Universitat Rovira i Virgili

UOC www.uoc.edu

UAB Universitat Autònoma de Barcelona

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

PRESENTACIÓN DEL PROYECTO

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013

CYBSA Cosmética y Belleza S.A

MARÍA BELÉN RAYO LANZAS

Trabajo Fin de Máster (TFM)

CONTENIDO

CYBSA Cosmética y Belleza S.A

INTRODUCCIÓN

CYBSA Cosmética y Belleza S.A

Sistema de Gestión de la Seguridad de la Información (SGSI)

Conjunto de políticas y procedimientos que normalizan la gestión de la seguridad de la información de toda una organización o de uno o varios de sus procesos de negocio.

Plan Director de Seguridad (PDS)

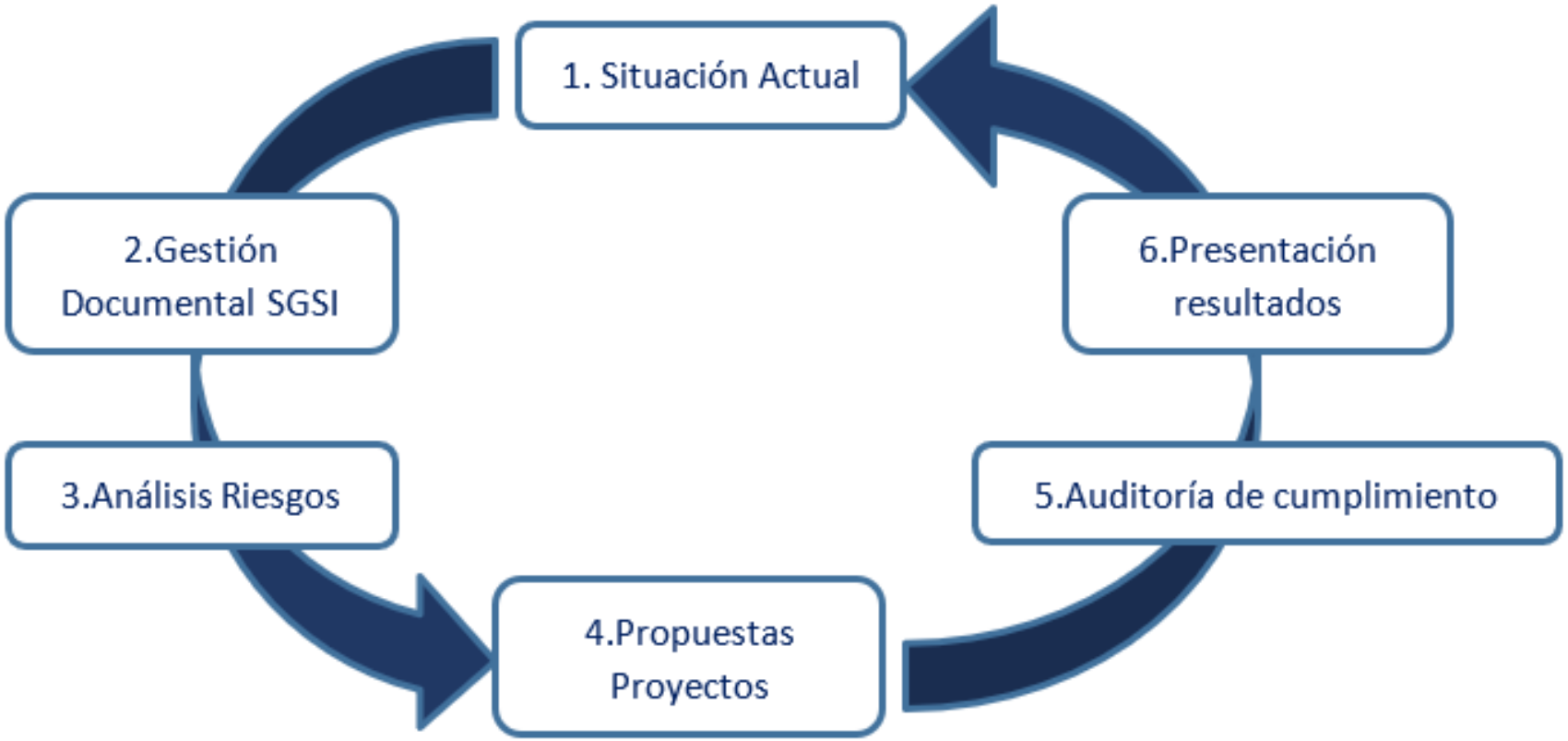
Proyecto desarrollado con el objetivo de establecer una serie de criterios que actúen como base para la implementación de un SGSI.

Plan Director de Seguridad CYBSA

Modelo de mejora continua PDCA (Plan-Do-Check-Act)
Normas ISO/IEC 27001:2013 / ISO/IEC 27002:2013

FASES DEL PROYECTO

CYBSA Cosmética y Belleza S.A



CONTEXTO DE LA ORGANIZACIÓN

Cosmética y Belleza S.A

- Cosmética y Belleza S.A (CYBSA) es una compañía española, creada en 1990, especializada en venta directa de diferentes líneas de negocio, que integran una oferta de productos de belleza completa 360º.

- Son distribuidores de marcas de otros proveedores y también disponen de marca propia en cada una de las líneas

- Tiene presencia en 12 países, en 3 continentes (Europa, América y África) y su modelo de negocio se sustenta en una actividad comercial desarrollada a través de una red de ventas formada por más de 10.000 personas y a través de la venta online.

CONTEXTO DE LA ORGANIZACIÓN

CYBSA Cosmética y Belleza S.A

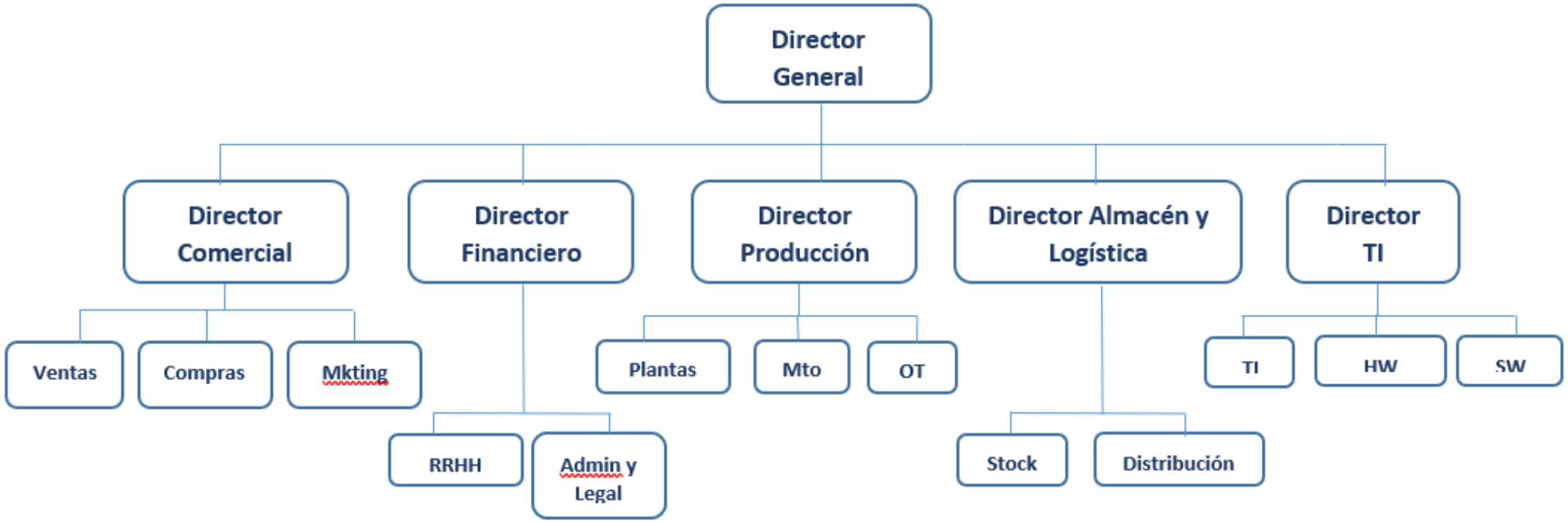
Estructura Organizativa

- La compañía tiene 20.000 empleados a lo largo de los 12 países y toda la actividad se gestiona desde la sede matriz, ubicada en España.
- En cada una de las sedes hay consejo ejecutivo en el que cada responsable reporta directamente al Director del consejo de administración de su área.
- Las plantas de producción de la marca propia también se ubican en España.

CONTEXTO DE LA ORGANIZACIÓN

CYBSA Cosmética y Belleza S.A

Estructura Organizativa



CONTEXTO DE LA ORGANIZACIÓN

CYBSA Cosmética y Belleza S.A

Infraestructura e instalaciones

- 2 CPDs (de proveedores externos), uno principal ubicado en Madrid y otro ubicado en Santiago de Chile, configurados como un único CPD extendido,
- En cada CPD tienen equipamiento de seguridad perimetral con doble barrera de FW de diferente tecnología. En cada sede cuentan con un FW.
- Solución antispam para proteger el correo en O36
- Solución NAC desplegada
- Solución EPP + Solución EDR en cada uno de los puestos de trabajo corporativos
- Solución VPN para empleados que trabajan en movilidad (comerciales).
- FW en las plantas industriales y centros de logística

MOTIVACIÓN

- **Debido a la transformación digital que está experimentando CYBSA, surge la necesidad de mejorar y alinear sus procesos de negocio con el cumplimiento de los estándares internacionales de seguridad en este nuevo reto.**

- **Se desarrolla un Plan Director de Seguridad de la Información para conocer su nivel actual en esta materia de seguridad, definir las acciones necesarias para alcanzar el nivel de seguridad deseado e identificar los procesos de mejora continua.**

OBJETIVOS

CYBSA Cosmética y Belleza S.A

- Definir un mapa de riesgos de seguridad de la información.
- Identificar procesos de negocio y dependencias.
- Valorar las necesidades de seguridad y posibles impactos según negocio.
- Análisis holístico de las amenazas que pueden suceder agrupadas por escenarios.
- Cálculo de riesgo potencial.
- Decidir el criterio de aceptación de riesgo.
- Definir una serie de proyectos para mitigar el mayor número de riesgos
- Realizar una auditoría de cumplimiento contra la ISO/IEC 27001 para certificar la minimización del riesgo.

ENFOQUE, METODOLOGÍA Y ALCANCE

Cosmética y Belleza S.A

- **ALCANCE**
  - **M odelización de los activos, sus dependencias, escenarios de riesgos, análisis y valoración de estos, de acuerdo a las normas de referencia ISO/IEC 27001 y 27002.**
  - **Se incluirán dentro de la definición del proyecto del PDSI:**
    - **Los activos relacionados con el tratamiento e intercambio de la información dentro de los procesos y las líneas de negocio de la compañía.**
    - **Los procesos a nivel técnico y organizativo relativos al tratamiento e intercambio de la información de la compañía.**
    - **Los recursos orgánicos e inorgánicos, externos e internos que tienen acceso a algún activo o proceso relativo al tratamiento e intercambio de la información de la compañía.**

ENFOQUE, METODOLOGÍA Y ALCANCE

CYBSA Cosmética y Belleza S.A

- **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.**
  - **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.**

ANÁLISIS DIFERENCIAL

CYBSA Cosmética y Belleza S.A

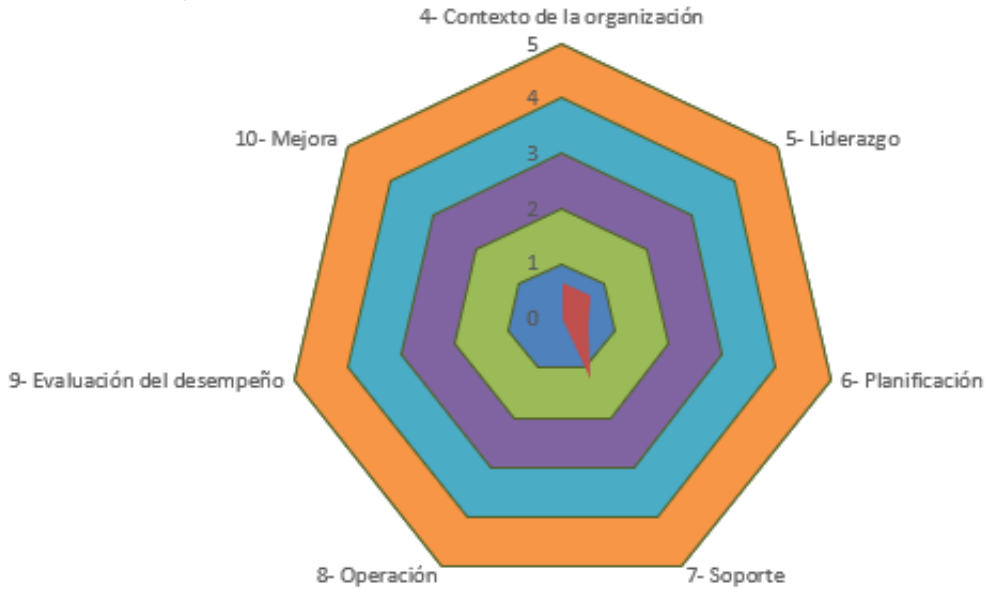
- Estudio del nivel de madurez con el que parte CYBSA sobre cada control de la ISO/IEC 27001:2013 y ISO/IEC 27002:2013 de acuerdo al modelo CMMI.

0- No se aplican procesos administrativos en lo absoluto
1- Los procesos son a medida y desorganizados
2- Los procesos siguen un patrón regular
3- Los procesos se documentan y comunican
4- Los procesos se monitorizan y se evalúan
5- Las buenas prácticas se siguen y se automatizan

ANÁLISIS DIFERENCIAL

CYBSA Cosmética y Belleza S.A

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



- Nivel de implantación (considerando como implantados aquellos con valor superior o igual a 3) del 0%.

- Nivel de madurez media de todos los dominios es de un 9%.

DOMINIOS	% madurez	Número de controles implantados
4- Contexto de la organización	13%	0
5- Liderazgo	13%	0
6- Planificación	10%	0
7- Soporte	24%	0
8- Operación	0%	0
9- Evaluación del desempeño	0%	0
10- Mejora	0%	0

ANÁLISIS DIFERENCIAL

CYBSA Cosmética y Belleza S.A

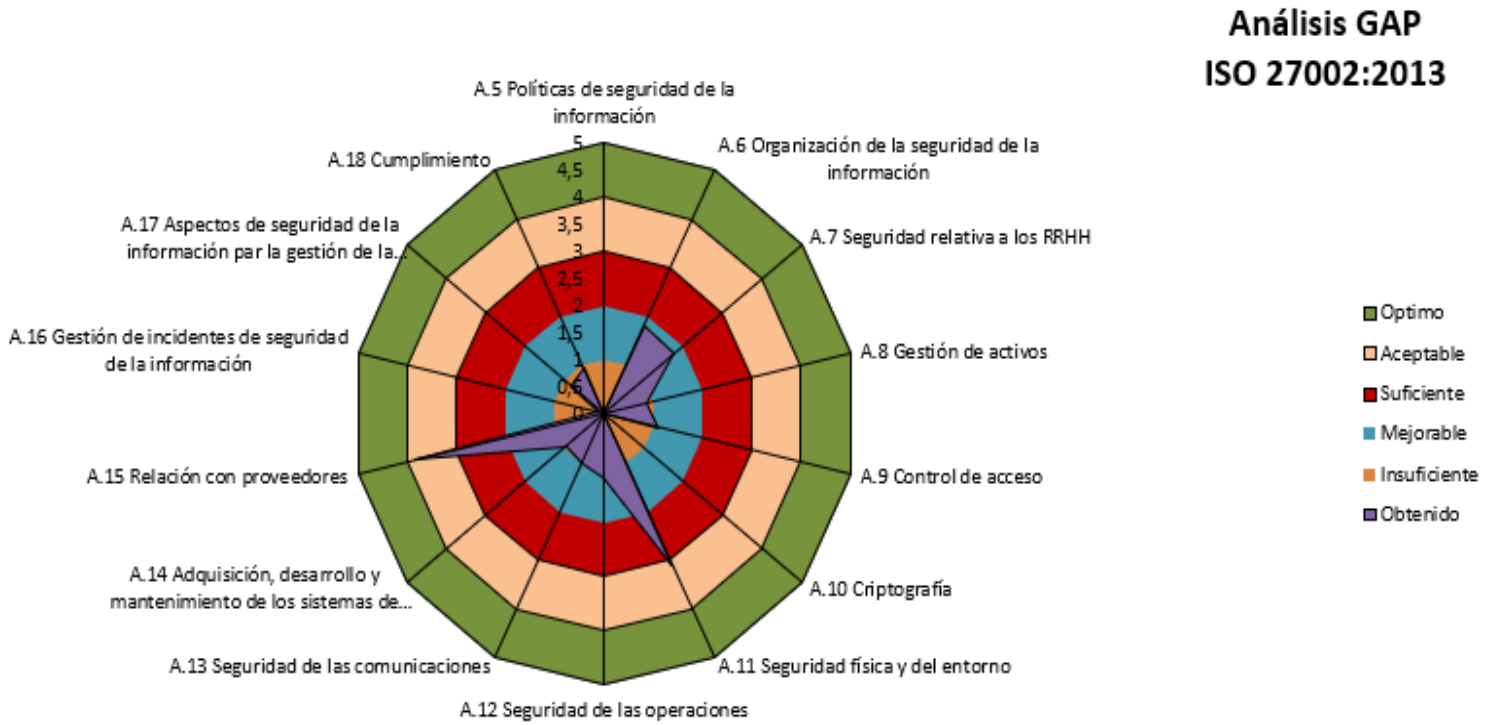
- **Nivel de cumplimiento en los dominios de la ISO/IEC 27002:2013**

	Madurez	Número de controles implantados
5. Políticas de Seguridad	0 %	0 de 2
6. Organización de la Seguridad	36%	3 de 7
7. Seguridad RRHH	36%	2 de 6
8. Gestión de Activos	17%	0 de 10
9. Control de Accesos	22%	1 de 14
10. Criptografía	0%	0 de 2
11. Seguridad Física y del entorno	62%	10 de 15
12. Seguridad de las Operaciones	24%	1 de 14
13. Seguridad de las Comunicaciones	20%	0 de 7
14. Adquisición, desarrollo, y mantenimiento.	20%	0 de 5
15. Relación con los proveedores	77%	5 de 5
16. Gestión de Incidentes	3%	0 de 7
17. Gestión de la Continuidad del Negocio	17%	1 de 4
18. Cumplimiento	19%	1 de 8

ANÁLISIS DIFERENCIAL

CYBSA Cosmética y Belleza S.A

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



- **Nivel de implantación (considerando como implantados aquellos con valor superior o igual a 3) del 22%.**
- **Nivel de madurez media de todos los dominios es de un 25%.**

SISTEMA DE GESTIÓN DOCUMENTAL

CYBSA Cosmética y Belleza S.A

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

ANÁLISIS DE RIESGOS

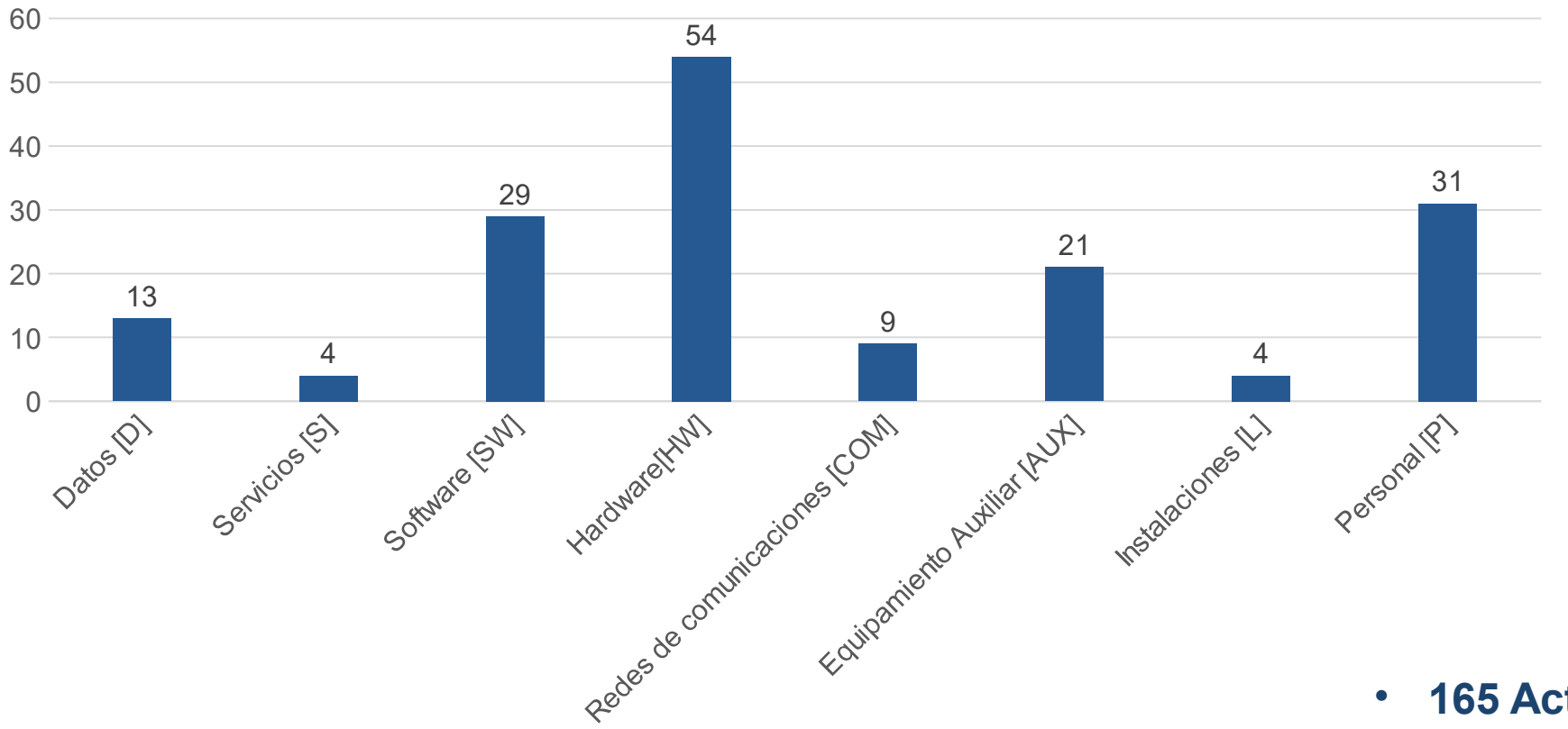
Cosmética y Belleza S.A

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

ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **INVENTARIO DE ACTIVOS. CLASIFICACIÓN**



- **165 Activos**
- **8 Categorías**

ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **INVENTARIO DE ACTIVOS. VALORACIÓN**

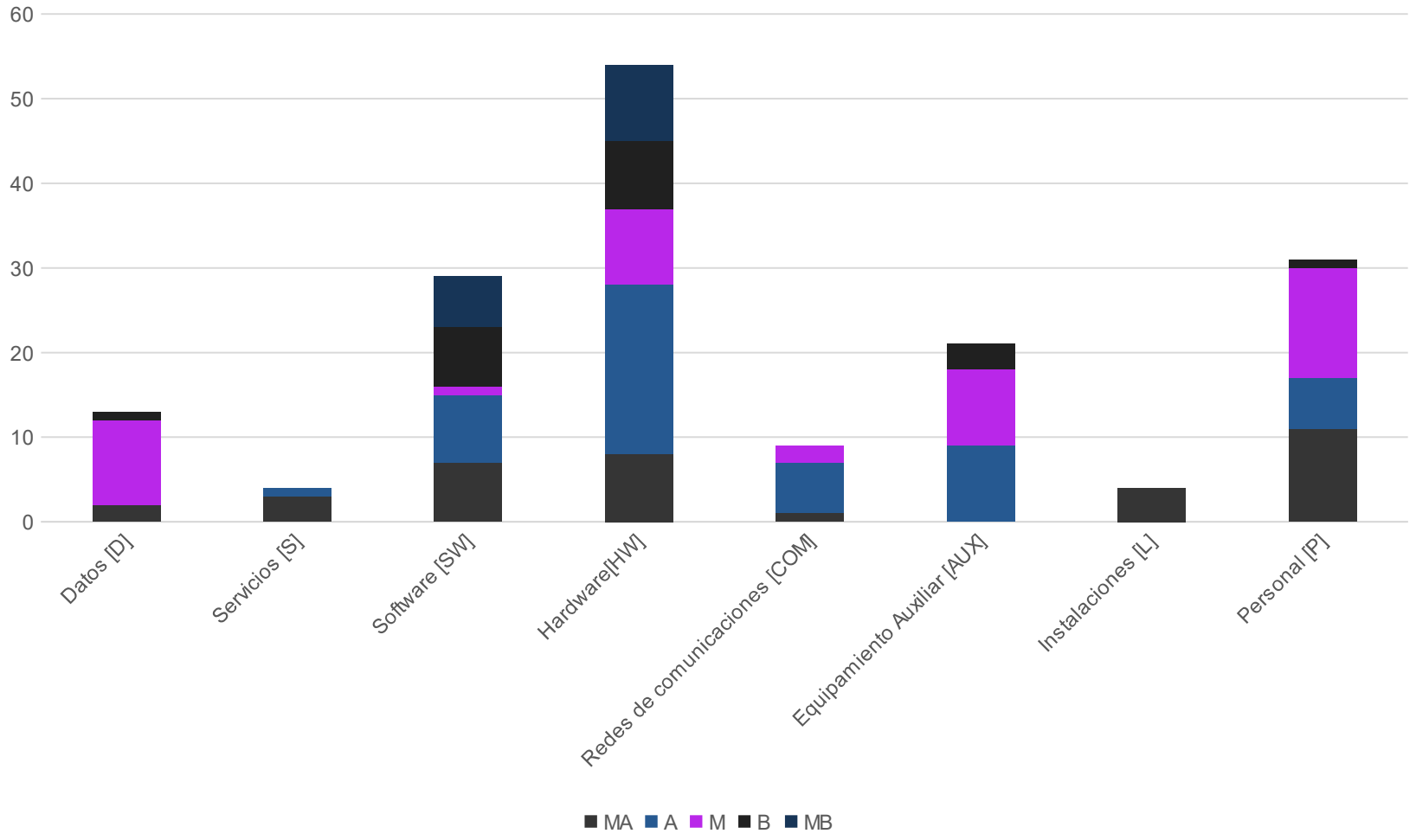
  - **El valor de uso:** las pérdidas que supone a CYBSA en su actividad de negocio durante el tiempo que no puede utilizar dicho activo.
  - **El valor de configuración:** es el tiempo que se necesita desde que se adquiere el nuevo activo hasta que se configura para realizar su función**.**
  - **El valor de sustitución:** es la capacidad que tiene CYBSA para sustituir el activo en caso de anomalía en la función habitual que desarrolla

ID	Valoración	Rango	Valor estimado
MA	Muy Alta	Valor > 300K€	350K€
A	Alta	100K€ < Valor < 300K€	200K€
M	Media	50K€ < Valor < 100K€	75K€
B	Baja	10K€ < Valor < 50K€	30K€
MB	Muy baja	Valor < 10K€	10K€

ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **INVENTARIO DE ACTIVOS. VALORACIÓN**



ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **INVENTARIO DE ACTIVOS. VALORACIÓN DIMENSIONES DE SEGURIDAD**

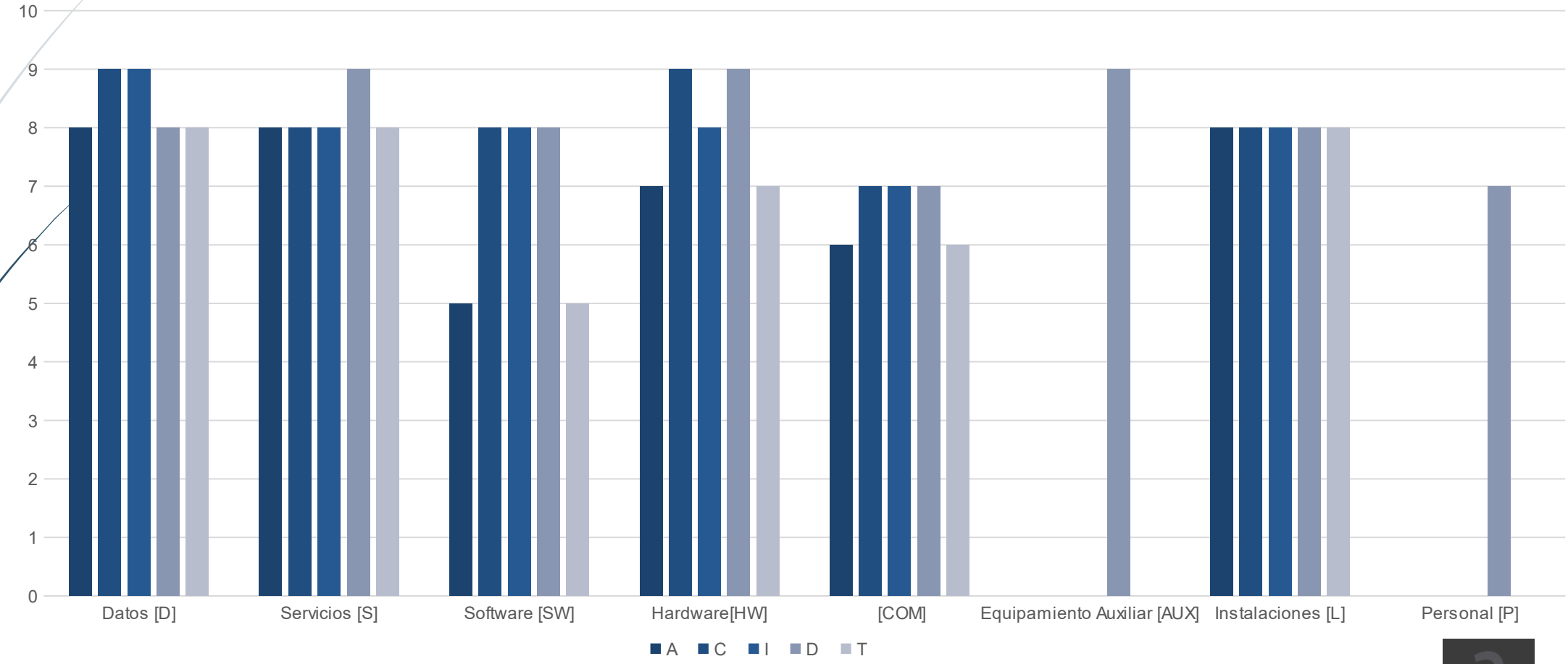
  - Autenticidad [A]
  - Confidencialidad [C]
  - Integridad [I]
  - Disponibilidad [D]
  - Trazabilidad [T

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

Cosmética y Belleza S.A

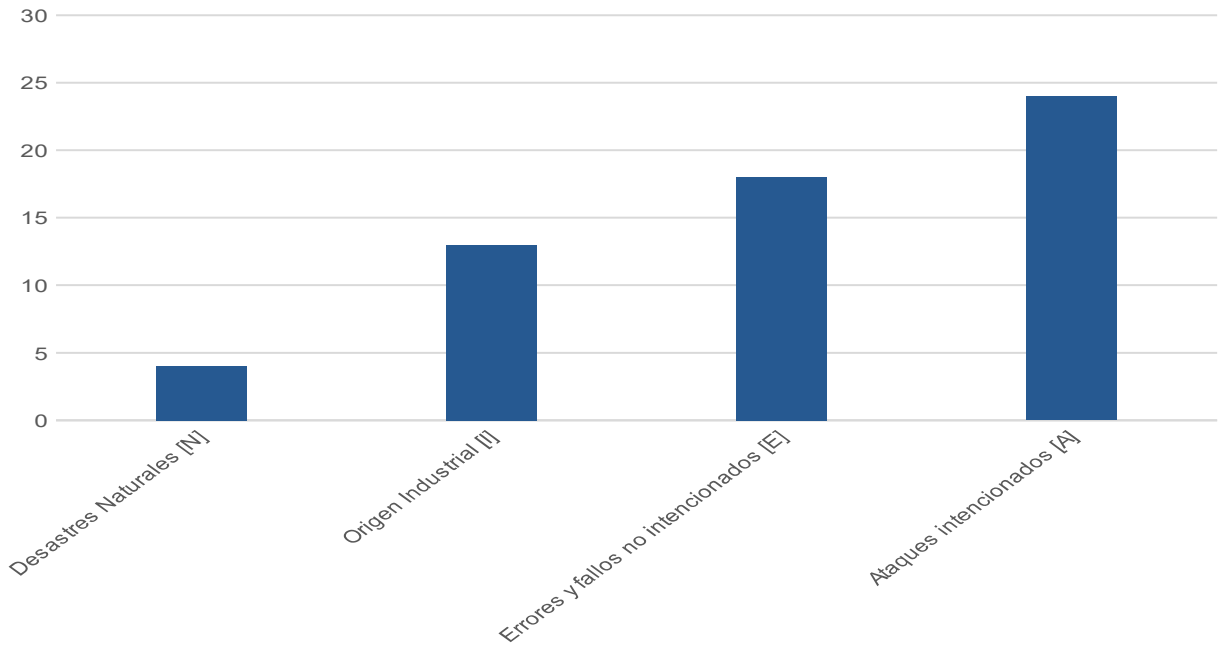
- **INVENTARIO DE ACTIVOS. VALORACIÓN MEDIA DIMENSIONES DE SEGURIDAD**



ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **ANÁLISIS DE AMENAZAS. CLASIFICACIÓN**
  - **Desastres Naturales [N]**
  - **De origen Industrial [I]**
  - **Errores y fallos no intencionados [E]**
  - **Ataques Intencionados [A]**



- **59 Amen**
- **4 Catego**

ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **ANÁLISIS DE AMENAZAS. VALORACIÓN**

  - **FRECUENCIA**

Vulnerabilidad	ID	Rango	Valor
Frecuencia Extrema	MA	1 vez al día	1
Frecuencia Alta	A	1 vez a la semana	52/365=0.14
Frecuencia Media	M	1 vez al mes	12/365=0.03
Frecuencia Baja	B	1 vez cada seis meses	2/365=0.005
Frecuencia Muy Baja	MB	1 vez al año	1/365=0.002

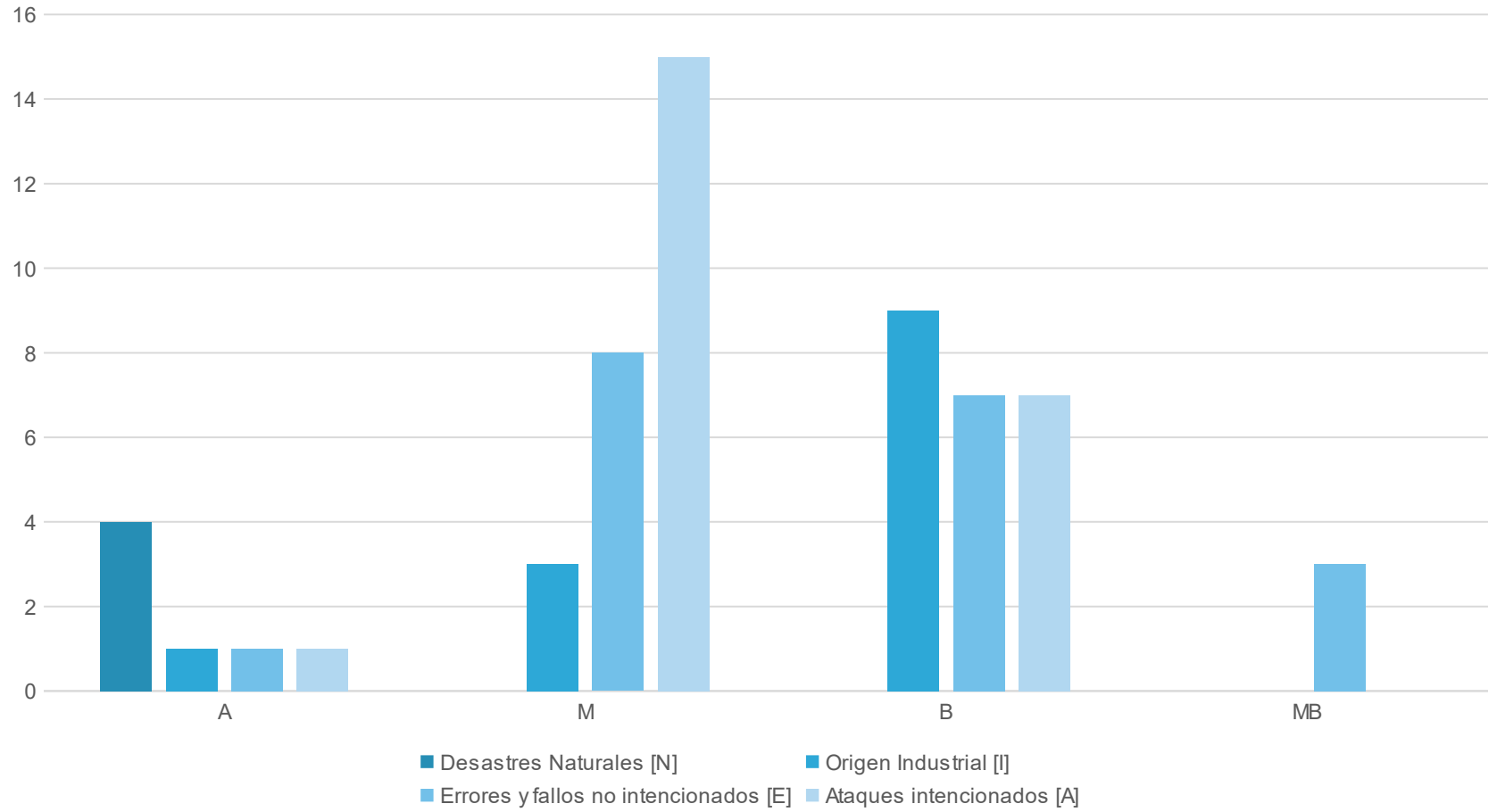
  - **IMPACTO EN LAS DIMENSIONES ACIDT**

Impacto	ID	Rango
Muy Alto	MA	Valor > 90%
Alto	A	70% < Valor < 90%
Medio	M	50% < Valor < 70%
Bajo	B	30% < Valor < 50%
Muy Bajo	MB	10%< Valor < 30%

ANÁLISIS DE RIESGOS

Cosmética y Belleza S.A

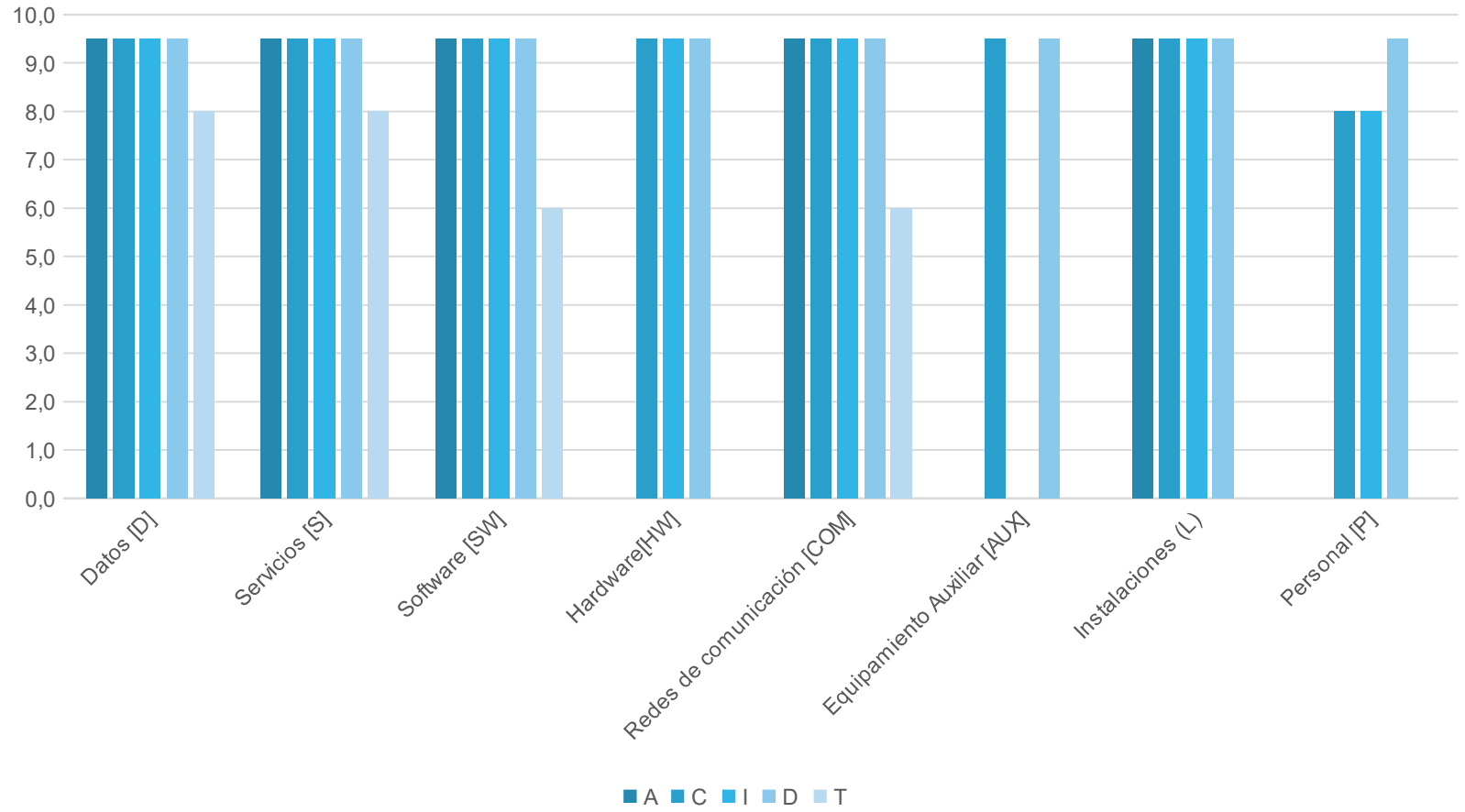
- **ANÁLISIS DE AMENAZAS. FRECUENCIA**



ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **ANÁLISIS DE AMENAZAS. VALOR ABSOLUTO DEL IMPACTO AMENAZAS POR GRUPOS DE ACTIVOS**



ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **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

Datos [D]					
Servicios [S]					
Software [SW]					
Hardware [HW]					
		OLE			

ANÁLISIS DE RIESGOS

CYBSA Cosmética y Belleza S.A

- **NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL**

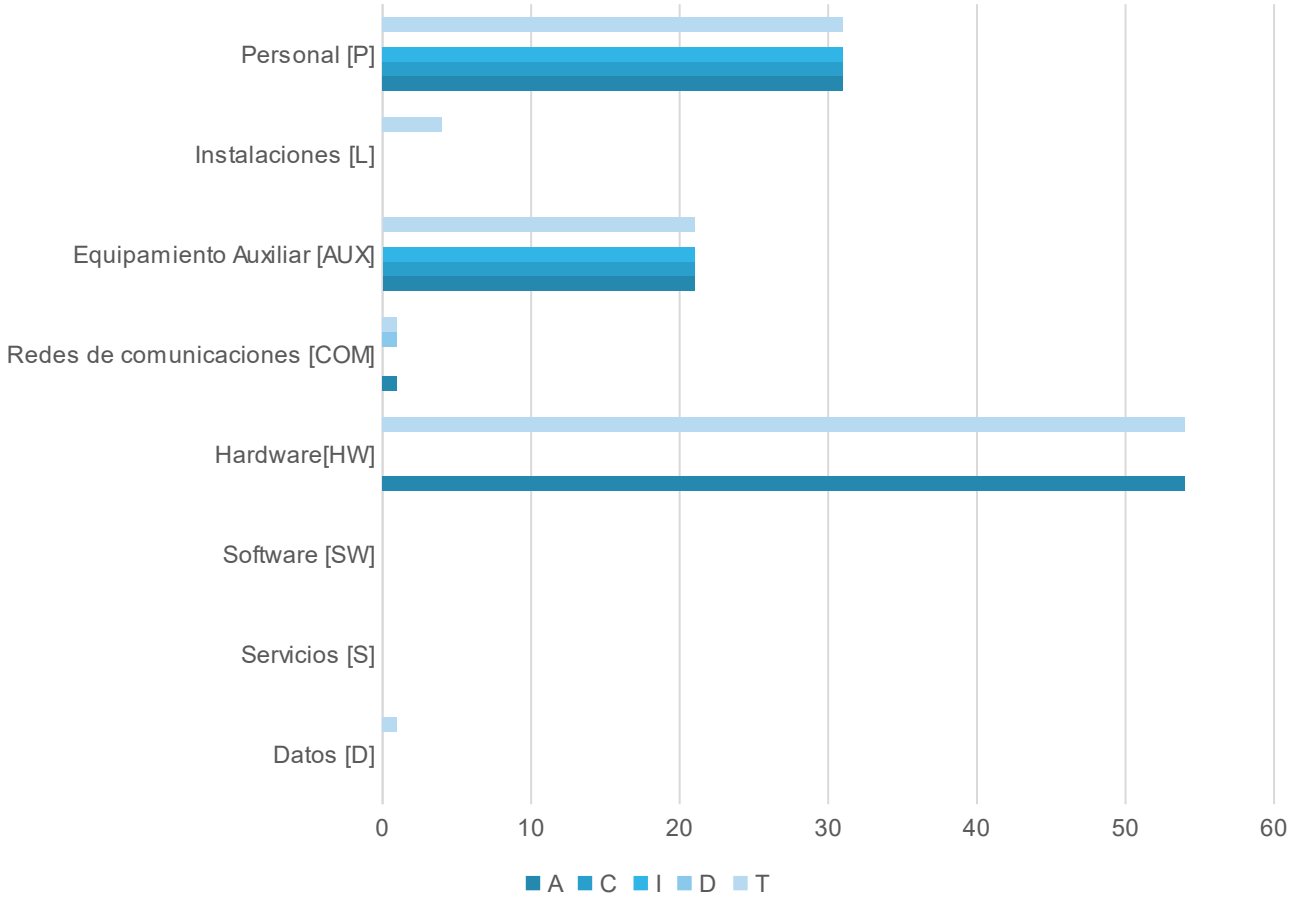
  - Se define un límite a partir del cual se pueda decidir si asumir un riesgo o por el contrario no asumirlo y aplicar controles
  - **Nivel de riesgo =** Impacto potencial x frecuencia de la amenaza
  - La dirección de CYBSA decide que el nivel de riesgo aceptable sea a partir de **MEDIO**.

Riesgo		Frecuencia				
		MB (0,002)	B (0,005)	M (0,03)	A (0,014)	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

Cosmética y Belleza S.A

- NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL
- ACTIVOS QUE SUPERAN EL NIVEL DE RIESGO



Propuesta de proyectos

CYBSA Cosmética y Belleza S.A

Proyectos
P1 - Definición y diseño de la política de seguridad de CYBSA
P2 – Revisión de gestión de activos y clasificación de la información
P3 – Formación continua en materia de seguridad
P4 – Multifactor de Autenticación para VPN, Correo electrónico, Odoo y Salesforce
P5 – Cifrado de los datos en PCs y portátiles
P6 – Despliegue herramienta de gestión en dispositivos móviles (MdM)

Propuesta de proyectos

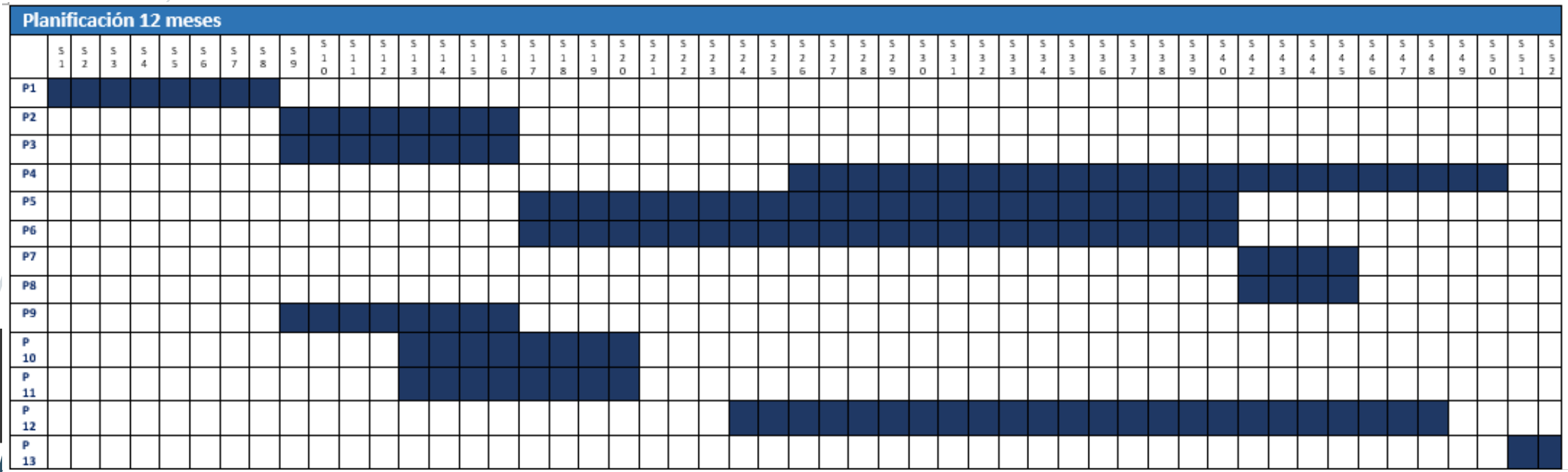
CYBSA Cosmética y Belleza S.A

Proyectos
P7 – Revisión políticas implementadas en soluciones EPP y EDR
P8 – Revisión políticas implementadas en la solución de protección de correo
P9 – Despliegue de una solución de protección de la navegación
P10 – Despliegue de una solución de protección de la web de comercio electrónico (WAF)
P11 – Cifrado de datos y comunicaciones en el proceso de ventas
P12 – Despliegue herramienta de monitorización y definición de política de gestión de incidentes
P13 – Revisión de la seguridad de la información

?

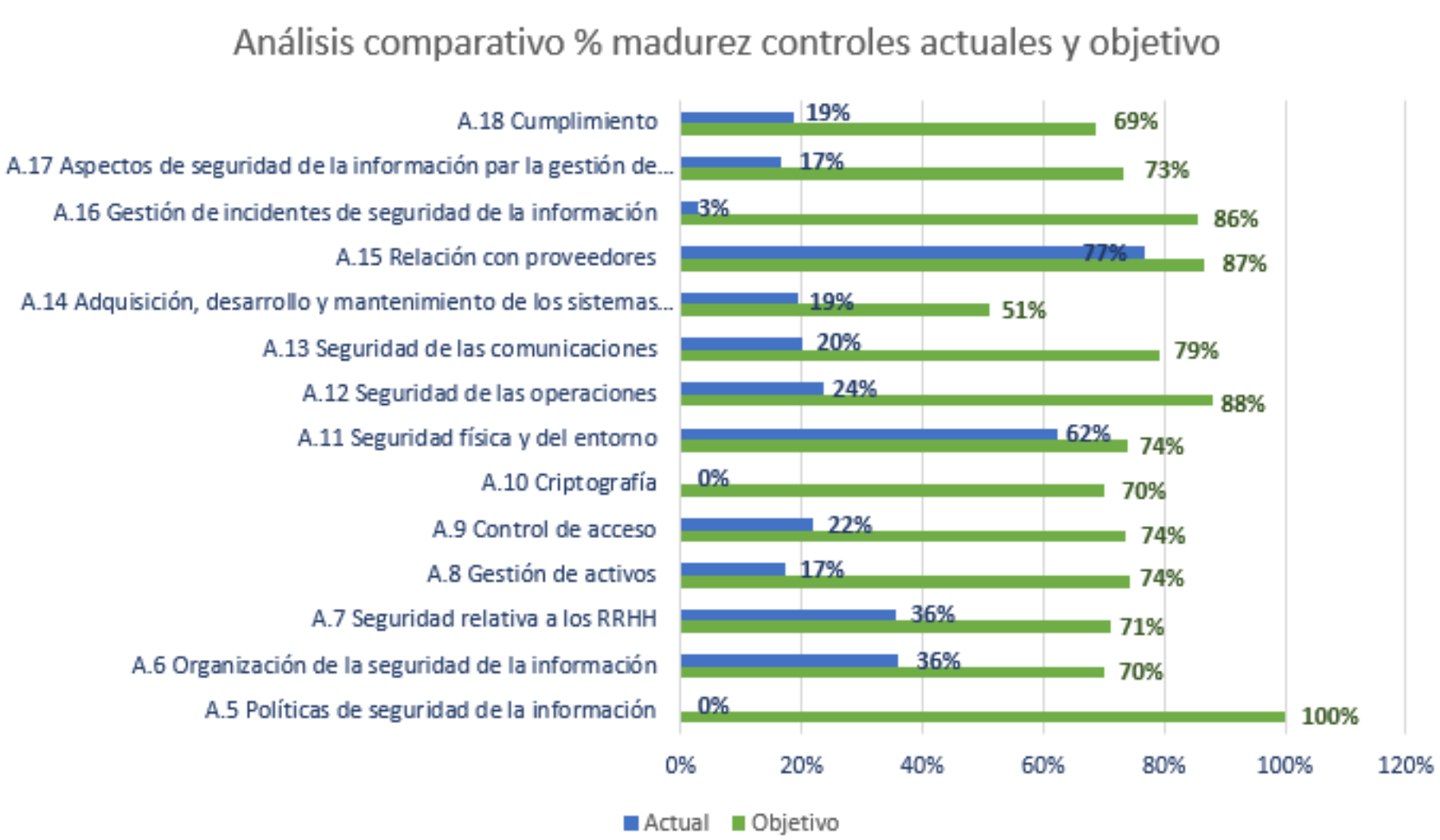
Propuesta de proyectos. Planificación

CYBSA Cosmética y Belleza S.A



Propuesta de proyectos. Análisis diferencial

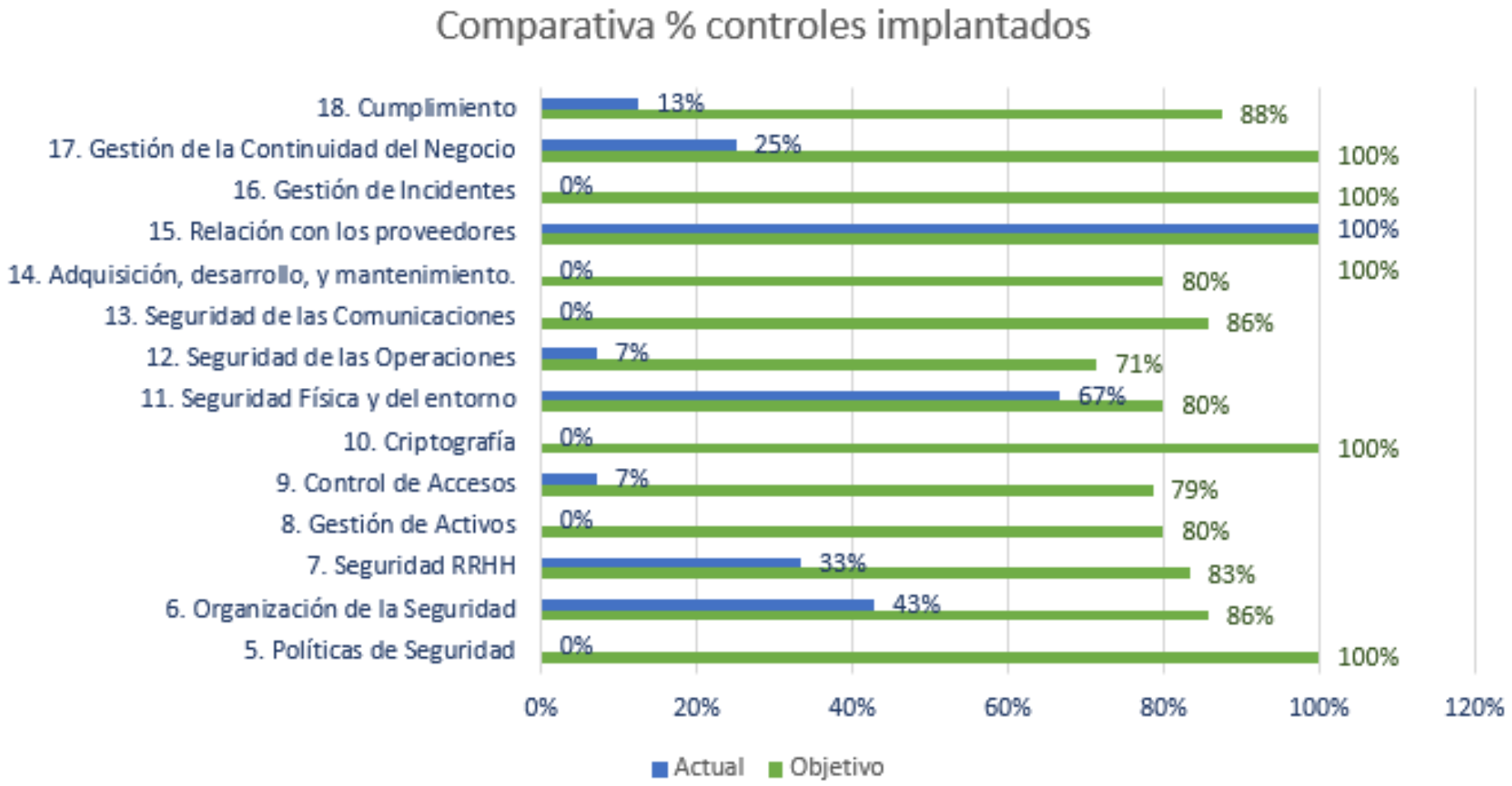
CYBSA Cosmética y Belleza S.A



?

Propuesta de proyectos. Análisis diferencial

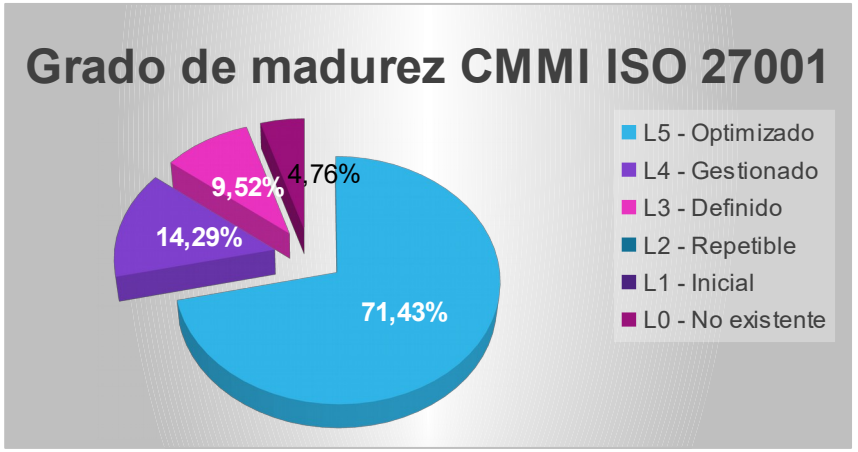
CYBSA Cosmética y Belleza S.A

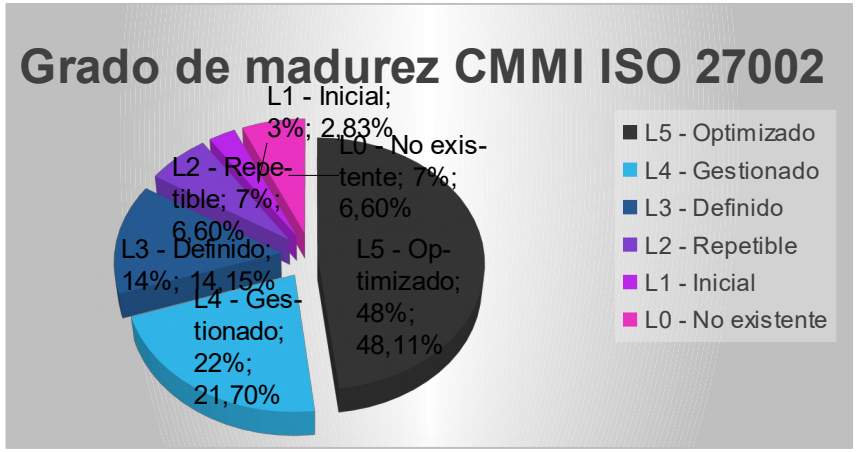


Auditoría. Resultados

Cosmética y Belleza S.A

- **Considerando que se han implantado todos los proyectos, se realiza la auditoría de cumplimiento contra la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013 .**





- **95% de todos los controles que aplican están por encima de nivel L3.**
- **5% de controles presentan No conformidades**

- **84% de todos los controles que aplican están por encima de nivel L3.**
- **16% de controles presentan No conformidades**

Auditoría. Resultados % madurez

CYBSA Cosmética y Belleza S.A

ISO/IEC 27002:2013

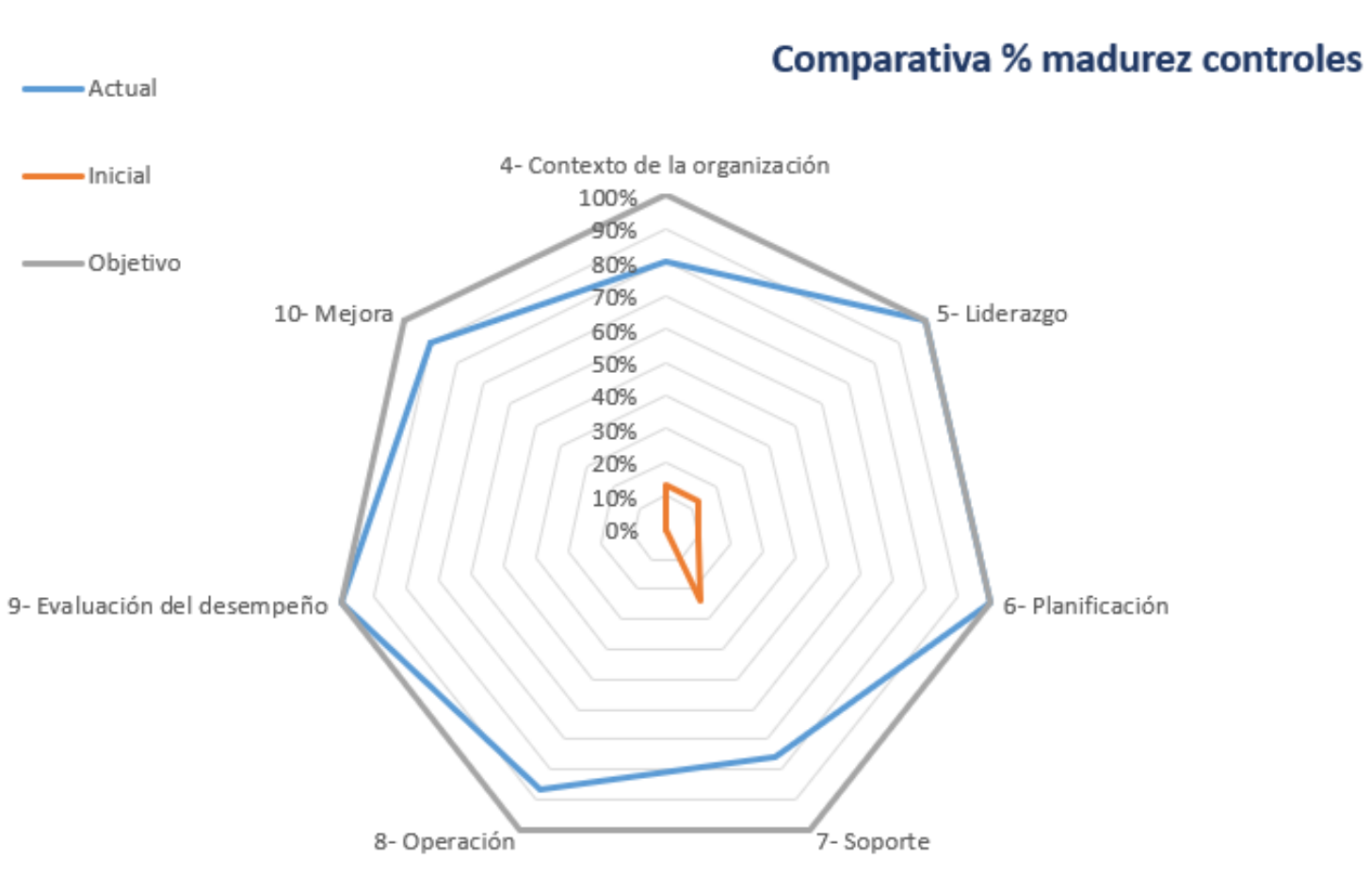
DOMINIOS	% MADUREZ
A.5 Políticas de seguridad de la información	100%
A.6 Organización de la seguridad de la información	81%
A.7 Seguridad relativa a los RRHH	70%
A.8 Gestión de activos	74%
A.9 Control de acceso	77%
A.10 Criptografía	80%
A.11 Seguridad física y del entorno	92%
A.12 Seguridad de las operaciones	88%
A.13 Seguridad de las comunicaciones	79%
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	47%
A.15 Relación con proveedores	87%
A.16 Gestión de incidentes de seguridad de la información	86%
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	87%
A.18 Cumplimiento	79%

ISO/IEC 27001:2013

DOMINIOS	% MADUREZ
4- Contexto de la organización	80%
5- Liderazgo	100%
6- Planificación	100%
7- Soporte	76%
8- Operación	87%
9- Evaluación del desempeño	100%
10- Mejora	90%

Auditoría. Comparativa % madurez

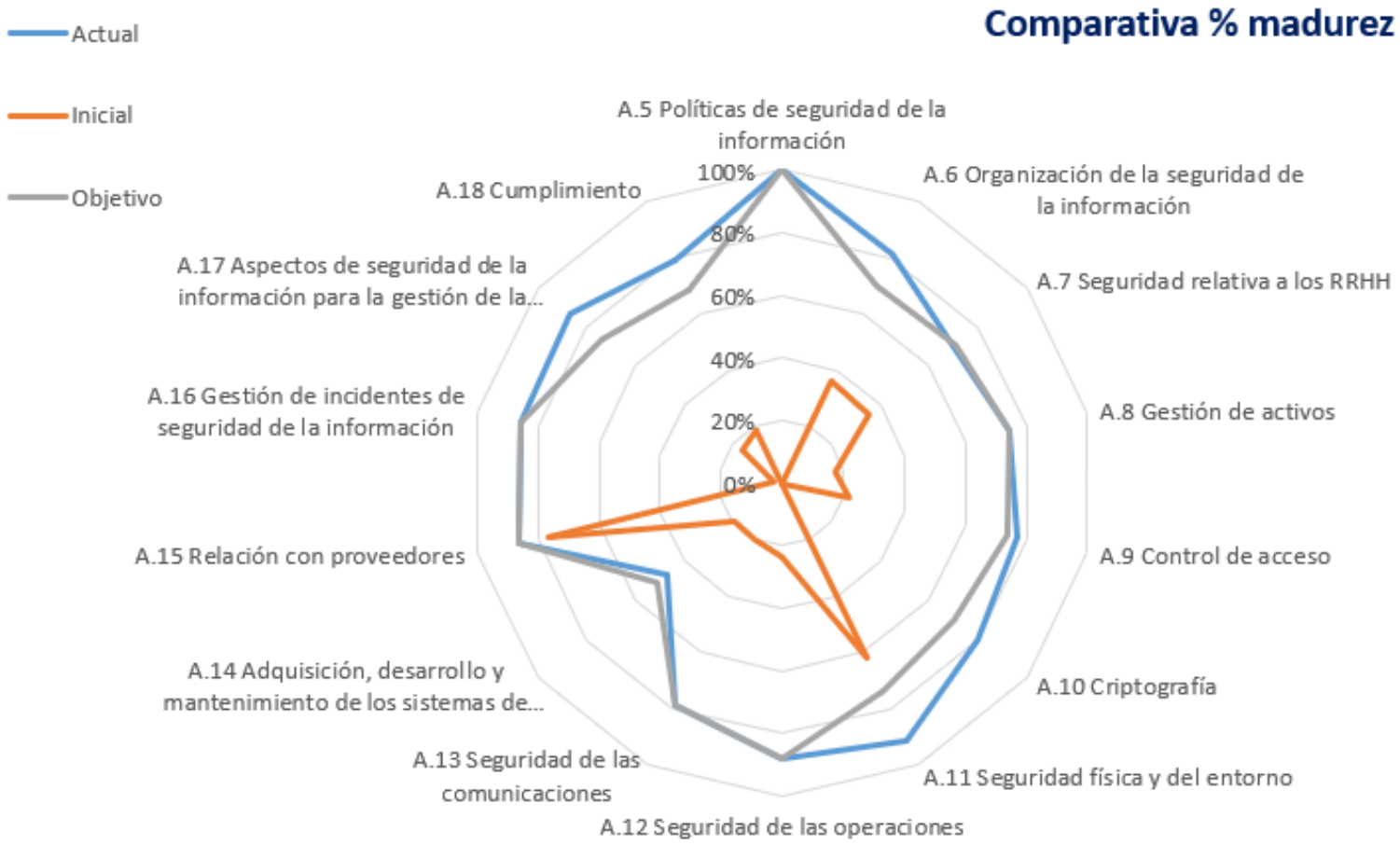
CYBSA Cosmética y Belleza S.A



ISO/IEC 27001:2013

Auditoría. Comparativa % madurez

Cosmética y Belleza S.A



ISO/IEC 27002:2013

Conclusiones

CYBSA Cosmética y Belleza S.A

- Como punto de partida se ha definido el estado inicial de la seguridad de la información de CYBSA
- Se ha desarrollado el esquema documental necesario para implementar el SGSI cumpliendo la ISO/IEC 27001:2013
- Se ha realizado el análisis de riesgos siguiendo la metodología MAGERIT a través del cual se ha realizado una evaluación del riesgo al que están expuestos los activos de CYBSA debido al impacto que supondría la materialización de posibles amenazas.
- Se han definido y ejecutado una serie de proyectos para mitigar los riesgos y aumentar el nivel de seguridad.
- Se ha realizado una auditoría de cumplimento en la que todos los dominios alcanzan el % de madurez esperado y por consiguiente CYBSA ha logrado el objetivo de mejorar el nivel de seguridad de la información en un porcentaje muy considerable que sin duda justifica las inversiones y esfuerzos realizados.

?

MUCHAS GRACIAS