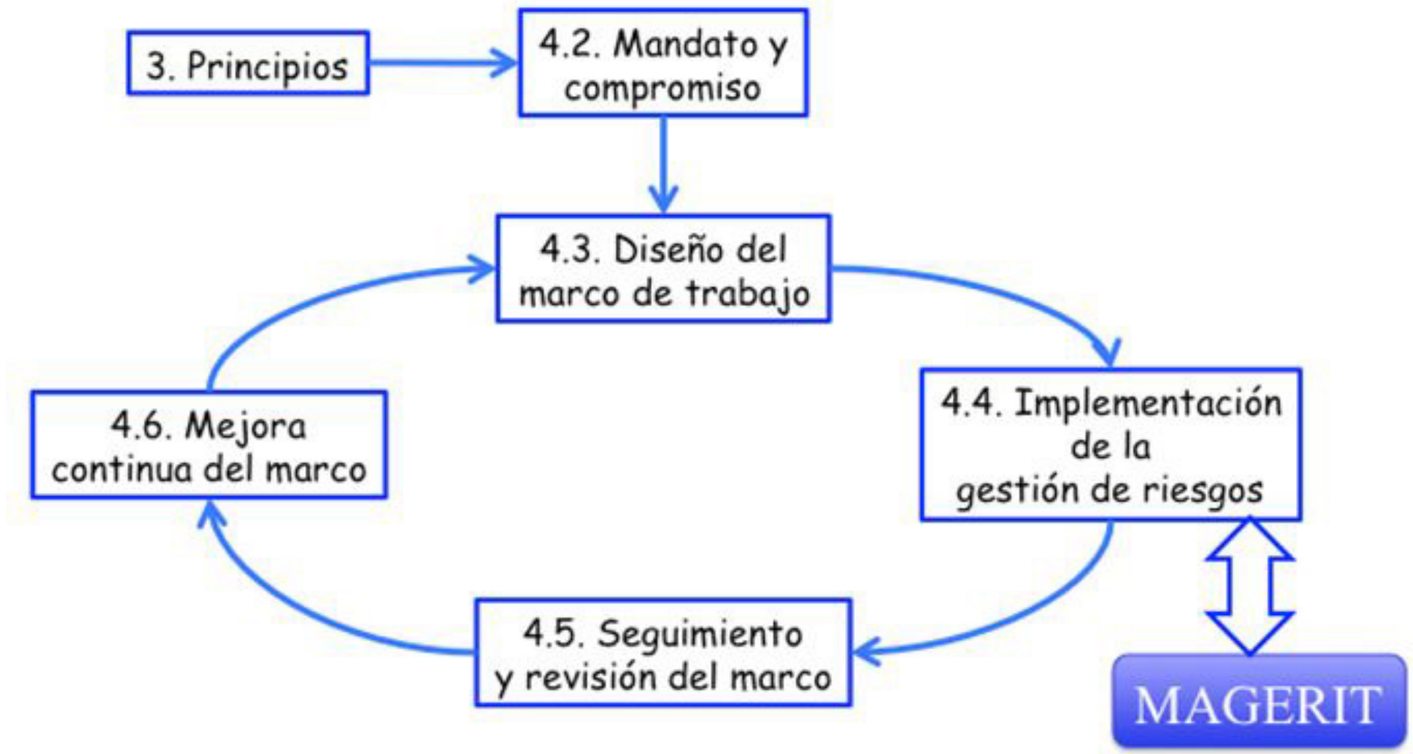
0. Introducción	
1. Alcance	
2. Referencias normativas	
3. Términos y definiciones	
4. Contexto de la organización	Conocimiento de la organización y de su contexto Comprensión de las necesidades y expectativas de las partes interesadas Determinación del alcance del SGSI
5. Liderazgo	Liderazgo y compromiso 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

METODOLOGÍA

MAGERIT: una metodología de análisis y gestión de riesgos elaborada por el C*onsejo Superior de Administración Electrónica de España*, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma ***implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados***. Dispone de documentación donde se reunen técnicas y ejemplos de cómo realizar el análisis de riesgos.



ANÁLISIS DE RIESGOS

Metodología MAGERIT

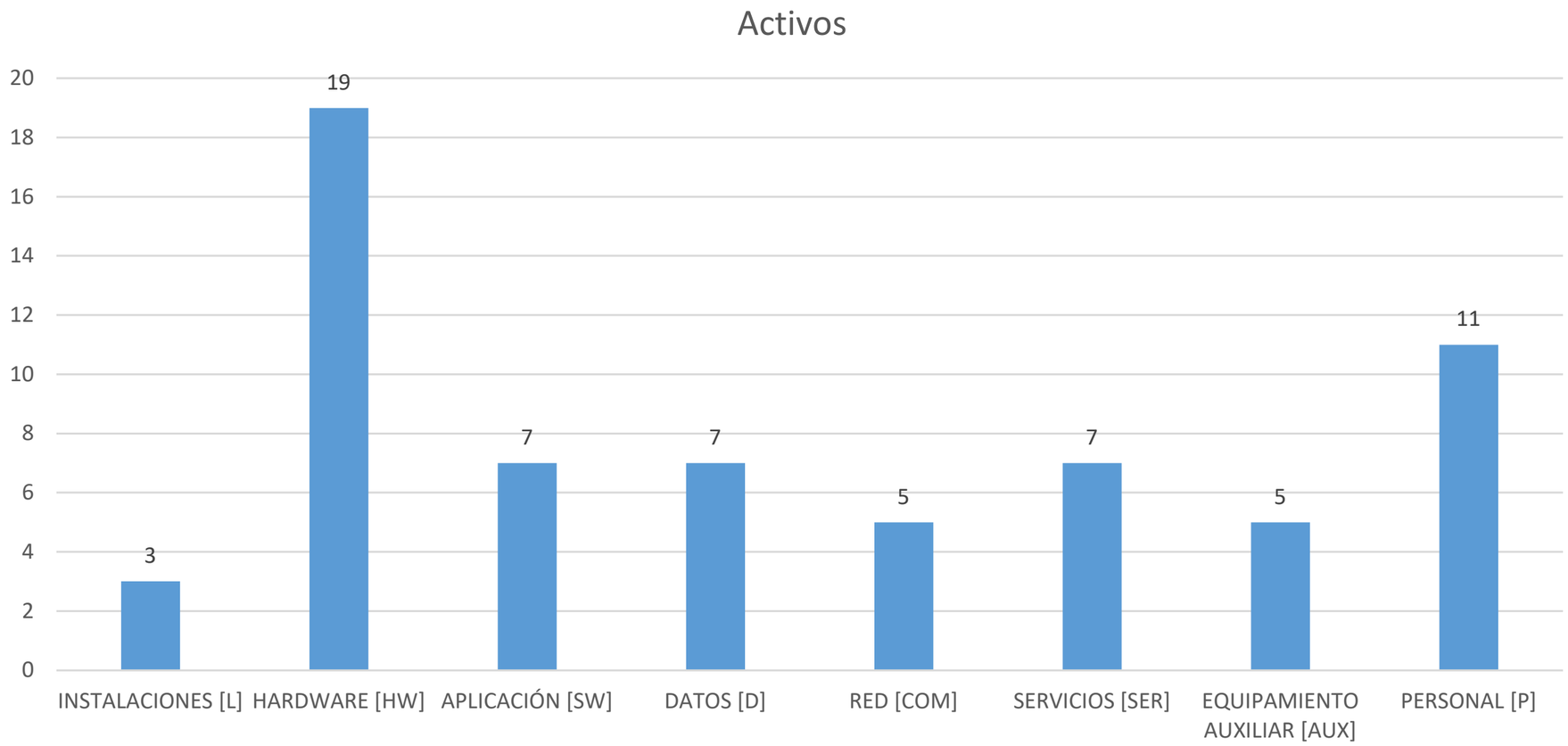
una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Dispone de documentación donde se reunen técnicas y ejemplos de cómo realizar el análisis de 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.

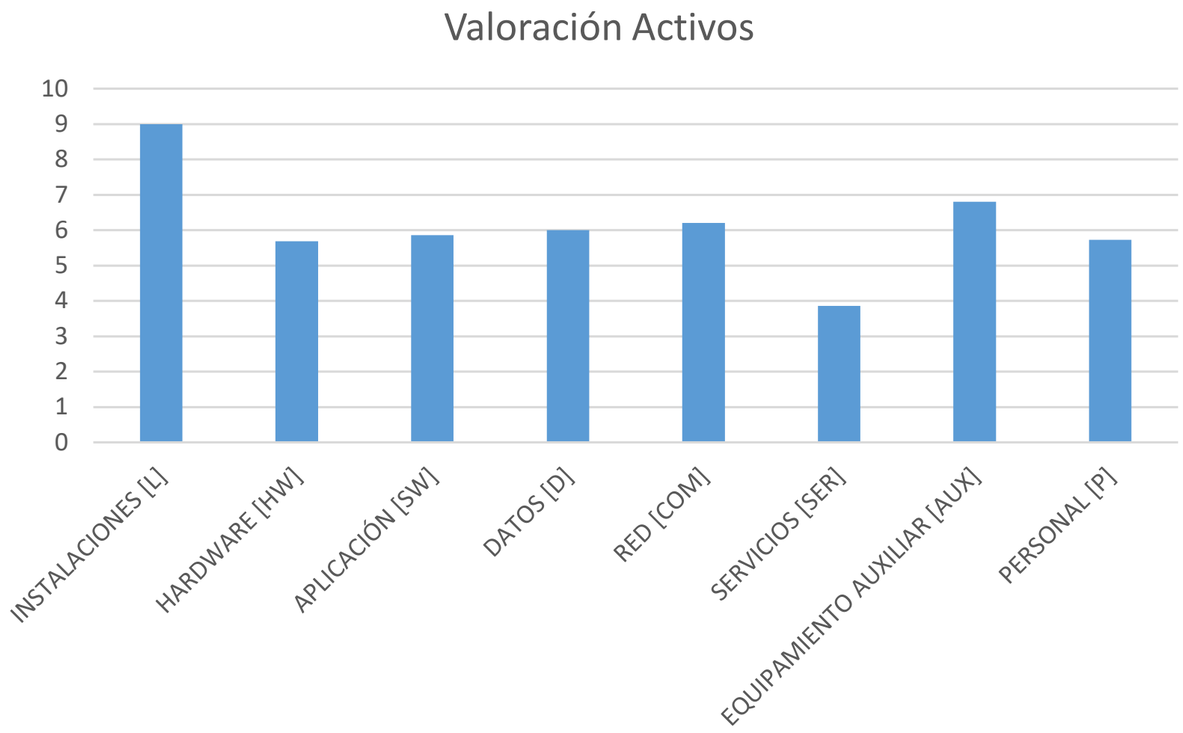
INVENTARIO DE ACTIVOS. POR CATEGORÍA

1º Se efectúa un inventario de los activos de la organización.
8 Categorías y 64 activos



VALORACIÓN DE LOS ACTIVOS

2º Se elabora una valoración de los activos de la organización.
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.

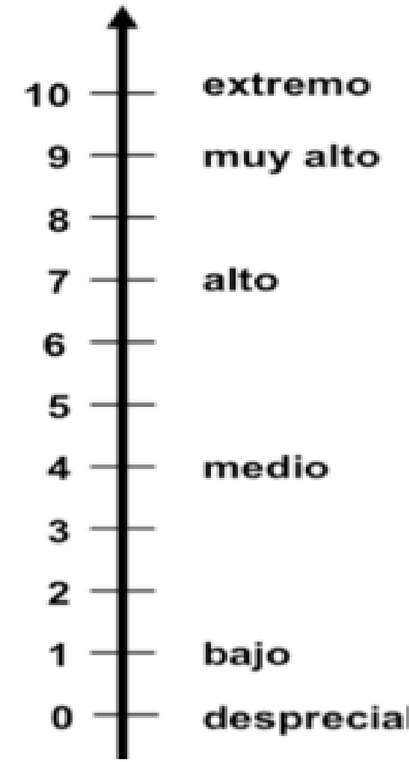


El rango de la valoración económica:	RANGO	VALOR
Muy alta	Valor>50.000€	100.000€
Alta	10.000€<valor>50.000€	25.000€
Media	5.000€<valor>10.000€	7.500€
Baja	1.000€<valor>5.000€	2.500€
Muy baja	Valor<1.000€	1.000€

VALORACIÓN DE LOS ACTIVOS RESPECTO A LAS DIMENSIONES DE SEGURIDAD

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

LA VALORACIÓN DE LOS ACTIVOS RESULTA:

AMBITO	ACTIVO	NUMERO	VALOR	A	C	I	D	T
INSTALACIONES [L]	Oficina	[L-01]	Alto	7	8	8	9	5
	CPD	[L-02]	Alto	9	9	9	9	9
	Recepción	[L-03]	Bajo	5	5	1	1	1
HARDWARE [HW]	Servidor de aplicaciones	[HW-01]	Alto	7	7	7	3	4
	Servidor de desarrollo y pruebas	[HW-02]	Bajo	7	3	3	3	4
	Servidor de Web	[HW-03]	Alto	7	7	7	3	4
	Servidor BBDD	[HW-04]	Alto	9	5	5	9	4
	Servidor DNS/Proxy/Dominio	[HW-05]	Bajo	7	1	3	3	4
	Servidor de ficheros	[HW-06]	Alto	9	5	5	9	4
	Servidor de Email	[HW-07]	Alto	9	5	5	9	4
	Equipamiento de respaldo	[HW-08]	Alto	7	7	7	3	4
	Enrutador de Internet	[HW-09]	Medio	5	5	5	5	5
	Switch	[HW-10]	Medio	5	5	5	5	5
	Cortafuegos	[HW-11]	Muy alto	9	9	9	9	9
	Punto de acceso inalámbrico	[HW-12]	Bajo	5	3	3	3	3
	Equipos escritorio pc	[HW-13]	Medio	7	7	3	3	4
	Portátiles	[HW-14]	Medio	7	7	3	3	4
	Impresoras y escáneres	[HW-15]	Bajo	3	3	1	1	4
	Centralita	[HW-16]	Bajo	3	3	3	1	3
	Teléfonos fijos	[HW-17]	Bajo	3	3	3	1	3
	Teléfonos móviles	[HW-18]	Bajo	3	3	3	1	3
	Cámaras de vigilancia	[HW-19]	Bajo	3	3	3	4	3
APLICACIÓN [SW]	Sistemas operativos	[SW-01]	Medio	3	7	7	3	3
	Paquete ofimático	[SW-02]	Bajo	3	3	3	1	
	Antivirus	[SW-03]	Bajo	3	3	3	5	3
	Software de desarrollo	[SW-04]	Alto	5	7	5	5	3
	Software de contabilidad	[SW-05]	Alto	5	7	5	5	3
	Email	[SW-06]	Bajo	3	3	3	5	3
	Servidores	[SW-07]	Alto	10	9	10	9	3
DATOS [D]	Bases de datos	[D-01]	Muy alto	10	9	10	9	10
	Datos de soporte y licencias	[D-02]	Bajo	3	3	1	1	3
	Desarrollos propios	[D-03]	Medio	3	1	5	3	3
	Backups (copias de seguridad)	[D-04]	Alto	7	7	7	3	7
	Correo electrónico	[D-05]	Medio	3	1	5	3	3
	Logs de servidores y clientes	[D-06]	Medio	3	3	4	8	4
	Credenciales y datos de control de acceso.	[D-7]	Medio	3	3	4	8	4
RED [COM]	Internet	[COM-01]	Alto	3	9	9	3	7
	Red inalámbrica	[COM-02]	Bajo	3	7	3	3	5
	Red cableada	[COM-03]	Alto	3	9	9	3	7
	Telefonía fija	[COM-04]	Medio	5	5	1	5	3
	Telefonía móvil	[COM-05]	Medio	5	5	1	5	3
SERVICIOS [SER]	Acceso remoto	[SER-01]	Bajo	1	3	1	1	0
	Red de control e instrumentación	[SER-02]	Bajo	0	0	0	1	0
	Acceso a internet	[SER-03]	Medio	3	3	0	1	0
	Correo electrónico	[SER-04]	Bajo	3	3	5	3	7
	Servicio web	[SER-05]	Medio	5	5	5	5	5
	Servicio aplicaciones	[SER-06]	Medio	0	7	0	7	0
	Servicio ficheros	[SER-07]	Bajo	0	7	0	7	0
EQUIPAMIENTO AUXILIAR [AUX]	Aire acondicionado	[AUX-01]	Alto	9	9	9	9	0
	Archivadores	[AUX-02]	Bajo	3	1	1	3	0
	Consumibles varios	[AUX-03]	Bajo	1	1	1	3	0
	SAI	[AUX-04]	Alto	7	7	7	7	0
	Corriente eléctrica	[AUX-05]	Muy alto	9	9	9	9	0
PERSONAL [P]	Director General	[P-01]	Muy alto	9	3	3	3	3
	Director comercial	[P-02]	Medio	9	3	3	3	3
	Director de proyectos	[P-03]	Medio	9	3	3	3	3
	Director financiero	[P-04]	Medio	9	3	3	3	3
	Director Sistemas TI	[P-05]	Alto	9		7	7	9
	Responsable seguridad de la información.	[P-06]	Muy alto	9	7	7	7	7
	Key Account Manager	[P-07]	Medio	9	0	0	3	3
	Técnicos de sistemas	[P-08]	Medio	9	0	0	3	9
	Personal del departamento comercial	[P-09]	Bajo	3	0	0	3	3
	Personal del departamento de proyectos	[P-10]	Bajo	3	0	0	3	3
	Personal del departamento financiero	[P-11]	Bajo	3	0	0	1	3

ANÁLISIS DE AMENAZAS. CLASIFICACIÓN

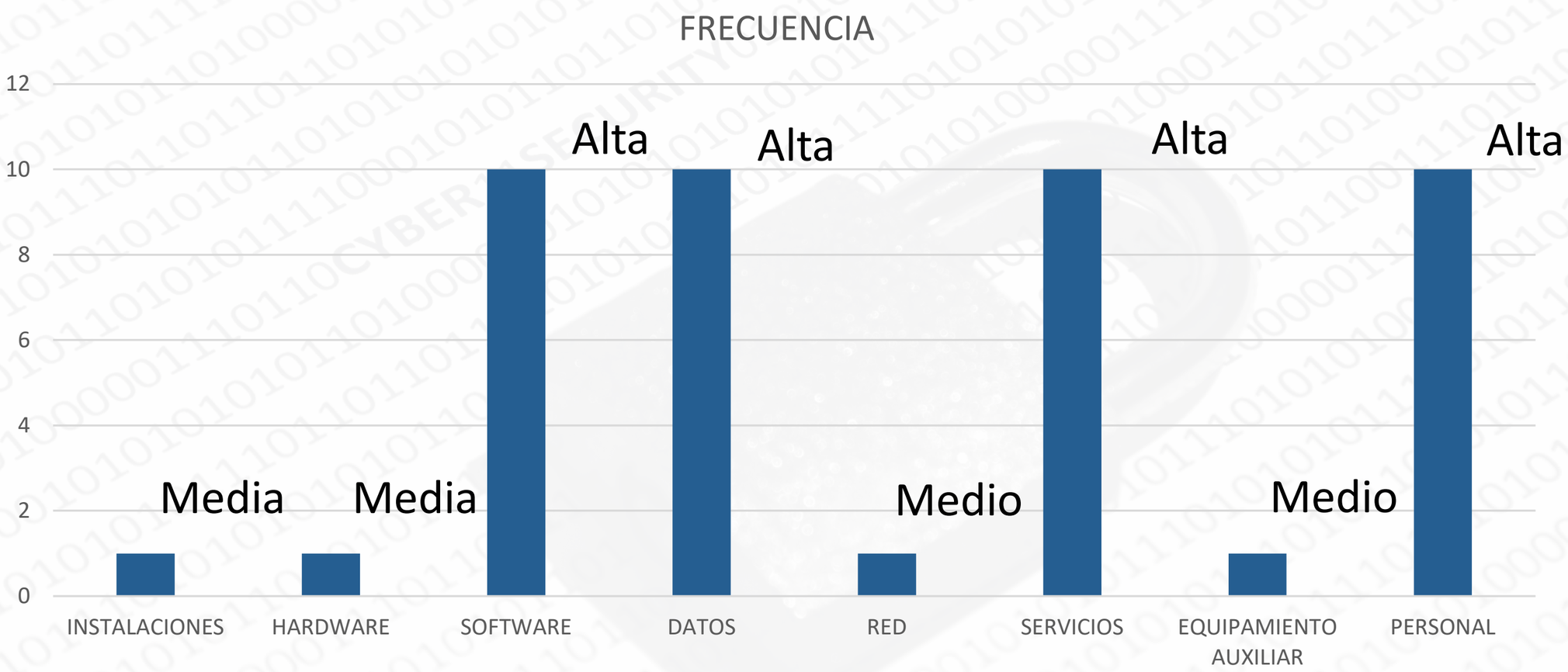
Desastres Naturales [N]
De origen Industrial [I]
Errores y fallos no intencionados [E]
Ataques Intencionados [A]

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:

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

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%.

ANÁLISIS DE AMENAZAS. FRECUENCIA.



RESULTADOS DEL ANÁLISIS DE AMENAZAS.

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%
HARDWARE							
[HW – 01] Servidor de aplicaciones	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 02] Servidor de desarrollo y pruebas	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 03] Servidor web	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 04] Servidor BBDD	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 05] Servidor DNS/Proxy/Dominio	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 06] Servidor de ficheros	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 07] Servidor de email	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 08] Equipo de respaldo	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 09] Enrutador de Internet	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 10] Switch	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 11] Cortafuegos	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 12] Punto acceso wifi	Medio[M]	1	0%	100%	50%	100%	0%
[HW – 13] Ordenadores	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 14] Portátiles	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 15] Impresoras y escaneres	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 16] Centralita	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 17] Teléfono fijo	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 18] Teléfonos móviles	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 19] Cámaras de vigilancia	Medio[M]	1	0%	100%	30%	100%	0%
PERSONAL							
[P-01] - Director General	Alto[A]	10	0%	20%	30%	100%	0%
[P-02] - Director comercial	Alto[A]	10	0%	20%	30%	100%	0%
[P-03] - Director de proyectos	Alta[A]	10	0%	20%	30%	100%	0%
[P-04] - Director financiero	Alta[A]	10	0%	20%	30%	100%	0%
[P-05] - Director de Sistemas TI	Alta[A]	10	0%	20%	30%	100%	0%
[P-06] - Responsable de seguridad de la información	Alta[A]	10	0%	20%	30%	100%	0%
[P-07] - Key Account Manager	Alta[A]	10	0%	20%	30%	100%	0%
[P-08] - Técnicos de sistemas	Alta[A]	10	0%	20%	30%	100%	0%
[P-09] - Personal departamento comercial	Alta[A]	10	0%	20%	30%	100%	0%
[P-10] - Personal departamento proyectos	Alta[A]	10	0%	20%	30%	100%	0%
[P-11] - Personal departamento financiero	Alta[A]	10	0%	20%	30%	100%	0%

SOFTWARE							
[SW - 01] Sistemas operativos	Alta [A]	10	100%	100%	100%	100%	30%
[SW-02] – Paquete ofimático	Alta [A]	10	100%	100%	100%	100%	30%
[SW-03] - Antivirus	Alta [A]	10	100%	100%	100%	100%	30%
[SW-04] – Software desarrollo	Alta [A]	10	100%	100%	100%	100%	30%
[SW-05] – Software de contabilidad	Alta [A]	10	100%	100%	100%	100%	30%
[SW-06] – Email	Alta [A]	10	100%	100%	100%	100%	30%
[SW-07] – Servidores	Alta [A]	10	100%	100%	100%	100%	30%
DATOS							
[D-01] Bases de datos	Alta [A]	10	100%	100%	30%	100%	0%
[D-02] Datos de soporte y licencias	Alta [A]	10	100%	100%	30%	100%	0%
[D-03] Desarrollos propios	Alta [A]	10	100%	100%	30%	100%	0%
[D-04] Backups copias de seguridad)	Alta [A]	10	100%	100%	30%	100%	0%
[D-5] Correo electrónico	Alta [A]	10	100%	100%	30%	100%	0%
[D-06] Logs de servidores y clientes	Alta [A]	10	100%	100%	30%	100%	0%
[D-07] Credenciales y datos de control de acceso	Alta [A]	10	100%	100%	30%	100%	0%
RED							
[COM-01] – Internet	Media[M]	1	50%	50%	30%	50%	0%
[COM-02] – Red inalámbrica	Media[M]	1	50%	50%	30%	50%	0%
[COM-03] – Red cableada	Media[M]	1	50%	50%	30%	50%	0%
[COM-04] – Telefonía fija	Media[M]	1	50%	50%	30%	50%	0%
[COM-05] – Telefonía móvil	Media[M]	1	50%	50%	30%	50%	0%
SERVICIOS							
[SER-01] – Acceso remoto	Alto[A]	10	100%	100%	50%	100%	0%
[SER-02] – Red de control e instrumentación	Alto[A]	10	100%	100%	50%	100%	0%
[SER-03] – Acceso a internet	Alto[A]	10	100%	100%	50%	100%	0%
[SER-04] – Correo electrónico	Alto[A]	10	100%	100%	50%	100%	0%
[SER-05] – Servicios web	Alto[A]	10	100%	100%	50%	100%	0%
[SER-06] – Servicio de aplicaciones	Alto[A]	10	100%	100%	50%	100%	0%
[SER-07] – Servicio ficheros	Alto[A]	10	100%	100%	50%	100%	0%
EQUIPAMIENTO AUXILIAR							
[AUX-01] – Aire acondicionado	Medio[M]	1	0%	50%	30%	100%	0%
[AUX-02] – Archivadores varios	Media[M]	1	0%	50%	30%	100%	0%
[AUX-03] – Consumibles varios	Media[M]	1	0%	50%	30%	100%	0%
[AUX-04] – SAI	Medio[M]	1	0%	50%	30%	100%	0%
[AUX-05] – Corriente eléctrica	Medio[M]	1	0%	50%	30%	100%	0%

CÁLCULO DEL IMPACTO

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

Impacto potencial = valor del activo X valor del 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

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:

			VALORACIÓN ACTIVOS					VALORACIÓN AMENAZAS					VALORACIÓN IMPACTO				
NUMERO	ACTIVO	VALOR	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
[L-01]	Oficina	Alto	7	8	8	9	5	0%	100%	100%	100%	0%	0	8	8	9	0
[L-02]	CPD	Muy Alto	9	9	9	9	9	0%	100%	100%	100%	0%	0	9	9	9	0
[L-03]	Recepción	Bajo	5	5	1	1	1	0%	100%	100%	100%	0%	0	5	1	1	0

RESULTADO CÁLCULO DEL 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 DEL 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

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

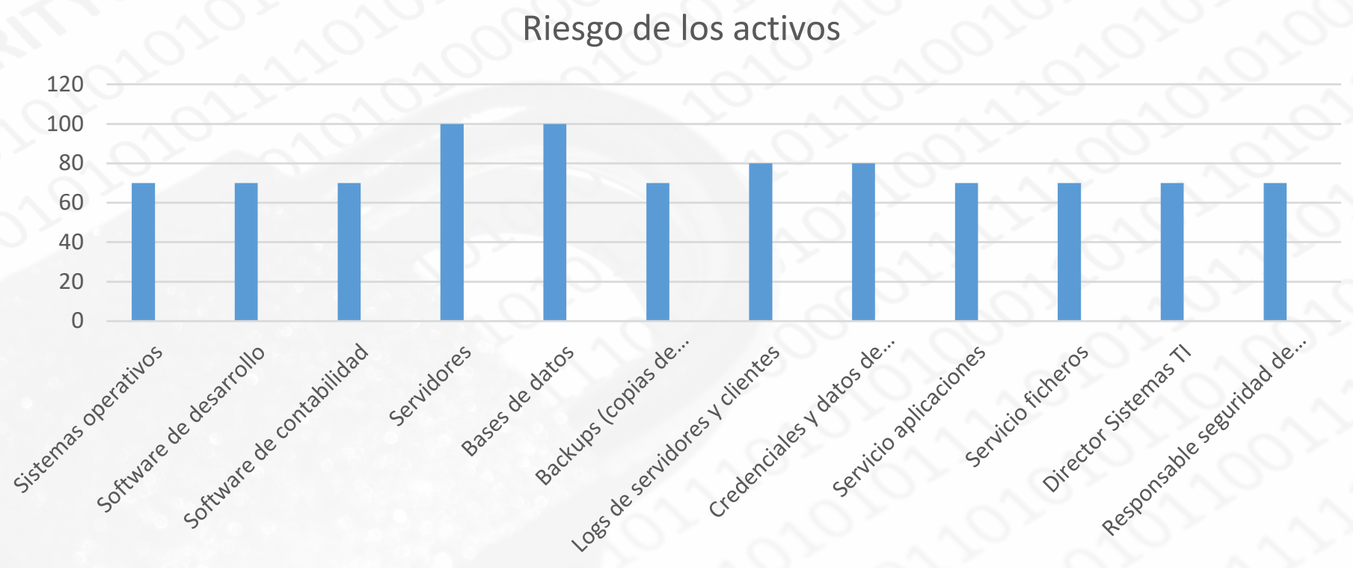
riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

				VALORACIÓN IMPACTO					VALORACIÓN RIESGO				
ACTIVO	**VALOR**	**FRECUENCIA**		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
Oficina	Alto	Medio[M]	1	0	8	8	9	0	0	8	8	9	0
CPD	Muy Alto	Medio[M]	1	0	9	9	9	0	0	9	9	9	0
Recepción	Bajo	Medio[M]	1	0	5	1	1	0	0	5	1	1	0

ANÁLISIS DE RIESGOS

RESULTADOS RIESGO

NUMERO	ACTIVO	VALOR	RIESGO
[SW-01]	Sistemas operativos	Medio	70
[SW-04]	Software de desarrollo	Medio	70
[SW-05]	Software de contabilidad	Medio	70
[SW-07]	Servidores	Alto	100
[D-01]	Bases de datos	Muy alto	100
[D-04]	Backups (copias de seguridad)	Alto	70
[D-06]	Logs de servidores y clientes	Medio	80
[D-7]	Credenciales y datos de control de acceso.	Medio	80
[SER-06]	Servicio aplicaciones	Medio	70
[SER-07]	Servicio ficheros	Bajo	70
[P-05]	Director Sistemas TI	Alto	70
[P-06]	Responsable seguridad de la información.	Muy alto	70



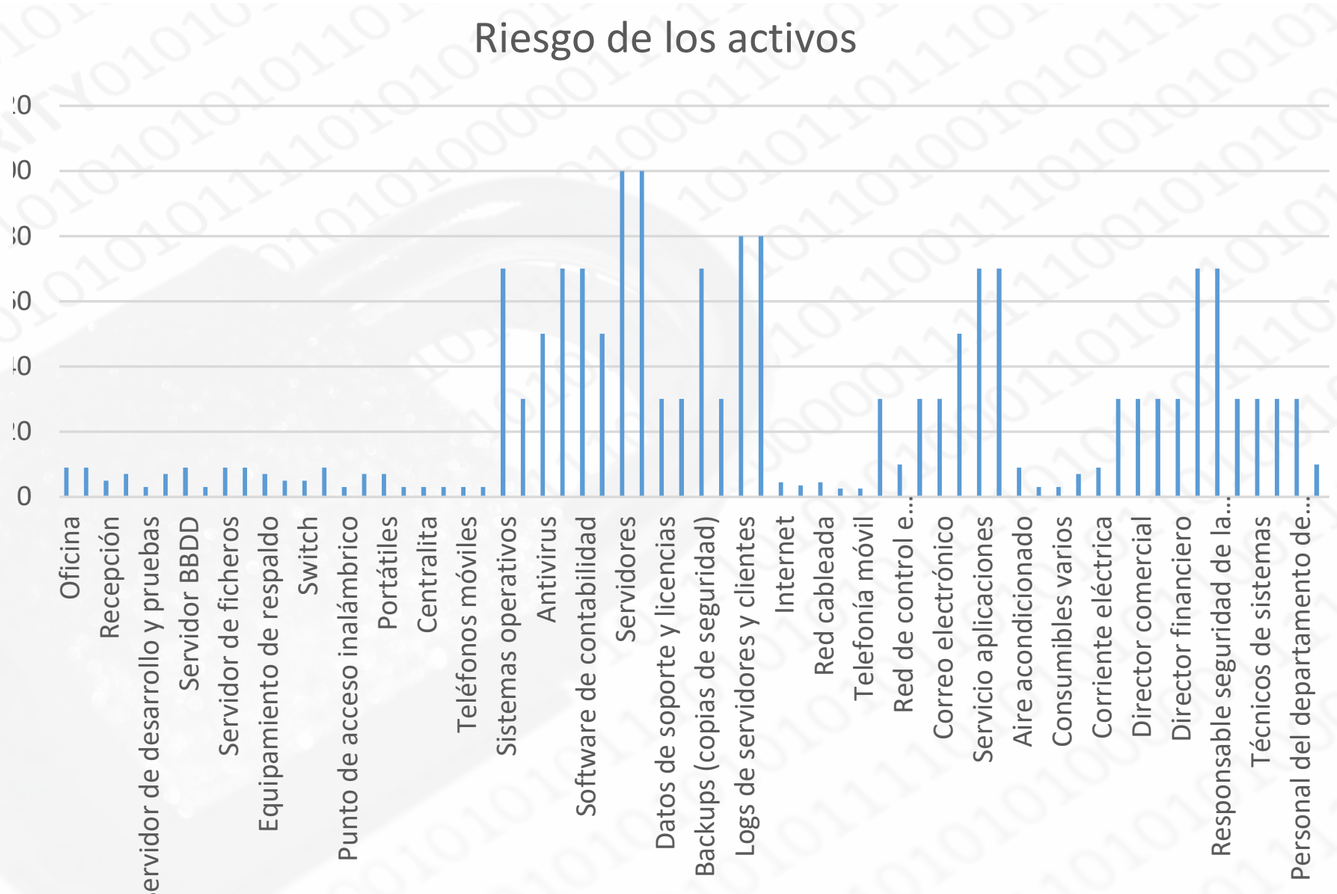
ANÁLISIS DE RIESGOS

RESULTADOS RIESGO

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



ANÁLISIS DE RIESGOS

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**

ANÁLISIS DE RIESGOS

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

ANÁLISIS DE RIESGOS

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

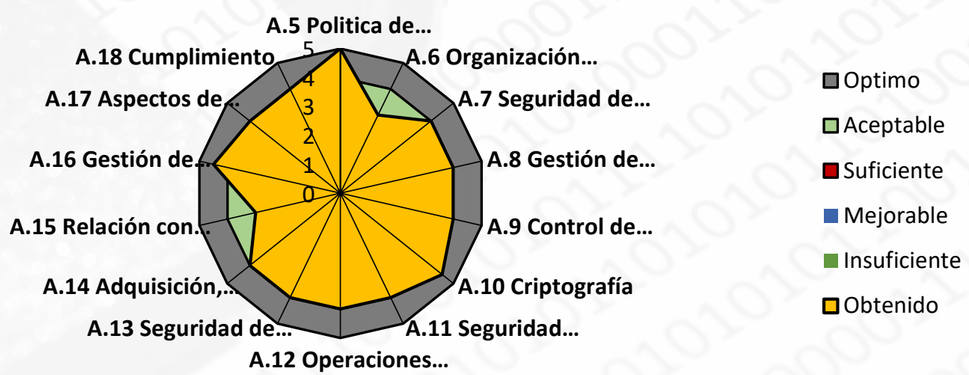
ANÁLISIS DE RIESGOS

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

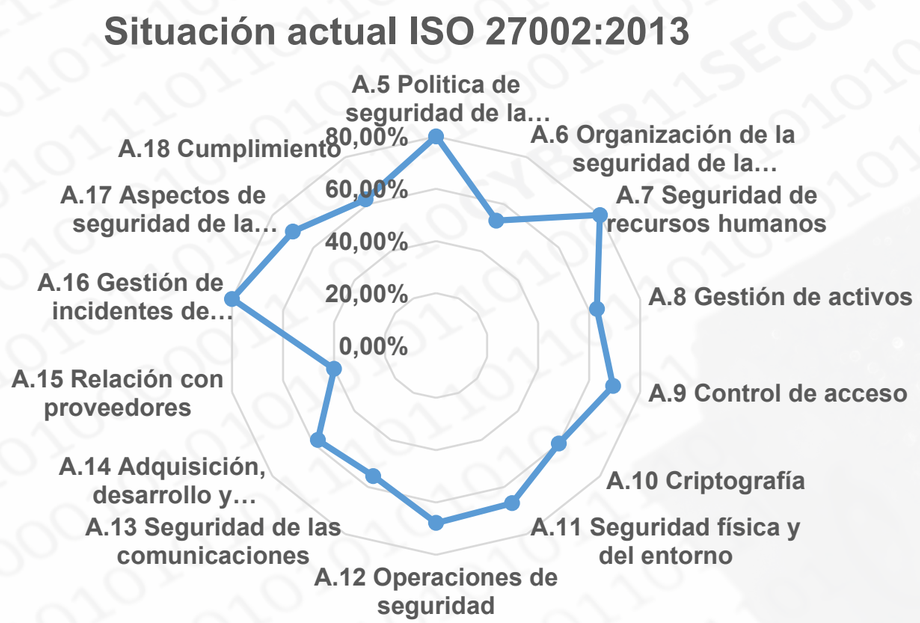
CUMPLIMIENTO ESPERADO ISO 27002:2013



ANÁLISIS DE RIESGOS

Resultados % madurez

ISO/IEC 27002:2013



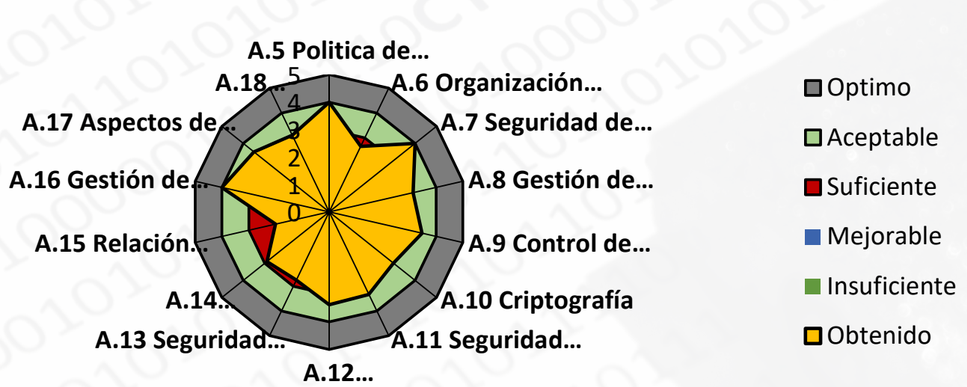
CONTROL	Situación actual	Objetivo	Óptimo
A.5 Política de seguridad de la información	80%	100%	100%
A.6 Organización de la seguridad de la información	53%	60%	100%
A.7 Seguridad de recursos humanos	80%	80%	100%
A.8 Gestión de activos	63%	80%	100%
A.9 Control de acceso	69,33%	80%	100%
A.10 Criptografía	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%

ANÁLISIS DE RIESGOS

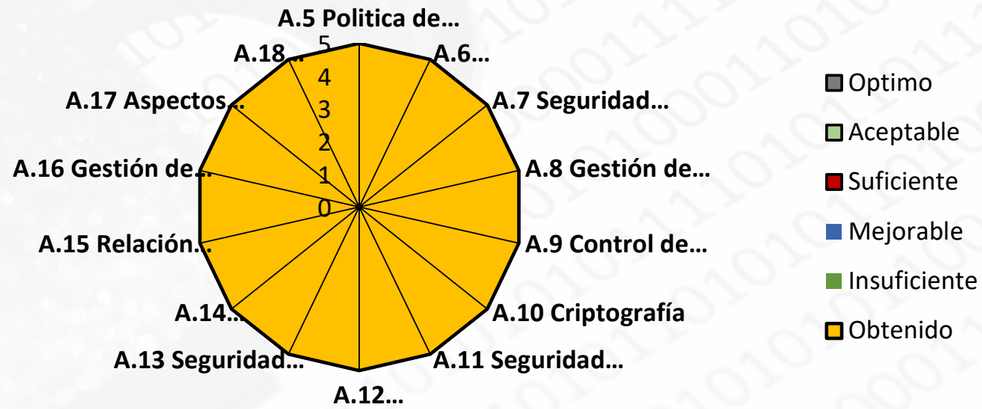
Situación actual

ISO/IEC 27002:2013

Situación actual
ISO 27002:2013

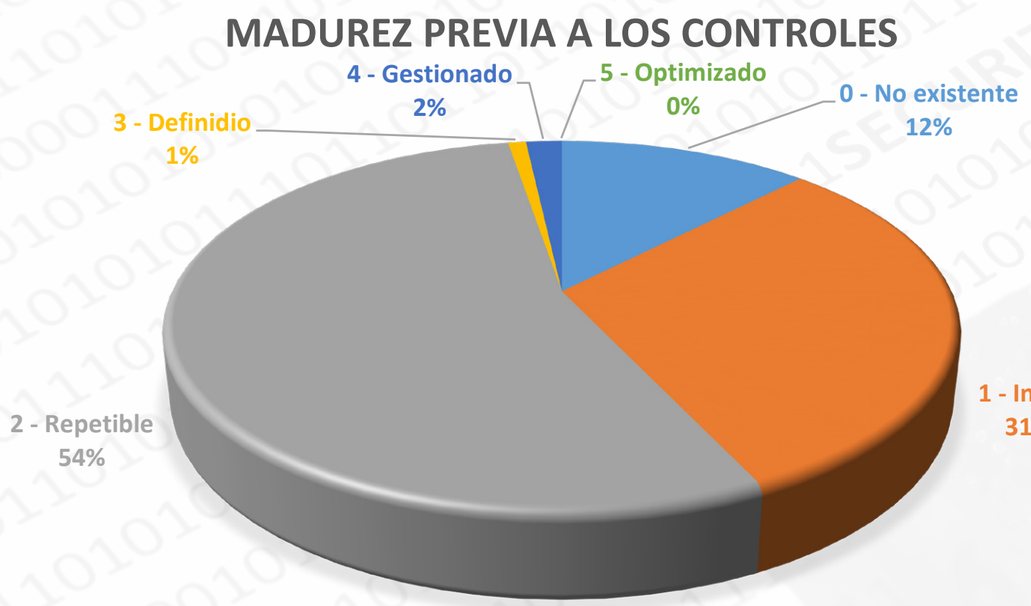


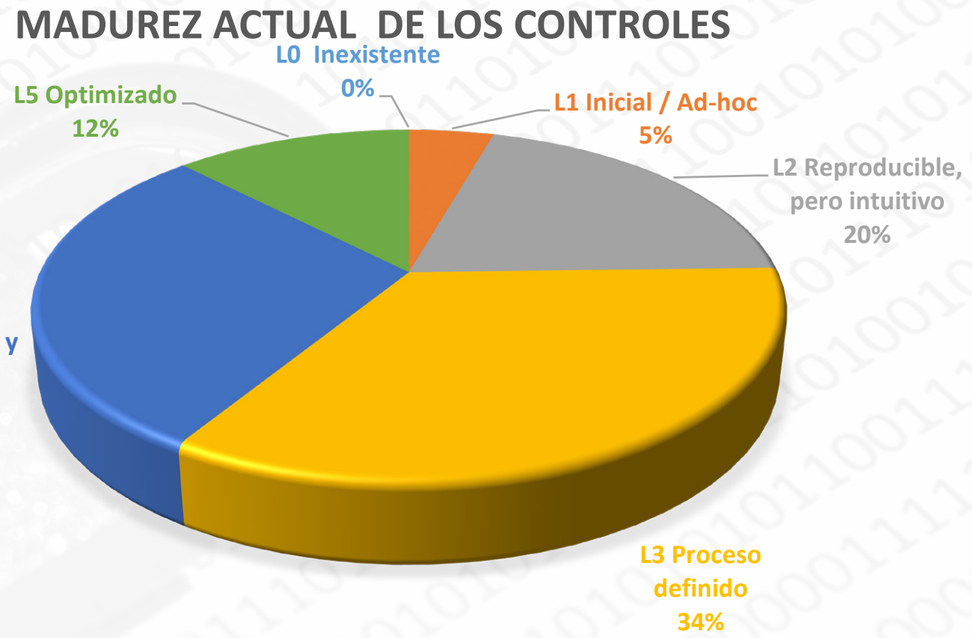
Óptimo ISO 27002:2013



ANÁLISIS DE RIESGOS

Auditoría. Comparativa madurez.





ANÁLISIS DE RIESGOS

CONCLUSIONES

- 1º Se ha definido el estado inicial de la seguridad de la información.
- 2º Se ha desarrollado el esquema documental necesario para implementar el SGSI cumpliendo la ISO/IEC 27001:2013
- 3º Se ha efectuado el análisis de riesgos siguiendo la metodología MAGERIT. Evaluación del riesgo al que están expuestos los activos, el cálculo del impacto que supondría la materialización de posibles amenazas.
- 4º Se han planteado y ejecutado una serie de proyectos para mitigar los riesgos y aumentar el nivel de seguridad.
- 5º Mediante una auditoría de cumplimento se ha analizado el cumplimiento de todos los dominios, si alcanzan el % de madurez esperado y si se ha conseguido mejorar el nivel de seguridad de la información.

ANÁLISIS DE RIESGOS

RECOMENDACIONES

- Seguir trabajando para mitigar las No conformidades encontradas, casi todas de tipo menor.
- Realizar una planificación del esfuerzo y de la inversión económica para resolver las No conformidades.
- Efectuar revisiones periódicas del SGSI, cumplir los protocolos establecidos, tener la documentación actualizada, ..etc
- Mantener actualizado el SGSI para garantizar unos que se mantienen los niveles de madurez implementados.
- Tener presente la seguridad de la información en todos los procesos de negocio de la organización.

Máster Universitario
Ciberseguridad y Privacidad (MUCIP)

UOC
www.uoc.edu

MUCHAS GRACIAS

RESULTADOS ANÁLISIS DE RIESGOS Y PROYECTOS

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

Trabajo Fin de Máster (TFM)

Natividad García Lacárcel