Plan Director de Seguridad

Autor: Luis Rodríguez Conde
Dirección: Antonio José Segovia Henares
Fecha: Junio, 2017

Universitat Rovira i Virgili
Universitat Oberta de Catalunya
Universitat Autònoma de Barcelona

Contenido

Introducción

- Un Plan Director de Seguridad es uno de los elementos clave con que debe contar el Responsable de Seguridad de una organización
- Se basa en un modelo de mejora continua PDCA (Plan-Do-Check-Act).
- La implementación de este se basa en las normas:
  - ISO/IEC 27001:2013
  - ISO/IEC 27002:2013

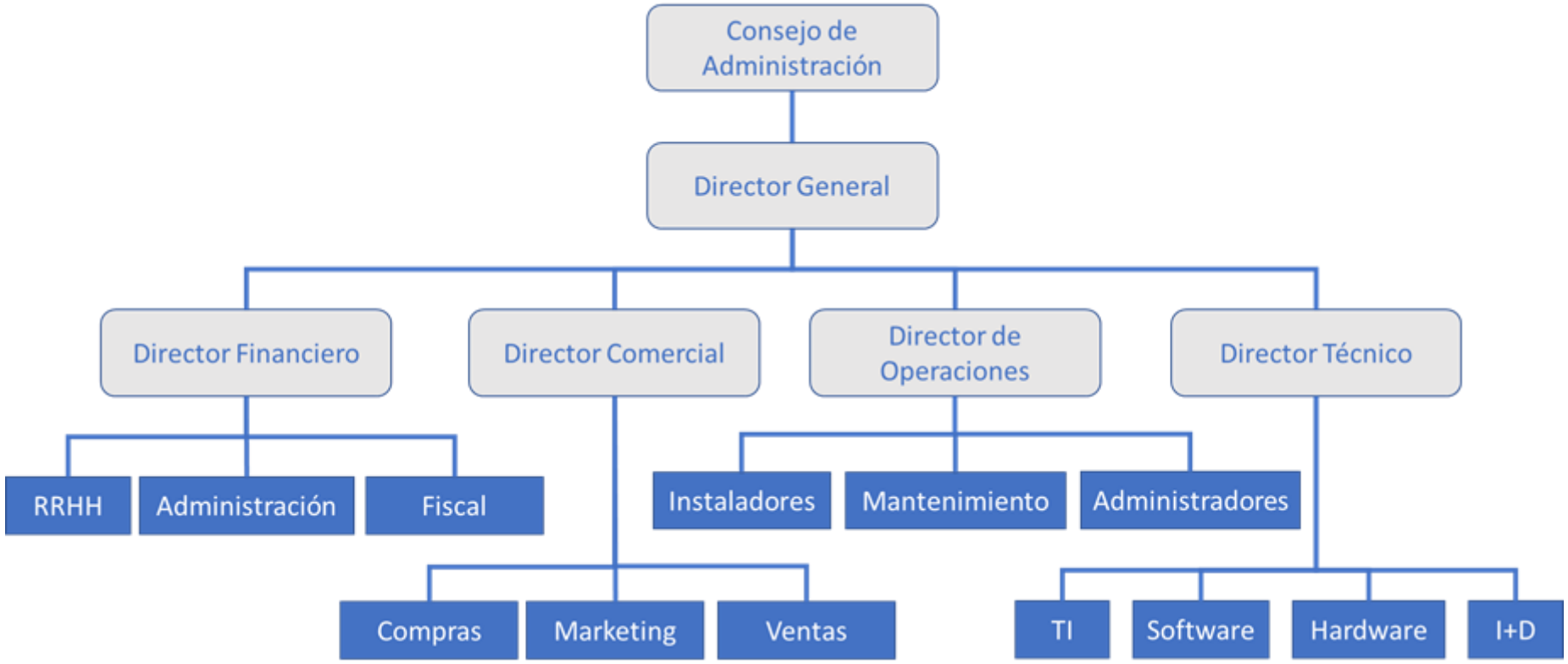
Contexto de la empresa

Presentación

- Ícaro S.A. es una empresa dedicada al diseño, implementación y administración de sistemas de gestión de plantas solares fotovoltaicas en España. Actualmente la empresa se encuentra en una etapa de crecimiento donde algunos fondos de inversión están interesados en apostar por ella.
- Su core de negocio es Sirio, un sistema de monitorización compuesto por una parte software y otra hardware ambas de desarrollo propio.
- Actualmente la empresa se encuentra en una etapa de crecimiento donde algunos fondos de inversión están interesados en apostar por ella.
- En sus planes a medio y corto plazo la empresa pretende comenzar a realizar proyectos en Latinoamérica y el norte de África.

Contexto de la empresa
Organización

- Ícaro cuenta con alrededor de 120 empleados repartidos en el organigrama que se muestra a continuación.



Contexto de la empresa

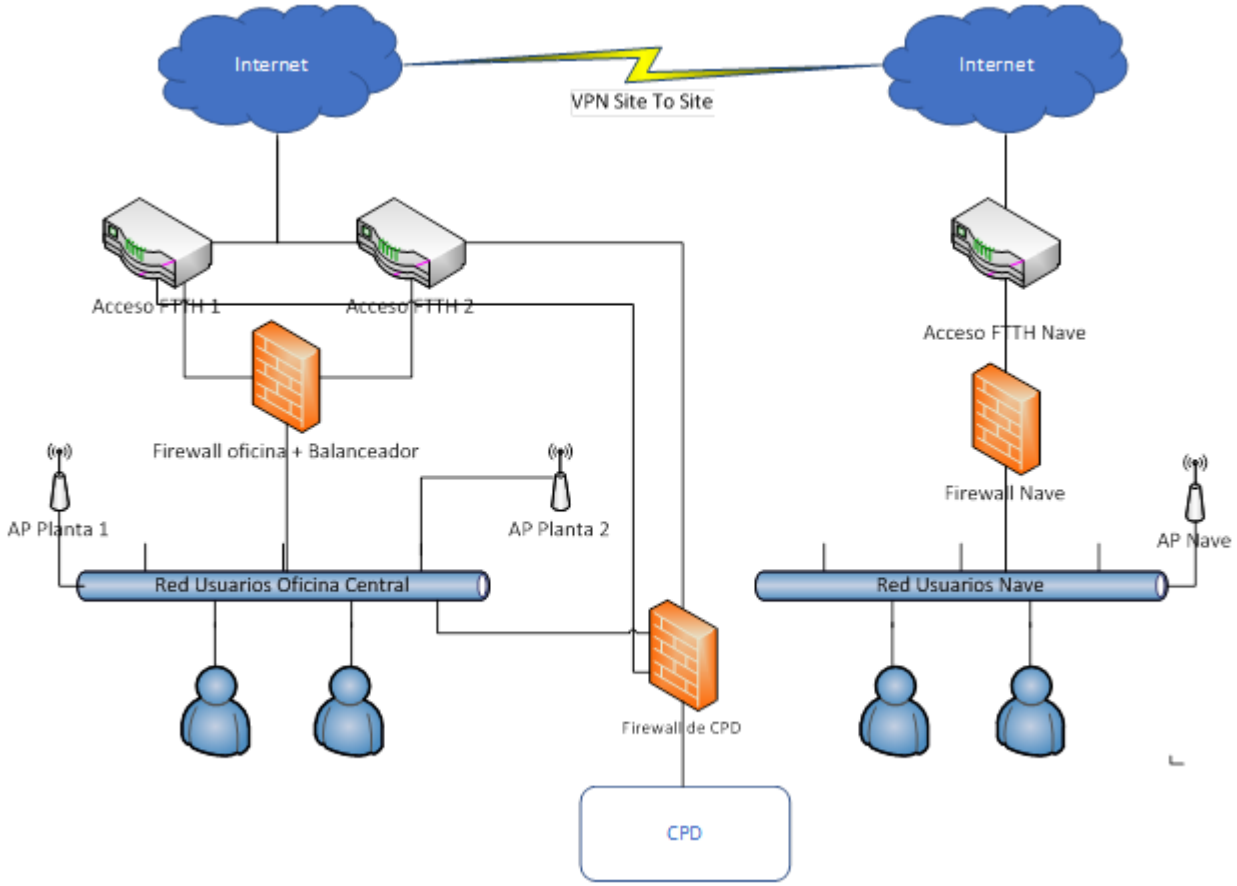
Instalaciones

- La empresa cuenta con:
  - Una sede central en Madrid compuesta por dos plantas y un sótano.
  - Una nave industrial a las afueras de Madrid para albergar los materiales y como centro de referente para los instaladores.
  - Armarios técnicos en las siguientes plantas fotovoltaicas

Almendralejo	Badajoz
Puertollano	Ciudad Real
Olmedilla De Alarcón	Cuenca
Arnedo	La Rioja
Las Gabias	Granada
Jumilla	Murcia
Lorca	Murcia
Olivenza	Badajoz
Calasparra	Murcia
Beneixama	Alicante
Salamanca	Salamanca
El Coronil	Sevilla
Almaraz	Cáceres
El Bonillo	Albacete
Guadarranque	Cádiz

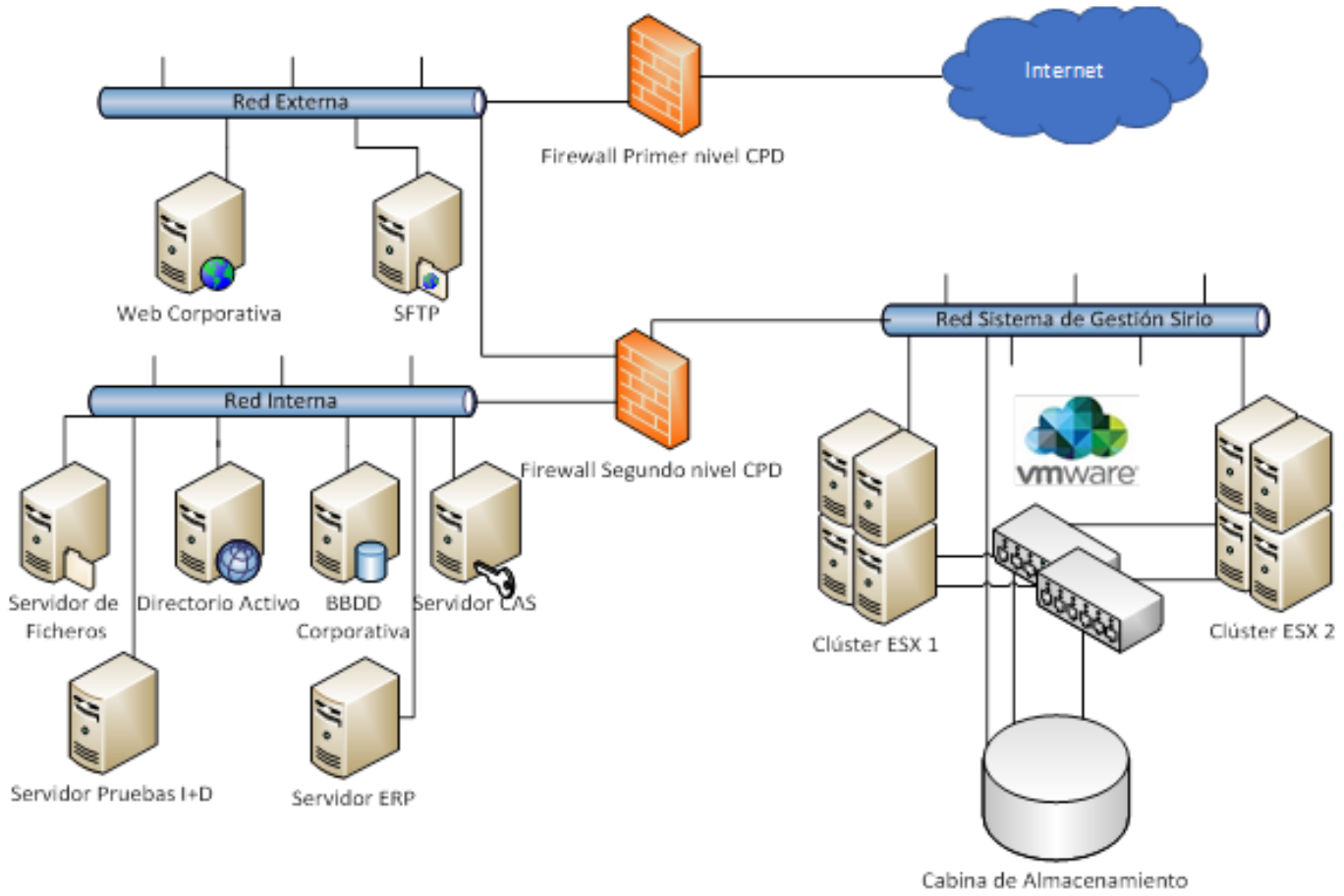
Contexto de la empresa
Comunicaciones y red

- Las oficinas centrales y la nave cuentan con dos accesos FTTH de 300Mb conectadas mediante una VPN Site to Site.
- Los Firewalls perimetrales son de tipo software
- El Firewall de acceso al CPD es físico
- Las conexiones con las plantas fotovoltaicas se realizan mediante conexiones VPN



Contexto de la empresa
Centro de datos

- El CPD cuenta con dos niveles de firewalls físicos.
- La red está segmentada en 3 ramas:
  - Externa
  - Interna
  - Sistema Sirio
- El sistema Sirio es el único virtualizado. El resto se basa en sistemas físicos.



Motivación del proyecto

- Debida a esta situación de crecimiento se ha identificado la necesidad de mejorar y alinear sus procesos de negocio con el cumplimiento de los estándares internacionales para afrontar este nuevo reto.

- De esta iniciativa general, surge la motivación de definir un Plan Director de Seguridad de la Información, el cual permitirá a la empresa en primer lugar conocer su nivel actual en esta materia de seguridad y definir las acciones necesarias para alcanzar el nivel de seguridad deseado y en segundo lugar identificar los procesos que le permitan ejecutar una mejora continua.

Enfoque y alcance del proyecto

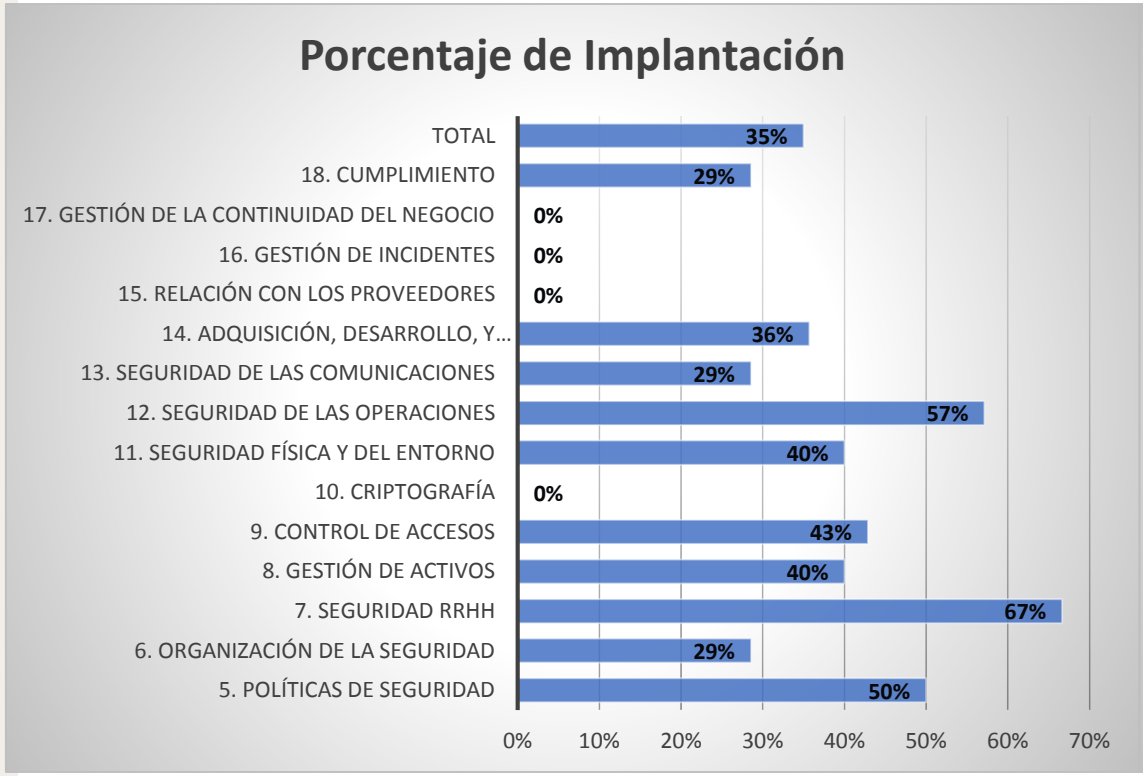
- El proyecto está alineado bajo los estándares ISO/IEC 27001 y 27002 en su ultima versión del año 2013.
- El alcance del mismo son todos los sistemas de información que dan soporte a los procesos, actividades y servicios de la empresa.
- Actividades principales del Plan Director de Seguridad:
  - Análisis diferencial contra la ISO/IEC 27002 para conocer el estado previo.
  - Identificación de los activos relacionados con los procesos, actividades y servicios relacionados con la información.
  - Valoración de los activos identificados.
  - Análisis de amenazas de los activos respecto a las cinco dimensiones de seguridad.
  - Análisis del nivel de riesgo respecto a los activos, su valoración y sus amenazas.
  - Proposición de proyectos para la mitigación de los riesgos identificados como críticos.
  - Realización de una auditoría de cumplimiento tras la implementación de los proyectos.

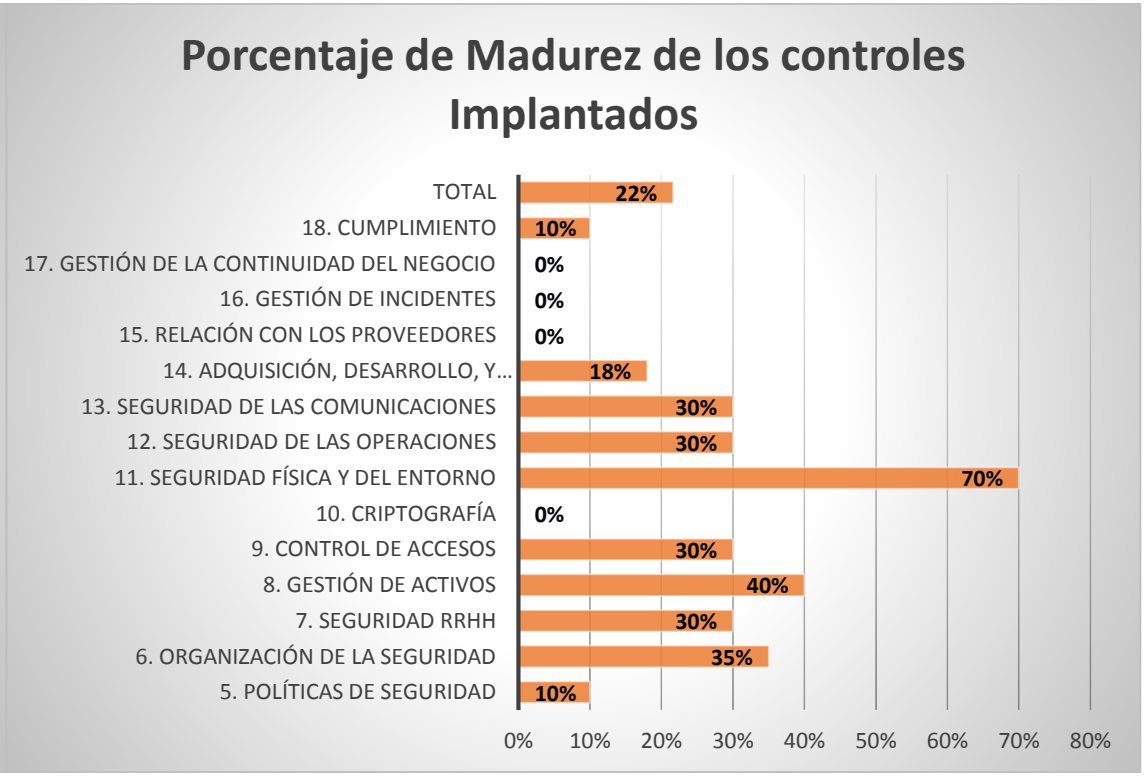
Análisis diferencial

Nivel	Estado	Madurez	Descripción
Nivel 0	Incompleto	0%	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso
Nivel 1	Ejecutado	10%	El proceso está implementado y alcanza su propósito básico.
Nivel 2	Gestionado	50%	El proceso ejecutado, está implementado de forma gestionada y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
Nivel 3	Establecido	90%	El proceso gestionado, está implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (Se documenta, se comunica y se da formación).
Nivel 4	Predecible	95%	El proceso establecido descrito anteriormente, ahora se ejecuta dentro de los límites definidos para alcanzar sus resultados de proceso.
Nivel 5	Optimizado	100%	El proceso descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.

DOMINIO	MADUREZ	CONTROLES IMPLANTADOS
5. Políticas de Seguridad	10%	1 de 2
6. Organización de la Seguridad	35%	2 de 7
7. Seguridad RRHH	30%	4 de 6
8. Gestión de Activos	40%	4 de 10
9. Control de Accesos	30%	6 de 14
10. Criptografía	0%	0 de 2
11. Seguridad Física y del entorno	70%	6 de 15
12. Seguridad de las Operaciones	30%	8 de 14
13. Seguridad de las Comunicaciones	30%	2 de 7
14. Adquisición, desarrollo, y mantenimiento.	18%	5 de 14
15. Relación con los proveedores	0%	0 de 5
16. Gestión de Incidentes	0%	0 de 7
17. Gestión de la Continuidad del Negocio	0%	0 de 4
18. Cumplimiento	10%	2 de 7

Análisis diferencial



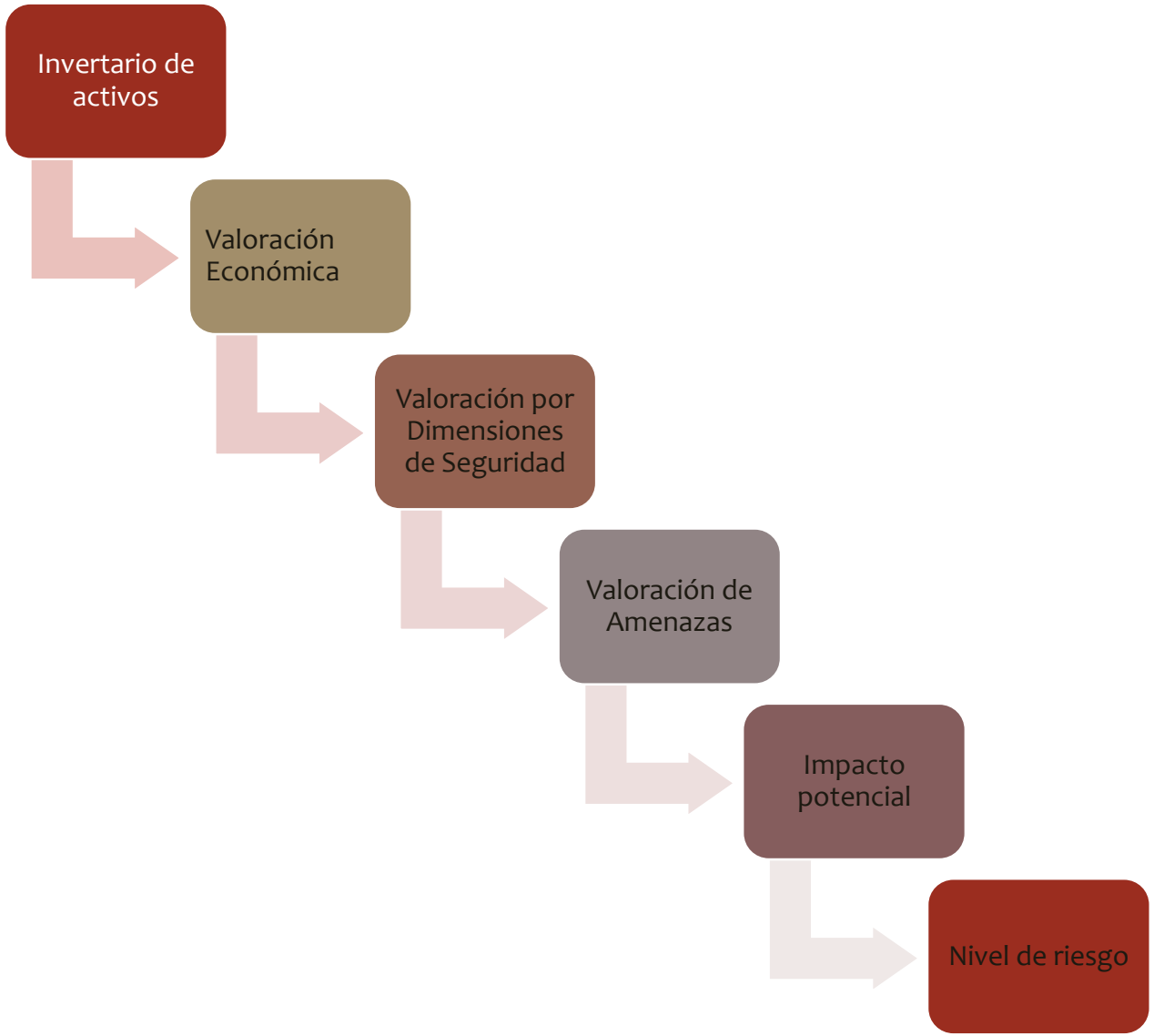


Sistema de gestión documental

- El sistema de gestión documental se compone de los siguientes documentos:
  - Política de seguridad
  - Procedimiento de auditoría
  - Gestión de indicadores
  - Procedimiento de revisión por la dirección
  - Gestión de roles y responsabilidades
  - Metodología de análisis de riesgos
  - Declaración de aplicabilidad

Análisis de riesgos

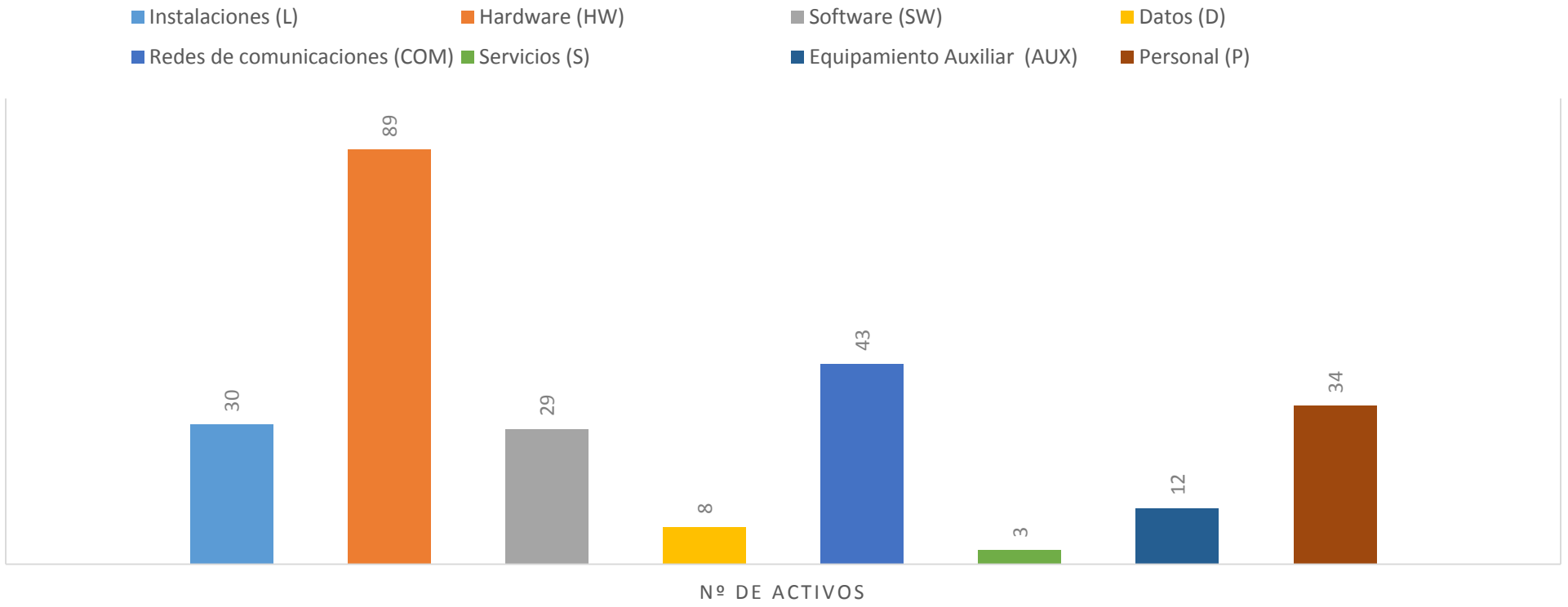
Esquema



Análisis de riesgos

Inventario de activos

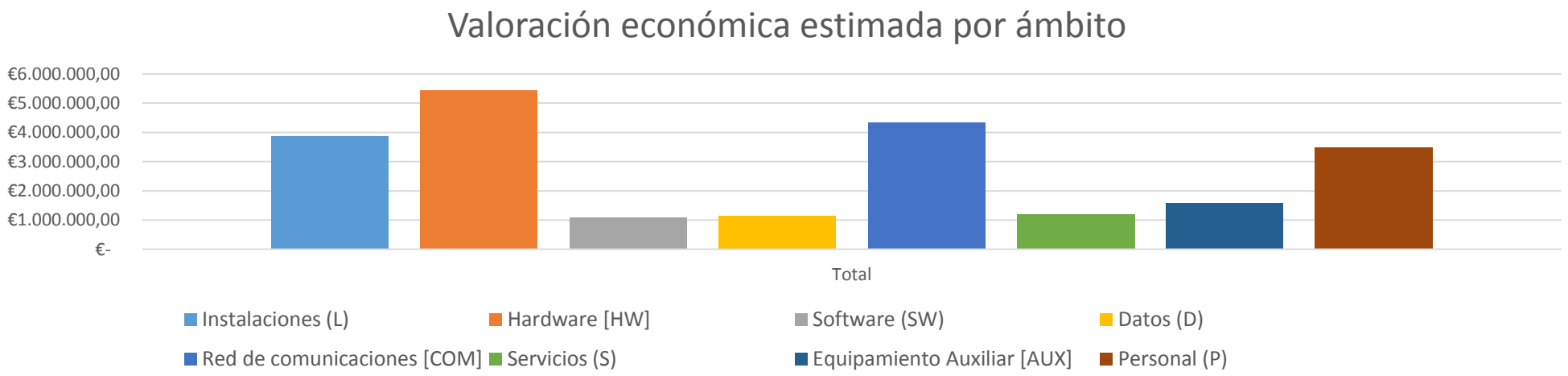
- El inventario de activos se realiza siguiendo la metodología MAGERIT.
- Tras el levantamiento de planta se han identificado 248 activos repartidos en 8 ámbitos.



Análisis de riesgos

Valoración económica de los activos

- Se ha utilizado la metodología MAGERIT para la valoración. Esta tiene en cuenta:
  - El valor de reposición, configuración, uso del activo y de pérdida de oportunidad.
- La valoración económica total estimada es de 22.165.750€

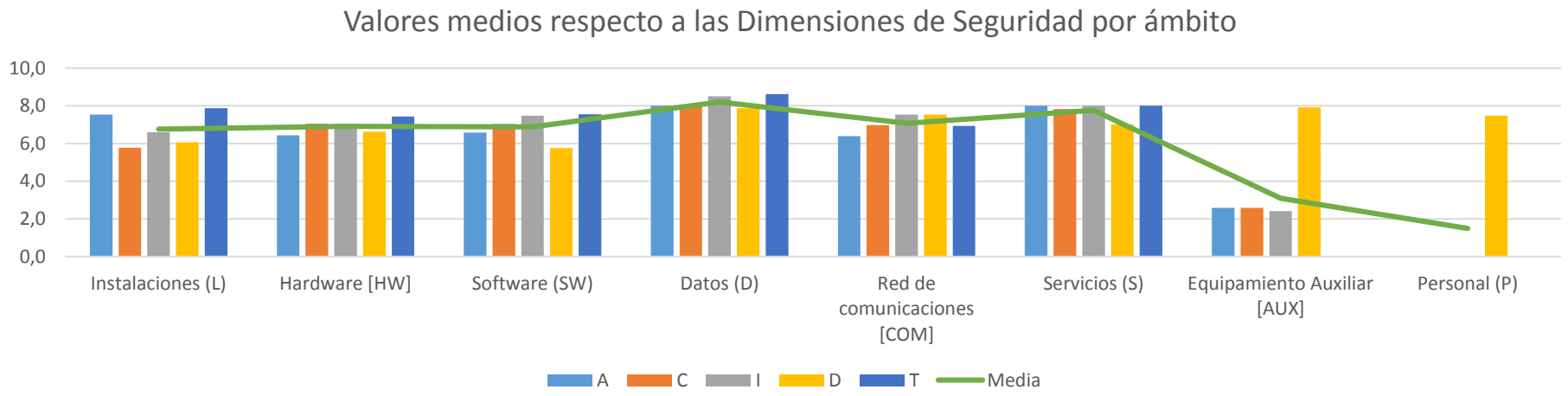


Valoración	Rango	Valor estimado
Muy Alta	Valor > 200K€	300K€
Alta	100K€ < Valor < 200K€	150K€
Media	50K€ < Valor < 100K€	75K€
Baja	10K€ < Valor < 50K€	30K€
Muy baja	Valor < 10K€	10K€

Análisis de riesgos
Valoración de activos por Dimensiones

- Se ha utilizado la metodología MAGERIT para la valoración de las Dimensiones de Seguridad que son: Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

- La valoración media es para todas las dimensiones y todos los ámbitos es de 6 puntos.



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

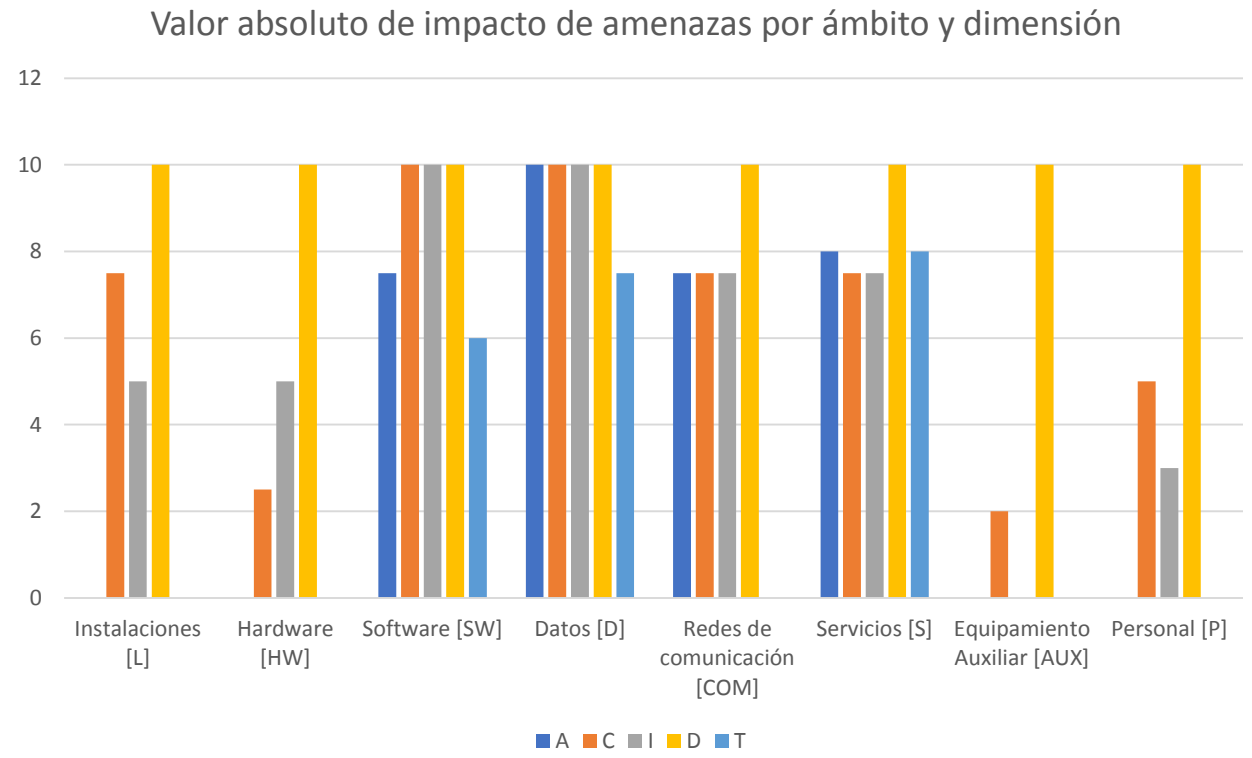
Análisis de riesgos

Valoración de las amenazas - Impacto

- Se ha utilizado el catalogo de amenazas de MAGERIT. Las divide en:
  - Desastres naturales, de origen industrial, no intencionados e intencionados.
- Se estima la vulnerabilidad de cada activo por el impacto de las amenazas y la posibilidad de ocurrencia de estas.

Rangos de valoración de Impacto

Impacto	ID	Rango
Muy Alto	MA	Valor > 95%
Alto	A	75% < Valor < 95%
Medio	M	50% < Valor < 75%
Bajo	B	30% < Valor < 50%
Muy Bajo	MB	10%< Valor < 30%



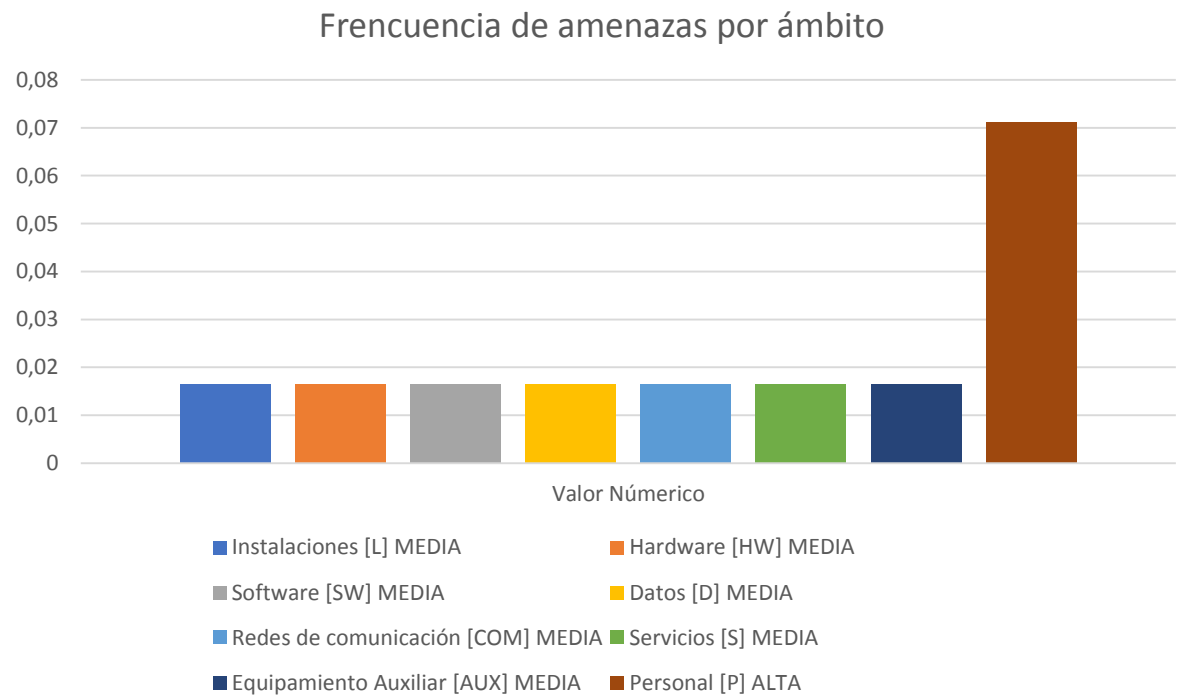
Análisis de riesgos

Valoración de las amenazas - Frecuencia

- Se ha utilizado el catalogo de amenazas de MAGERIT. Las divide en:
  - Desastres naturales, de origen industrial, no intencionados e intencionados.
- Se estima la vulnerabilidad de cada activo por el impacto de las amenazas y la posibilidad de ocurrencia de estas.

Categorías de frecuencia de amenazas

Vulnerabilidad	ID	Rango	Valor
Frecuencia Extrema	MA	1 vez al día	1
Frecuencia Alta	A	1 vez cada 2 semanas	26/365=0.071233
Frecuencia Media	M	1 vez cada 2 meses	6/365=0.016438
Frecuencia Baja	B	1 vez cada seis meses	2/365=0.005479
Frecuencia Muy Baja	MB	1 vez al año	1/365=0.002739



Análisis de riesgos
Impacto potencial

- Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.
- **Impacto potencial = Valor económico del activo x Valor del impacto de la amenaza**

	Impacto Dimensiones				
Grupo de Activos	A	C	I	D	T
Instalaciones [L]	0	7,5	5	10	0
Hardware [HW]	0	2,5	5	10	0
Software [SW]	7,5	10	10	10	6
Datos [D]	10	10	10	10	7,5
Redes de comunicación [COM]	7,5	7,5	7,5	10	0
Servicios [S]	8	7,5	7,5	10	8
Equipamiento Auxiliar [AUX]	0	2	0	10	0
Personal [P]	0	5	3	10	0

Análisis de riesgos

Nivel de Riesgo Aceptable y riesgo Residual

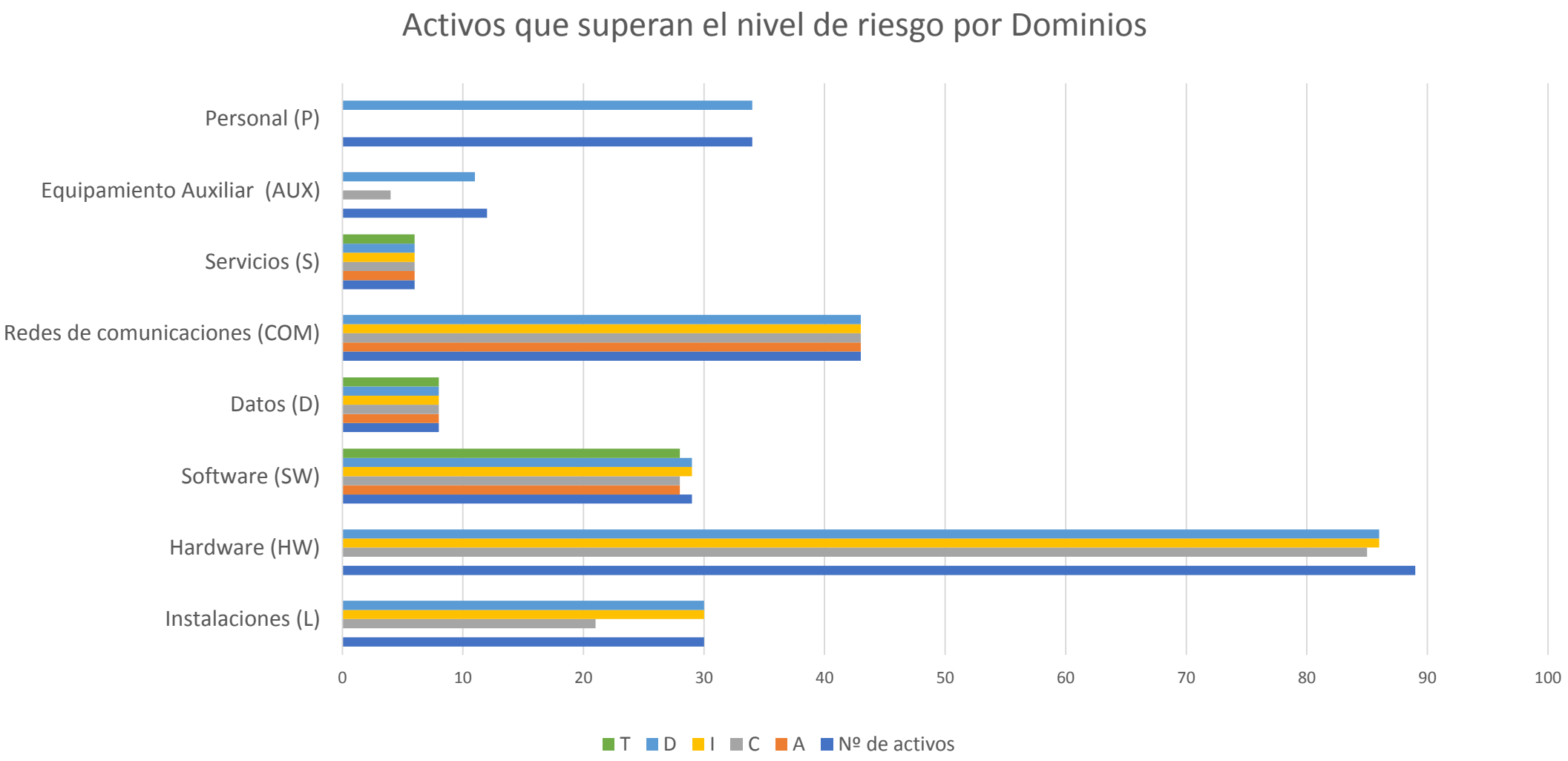
- La eliminación absoluta del riesgo es una situación casi imposible de alcanzar
- Se define un límite a partir del cual se pueda decidir si asumir un riesgo o por el contrario no asumirlo y aplicar controles.
- **Nivel de riesgo = Impacto potencial x frecuencia de la amenaza.**
- La dirección de Ícaro S.A. ha decidido que el nivel de riesgo aceptable sea el **MEDIO** o inferior.

Relación Impacto/Frecuencia

Riesgo		Frecuencia				
		MB (0,002)	B (0,005)	M (0,016)	A (0,071)	MA (1)
Impacto	MA (10)	A	MA	MA	MA	MA
	A (7-9)	M	A	A	MA	MA
	M (4-6)	B	M	M	A	A
	B (2-3)	MB	B	B	M	M
	MB (1)	MB	MB	MB	B	B

Análisis de riesgos

Activos que superan el nivel de riesgo



Propuestas de proyectos

Objetivo principal 1 de2

Proyecto	Objetivo Principal
Mejora Política de seguridad	Implantar una política de seguridad que mitigue los riesgos identificados
Formación continua en materia de seguridad	Concienciar a los empleados de la empresa de la importancia de la seguridad de la información
Mejora de la seguridad física hardware desplegados en las plantas	Aumentar la integridad, disponibilidad y confidencialidad del hardware propio desplegado en las plantas fotovoltaicas
Mejora de la seguridad física en los accesos de la empresa y a estancias sensibles	Aumentar todas las dimensiones de seguridad de los activos que se encuentran emplazados dentro de las instalaciones de la empresa y especialmente en estancias sensible.
Mejora de la disponibilidad de la infraestructura TI del sistema Sirio	Mejorar la disponibilidad del sistema principal de la empresa para garantizar mejores niveles de servicio
Cifrado de los datos y comunicaciones del sistema Sirio	Aumentar la integridad, autenticidad y confidencialidad de la información relativa el sistema core de la empresa
Cifrado de los datos de los PC's y móviles	Aumentar la integridad, autenticidad y confidencialidad de la información de la empresa

Propuestas de proyectos

Objetivo principal 2 de 2

Proyecto	Objetivo Principal
Virtualización servidores entorno corporativo	Mejorar la disponibilidad de los sistemas corporativos de la empresa
Comunicaciones profesionales de acceso a Internet para la sede central	Aumentar la disponibilidad e integridad del acceso a internet de la sede central.
Red MPLS para monitorización de plantas	Mejorar el acceso, la disponibilidad, e integridad de la red de monitorización de plantas fotovoltaicas.
Mejora seguridad perimetral de red de CPD	Dotar de mayor confidencialidad e integridad a los activos y datos que de alojan en el CPD corporativo.
Revisión de la seguridad de la información	Comprobar el cumplimiento de las políticas de seguridad de la información y los procesos y sistemas que las soportan.
Modelo de relación con proveedores	Crear un modelo de relación único con los proveedores de la empresa que mejore la seguridad de la información.

Propuestas de proyectos

Planificación

<table>
<tr><th rowspan="2">Proyecto</th><th colspan="52">AÑO 1</th></tr>
<tr><th>S1</th><th>S2</th><th>S3</th><th>S4</th><th>S5</th><th>S6</th><th>S7</th><th>S8</th><th>S9</th><th>S10</th><th>S11</th><th>S12</th><th>S13</th><th>S14</th><th>S15</th><th>S16</th><th>S17</th><th>S18</th><th>S19</th><th>S20</th><th>S21</th><th>S22</th><th>S23</th><th>S24</th><th>S25</th><th>S26</th><th>S27</th><th>S28</th><th>S29</th><th>S30</th><th>S31</th><th>S32</th><th>S33</th><th>S34</th><th>S35</th><th>S36</th><th>S37</th><th>S38</th><th>S39</th><th>S40</th><th>S41</th><th>S42</th><th>S43</th><th>S44</th><th>S45</th><th>S46</th><th>S47</th><th>S48</th><th>S49</th><th>S50</th><th>S51</th><th>S52</th></tr>
<tr><td>4.2.1</td><td colspan="4">4 semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1 S</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1 S</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.3</td><td></td><td></td><td></td><td></td><td></td><td colspan="41">40 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.4</td><td></td><td></td><td></td><td></td><td></td><td colspan="29">26 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.5</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="27">26 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.6</td><td></td><td></td><td></td><td></td><td></td><td colspan="13">12 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.7</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="10">10 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="15">15 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.9</td><td></td><td></td><td></td><td></td><td></td><td colspan="3">3 Sem.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.10</td><td></td><td></td><td></td><td></td><td></td><td colspan="27">26 Semanas</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4.2.11</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="13">12 Semanas</td><td></td><td></td></tr>
<tr><td>4.2.12</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="2">2 S.</td></tr>
<tr><td>4.2.13</td><td></td><td></td><td></td><td></td><td colspan="2">2 S.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

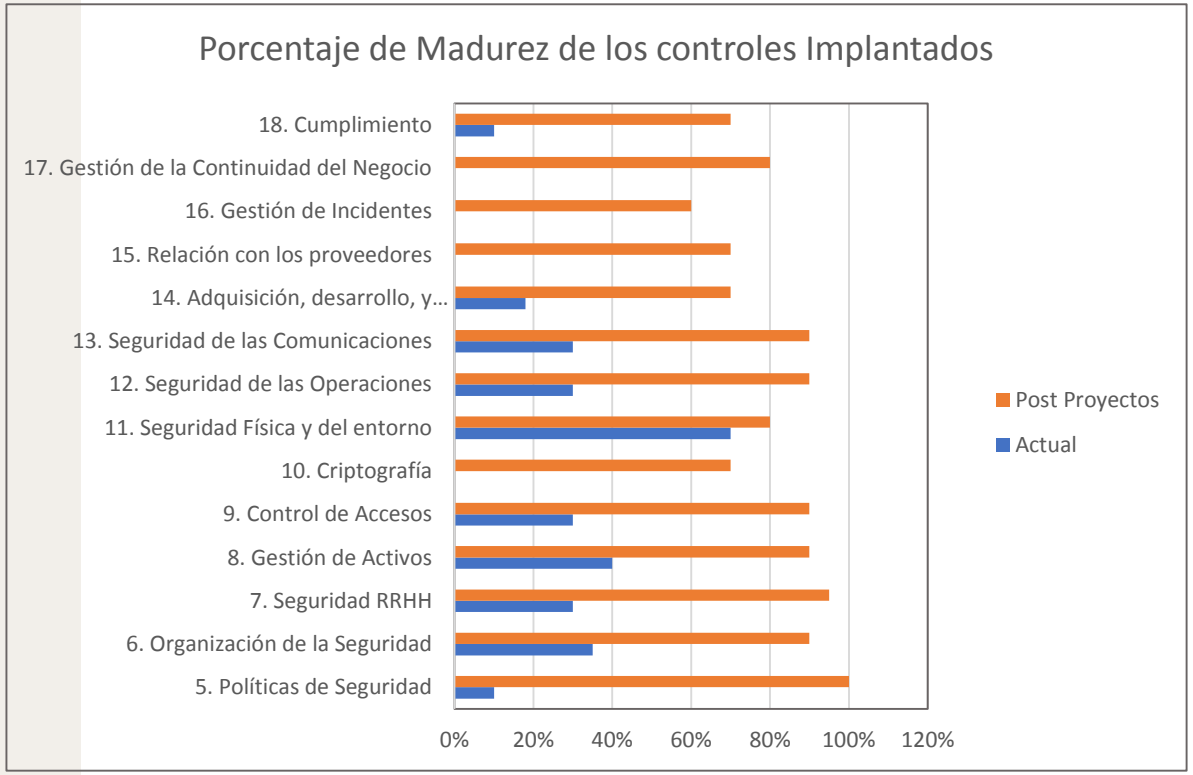
Propuestas de proyectos

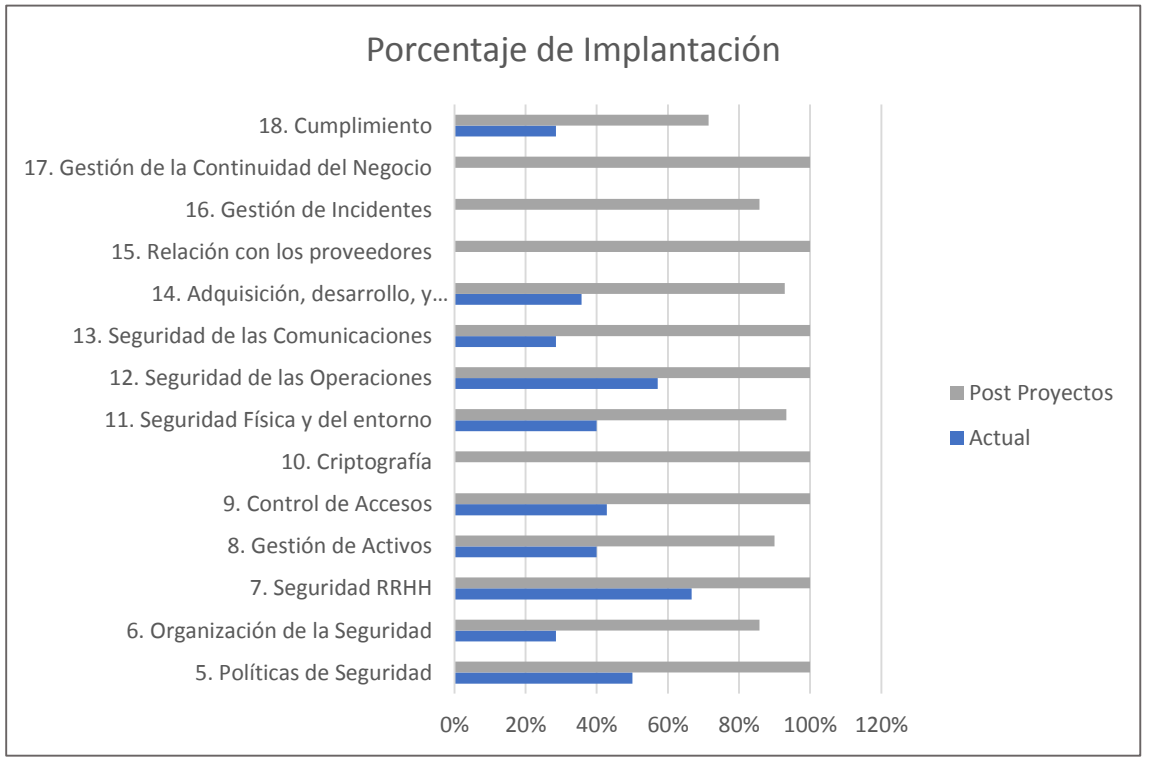
Análisis diferencial deseable tras la implantación

DOMINIO	INICIAL		TRAS PROYECTOS	
	MADUREZ	CONTROLES IMPLANTADOS	MADUREZ	CONTROLES IMPLANTADOS
5. Políticas de Seguridad	10%	1 de 2	100%	2 de 2
6. Organización de la Seguridad	35%	2 de 7	90%	6 de 7
7. Seguridad RRHH	30%	4 de 6	95%	6 de 6
8. Gestión de Activos	40%	4 de 10	90%	9 de 10
9. Control de Accesos	30%	6 de 14	90%	14 de 14
10. Criptografía	0%	0 de 2	70%	2 de 2
11. Seguridad Física y del entorno	70%	6 de 15	80%	14 de 15
12. Seguridad de las Operaciones	30%	8 de 14	90%	14 de 14
13. Seguridad de las Comunicaciones	30%	2 de 7	90%	7 de 7
14. Adquisición, desarrollo, y mantenimiento.	18%	5 de 14	70%	13 de 14
15. Relación con los proveedores	0%	0 de 5	70%	5 de 5
16. Gestión de Incidentes	0%	0 de 7	60%	6 de 7
17. Gestión de la Continuidad del Negocio	0%	0 de 4	80%	4 de 4
18. Cumplimiento	10%	2 de 7	70%	5 de 7

Propuestas de proyectos

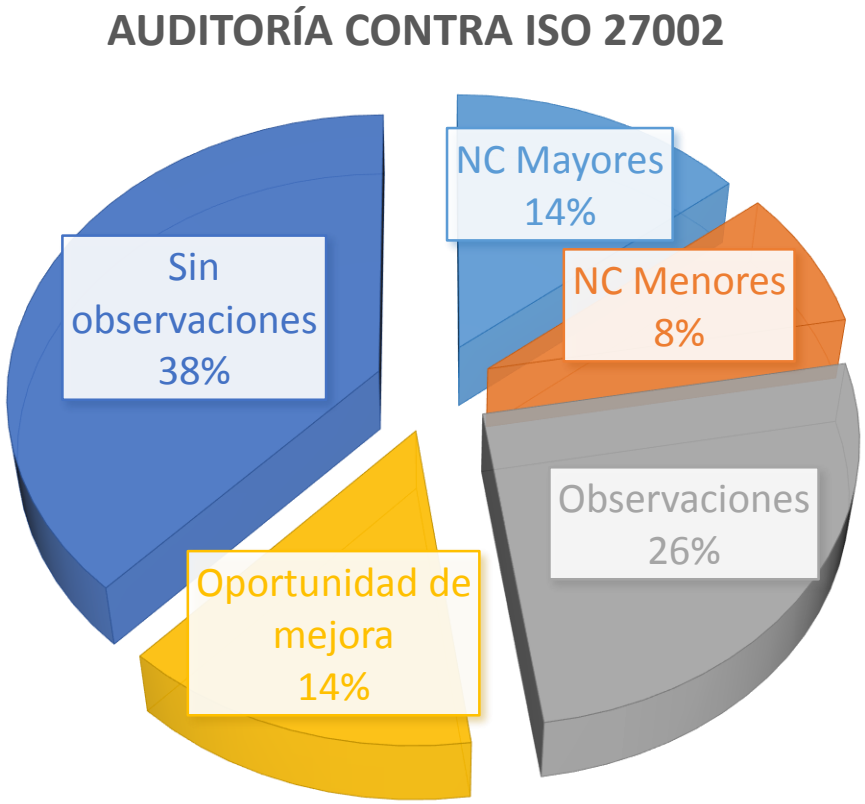
Análisis diferencial tras la implantación





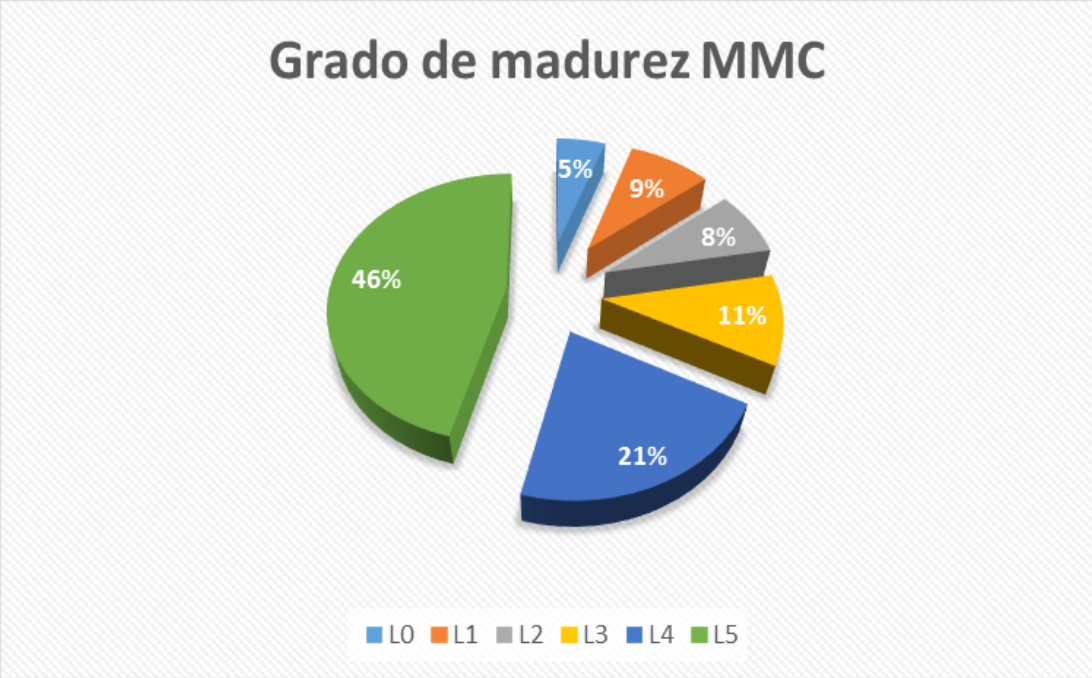
Auditoría
Resultados

- Una vez que ha transcurrido el año de implantación de los proyectos de mitigación del riesgo, es hora de analizar su impacto realizando una auditoría.
- Está se realizará contra la norma ISO/IEC 27002.
- El 78% de los controles están implantados y han superado la auditoría contra la norma.
- El 14% de los controles ha presentan No Conformidades Mayores
- El 8% de los controles ha presentado No Conformidades Menores



Auditoría
Resultados

- Una vez que ha transcurrido el año de implantación de los proyectos de mitigación del riesgo, es hora de analizar su impacto realizando una auditoría

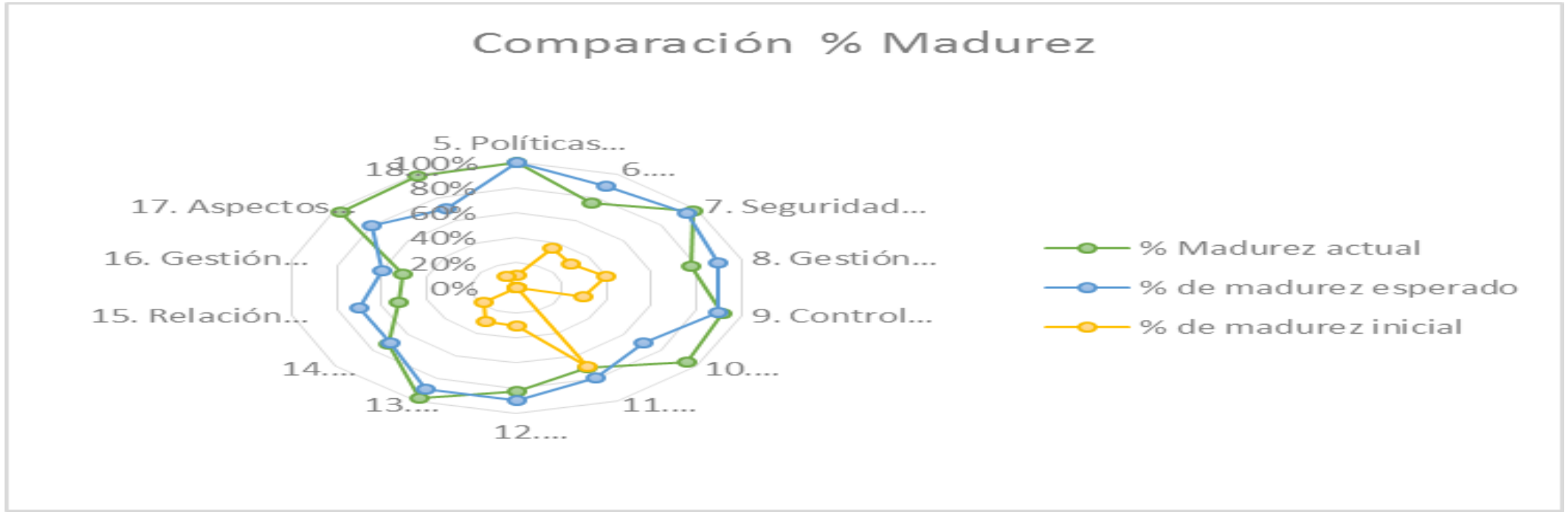


Dominio	% Madurez
5. Políticas de Seguridad	100%
6. Organización de la seguridad de la información	75%
7. Seguridad relativa a los RRHH	98%
8. Gestión de activos	78%
9. Control de acceso	92%
10. Criptografía	95%
11. Seguridad física y del entorno	71%
12. Seguridad de las operaciones	82%
13. Seguridad de las comunicaciones	97%
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	71%
15. Relación con proveedores	52%
16. Gestión de incidentes de seguridad de la información	51%
17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	98%
18. Cumplimiento	99%

Auditoría de cumplimiento

Comparación de la madurez

- Para comprobar el estado de la seguridad de la información de la empresa, se vuelve a utilizar el Modelo de Madurez.



Conclusiones

Objetivos conseguidos

- Se ha establecido el estado inicial de la seguridad de la información de la organización, así como los objetivos a alcanzar tras la implantación del SGSI.
- Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2013.
- Se ha realizado el análisis de riesgos de la organización del que se ha obtenido la lista de todos los activos de la empresa, las amenazas posibles a las que está expuesta la organización así el impacto y el riesgo de todos los activos de la empresa que ha permitido identificar los activos más prioritarios en cuanto a seguridad de la información.
- Se han definido y completado con éxito una serie de proyectos para mejorar la seguridad de la información de la organización, teniendo en cuenta al análisis de riesgos obtenido.
- Se ha evaluado el nivel de madurez de la seguridad de la información de la organización respecto a la norma ISO 27002:2013.
- Se ha conseguido reducir el riesgo de los activos de la organización y con ello mejorar significativamente el estado inicial de la seguridad de la información de la organización.
- Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información.
- Existe el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

Gracias por su atención

Universitat Rovira i Virgili

Luis Rodríguez Conde