MISTIC
Trabajo Final de Master

Presentación de Resultados

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

Introducción

- En el año 2010 entra en vigencia la nueva Ley Orgánica de Educación Superior en el Ecuador
- Conjuntamente con la Ley el gobierno crea dos organismos de control de la educación superior
  - CES (Consejo de Educación Superior)
  - CEAACES(Consejo de Evaluación Acreditación y Aseguramiento de la Calidad de la Educación Superior)

Introducción

- Antes del 2010:
  - Bajo el concepto de autonomía, la UPS manejaban su información sin ningún tipo de control sobre:
    - La confidencialidad
    - La integridad
    - La disponibilidad
    - Datos Personales
  - Los diferentes sistemas de información solo debían responder a la lógica operativo del negocio.

Introducción

- Después del 2010:
  - La LOES define a la educación superior como "Bien Público", por lo tanto interviene a todas las universidades del país a través de la solicitud de información de diverso índole.
  - En la UPS se detecta:
    - Que la integridad es un punto débil
    - Que la confidencialidad es vital para mantener la competitividad frente a las otras universidades
    - Que se necesita una alta disponibilidad porque los organismos de control requieren información en cualquier momento
    - Que se ha recolectado una infinidad datos personales

Introducción

La información es un punto relevante en la planificación estratégica:
"*Las dependencias universitarias tienen acceso a información relevante, consistente, congruente y oportuna a través de las tecnologías de la información y comunicación.(Carta de Navegación 2014-2018)*"

La información solo es un resultado de la operativización de los procesos

PUNTO DE INFLEXIÓN

Antecedentes

- Bajo la nueva política pública la universidad se ve en la necesidad de:
  - Implementar controles para la seguridad de la información (confidencialidad, integridad y disponibilidad)
- Se destina partidas presupuestarias considerables
- Sin embargo los resultados no son consistentes con la inversión

Antecedentes

- Las diferentes soluciones son propuestas Ad-hoc
  - Iniciativa de los diferentes coordinadores del Departamento de Tecnologías de la Información
  - No se documentan dichos procesos
  - Se afecta la usabilidad de los sistemas informáticos

Antecedentes

- La Dirección ante los problemas decide reestructurar el Departamento de Tecnologías de la Información (2012).
- Al año 2014 la dirección de la UPS, detecta ciertas mejorías pero la inconformidad persiste debido a la gran inversión y los pocos resultados.

No existe un Sistema de Gestión de Seguridad de la Información

Implementación del SGSI

- Se toma como referencia la norma ISO/IEC 27001:2013
- Se presenta un proyecto divido en cinco fases:
  1. Análisis Diferencial (GAP) del estado actual de la UPS con respecto a la norma
  2. Creación del Sistema de Gestión Documental
  3. Ejecución de un Análisis de Riesgos
  4. Planteamiento de Proyectos de Mejora
  5. Auditoría Interna
- Se pretende cumplir un ciclo PDCA

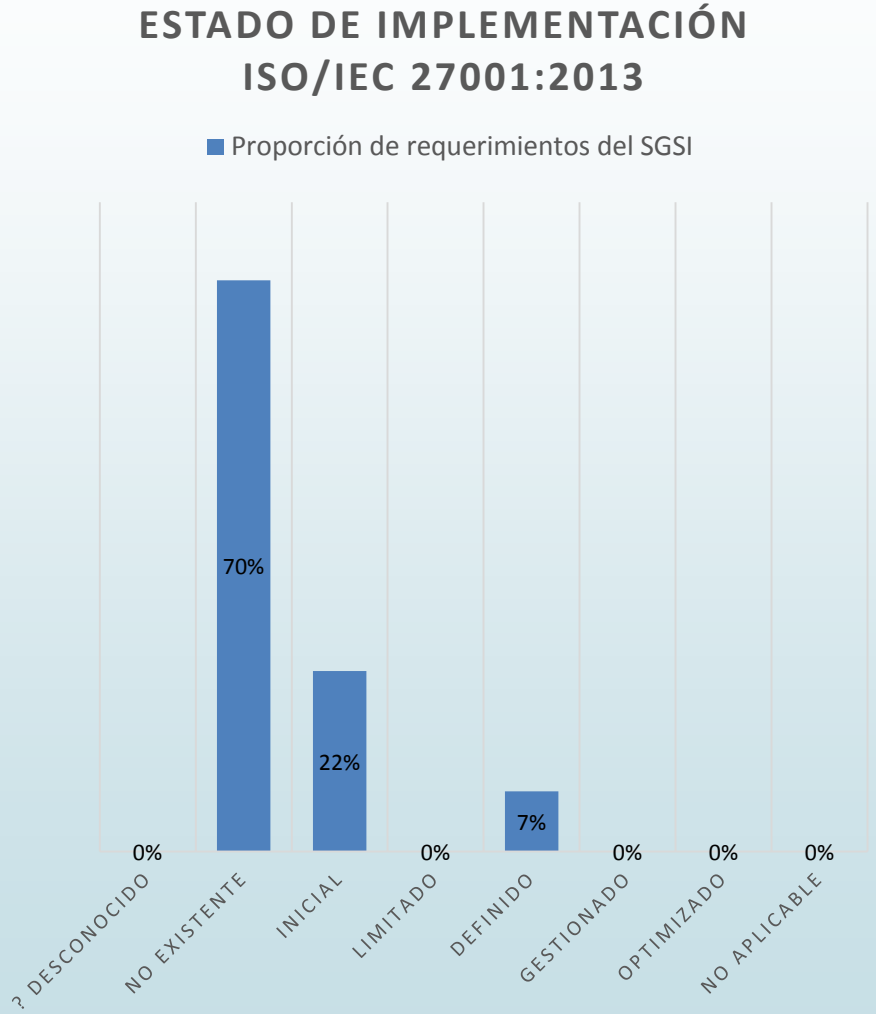
1. Análisis Diferencial (GAP)

- El análisis diferencial se lo realiza desde:
  - La parte mandatoria de la ISO/IEC 27001:2013
  - El estado de la implementación de los controles de la ISO/IEC 27002:2013
  - Para la valoración se utiliza métricas basadas en el modelo de madurez de CobIT y CMM

1. Análisis Diferencial (GAP)

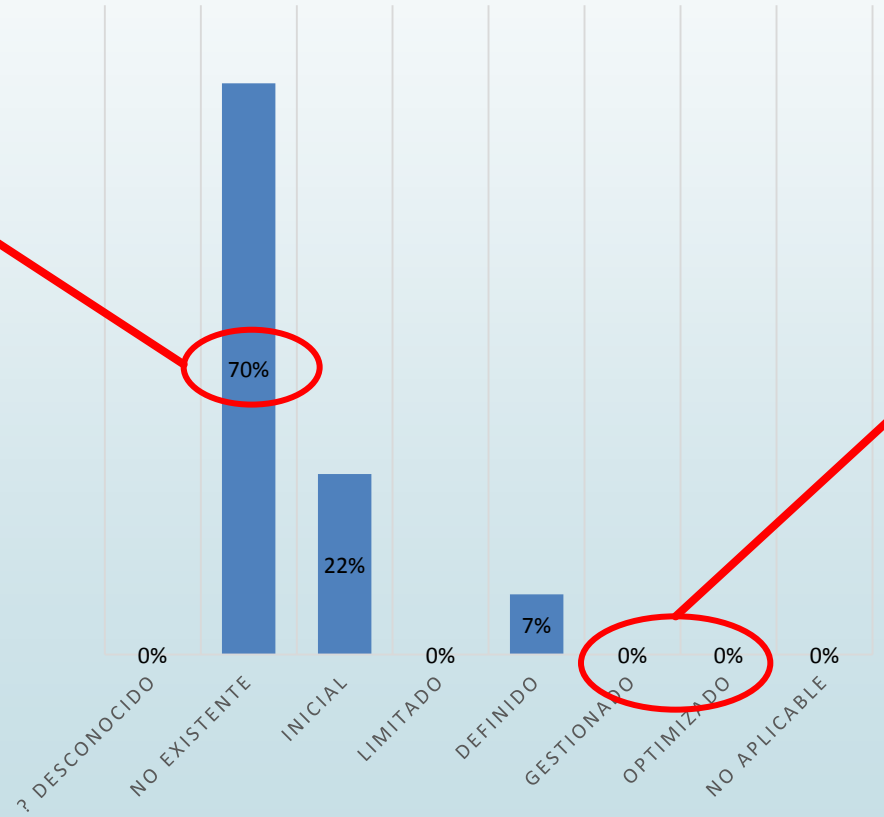
Estado	Significado
? Desconocido	Todavía no ha sido chequeado
No existente	Falta completa de política reconocible, proceso, control, etc.
Inicial	Desarrollo apenas iniciado y requerirá un significante trabajo para completar los requerimientos.
Limitado	Progresando de manera correcta pero todavía no completado
Definido	Desarrollo más o menos completo aunque el detalle es deficiente y/o todavía no se ha implementado y respaldado activamente por la Dirección
Gestionado	Desarrollo está completo, el proceso/control ha sido implementado y recientemente comenzó a operar
Optimizado	El requerimiento es completamente satisfactorio, está operando plenamente como era de esperar, está iniciando el monitoreo y mejora activamente, y existe evidencia substancial para probar todo a los auditores
No aplicable	Este requerimiento no es aplicable a la organización. Nota: Todos los requerimientos en el cuerpo de ISO/IEC 27001 son mandatorios, si el SGSI

1. Análisis Diferencial (GAP)



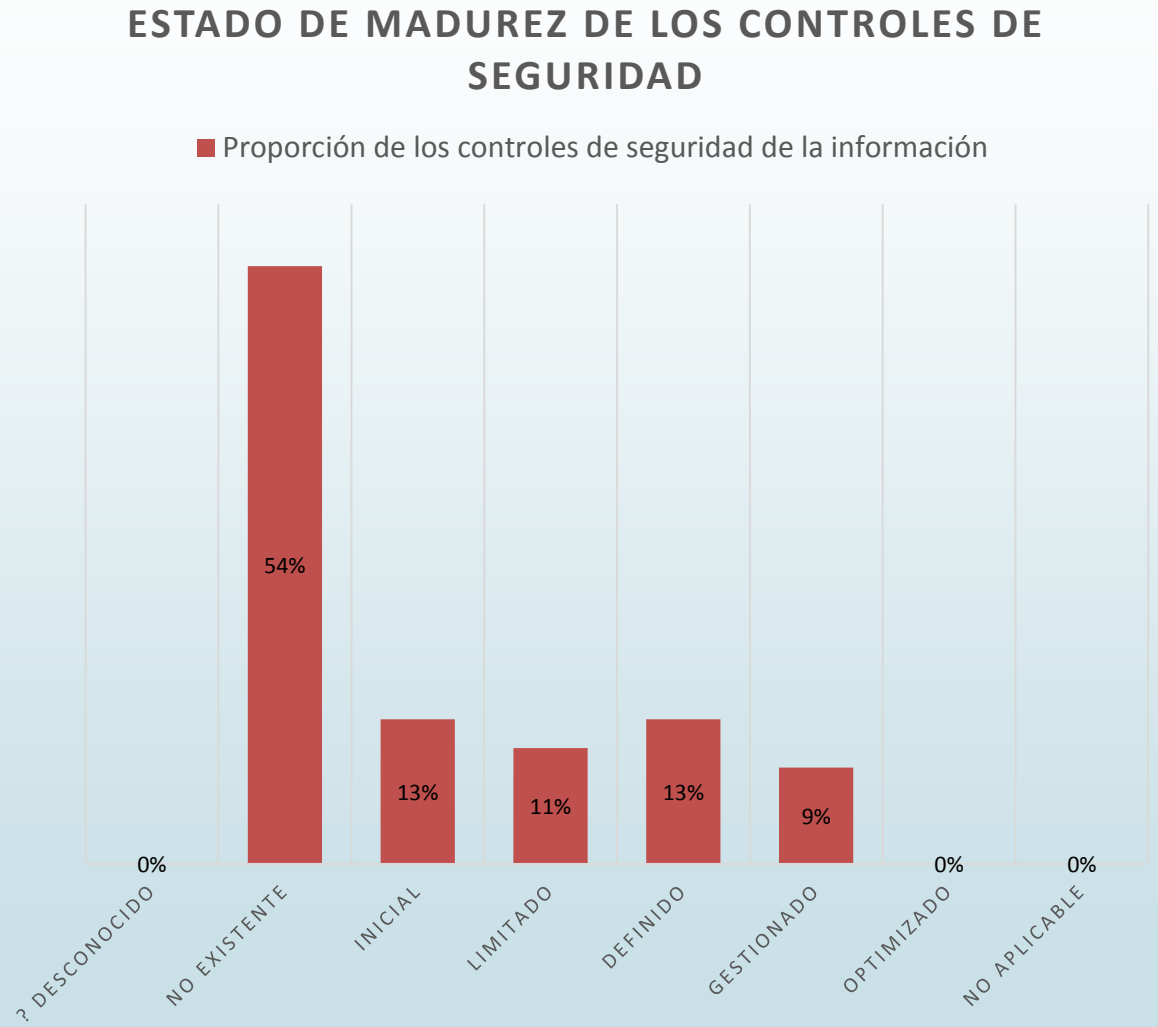
1. Análisis Diferencial (GAP)

El 70 % de los requerimientos no existen en la UPS

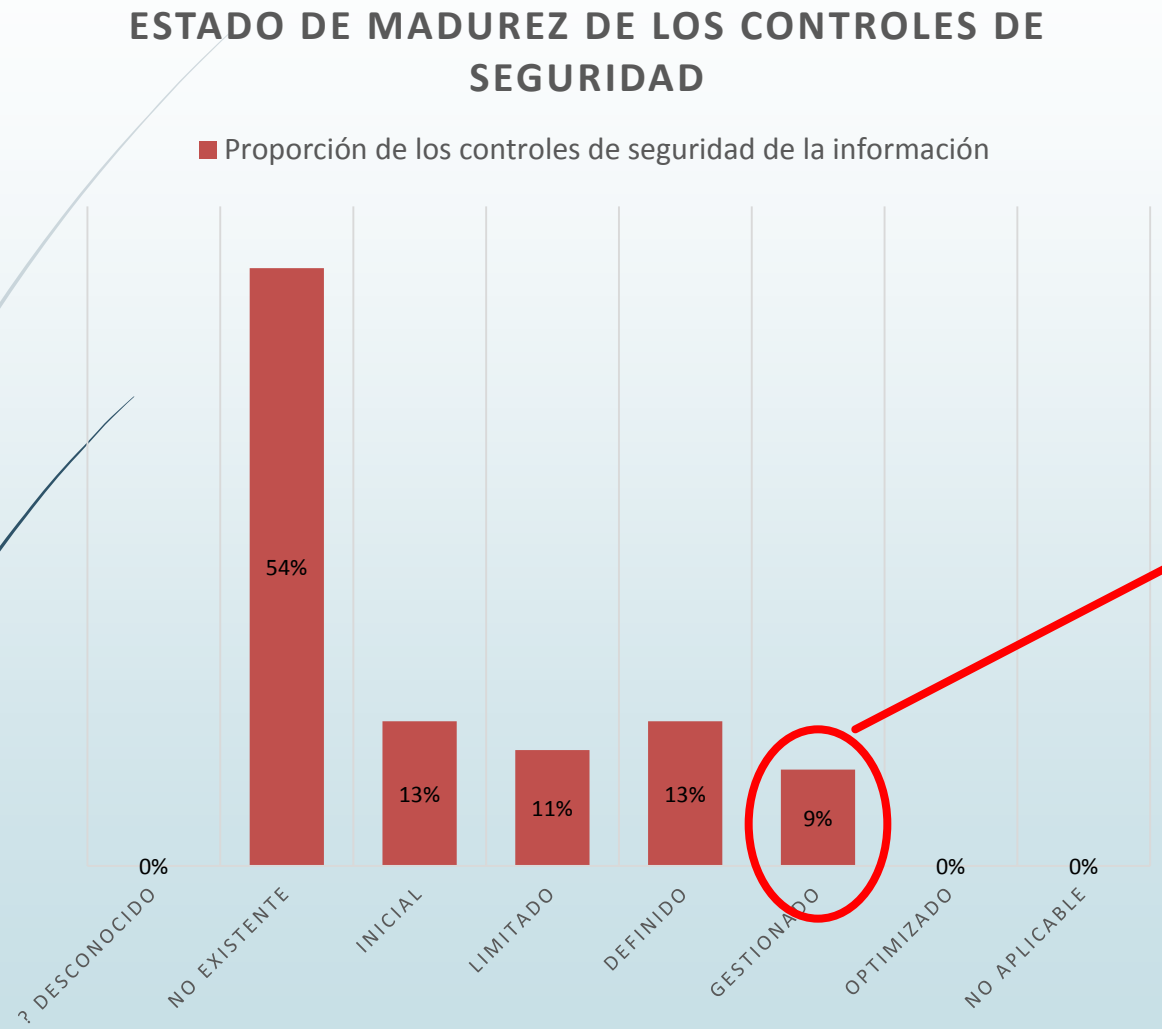


La UPS no cumple requerimientos que alcancen por lo menos el estado de madurez Gestionado

1. Análisis Diferencial (GAP)



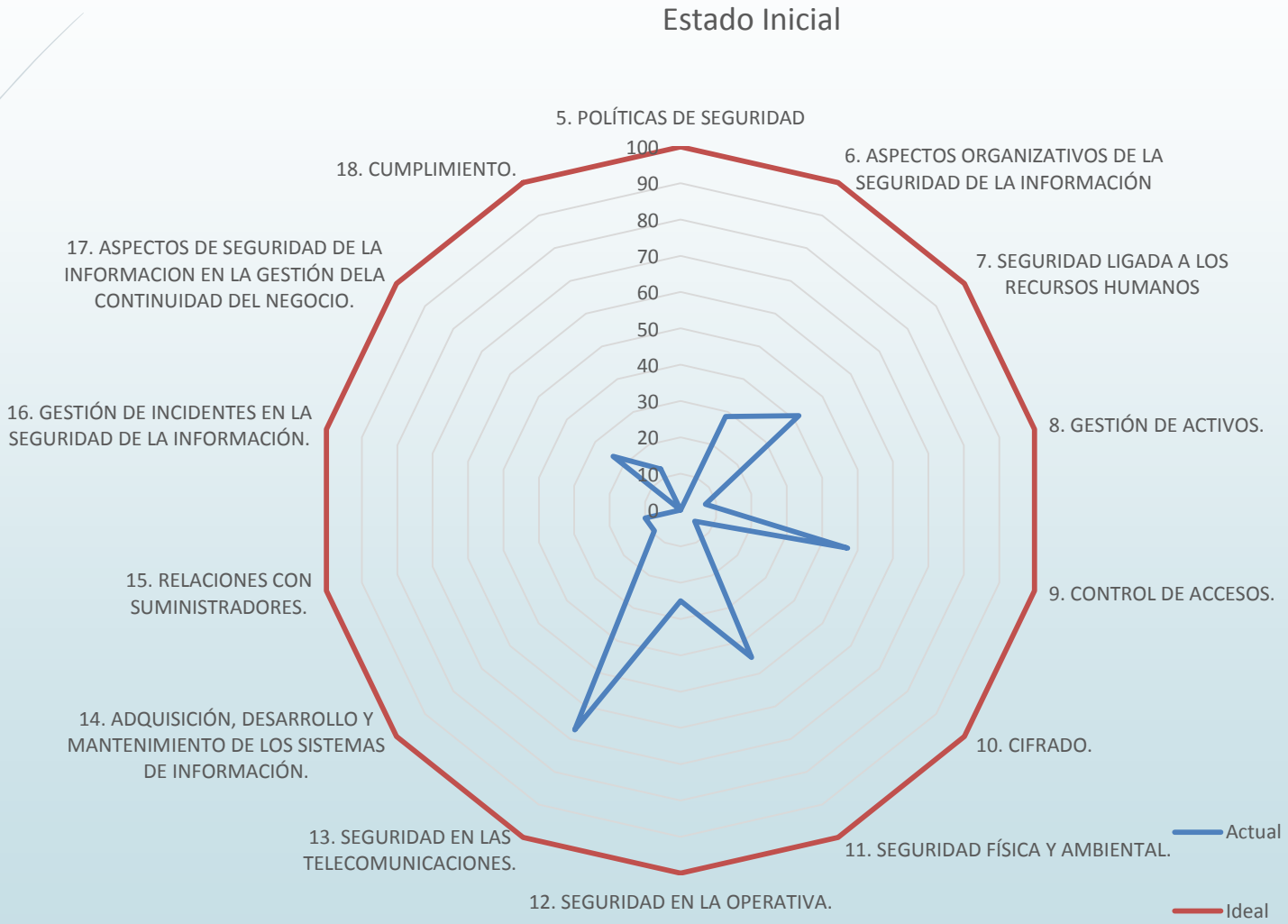
1. Análisis Diferencial (GAP)



?

Algunos controles Ad-hoc llegan a tener aprobación de la dirección (política híbrida) y su nivelde madurez ha alcanzado el estado de Gestionado

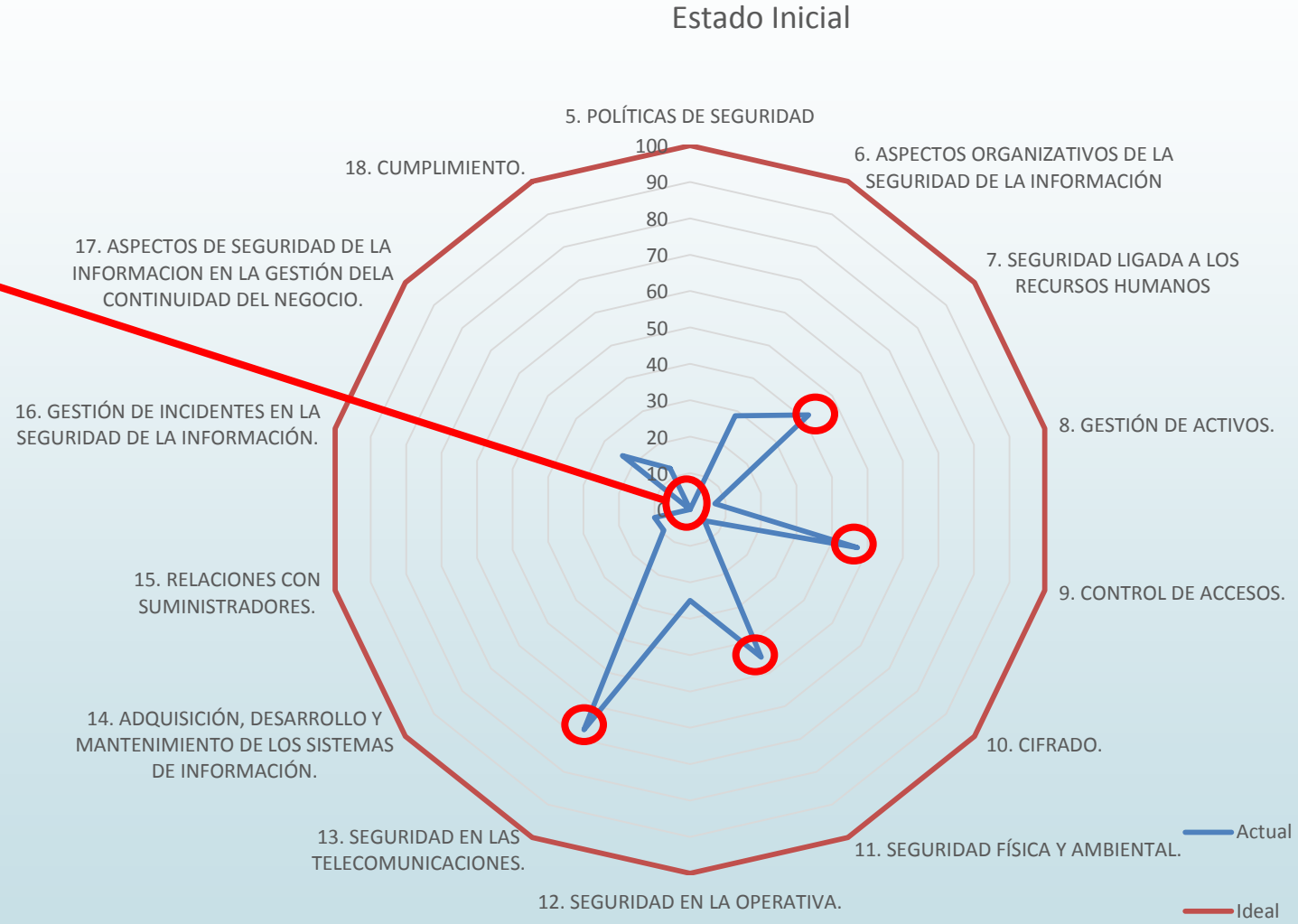
1. Análisis Diferencial (GAP)



1. Análisis Diferencial (GAP)

Varios dominios están en cero o tienden a cero

Varios dominios tienen picos de madurez debido a las iniciativas Ad-hoc



2. Sistema de Gestión Documental

- Finalidades:
  - Normalizar la estructura, forma, presentación, control, gestión, difusión y registro de la documentación generada en el SGSI de la UPS
  - Establecer una base de políticas "Marco" que permitan iniciar la implementación del SGSI

2. Sistema de Gestión Documental

2. Sistema de Gestión Documental

2. Sistema de Gestión Documental

Declaración de Aplicabilidad

3. Análisis de Riesgos

- Según el Documento "Metodología de análisis de Riesgos" se realizan las siguientes actividades:
  1. Inventario de Activos
  2. Valoración de Activos
  3. Análisis de Amenazas
  4. Determinación del Impacto Potencial y Residual
  5. Determinación del Nivel de Riesgo

3. Análisis de Riesgos
3.1 Inventario de Activos

- Según el catálogo de MAGERIT se procedió a inventariar y caracterizar los activos.

Caracterización de Activos	Cantidad de Activos
[AUX] Equipamiento Auxiliar	2
[COM] Redes de comunicaciones	7
[D] Datos	6
[HW] Hardware	19
[inf] Información	3
[K] Claves criptográficas	1
[L] Instalaciones	6
[M] Media	4
[P] Personal	7
[S] Servicios Generales	18
[service] Servicio	4
[SW] Software	7
Total general	**84**

3. Análisis de Riesgos
3.1 Inventario de Activos

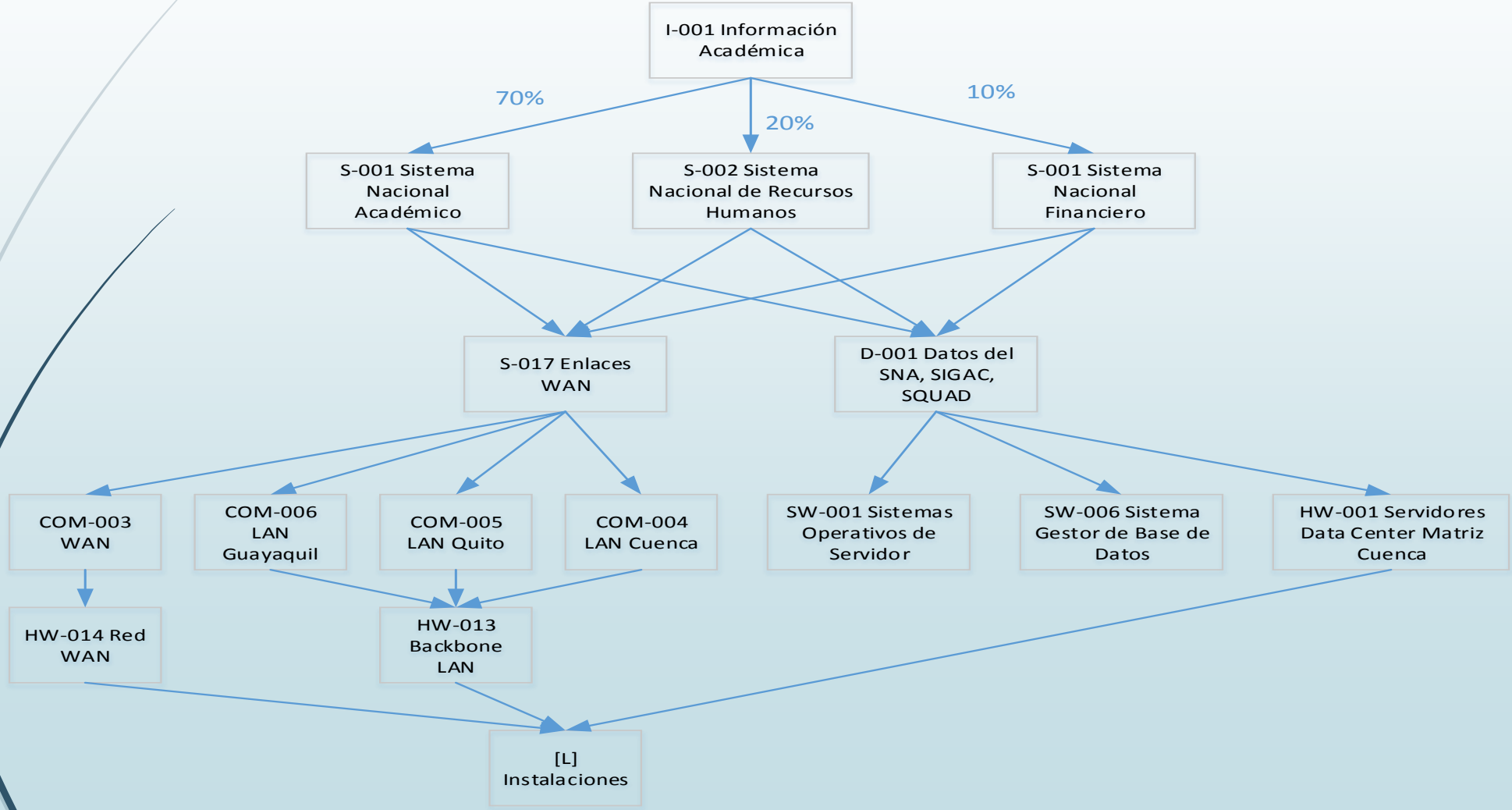
Código activo	Denominación	Caracterización	Propietario	Observación
I-001	Información académica	[inf] Información	Vicerrector Docente	[essential] Activo esencial para la UPS
I-02	Información Talento Humano	[inf] Información	Secretario Técnico de Recursos Humanos	[essential] Activo esencial para la UPS
I-003	Información financiera	[inf] Información	Secretario Técnico de Finanzas	[essential] Activo esencial para la UPS
S-001	Sistema Nacional Académico (SNA)	[service] Servicio	Vicerrector Docente	[essential] Activo esencial para la UPS
S-002	Sistema Nacional de Recursos Humanos	[service] Servicio	Secretario Técnico de Recursos Humanos	[essential] Activo esencial para la UPS
S-003	Sistema Nacional Financiero	[service] Servicio	Secretario Técnico de Finanzas	[essential] Activo esencial para la UPS
S-004	AVAC	[service] Servicio	Vicerrector Docente	[essential] Activo esencial para la UPS
D-001	Datos del SNA, SIGAC y SQUAD	[D] Datos	DBA	[essential] Activo esencial para la UPS

Activos esenciales para la UPS

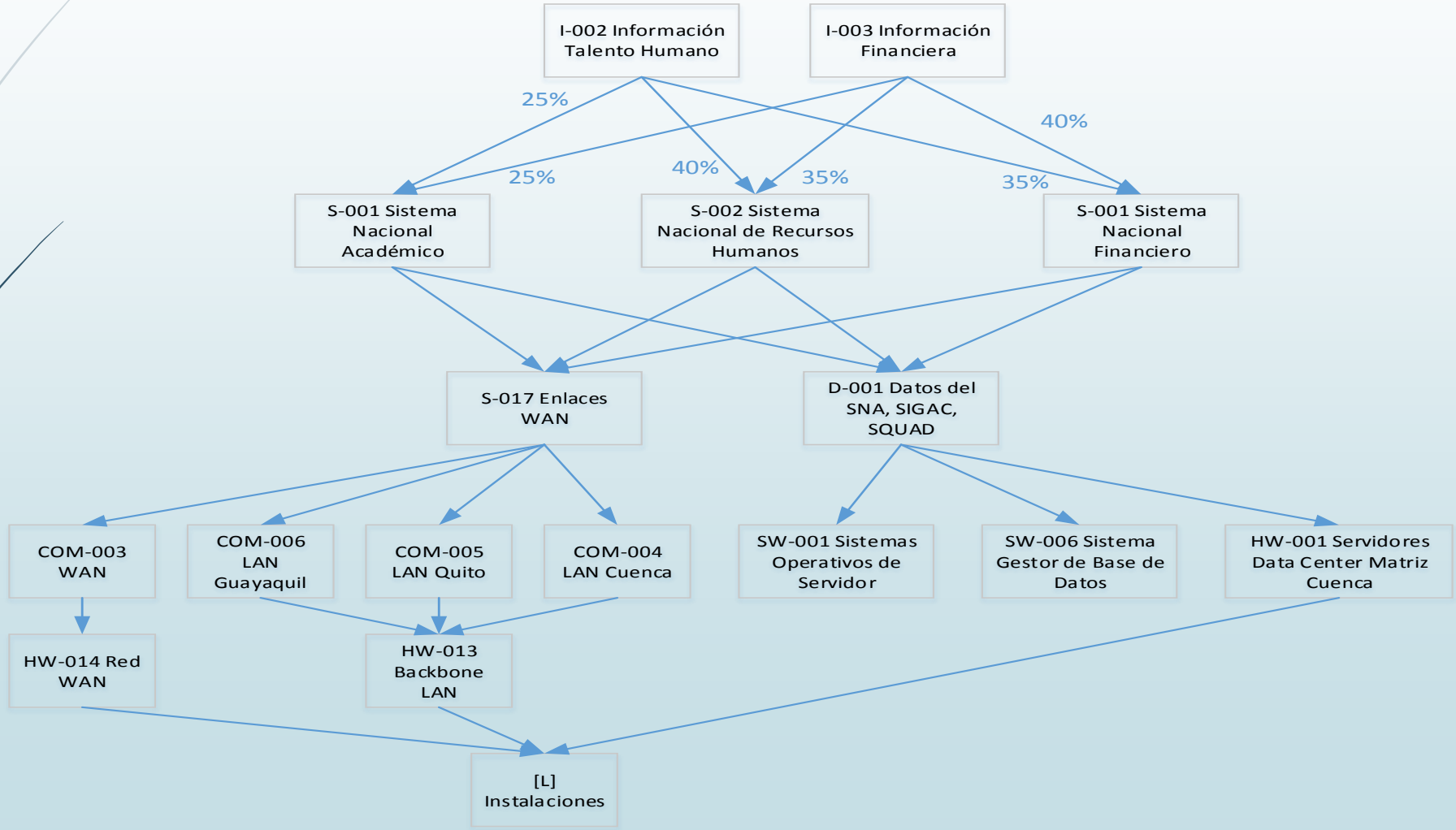
3. Análisis de Riesgos
3.2 Valoración de activos

- Construcción de los árboles de dependencias entre activos:
  - La información académica es el principal activo de la UPS, el negocio de la universidad gira en torno a la información académica
  - Estrecha relación entre academia-talento humano-finanzas que permiten la gestión eficiente de toda la universidad
  - Tres sistemas (académico, recursos humanos y financiero) son el soporte de toda la información
  - Las aulas virtuales de aprendizaje garantizan el desarrollo de la academia
  - La base de datos institucional, almacena y recopila todos los registros que se generan en los sistemas principales

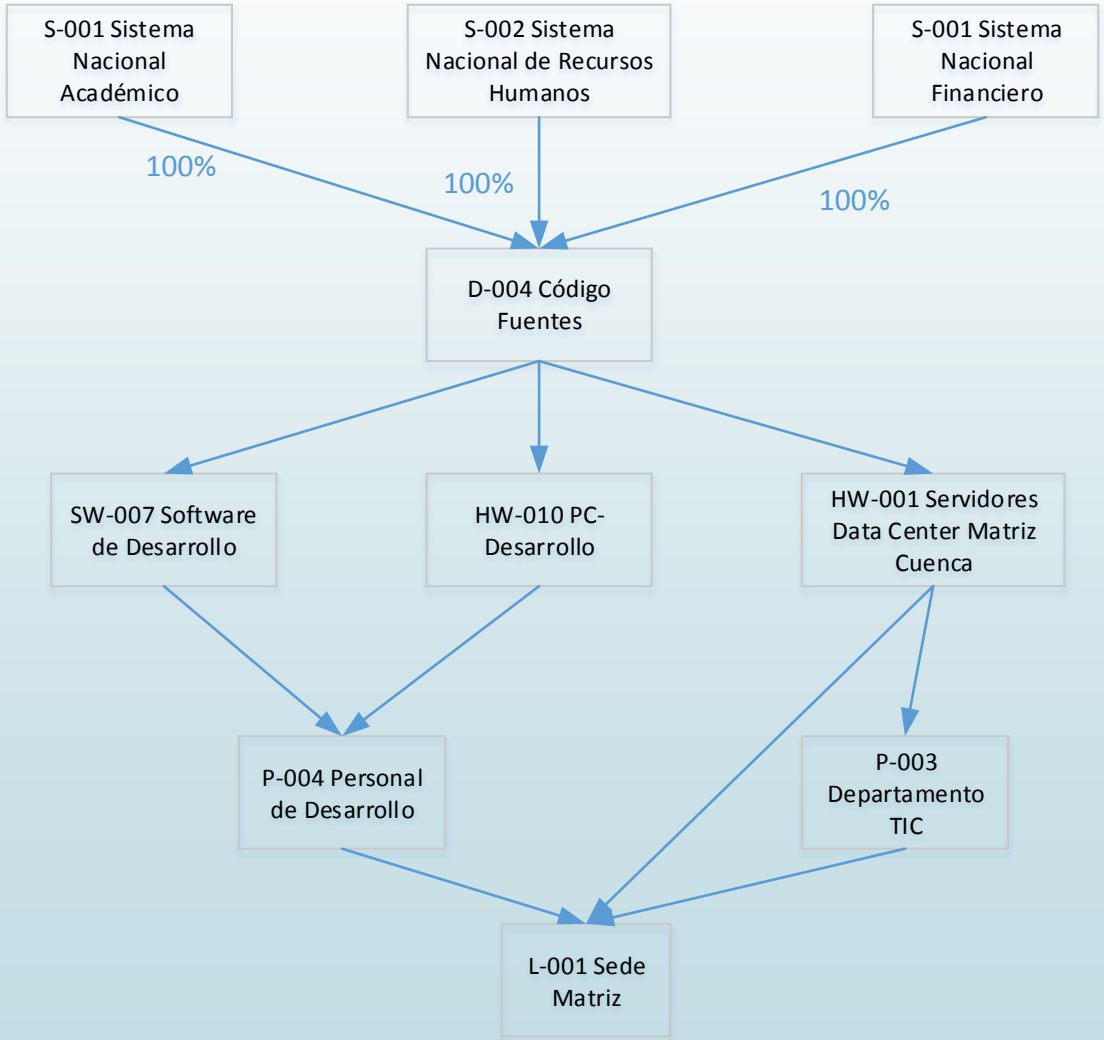
3. Análisis de Riesgos
3.2 Valoración de activos



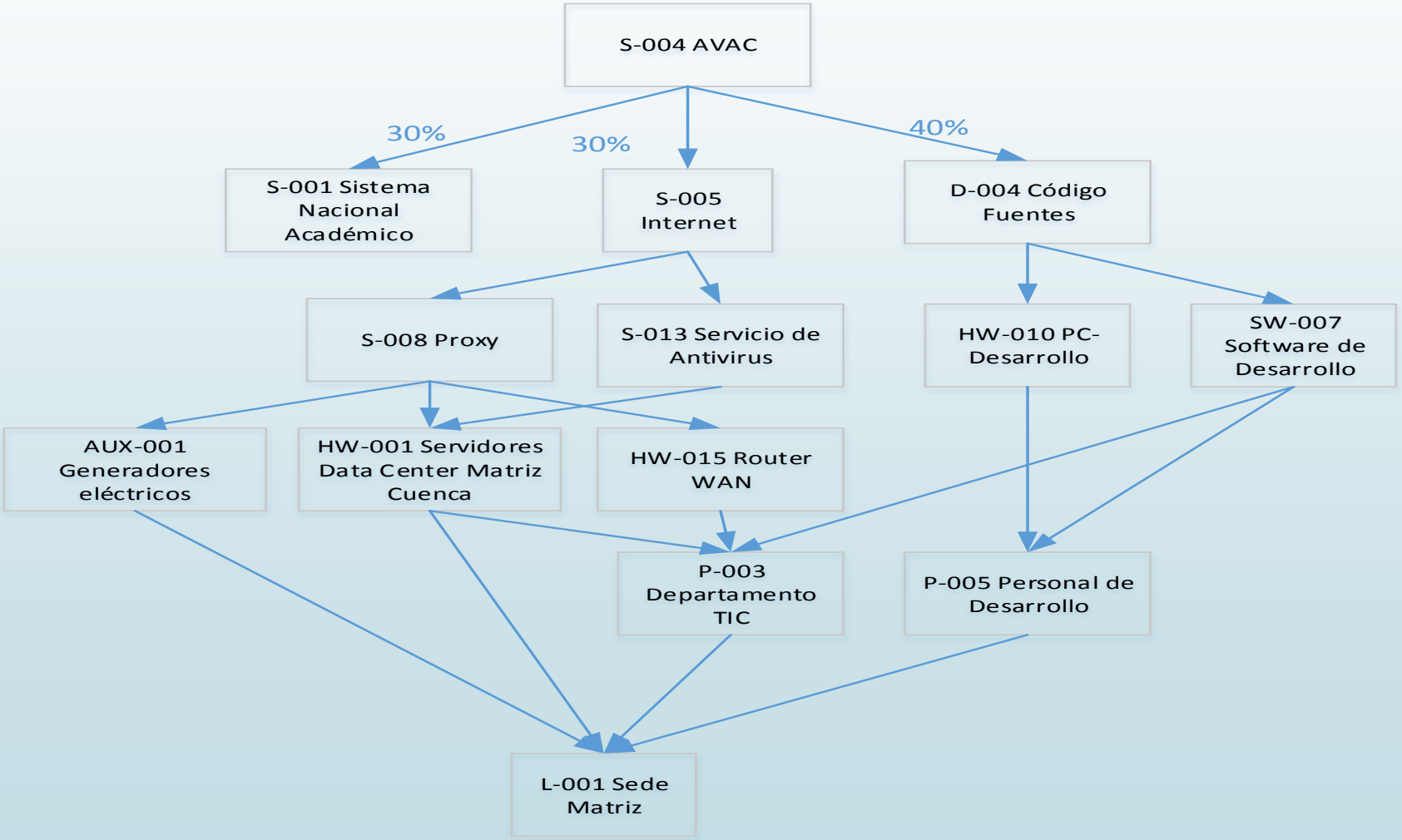
3. Análisis de Riesgos
3.2 Valoración de activos



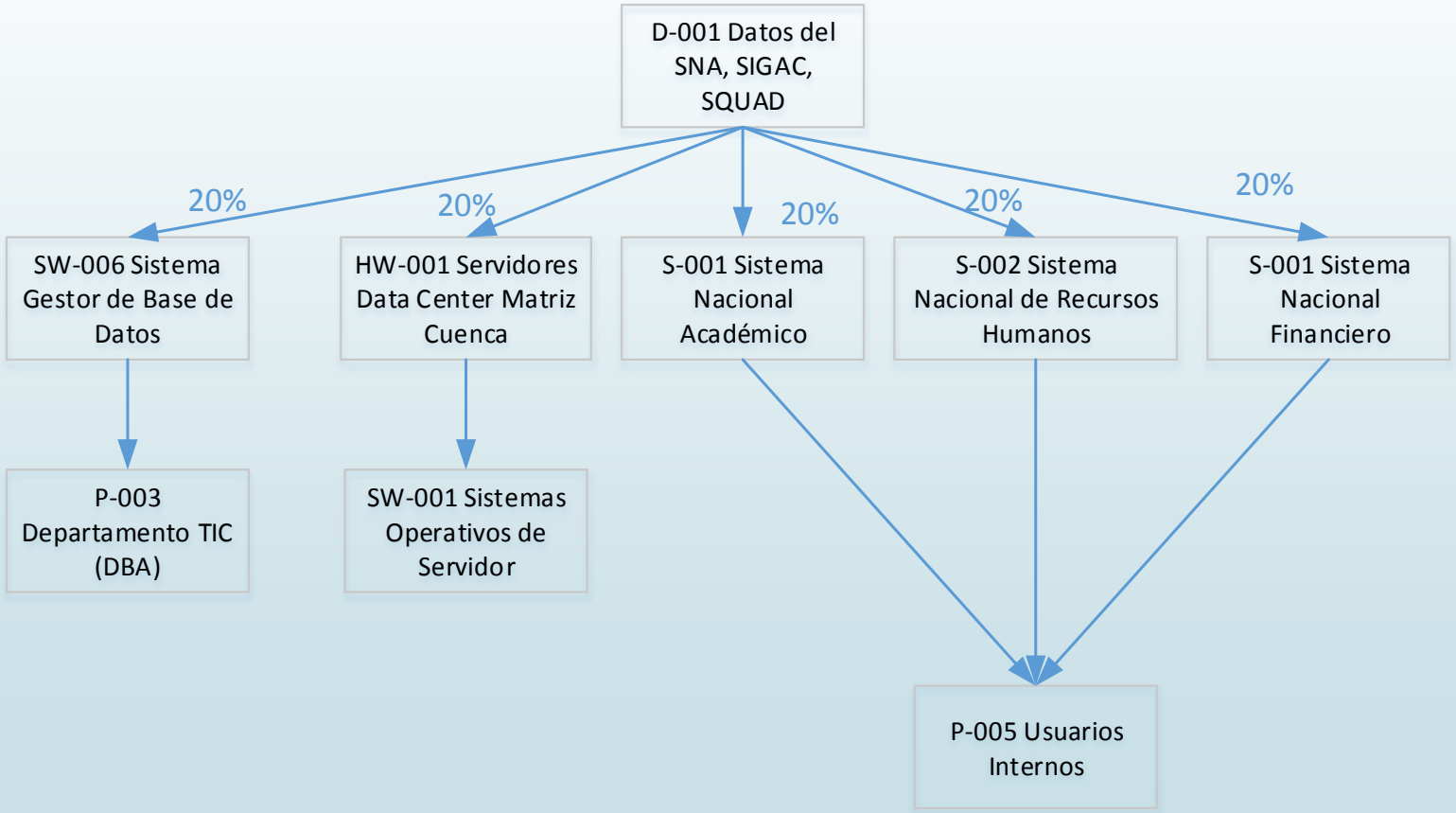
3. Análisis de Riesgos
3.2 Valoración de activos



3. Análisis de Riesgos
3.2 Valoración de activos



3. Análisis de Riesgos
3.2 Valoración de activos



3. Análisis de Riesgos
3.2 Valoración de activos

Valoración de activos		
Descripción	**Abreviatura**	**Valor**
Muy alto	MA	500.000,00 USD
Alto	A	300.000,00 USD
Medio	M	100.000,00 USD
Bajo	B	10.000,00 USD
Muy bajo	MB	1.000,00 USD

La valoración se completó con el impacto relacionado a cada dimensión de la seguridad

3. Análisis de Riesgos
3.2 Valoración de activos

Caracterización	Código activo	Denominación	Valoración cualitativa	Valoración cuantitativa	Autenticidad [A]	Confidencialidad [C]	Integridad [I]	Disponibilidad [D]	Trazabilidad [T]
[inf] Información	I-001	Información académica	MA	500.000,00 USD	2	4	9	6	2
[inf] Información	I-002	Información Talento Humano	MA	500.000,00 USD	2	6	9	4	2
[inf] Información	I-003	Información financiera	MA	500.000,00 USD	2	6	9	4	2
[service] Servicio	S-001	Sistema Nacional Académico (SNA)	MA	500.000,00 USD	4	4	6	8	2
[service] Servicio	S-002	Sistema Nacional de Recursos Humanos	MA	500.000,00 USD	4	4	6	6	2
[service] Servicio	S-003	Sistema Nacional Financiero	MA	500.000,00 USD	4	8	6	6	2
[service] Servicio	S-004	AVAC	MA	500.000,00 USD	2	0	2	8	0
[D] Datos	D-001	Datos del SNA, SIGAC y SQUAD	MA	500.000,00 USD	6	6	9	9	2

3. Análisis de Riesgos
3.3 Análisis de Amenazas

- Según el catálogo de amenazas de MAGERIT se procedió a valorar la frecuencia de ocurrencia de la amenaza en cuestión con los diferentes activos.

3. Análisis de Riesgos
3.3 Análisis de Amenazas

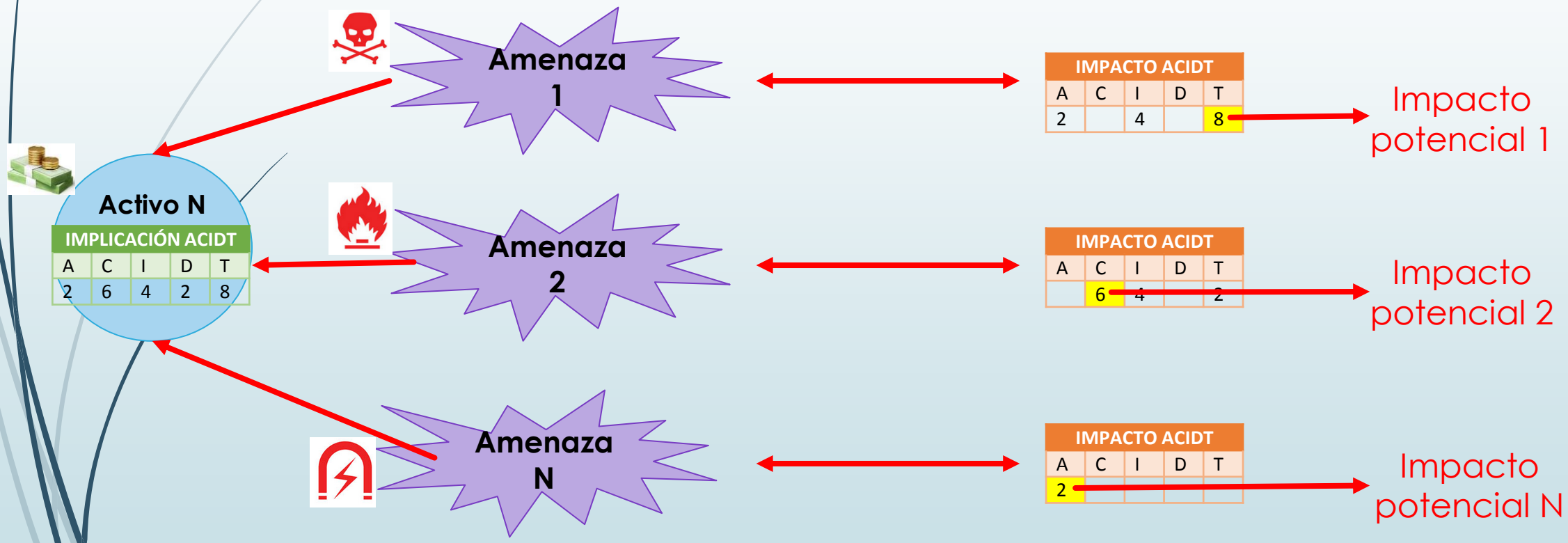
Código	Amenaza	Dimensiones					Activos según la categorización											
		A	C	I	D	T	[inf]	[service]	[D]	[k]	[S]	[SW]	[HW]	[COM]	[M]	[AUX]	[L]	[P]
[N.1]	Fuego				x								x		x	x	x	
[N.2]	Daños por agua				x								x		x	x	x	
[N.3]	Desastres naturales				x								x		x	x	x	
..	..																	

3. Análisis de Riesgos
3.4 Impacto Potencial y Residual

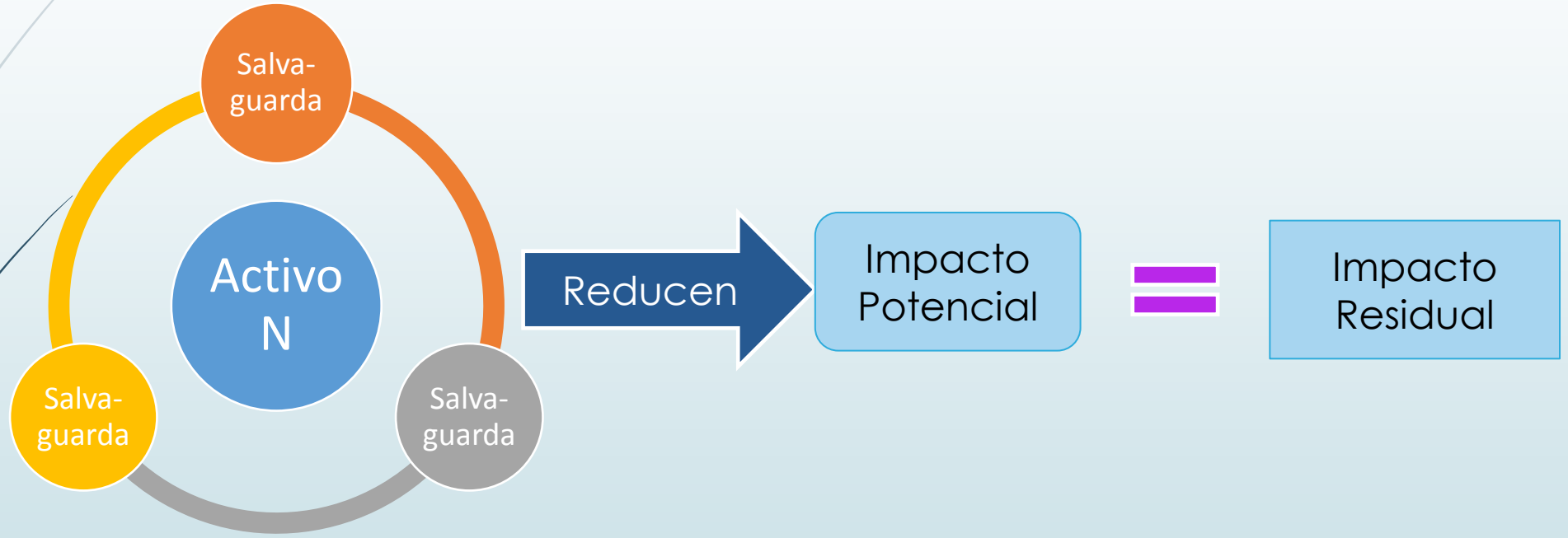
- Impacto Potencial = Valoración Activo*Frecuencia*max(propiedad ACIDT)

- Impacto Residual = Impacto Potencial * Valor Disminución Salvaguarda

3. Análisis de Riesgos
3.4 Impacto Potencial y Residual



3. Análisis de Riesgos
3.4 Impacto Potencial y Residual



3. Análisis de Riesgos
3.5 Nivel de Riesgo

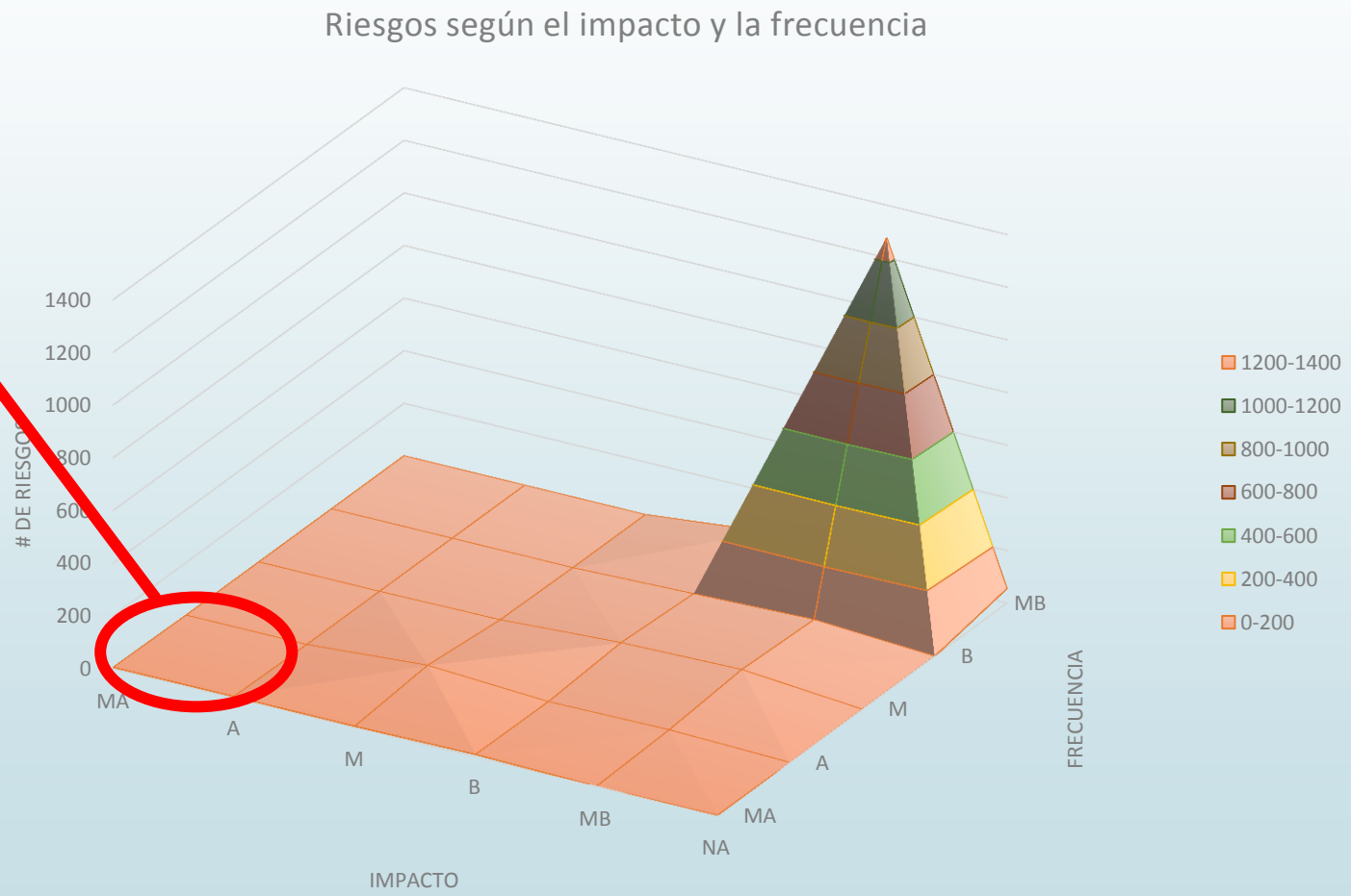
La UPS asume los riegos cuyo impacto sea considerado bajo sin importar la frecuencia de ocurrencia (igual o menor a 10.000,00 USD)

Riesgos a tratar			
	Frecuencia		
Impacto	**MA**	**A**	**M**
MA	4	5	4
A			33
M			4

3. Análisis de Riesgos
3.5 Nivel de Riesgo

Zona Crítica
Impacto Muy Alto
Frecuencia Muy Alta

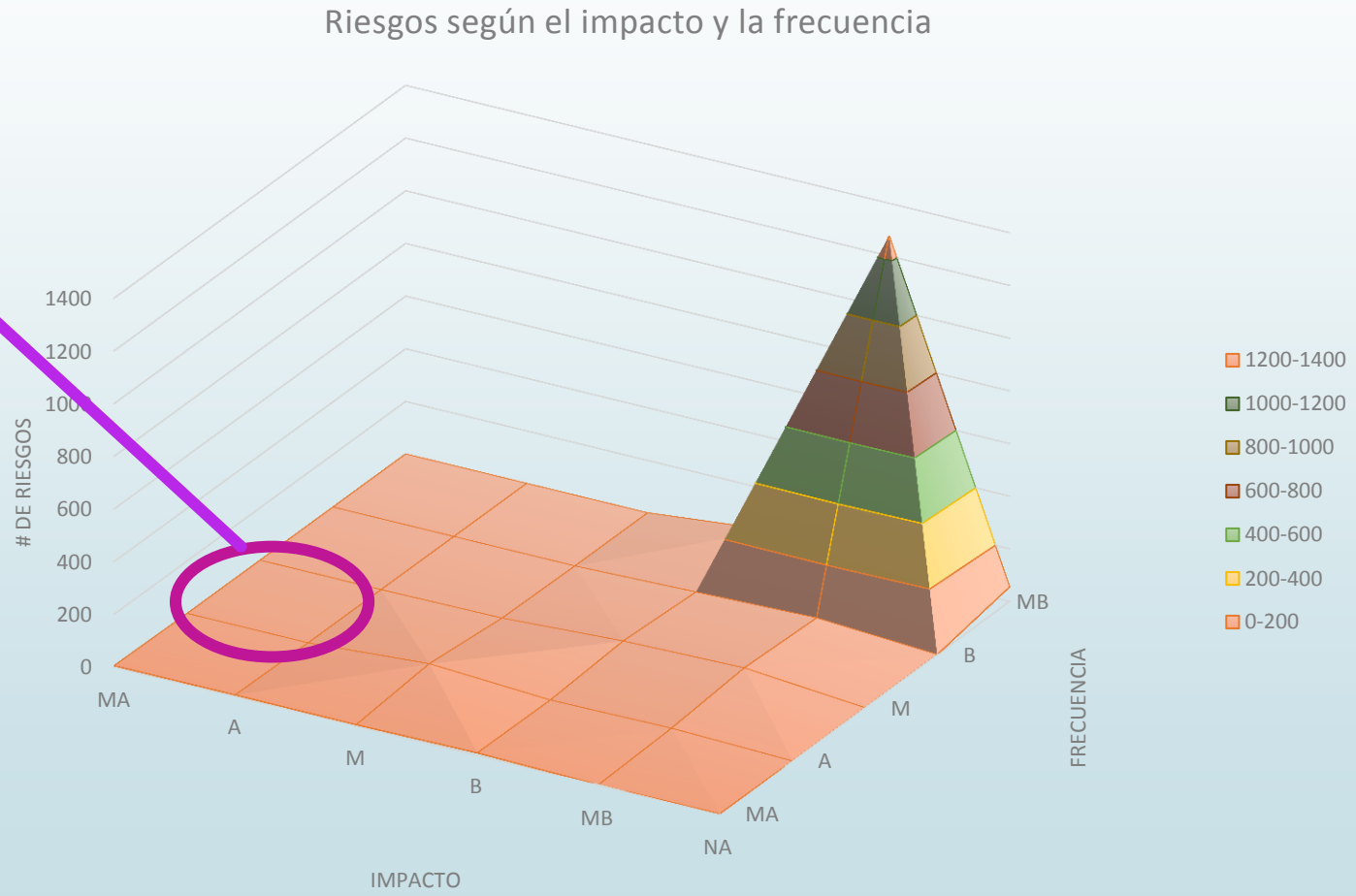
Existen 5 Riesgos en esta zona



3. Análisis de Riesgos
3.5 Nivel de Riesgo

Zona Criticidad Media
Impacto Muy Alto
Frecuencia Alta

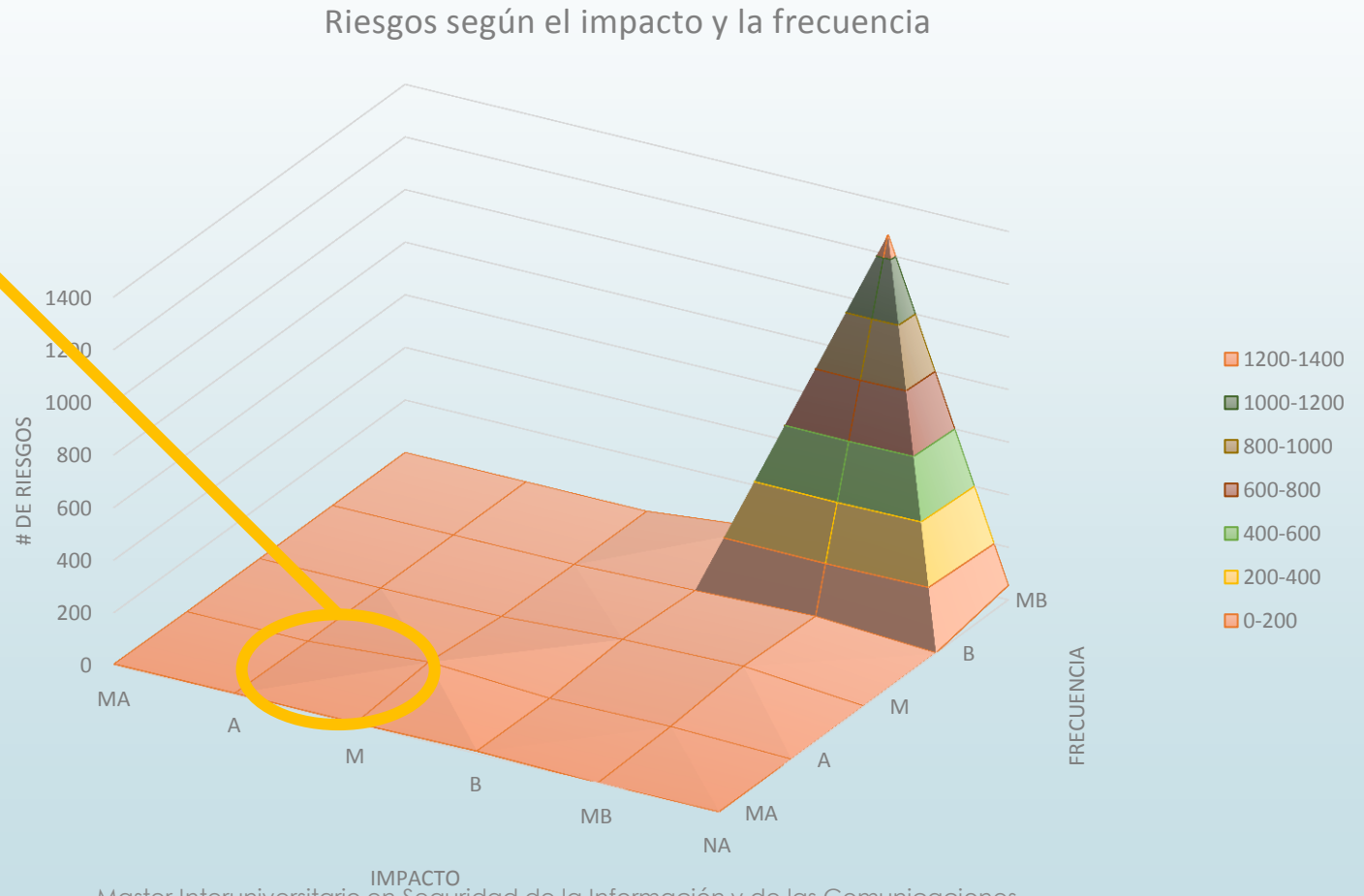
Existen 0 Riesgos en esta zona



3. Análisis de Riesgos
3.5 Nivel de Riesgo

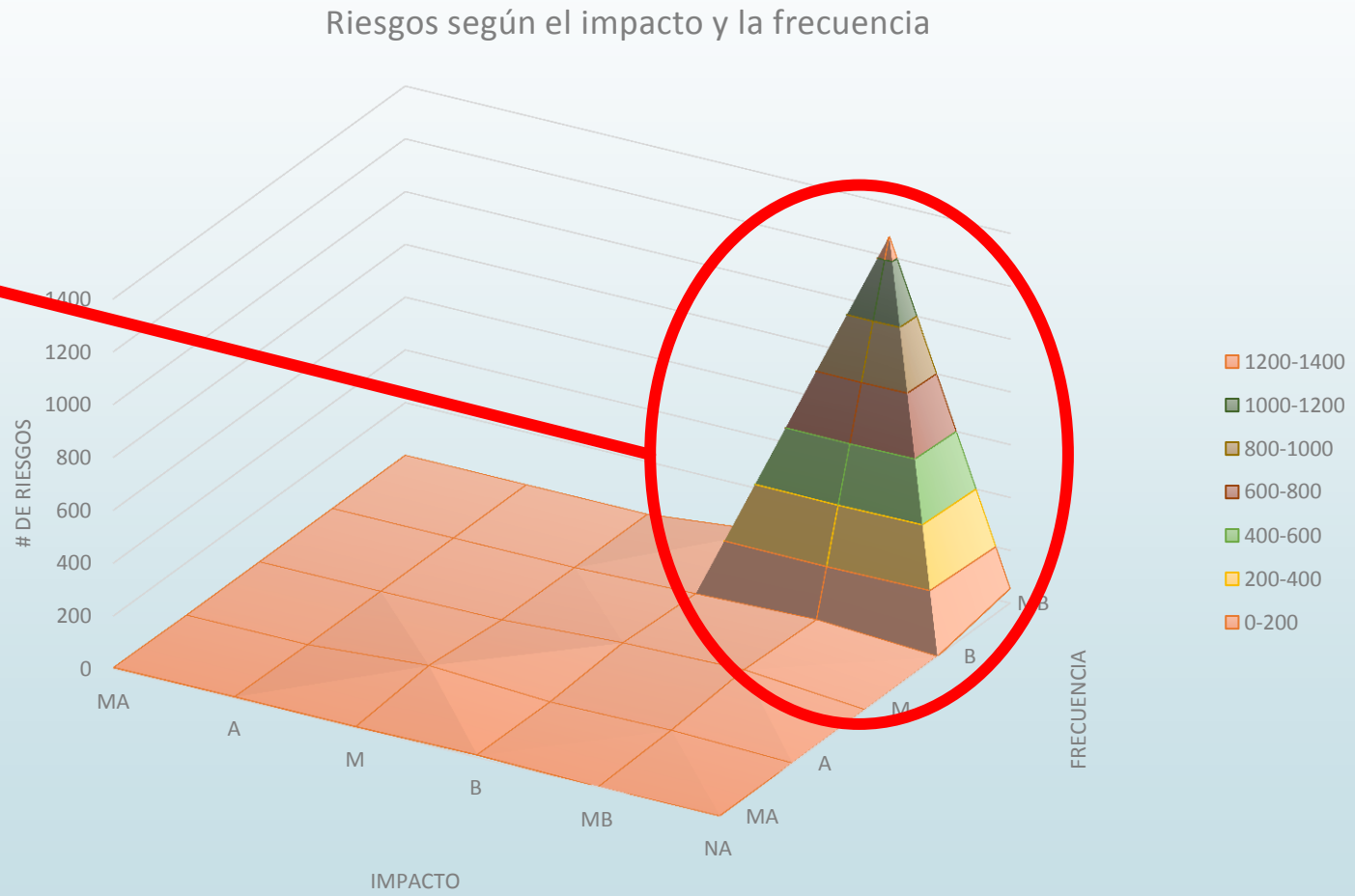
Zona Criticidad Media
Impacto Alto
Frecuencia Muy Alta

Existen 5 Riesgos en esta zona



3. Análisis de Riesgos
3.5 Nivel de Riesgo

La gran mayoría de riesgos se encuentran por debajo del umbral aceptado por la UPS.
Impacto: Bajo – Muy Bajo
Frecuencia Baja – Muy Baja



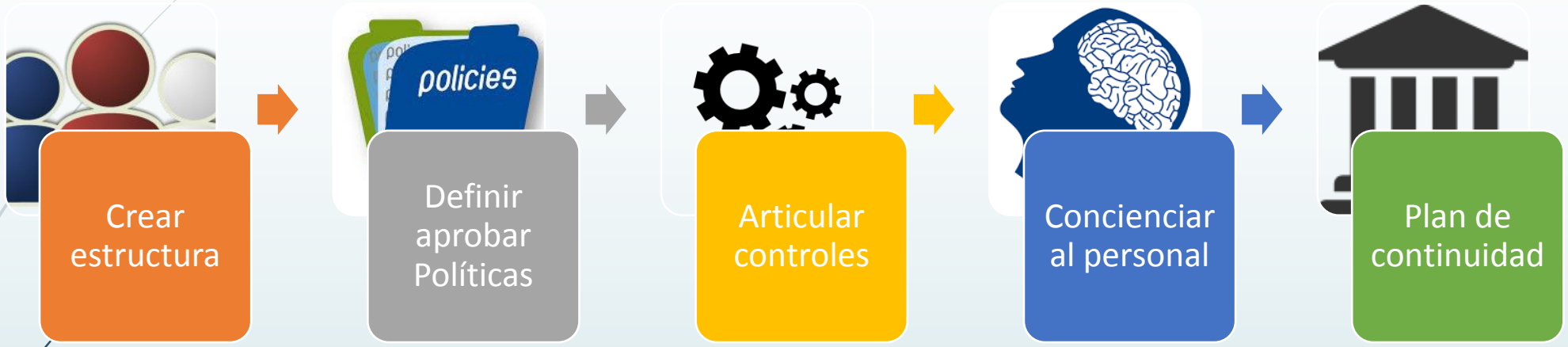
3. Análisis de Riesgos
3.5 Nivel de Riesgo

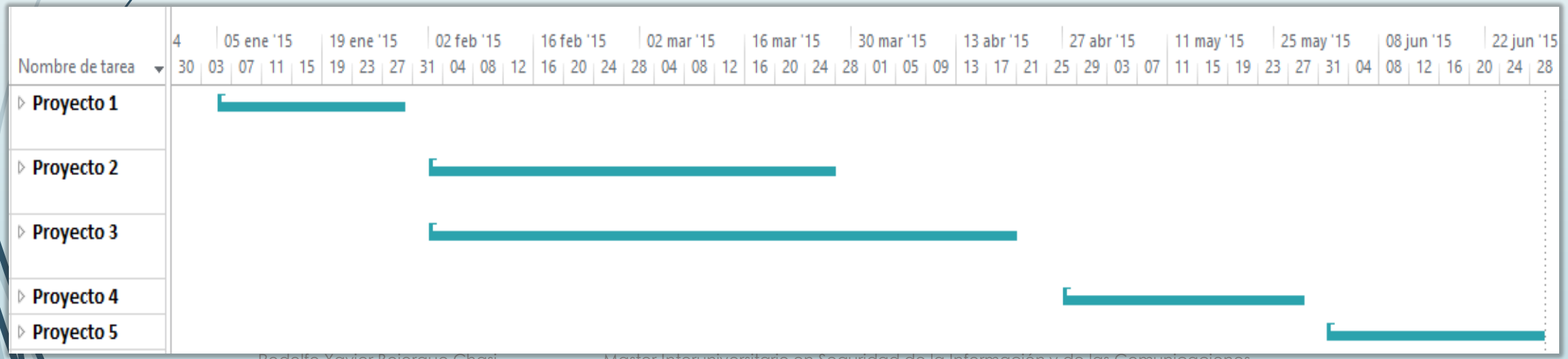
Código Activo	Activo	Código Amenaza	Amenaza	Frecuencia	Valor. Freq	Valor Impacto	Impacto
I-002	Información Talento Humano	[A.19]	Divulgación de información	MA	1	300.000,00 USD	MA
I-003	Información financiera	[A.19]	Divulgación de información	MA	1	300.000,00 USD	MA
S-001	Sistema Nacional Académico (SNA)	[E.1]	Errores de los usuarios	MA	1	300.000,00 USD	MA
S-003	Sistema Nacional Financiero	[E.1]	Errores de los usuarios	MA	1	300.000,00 USD	MA
I-001	Información académica	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
I-002	Información Talento Humano	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
I-003	Información financiera	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
S-002	Sistema Nacional de Recursos Humanos	[E.1]	Errores de los usuarios	MA	1	225.000,00 USD	A
I-001	Información académica	[A.19]	Divulgación de información	MA	1	200.000,00 USD	A

4. Propuesta de Proyectos

- **Proyecto 1:** Estructuración de la organización de la seguridad de la información
- **Proyecto 2:** Definición, Aprobación y difusión inmediata de las políticas de seguridad de la información
- **Proyecto 3:** Articulación de los controles existentes con la política del SGSI
- **Proyecto 4:** Plan de concienciación en materia de seguridad de la información
- **Proyecto 5:** Plan de Continuidad del Negocio

4. Propuesta de Proyectos



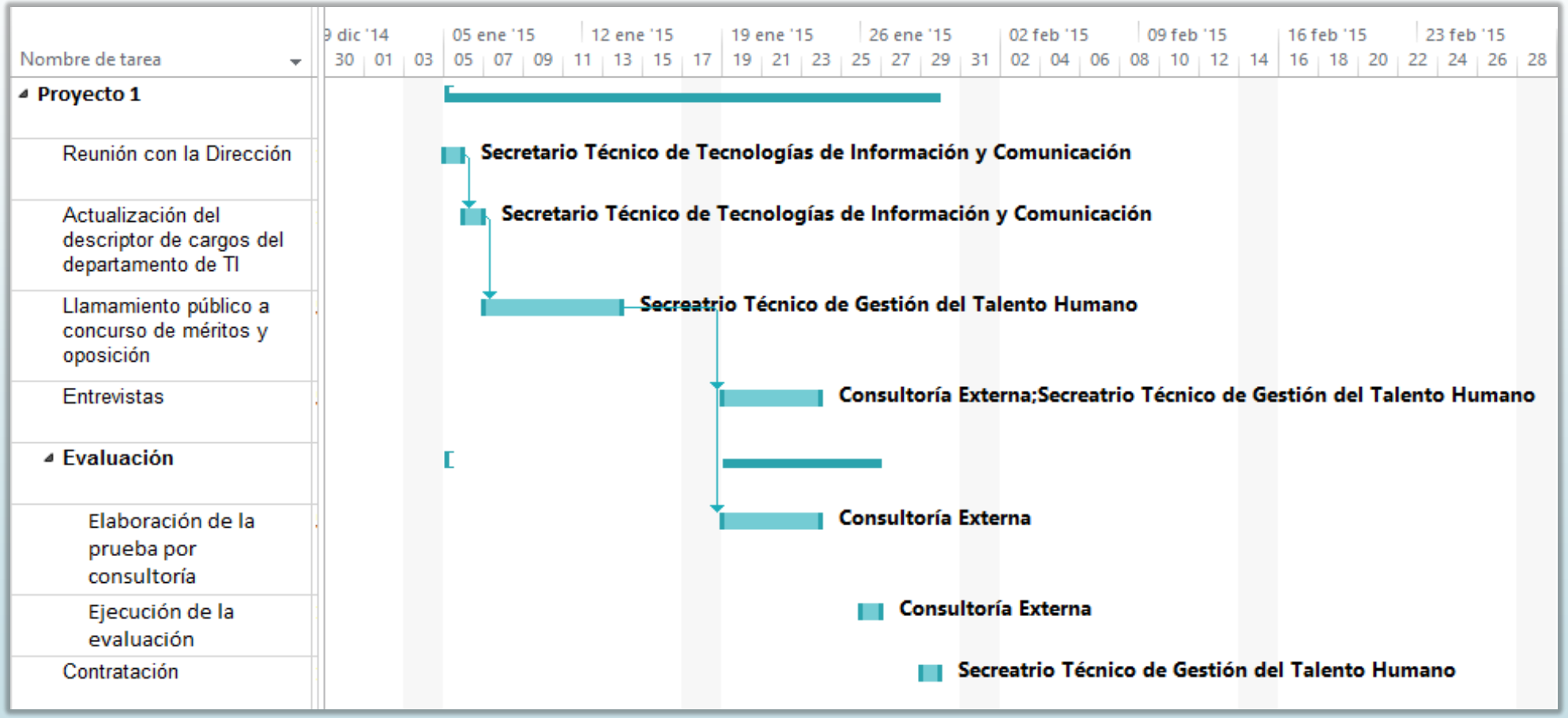


4. Propuesta de Proyectos
4.1 Proyecto 1

- Objetivos:
  - Contar con una estructura de organización de la seguridad de la información:
  - Crear nuevos cargos
  - Redefinir el descriptivo de cargos del Departamento de TI
  - Contratar a la persona adecuada

- Presupuesto: 6.400,00 USD

4. Propuesta de Proyectos
4.1 Proyecto 1

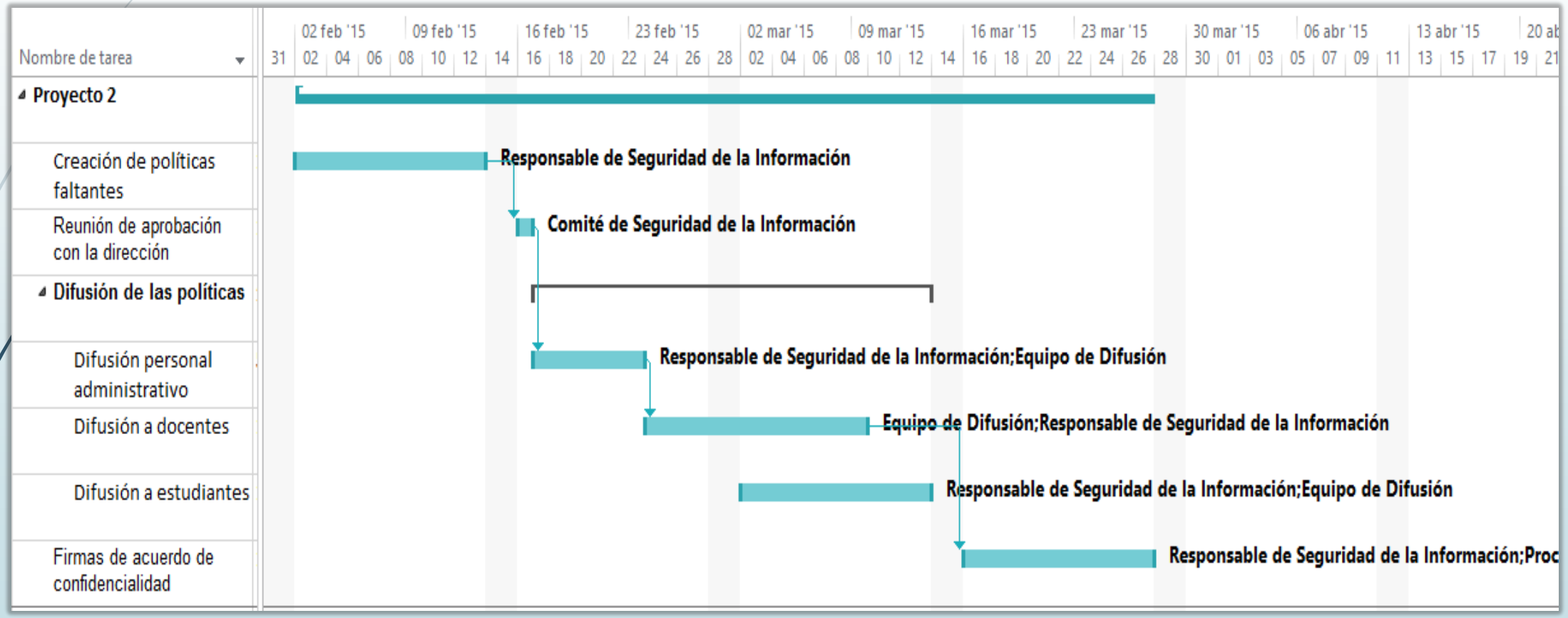


4. Propuesta de Proyectos
4.2 Proyecto 2

- Objetivos:
  - Alcanzar por lo menos el nivel de madurez de "Gestionado" en el dominio 5 de la norma ISO/IEC 27002:2013 "Políticas de Seguridad".
  - Alcanzar por lo menos el nivel de madurez de "Definido" en el domino 7 de la norma ISO/IEC 27002:2013 "Seguridad ligada a los recursos humanos":

- Presupuesto: 6.100,00 USD

4. Propuesta de Proyectos
4.2 Proyecto 2



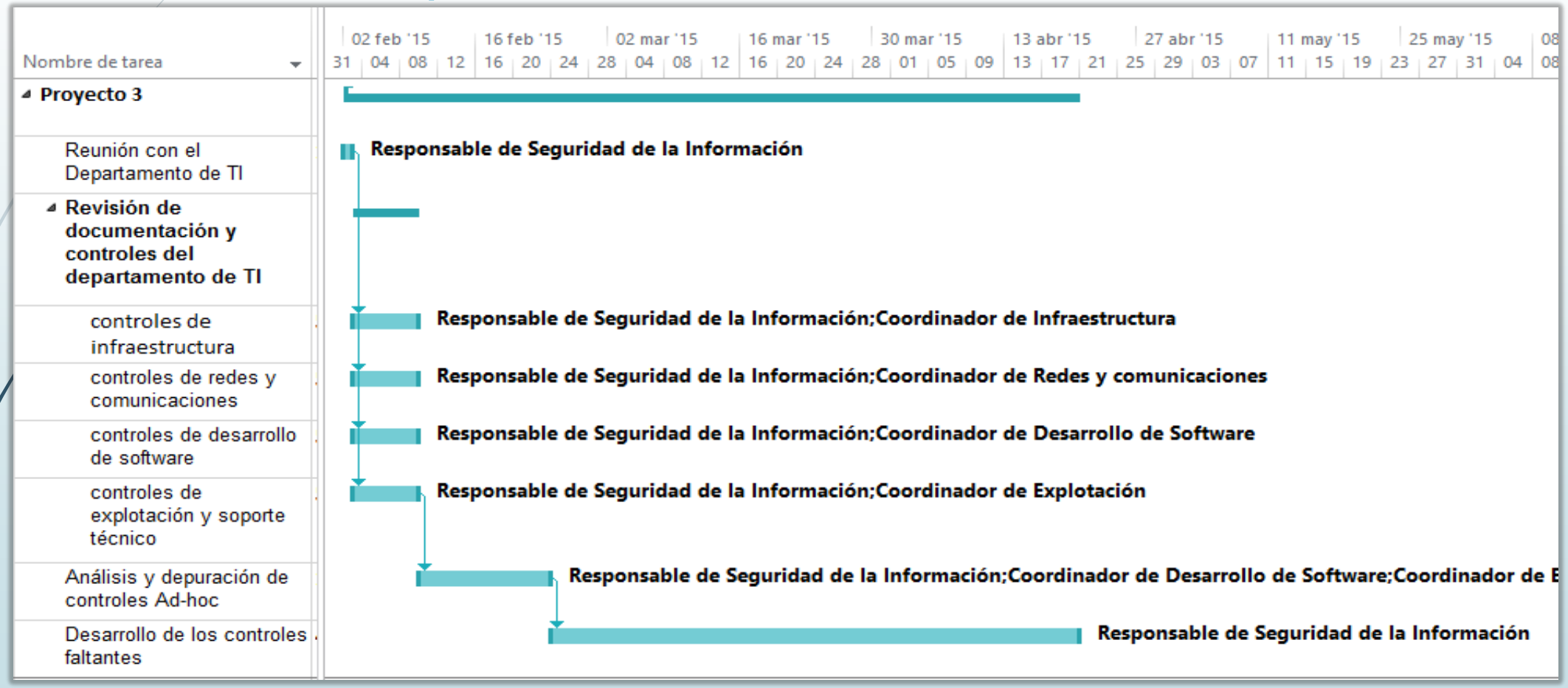
4. Propuesta de Proyectos
4.3 Proyecto 3

- Objetivos:
  - Alcanzar por lo menos el estado de madurez de "Definido" según la norma ISO/IEC 27002:2013 para los dominios:
    - Adquisición, desarrollo y mantenimiento de los sistemas de información.
    - Relación con suministradores.
    - Gestión de incidentes en la seguridad de la información.

4. Propuesta de Proyectos
4.3 Proyecto 3

- Objetivos:
  - Alcanzar por lo menos el estado de madurez de "Definido" según la norma ISO/IEC 27002:2013 para los dominios:
    - Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
    - Seguridad en la operativa.
    - Seguridad física y ambiental.
    - Cifrado
- Presupuesto: 30.400,00 USD

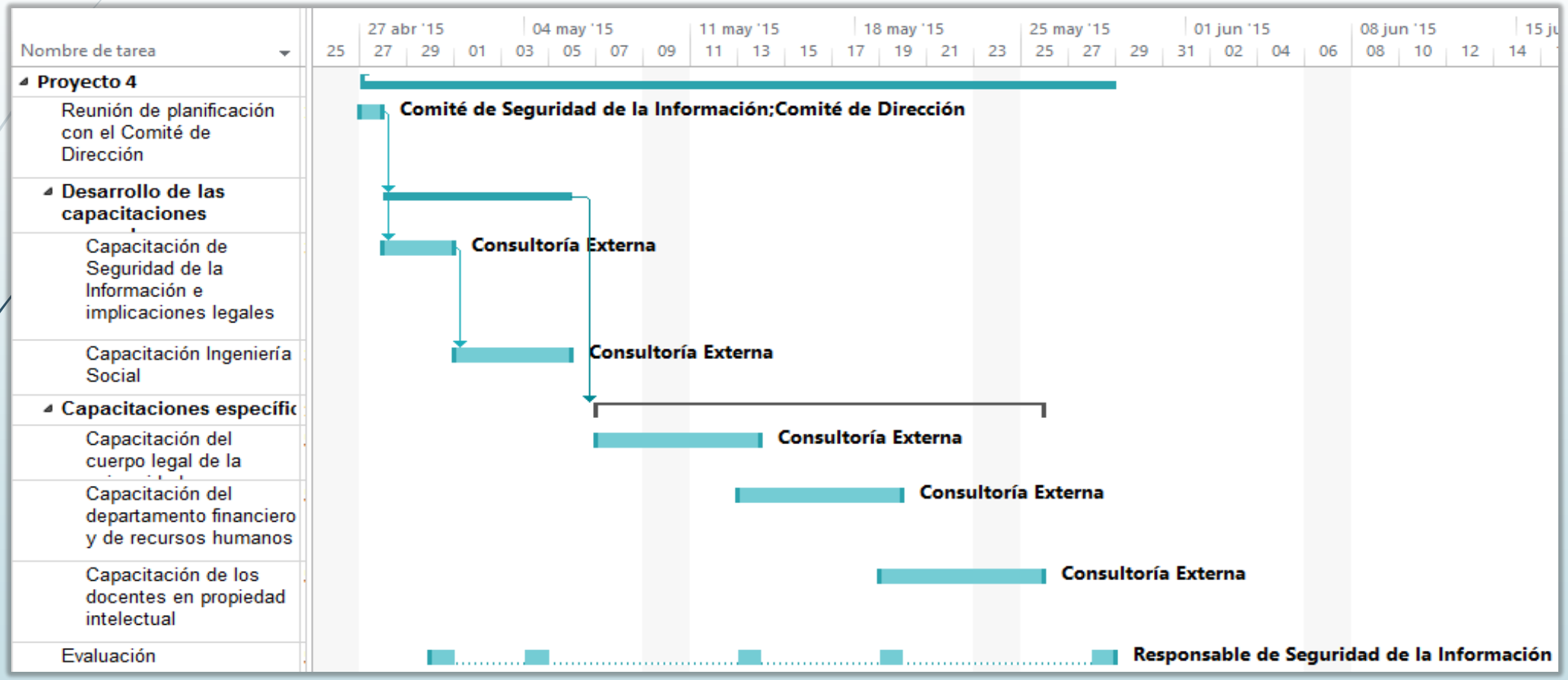
4. Propuesta de Proyectos
4.3 Proyecto 3



4. Propuesta de Proyectos
4.4 Proyecto 4

- Objetivos:
  - Alcanzar el nivel de madurez por lo menos de "Gestionado" en los dominios de la ISO/IEC 27002:2013:
    - Cumplimiento
    - Gestión de Incidentes en la seguridad de la información
    - Seguridad ligada a los recursos humanos
- Presupuesto: 6.300,00 USD

4. Propuesta de Proyectos
4.4 Proyecto 4

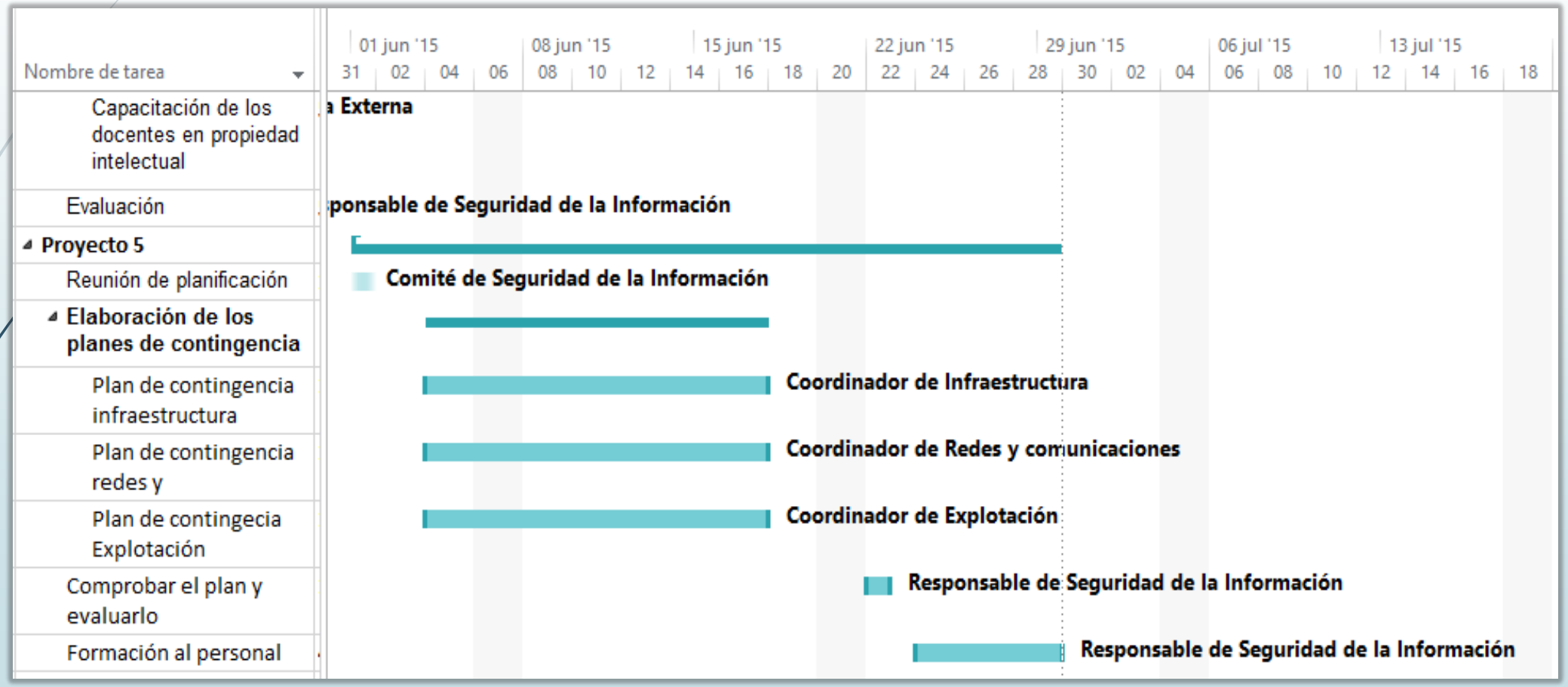


4. Propuesta de Proyectos
4.5 Proyecto 5

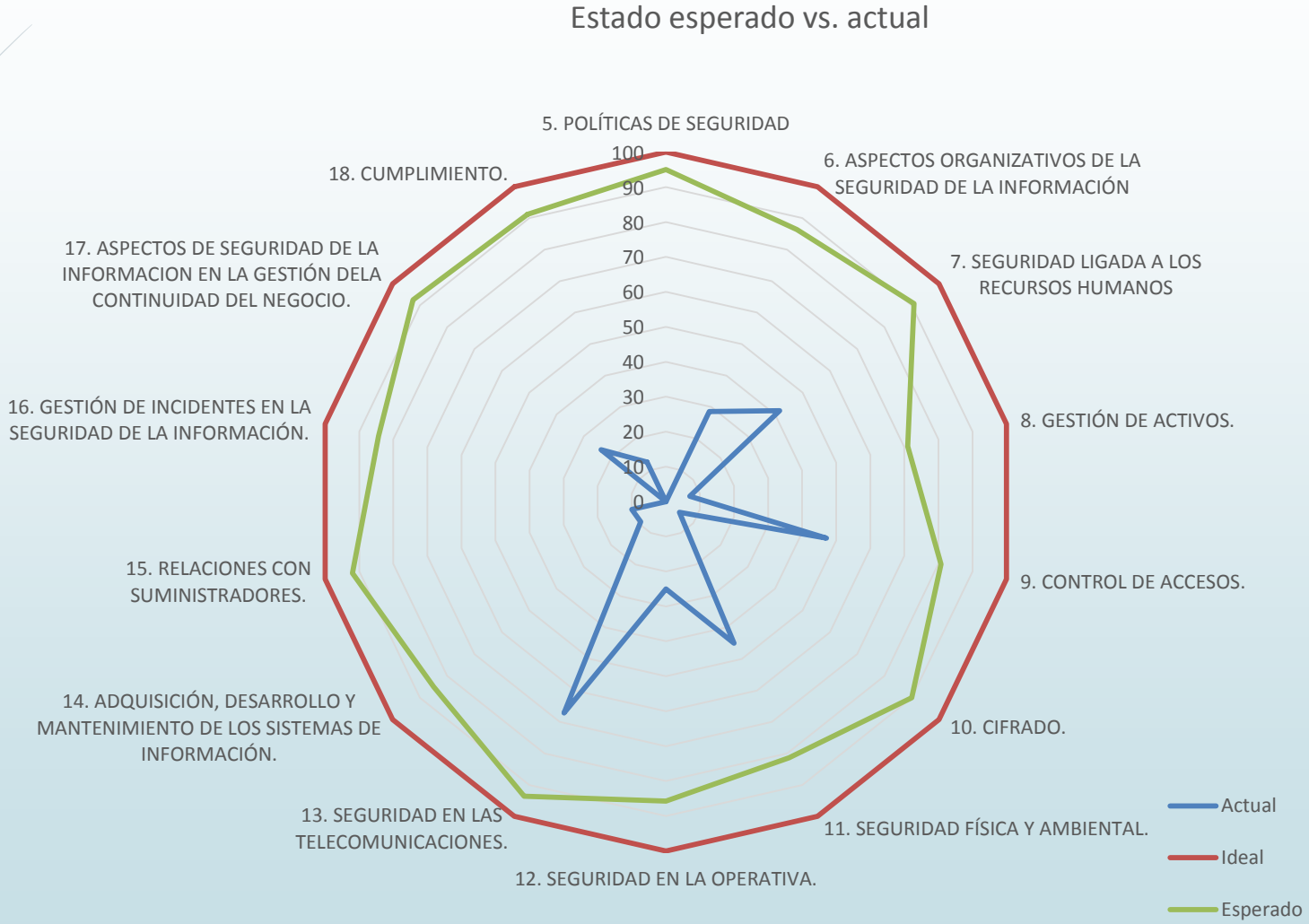
- Objetivos:
  - Asegurar que la UPS pueda seguir prestando sus servicios académicos y tener la información básica necesaria para el correcto funcionamiento de las actividades administrativas.
  - Alcanzar el nivel de madurez por lo menos de “Gestionado” en el dominio de la ISO/IEC 27002:2013 “Aspectos de seguridad de la información en la gestión dela continuidad del negocio”

- Presupuesto: 2.180,00 USD

4. Propuesta de Proyectos
4.5 Proyecto 5



4. Propuesta de Proyectos



5. Auditoría de cumplimiento

- Ejecutados los proyectos, se realiza la auditoría de cumplimiento:
  1. Objetivo
  2. Alcance
  3. Metodología
  4. Pruebas
  5. Análisis de resultados
  6. Informe

5. Auditoría de cumplimiento
5.1 Objetivo

- Verificar el estado de implementación y cumplimiento de la norma ISO/IEC 27001:2013 y de los controles establecidos en la declaración de aplicabilidad de la UPS

5. Auditoría de cumplimiento
5.2 Alcance

- Verificar el nivel de cumplimiento de la norma ISO/IEC 27001:2013 y de los 18 dominios de la norma ISO/IEC 27002:2013 según la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información

5. Auditoría de cumplimiento
5.3 Metodología

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A6**	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		**75**	
Objetivo	**A6.1**	**6.1 Organización interna**	**95**		
Control	A6.1.1	6.1.1 Asignación de responsabilidades para la seguridad de la información.	Optimizado	100	
Control	A6.1.2	6.1.2 Segregación de tareas.	Gestionado	95	
Control	A6.1.3	6.1.3 Contacto con las autoridades.	Gestionado	95	
Control	A6.1.4	6.1.4 Contacto con grupos de interés especial.	Definido	90	
Control	A6.1.5	6.1.5 Seguridad de la información en la gestión de proyectos.	Gestionado	95	
Objetivo	**A6.2**	**6.2 Dispositivos para movilidad y teletrabajo.**	**25**		**Mayor**
Control	A6.2.2		No existente	0	Menor

NO CONFORMIDAD MAYOR: Acumulación de no conformidades menores impiden el cumplimiento del objetivo

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A7**	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		**80**	
Objetivo	**A7.1**	**7.1 Antes de la contratación**	**95**		
Control	A7.1.1	7.1.1 Investigación de antecedentes.	Gestionado	95	
Control	A7.1.2	7.1.2 Términos y condiciones de contratación.	Gestionado	95	
Objetivo	**A7.2**	**7.2. Durante la contratación**	**65**		
Control	A7.2.1	7.2.1 Responsabilidades de gestión.	Gestionado	95	
Control	A7.2.2	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Definido	90	Oportunidad
Control	A7.2.3	7.2.3 Proceso disciplinario.	Inicial	10	Menor
Objetivo	**A7.3**	**7.3 Cese o cambio de puesto de trabajo.**	**95**		
Control	A7.3.1	7.3.1 Cese o cambio de puesto de trabajo.	Gestionado	95	

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A8**	**8. GESTIÓN DE ACTIVOS.**		**67**	
Objetivo	**A8.1**	**8.1 Responsabilidad sobre los activos.**	**83,75**		
Control	A8.1.1	8.1.1 Inventario de activos.	Gestionado	95	
Control	A8.1.2	8.1.2 Propiedad de los activos.	Gestionado	95	
Control	A8.1.3	8.1.3 Uso aceptable de los activos.	Limitado	50	Menor
Control	A8.1.4	8.1.4 Devolución de activos.	Gestionado	95	
Objetivo	**A8.2**	**8.2 Clasificación de la información.**	**91,6666667**		
Control	A8.2.1	8.2.1 Directrices de clasificación.	Gestionado	95	
Control	A8.2.2	8.2.2 Etiquetado y manipulado de la información.	Definido	90	
Control	A8.2.3	8.2.3 Manipulación de activos.	Definido	90	
Objetivo	**A8.3**	**8.3 Manejo de los soportes de almacenamiento.**	**20**		
Control	A8.3.1	8.3.1 Gestión de soportes extraíbles.	Limitado	50	Menor
Control	A8.3.2	8.3.2 Eliminación de soportes.	Inicial	10	
Control	A8.3.3	8.3.3 Soportes físicos en tránsito.	No existente	0	

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A11**	**11. SEGURIDAD FÍSICA Y AMBIENTAL.**		**77**	
Objetivo	**A11.1**	**11.1 Áreas seguras.**	**86,6666667**		
Control	A11.1.1	11.1.1 Perímetro de seguridad física.	Gestionado	95	
Control	A11.1.2	11.1.2 Controles físicos de entrada.	Gestionado	95	
Control	A11.1.3	11.1.3 Seguridad de oficinas, despachos y recursos.	Gestionado	95	
Control	A11.1.4	11.1.4 Protección contra las amenazas externas y ambientales.	Gestionado	95	
Control	A11.1.5	11.1.5 El trabajo en áreas seguras.	Limitado	50	
Control	A11.1.6	11.1.6 Áreas de acceso público, carga y descarga.	Definido	90	
Objetivo	**A11.2**	**11.2 Seguridad de los equipos.**	**70,5555556**		
Control	A11.2.1	11.2.1 Emplazamiento y protección de equipos.	Definido	90	Menor
Control	A11.2.2	11.2.2 Instalaciones de suministro.	Gestionado	95	
Control	A11.2.3	11.2.3 Seguridad del cableado.	Gestionado	95	
Control	A11.2.4	11.2.4 Mantenimiento de los equipos.	Gestionado	95	Oportunidad
Control	A11.2.5	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Inicial	10	Menor
Control	A11.2.6	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Inicial	10	Menor
Control	A11.2.7	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Limitado	50	
Control	A11.2.8	11.2.8 Equipo informático de usuario desatendido.	Gestionado	95	
Control	A11.2.9	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Gestionado	95	

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A13**	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**		**93,57142857**	
Objetivo	**A13.1**	**13.1 Gestión de la seguridad en las redes.**	**95**		
Control	A13.1.1	13.1.1 Controles de red.	Gestionado	95	
Control	A13.1.2	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Gestionado	95	Oportunidad
Control	A13.1.3	13.1.3 Segregación de redes.	Gestionado	95	
Objetivo	**A13.2**	**13.2 Intercambio de información con partes externas.**	**92,5**		
Control	A13.2.1	13.2.1 Políticas y procedimientos de intercambio de información.	Definido	90	
Control	A13.2.2	13.2.2 Acuerdos de intercambio.	Definido	90	
Control	A13.2.3	13.2.3 Mensajería electrónica.	Gestionado	95	Oportunidad
Control	A13.2.4	13.2.4 Acuerdos de confidencialidad y secreto	Gestionado	95	

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A14**	**14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**		60	
Objetivo	**A14.1**	**14.1 Requisitos de seguridad de los sistemas de información.**	**90**		
Control	A14.1.1	14.1.1 Análisis y especificación de los requisitos de seguridad.	Definido	90	
Control	A14.1.2	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Definido	90	
Control	A14.1.3	14.1.3 Protección de las transacciones por redes telemáticas.	Definido	90	
Objetivo	**A14.2**	**14.2 Seguridad en los procesos de desarrollo y soporte.**	**55,5555556**		**Mayor**
Control	A14.2.1	14.2.1 Política de desarrollo seguro de software.	Gestionado	95	
Control	A14.2.2	14.2.2 Procedimientos de control de cambios en los sistemas.	Definido	90	
Control	A14.2.3	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Inicial	10	Menor
Control	A14.2.5	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Inicial	10	
Control	A14.2.6	14.2.6 Seguridad en entornos de desarrollo.	Definido	90	Observación
Control	A14.2.7	14.2.7 Externalización del desarrollo de software.	Definido	90	
Control	A14.2.8	14.2.8 Pruebas de seguridad de los sistemas.	Inicial	10	Menor
Control	A14.2.9	14.2.9 Pruebas de aceptación.	Gestionado	95	
Objetivo	**A14.3**	**14.3 Datos de prueba.**	**10**		
Control	A14.3.1	14.3.1 Protección de los datos utilizados en pruebas.	Inicial	10	Menor

NO CONFORMIDAD MAYOR: Acumulación de no conformidades menores impiden el cumplimiento del objetivo

5. Auditoría de cumplimiento
5.4 Pruebas – No conformidades

Tipo	Apartado	Dominio / Objetivo / Control	Madurez Auditada	Valoración cuantitativa	Desviación
Dominio	**A13**	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**		**93,57142857**	
Objetivo	**A13.1**	**13.1 Gestión de la seguridad en las redes.**	**95**		
Control	A13.1.1	13.1.1 Controles de red.	Gestionado	95	
Control	A13.1.2	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Gestionado	95	Oportunidad
Control	A13.1.3	13.1.3 Segregación de redes.	Gestionado	95	
Objetivo	**A13.2**	**13.2 Intercambio de información con partes externas.**	**92,5**		
Control	A13.2.1	13.2.1 Políticas y procedimientos de intercambio de información.	Definido	90	
Control	A13.2.2	13.2.2 Acuerdos de intercambio.	Definido	90	
Control	A13.2.3	13.2.3 Mensajería electrónica.	Gestionado	95	Oportunidad
Control	A13.2.4	13.2.4 Acuerdos de confidencialidad y secreto	Gestionado	95	

5. Auditoría de cumplimiento
5.4 Pruebas

No conformidades	Cantidad
Mayor	2
Menor	7
Observación	1
Oportunidad de mejora	4

Dos conformidades mayores por acumulación de no conformidades menores impiden cumplir dos objetivos de control de la norma

6.2 Dispositivos para movilidad y teletrabajo

14.2 Seguridad en los procesos de desarrollo y soporte.

5. Auditoría de cumplimiento
5.4 Pruebas

No conformidades	Cantidad
Mayor	2
Menor	7
Observación	1
Oportunidad de mejora	4

La mayoría de no conformidades menores responden a una política aprobada pero no implementada en controles o su estado está en desarrollo

5. Auditoría de cumplimiento
5.4 Pruebas

No conformidades	Cantidad
Mayor	2
Menor	7
Observación	1
Oportunidad de mejora	4

Existe la política, el control se ha implementado, pero no se cumple el literal j de la norma.

14.2.6 Seguridad en entornos de desarrollo.

5. Auditoría de cumplimiento
5.4 Pruebas

No conformidades	Cantidad
Mayor	2
Menor	7
Observación	1
Oportunidad de mejora	4

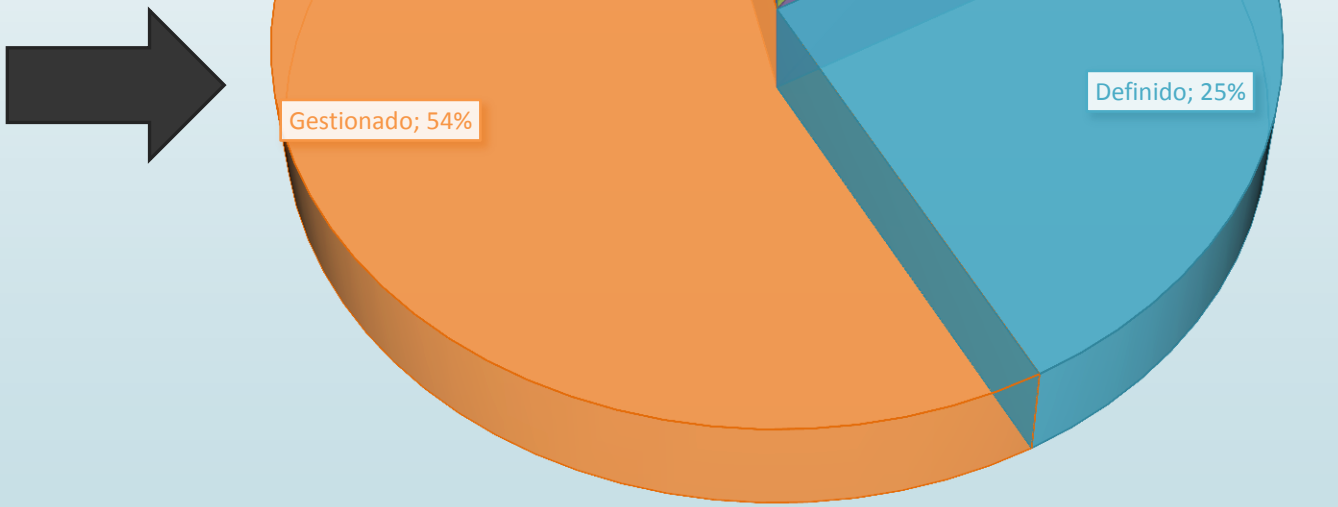
Existen tres oportunidades que permitirían pasar del estado gestionado al optimizado:

11.2.4 Mantenimiento de los equipos.
13.1.2 Mecanismos de seguridad asociados a servicios en red
13.2.3 Mensajería electrónica

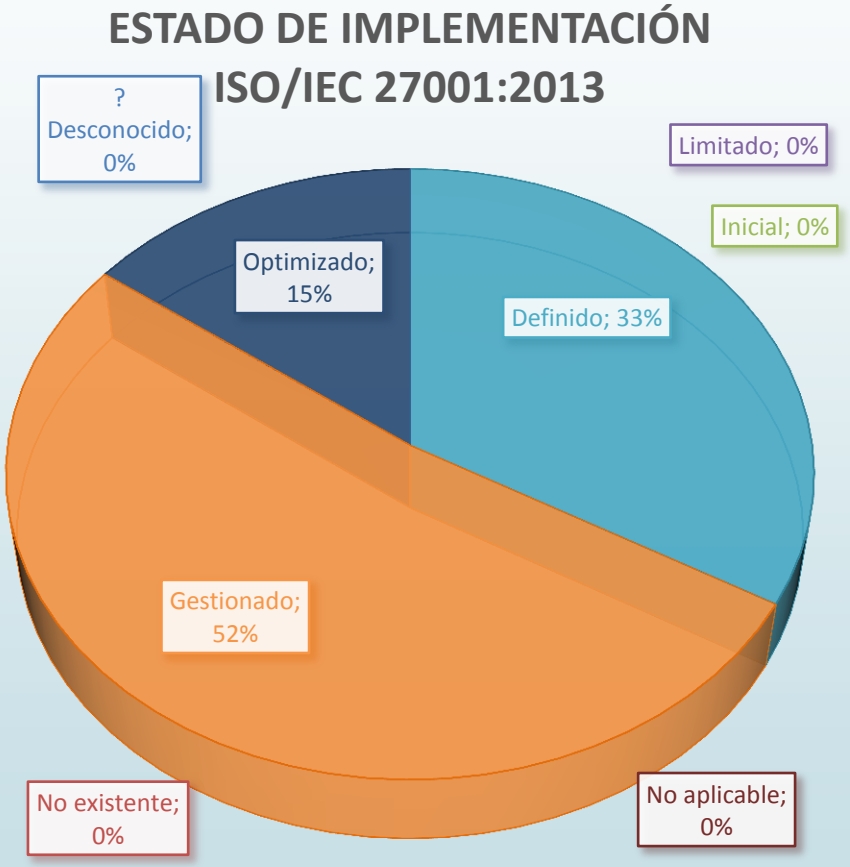
Una oportunidad de mejora, permitirá elevar a gestionado el control de concienciación

5. Auditoría de cumplimiento
5.5 Análisis

Estado de Madurez	Cantidad
No existente	2
Inicial	9
Limitado	8
Definido	29
Gestionado	62
Optimizado	4



5. Auditoría de cumplimiento
5.5 Análisis

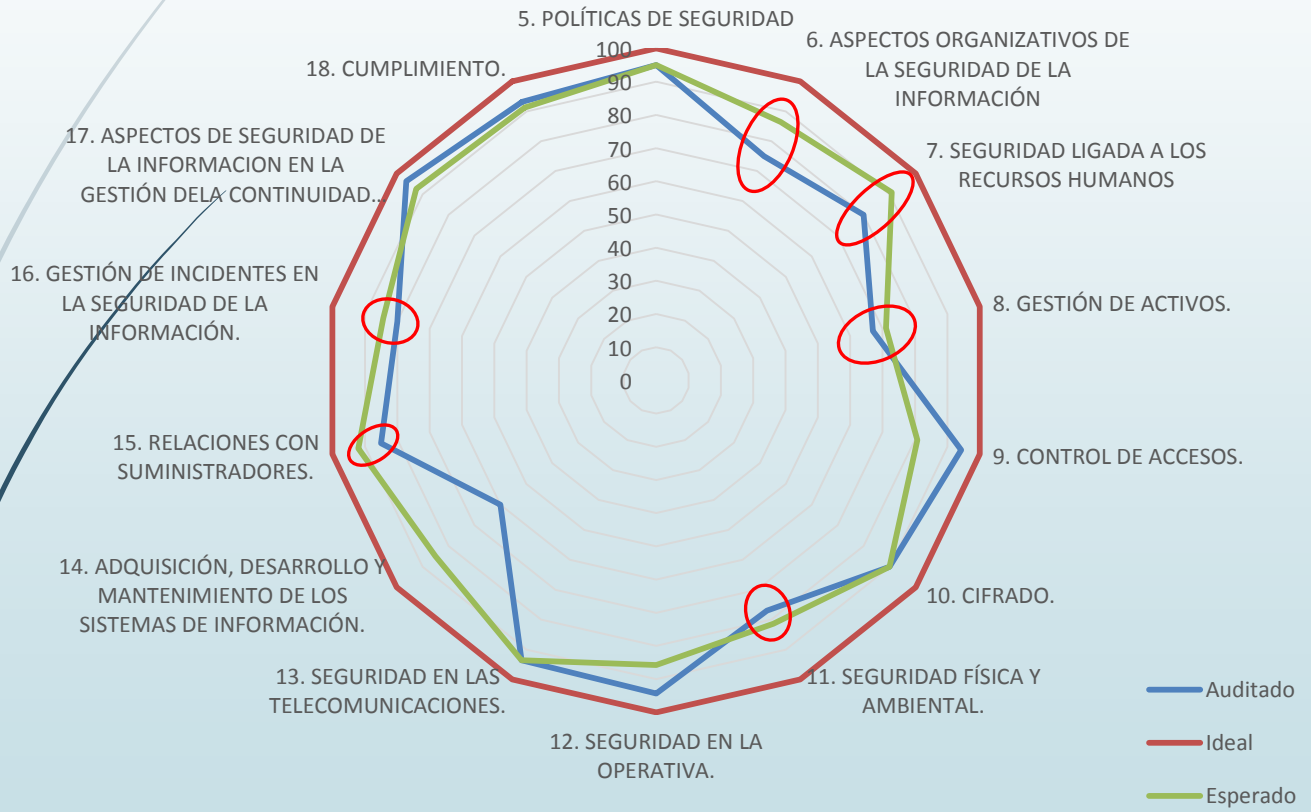


5. Auditoría de cumplimiento
5.5 Análisis

5. Auditoría de cumplimiento
5.5 Análisis

El Dominio de Desarrollo tienen un estado de madurez inferior al esperado

5. Auditoría de cumplimiento
5.5 Análisis

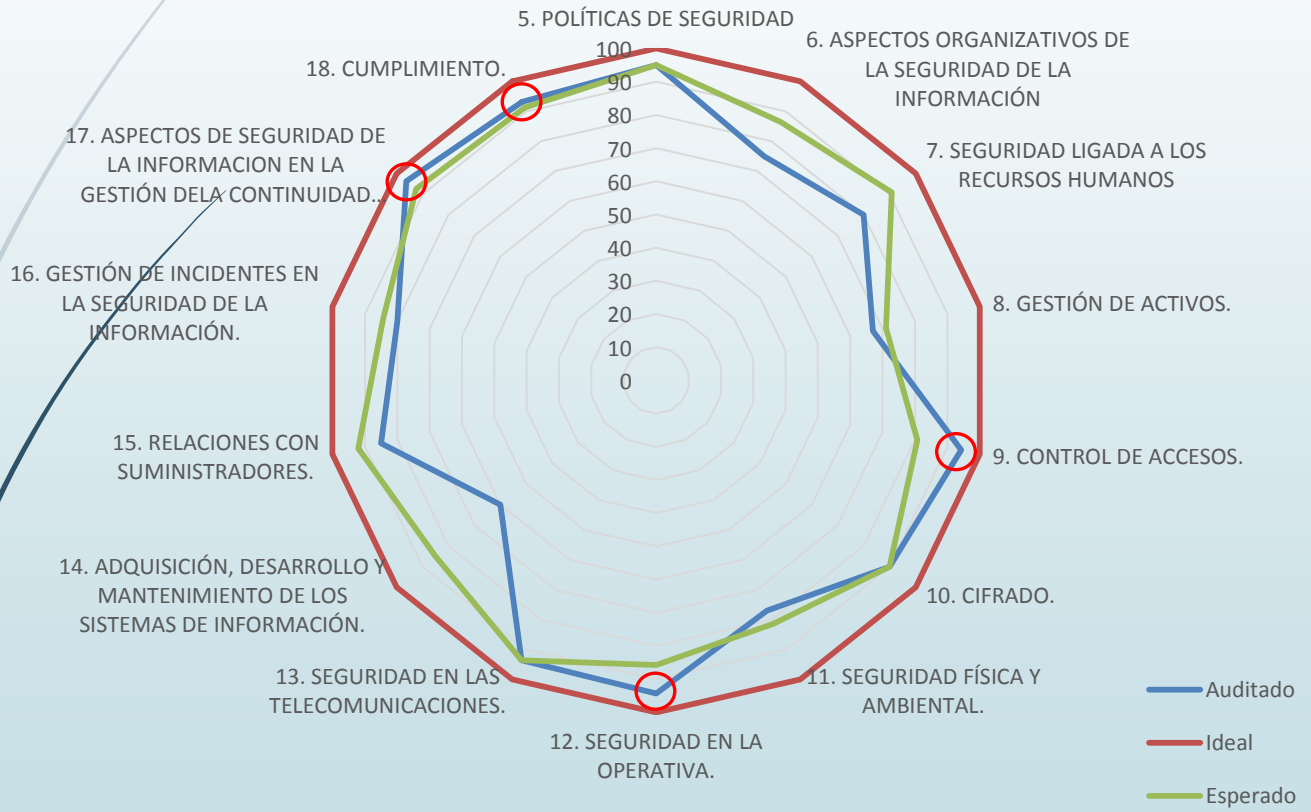


En 6 Dominios el estado de madurez está muy cercano al esperado

5. Auditoría de cumplimiento
5.5 Análisis

En 3 Dominios el estado de madurez es igual al esperado

5. Auditoría de cumplimiento
5.5 Análisis



En 4 Dominios el estado de madurez es mejor al esperado

5. Auditoría de cumplimiento
5.6 Informe - Conclusiones

- La principal amenaza para la UPS es la divulgación de información.
- Falta controles sobre los dispositivos y equipos que los usuarios pueden llevar libremente fuera de las instalaciones de la UPS, sin importar que contengan activos de información.

5. Auditoría de cumplimiento
5.6 Informe - Conclusiones

- El Desarrollo de Software es sensible para la UPS en ella se gestionan y crean todos los sistemas de información, el software que se produce no cumple con pruebas de seguridad, los programadores utilizan datos reales para las pruebas.
- Las no conformidades menores, requieren soluciones bastante específicas y de ejecución en corto plazo, ninguna de ellas requiere personal especializado o capacitación para solventarlas
- Con la auditoría se cumple el ciclo PDCA

5. Auditoría de cumplimiento
5.6 Informe - Recomendaciones

- Establecer lo más pronto posible controles que apoyen la Política de Uso de Dispositivos para movilidad
- Crear un plan de acción para el área de Desarrollo de Software
- Generar la base de datos para pruebas de manera inmediata entre el Área de Desarrollo y el Responsable de Seguridad de la Información
- Solventar las no conformidades que no requieren personal especializado