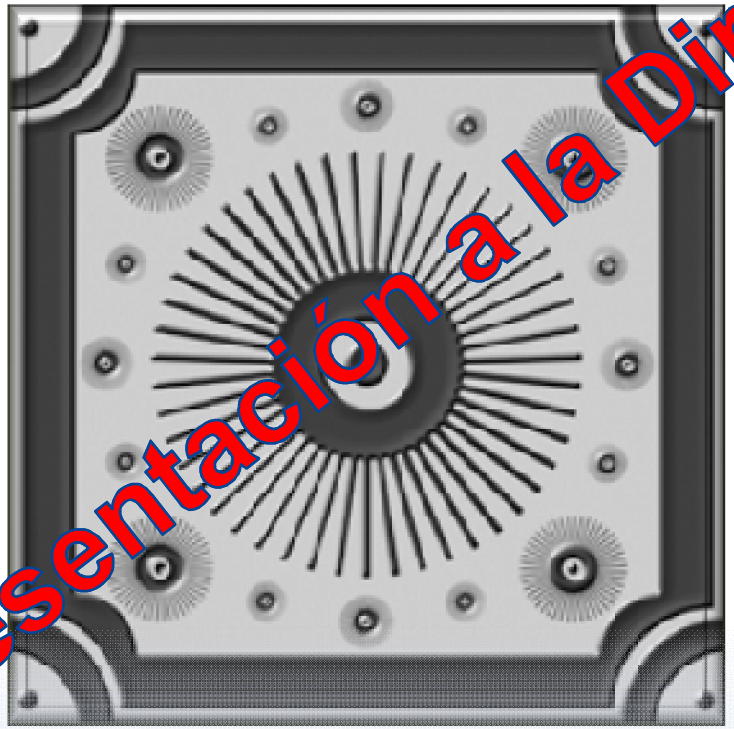
Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Elaboración Plan de Implementación de la ISO 27001-SOC



Presentación a la Dirección

(*)-Caja fuerte de pared con muchas ruedas de bloqueo para mayor seguridad (licencia Creative Commons-opendirtart)

ÍNDICE

Objetivo del Proyecto
Metodología
Descripción del Proyecto
Contextualización de la Organización
Análisis y diagnóstico de la Situación actual
Establecer un SGSI de base en la organización
Análisis de Riesgos de los Activos de la Organización
Evaluación del nivel de madurez de la Seguridad de la Información
Elaboración de Proyectos de mejora
Valoración de la mejora de la SI

Objetivo del Proyecto

El desarrollo del presente TFM tiene como objetivo la realización de un proyecto que lleve a cabo la realización de un **Plan Director de Seguridad de la Información** (PDSI) tomando como referencia un modelo de empresa real.

Para ello nos vamos a centrar en cuatro aspectos fundamentales

- El Conocimiento de las estrategias y objetivos de la Organización.
- El Conocimiento de la situación actual de la organización Seguridad de la Información.
- La Elaboración de las propuestas de los Proyectos a acometer y su planificación-
- La evaluación del estado actual de la Seguridad estableciendo el nivel de madurez de cumplimiento de la Seguridad por parte de la organización.

Metodología

Se ha establecido como base metodológica para poder abordar el PDS tomando como referencia los siguientes elementos:

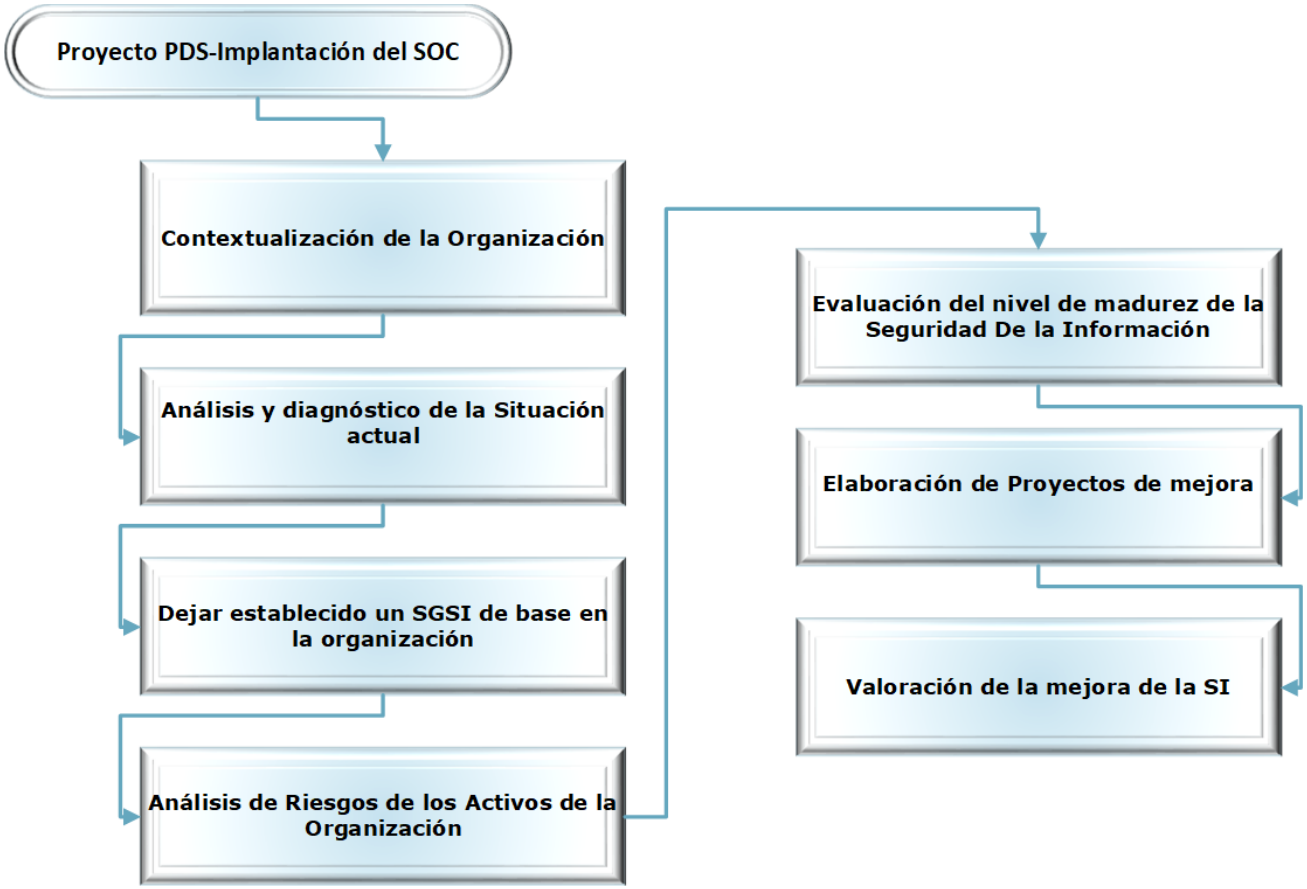
La UNE-ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información-Requisitos (UNE-ISO/IEC 27001-Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información (SGSI)-Requisitos)

La UNE-ISO/IEC 27002-Código de prácticas para os controles de Seguridad de la información (UNE-ISO/IEC 27002-Tecnología de la información-Técnicas de seguridad– Código de prácticas para los controles de seguridad de la información).

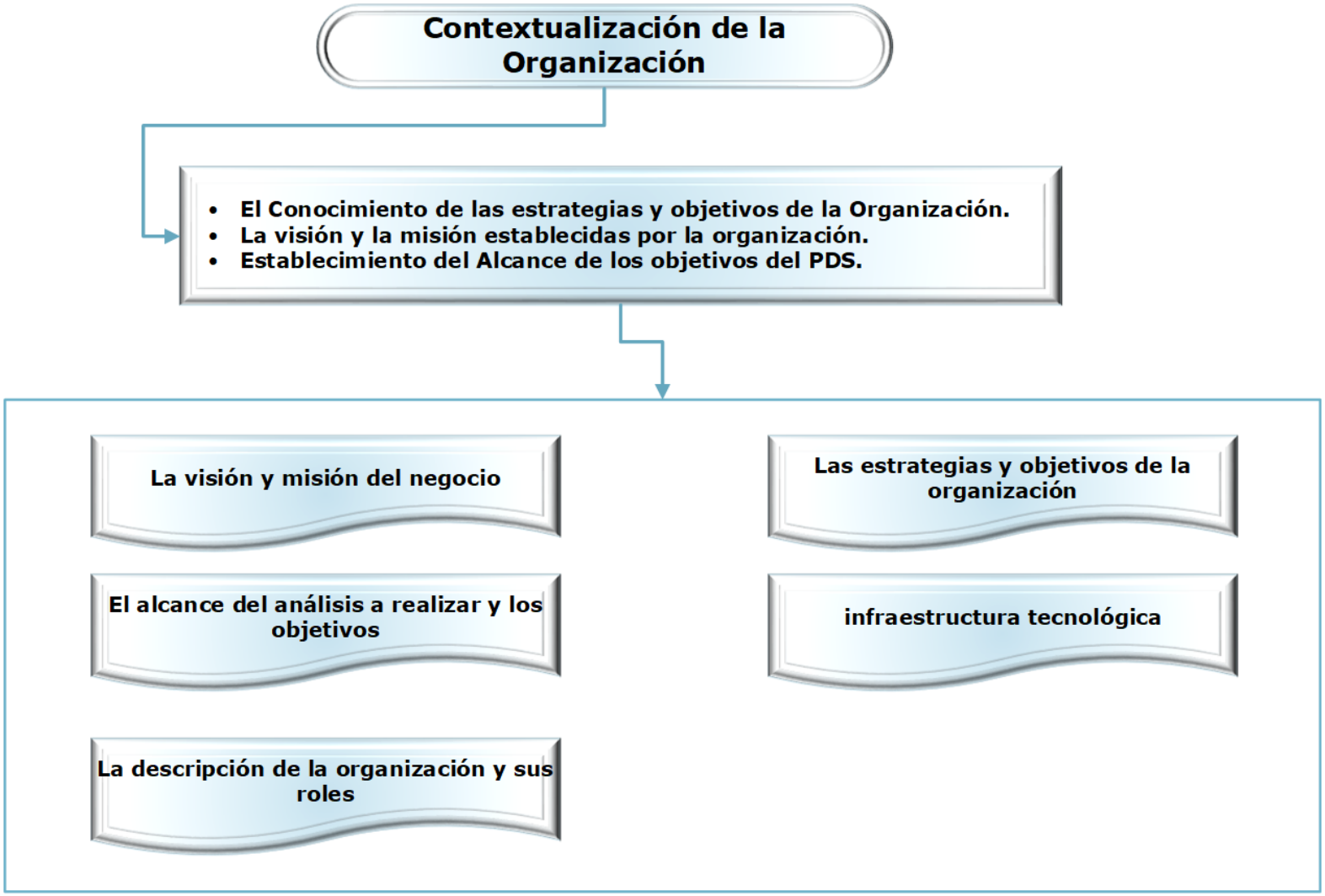
Modelo de Evaluación Nivel de Madurez-CMM		
CMM	Significado	Descripción
L0	Inexistente	• Carencia completa de cualquier proceso reconocible. • No se ha reconocido siquiera que existe un problema a resolver.
L1	Inicial / Ad-hoc	• Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. • Los procedimientos son inexistentes o localizados en áreas concretas.
L2	Reproducible, pero intuitivo	• Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. • Se normalizan las buenas prácticas en base a la experiencia y al método. • No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. • Se depende del grado de conocimiento de cada individuo.
L3	Proceso definido	• La organización entera participa en el proceso. • Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4	Gestionable y medible	• Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. • Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
L5	Optimizado	• Los procesos están bajo constante mejora. • En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Descripción del Proyecto

El proyecto que se ha abordado se estructura en las siguientes fases:

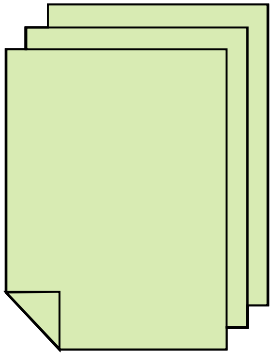


Contextualización de la organización



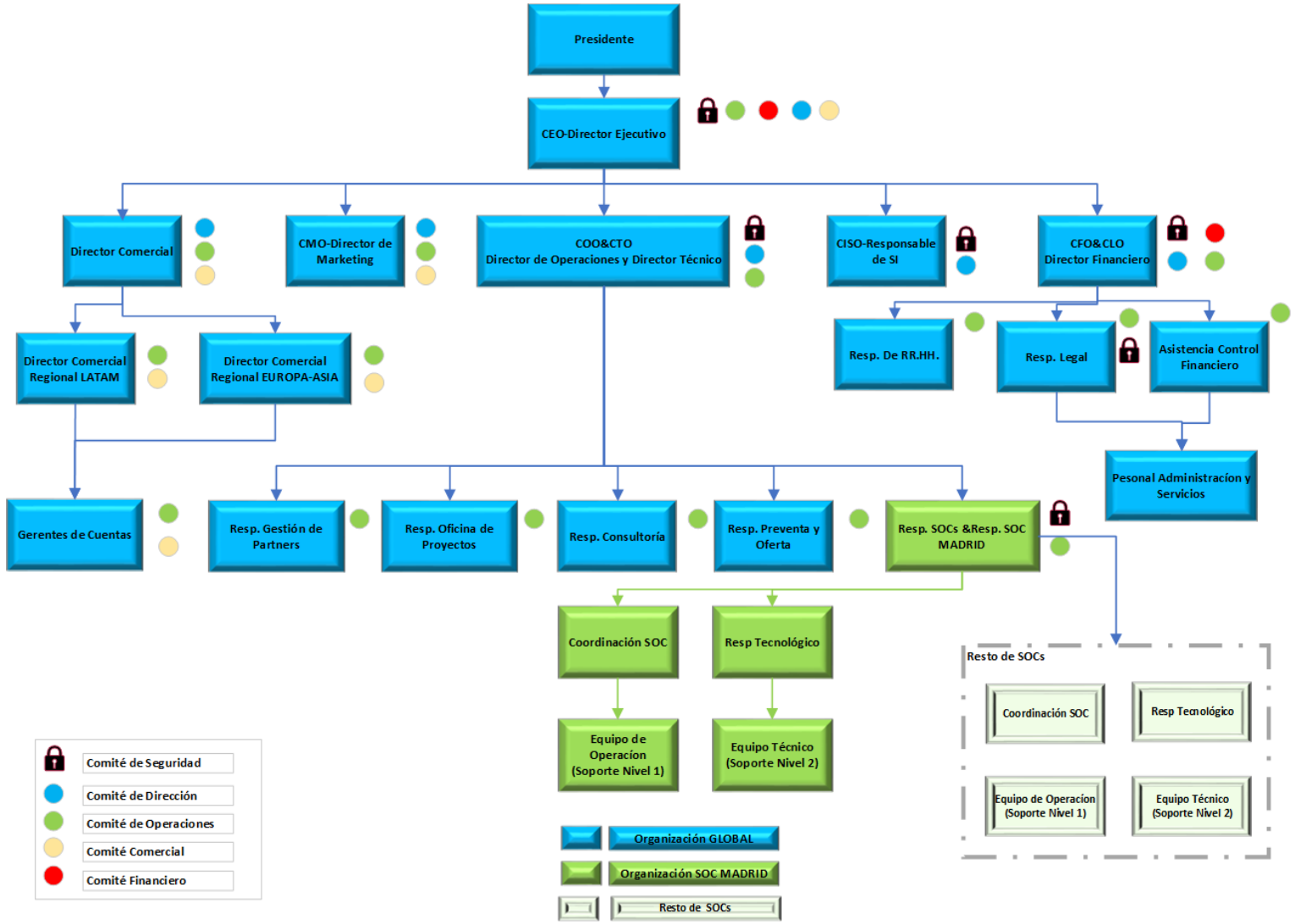
Contextualización de la organización-Estrategia y servicios prestados

Estrategias de la Organización	
Crecimiento	Dentro de las áreas geográficas en las que ya estamos presentes: • Para los clientes en los que ya estamos presentes aumentando nuestro volumen de actividad y de Servicios prestados. • Incorporar nuevos Clientes en base a la calidad de nuestros servicios y el reconocimiento de marca y actividad en las áreas regionales en las que prestamos Servicios.
Política de Partner	• Seguir fomentando y potenciando las alianzas actuales con proveedores de Productos y Servicios de Ciberseguridad. • Mantener nuestro nivel de independencia respecto de productos y soluciones de Ciberseguridad (adaptándonos a las mejoras tecnologías existentes en cada caso y a las necesidades concretas de nuestros clientes.
Evolución infr. IT hacia la Nube	• Evolución de la infraestructura IT de nuestros SOC hacia la Nube que nos va a permitir la estandarización de recursos y servicios, la gestión del rendimiento y la capacidad.
Estandarización SOC	• Estandarización y homogeneización en el Delivery de nuestros servicios de SOC.



Catálogo de Servicios Prestados	
Servicios de Consultoría	Integrada por los Servicios de asesoramiento, cumplimiento y evaluación de la Seguridad usando métodos y herramientas estándares del mercado
Servicios de Protección de infraestructuras	Dedicados a la protección de Centros de Procesos de datos, redes y dispositivos de clientes. Se protege tanto la información (datos, sistemas, aplicaciones) como las infraestructuras de comunicaciones.
Servicios de Seguridad Cloud	Dirigidos a desplegar la infraestructura desplegada por el cliente en el Cloud. Se proporcionan servicios soportados en clouds globales, que reducen los costes y los tiempos de acceso al mercado.

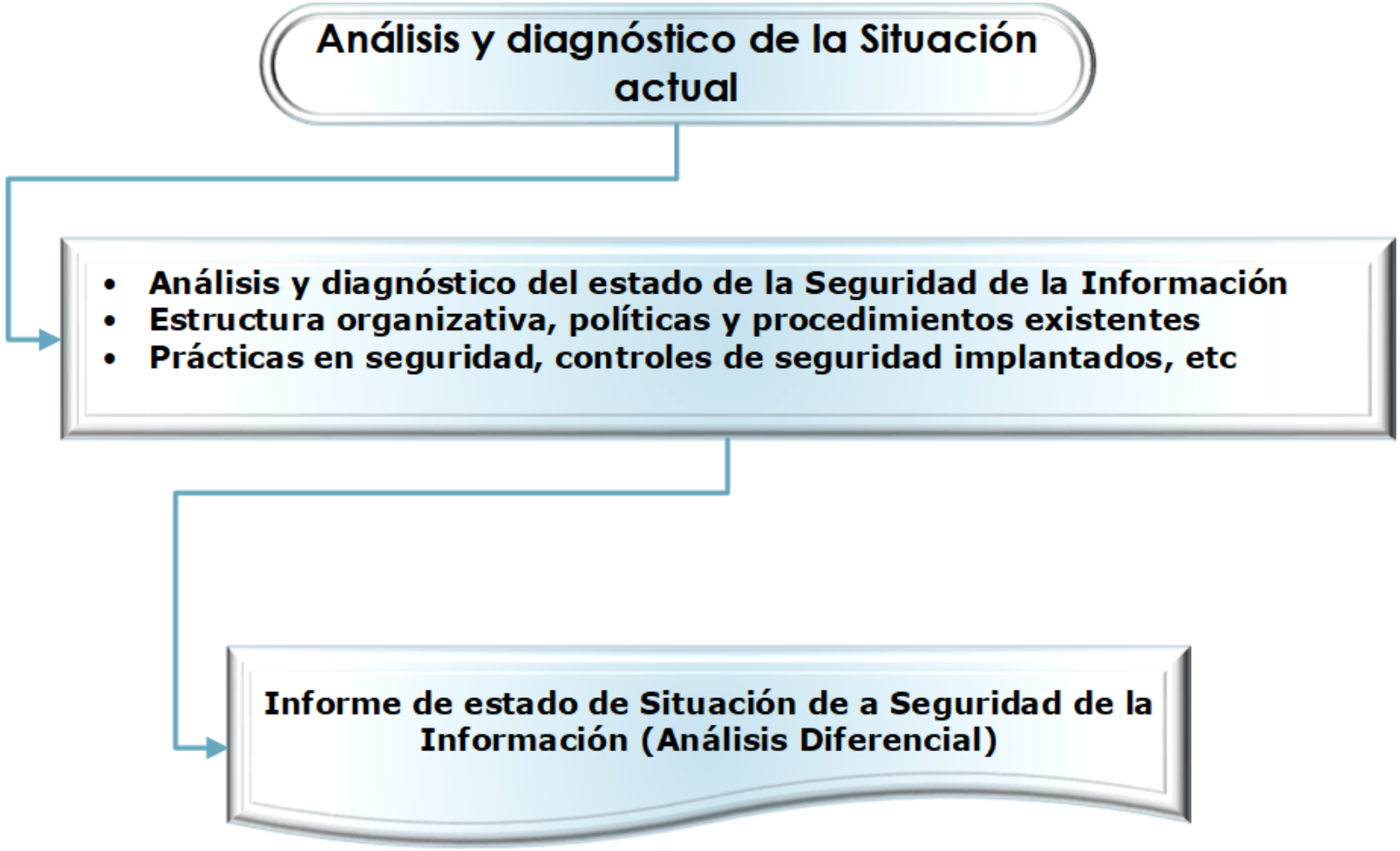
Contextualización de la organización-Organización



Contextualización de la organización-Objetivos Organización

OBJETIVOS PLAN DIRECTOR DE SEGURIDAD										
Objetivos Organización		Objetivo Compañía Ofrecer servicios de alta seguridad y calidad, con un gran rendimiento y servicio adaptado a las necesidades de cada uno de nuestros clientes.				Estrategias de la Organización				Objetivo PDSI (S/N)
#	Descripción	Servicios de Alta Seguridad	Servicios de Alta Calidad	Gran rendimiento	Servicios adaptados a clientes	Crecimiento	Política de Partners	Evolución infraest. IT Nube	Estandarización de los SOC	
OBJ_ORG_1	Control de los requisitos de Seguridad de los Proveedores (partners)	X	X		X		X			S
OBJ_ORG_2	**Construir una Arquitectura de Referencia para la infraestructura IT de los SOC en la nube**	X	X	X	X	X		X	X	S
OBJ_ORG_3	Evaluación de nivel de Seguridad de los SOC existentes (piloto de base de valoración SOC-MAD)	X	X		X	X			X	S
OBJ_ORG_4	**Establecimiento de SGSI para los SOC, estandarización de los Procesos de Gestión de la Seguridad**	X	X	X		X		X	X	S
OBJ_ORG_5	Establecimiento de SGSI para los SOC, estandarización de los Procesos de Delivery	X	X	X	X	X			X	S
OBJ_ORG_6	**Dotar a los SOC de Certificaciones de Seguridad y Certificaciones Técnicas**	X	X			X	X		X	S
OBJ_ORG_7	Formación técnica especializada y extendida de manera uniforme a todos los SOCs	X	X		X	X	X		X	S
OBJ_ORG_8	**Estandarización de los procesos de Operación IT de las infraestructuras de los SOCs**	X	X	X		X			X	S

Análisis y diagnóstico de la Situación actual



Análisis y diagnóstico de la Situación actual-Informe Análisis Diferencial 1/2

Resumen Resultados Análisis Diferencial -Existencia SGSI	
• La organización tiene un **conocimiento claro acerca del contexto** (actividades, negocio, mercado, regulación etc.) en el que se encuentra ubicada su actividad y tiene identificados los elementos propios y los terceros con los que se relaciona en la realización de sus actividades (**Partes interesadas**). • No obstante, la organización **no tiene desarrollado procedimientos** de recopilación, análisis y evaluación sistemática de estos elementos para poder gestionarlo desde la perspectiva de la SI (relaciones, contexto, riesgos, evaluación, etc.).	
Requerimiento	**Situación/Comentarios**
Prácticas en Seguridad de la Información	Existe una clara concienciación y conocimiento de las buenas prácticas de seguridad, pero • No es un proceso que esté claramente, definido, articulado y sistematizado.
Auditoría Interna.	Existe una cultura ya instalada de control en la organización; pero su aplicación se reduce a aspectos meramente técnicos (Pentesting y Análisis de Vulnerabilidades de sus Sistemas de Información).
Organización de la Seguridad de la Información	La organización tiene establecido un organigrama, en dónde se detallan las **funciones y competencias**; pero no los tiene expresamente adaptados y desarrollados para realizar una gestión eficiente de la Seguridad de la información.
Mejora continua	No está implementada.
Gestión de Riesgos	No están establecidos unos mecanismos de Gestión de Riesgos.

Análisis y diagnóstico de la Situación actual-Informe Análisis Diferencial 2/2

Resumen Resultados Análisis Diferencial-Controles de Seguridad			
• La organización tiene ya implementados Controles de Seguridad en dónde el nivel de implantación es heterogéneo.			
Requerimiento	**Situación/Comentarios**	**Control**	**Situación/Comentarios**
Políticas, estándares e Instrucciones técnicas	Existen políticas desarrolladas y en uso para temas como: • Políticas de uso Dispositivos móviles, Metodologías y herramientas para la Gestión de proyectos, Políticas de teletrabajo, etc.	**Gestión de RR.HH.**	La Gestión de RR.HH. está correctamente definida y los procesos asociados (Selección, contratación y gestión de recursos, baja). • Es necesario realizar los ajustes para que puedan garantizar el control y seguimiento formación y concienciación en SI.
Gestión de la Activos	• No existen criterios adoptados para la tipificación, categorización, clasificación y gestión adecuada de los activos. • Lo registros de activos existentes son parciales y no hay procedimientos para su mantenimiento y actualización (Infraestructura IT).	**Control de Acceso**	• Están declaradas e implementados políticas de control de accesos las aplicaciones y a los componentes de la infraestructura IT. • Están implantados mecanismos de segregación de funciones. • Se usan Herramientas de gestión para el control de acceso. • En paralelo, no se están realizando revisiones periódicas del cumplimiento de las políticas establecidas.
Controles Criptográficos	• Se echa en falta un inventario, control y seguimiento de los mismos (reglas de uso, mantenimiento de recursos asociados - P.e. ciclo de vida de los certificados -).	**Seguridad Física**	• Se está aplicando de manera correcta el mecanismo de seguridad física por capas. • Existen procedimientos de control y cumplimiento del acceso físico.
Seguridad de las Operaciones	• Respecto a la Seguridad de las Operaciones hay que hacer notar que este grupo de controles ya está gestionado por la organización. • Requiere ciertas mejoras y ajustes, pero los procesos ya existen y son usados con normalidad.	**Seguridad de las Comunicaciones**	• Se cumple estrictamente con los controles de seguridad en cuanto a arquitecturas, topologías y segmentación de redes. • Quedan pendientes por desarrollar y ajustar los acuerdos de intercambios de la información y su uso.
Adquisición Desarrollo y Mantenimiento de Sistemas	• No están establecidos y documentados los mecanismos de captación, evaluación y aprobación de los activos adquiridos por la organización que afectan SI.	**Política de Desarrollo Seguro**	• No hay establecida una Política de Desarrollo Seguro, sin ser la actividad principal objeto del SOC); sí que existe la necesidad de la existencia y uso de la misma.
Gestión de Proveedores	• En la Relación con los Proveedores no hay controles establecidos, dentro de la organización, para la gestión de la seguridad de los proveedores.	**Gestión de Incidentes**	• La gestión de incidencias está ya implantada y en uso; faltaría realizar las adaptaciones necesarias para recoger los incidentes de seguridad de manera clara, y poder realizar la gestión de los mismos reajustando los procedimientos, herramientas y flujos ya existentes.
Continuidad del Negocio	• No ha habido una evaluación previa de los Procesos gestionados y Servicios prestados para tener conciencia del grado de criticidad de los mismos (Análisis de Impacto de Negocio-BIAs).	**Cumplimiento**	• No existe una gestión procedimentada y ordenada de los aspectos de cumplimiento en la organización, con especial énfasis a los que afectan a SI.

Establecimiento de un SGSI

Análisis de Riesgos-Informes de Riesgo (Potencial y Actual)

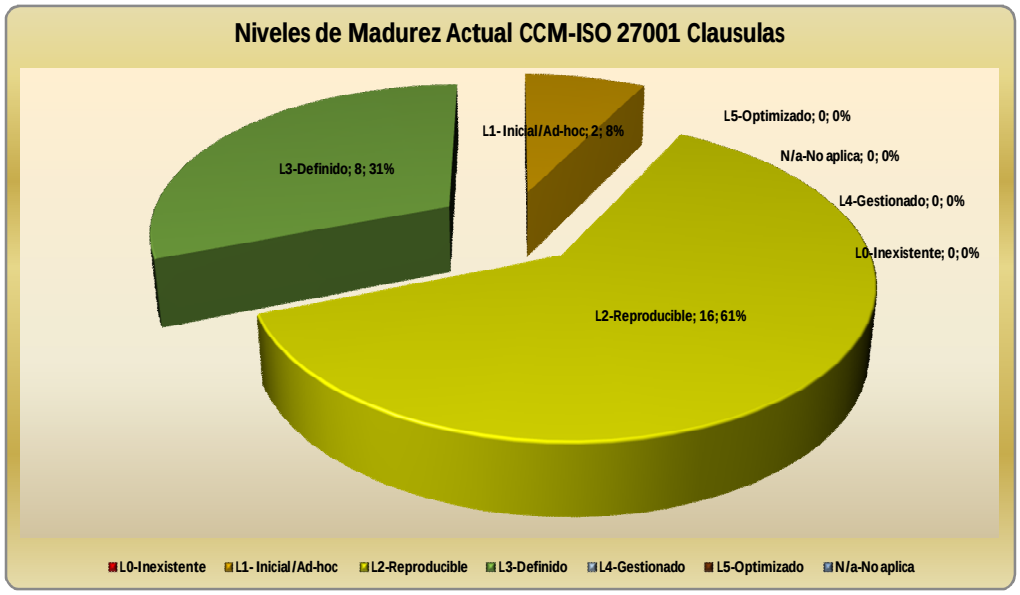
VALORACIÓN ACTIVOS-AMENAZAS	RIESGO POTENCIAL (Valor)			Riesgo Actual (Valor)		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[B] Activos esenciales						
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	6,3	0	0	4,3	0,0	0,0
[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES						
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	5,6	0,9	0,2	3,9	0,6	0,1
[B_D_SG_DES_TEC] Información Técnica de los Proyectos	4,9	2,1	0,7	3,4	1,5	0,5
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	4,9	2,1	0,7	3,4	1,5	0,5
[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS						
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	6,3	2,1	0,7	4,3	1,5	0,5
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	4,5	0,9	0,3	3,1	0,6	0,2
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	4,5	2,1	0,7	3,1	1,5	0,5
[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS						
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	6,3					
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	2,7					
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	2,7					
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	6,3					
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	2,7					
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	4,05					
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	5,4	2,1	0,7	3,8	1,5	0,5
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	5,4	1,5	0,6	3,7	1,1	0,4
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	1,35	2,1	0,7	0,9	1,5	0,5
[SRV] Servicios						
[SRVI] Servicios Internos						
[SRVI_IT] SERVICIOS GESTIONADOS IT						
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	2,7	0,0	0,0	2,0	0,0	0,0
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	6,3	0,0	0,0	4,7	0,0	0,0
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	4,5	0,0	0,0	3,4	0,0	0,0

NIVEL	RIESGO	CONDICIÓN	TRATAMIENTO	PROPIETARIO	REVISIÓN
>7-10	EXTREMO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>3,0-7	SIGNIFICATIVO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>2-3,0	APRECIABLE	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	TRIMESTRAL
>1-2	BAJO	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	ANUAL
0-1	DESPRECIABLE	ACEPTABLE	NO	PROPIETARIO DEL RIESGO	ANUAL

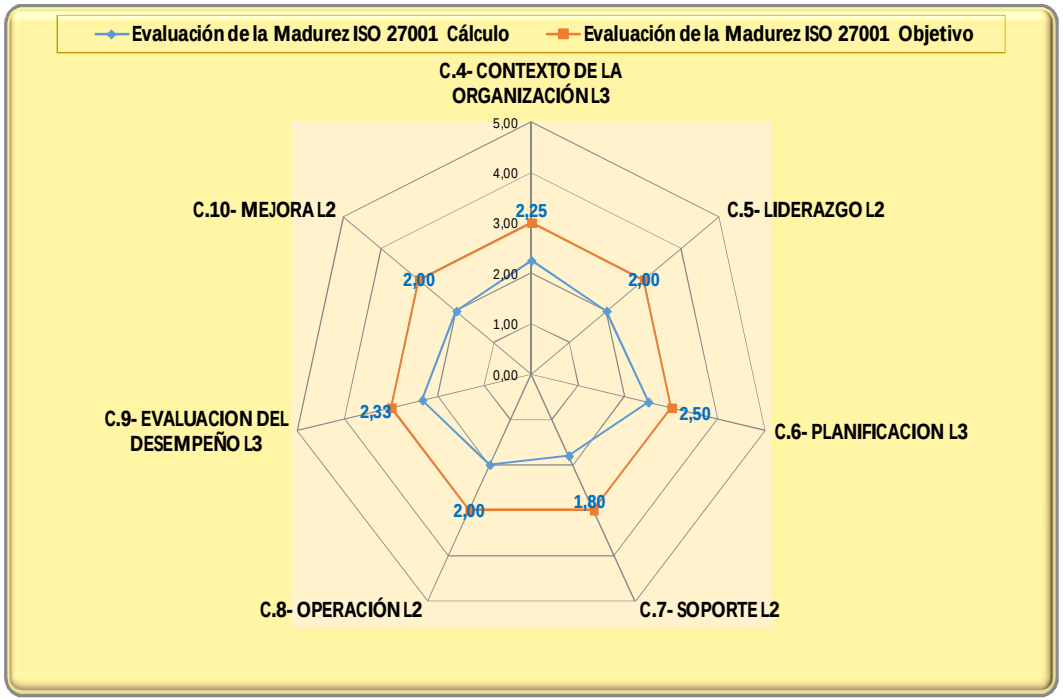
Evaluación del nivel de madurez en SI

Evaluación del nivel de madurez en SI- ISO 27001 (SGSI)

Madurez ISO 27001 en % sobre modelo CMM

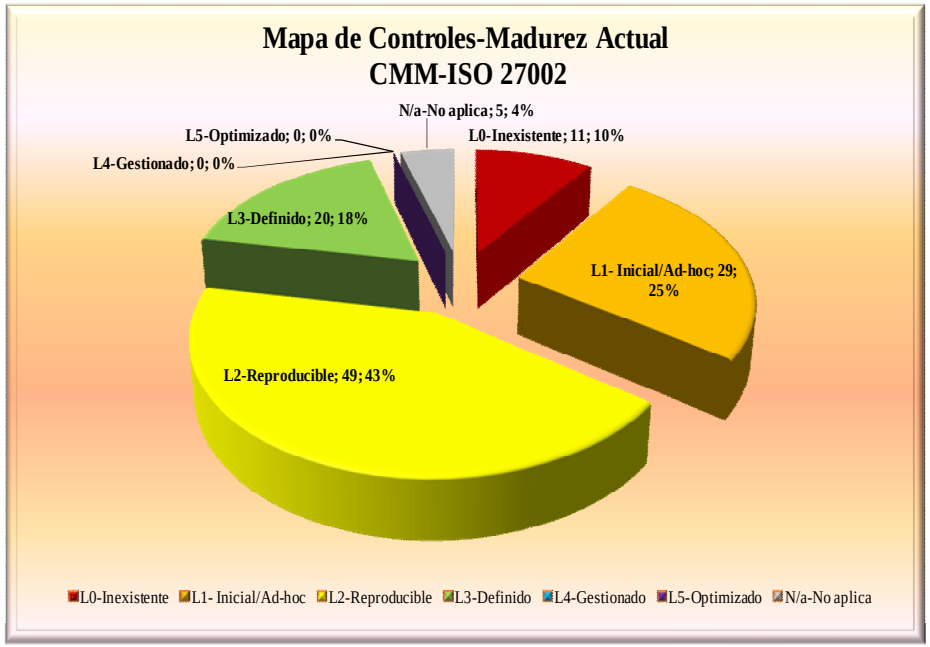


Radar situación ISO 27001- inicial/objetivo

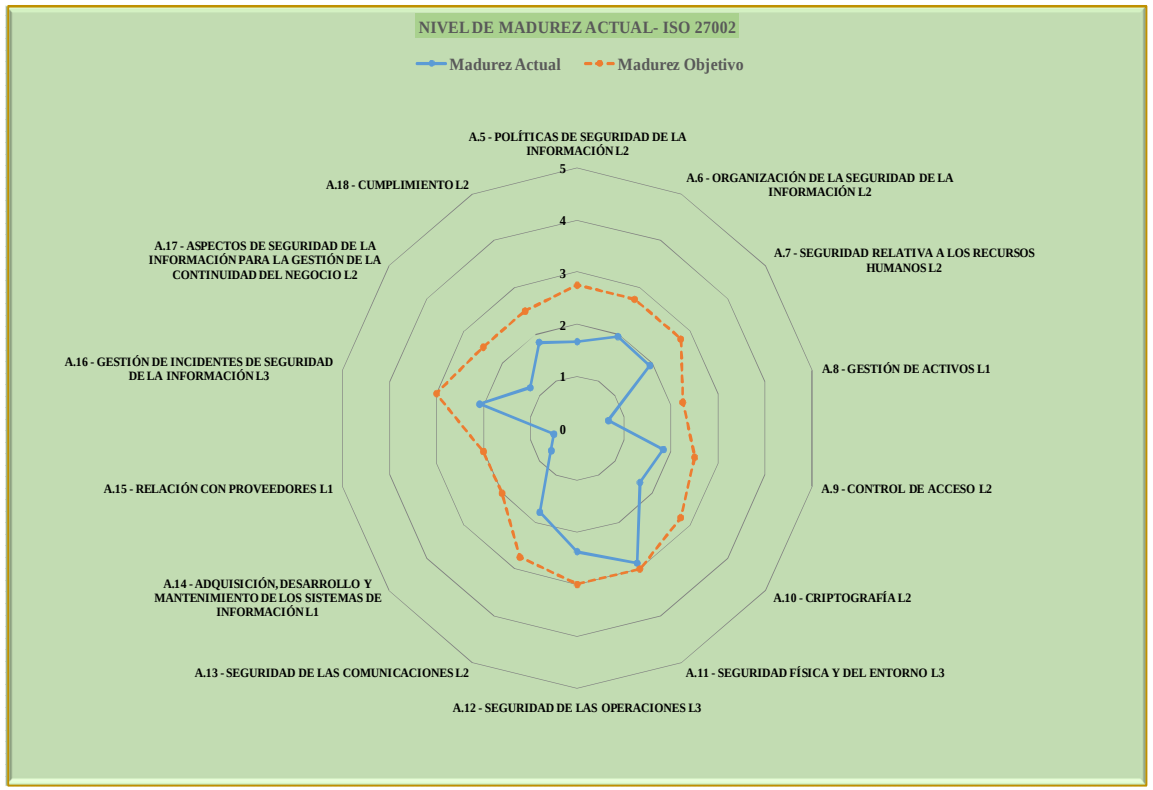


Evaluación del nivel de madurez en SI- ISO 27002 (Controles de Seguridad)

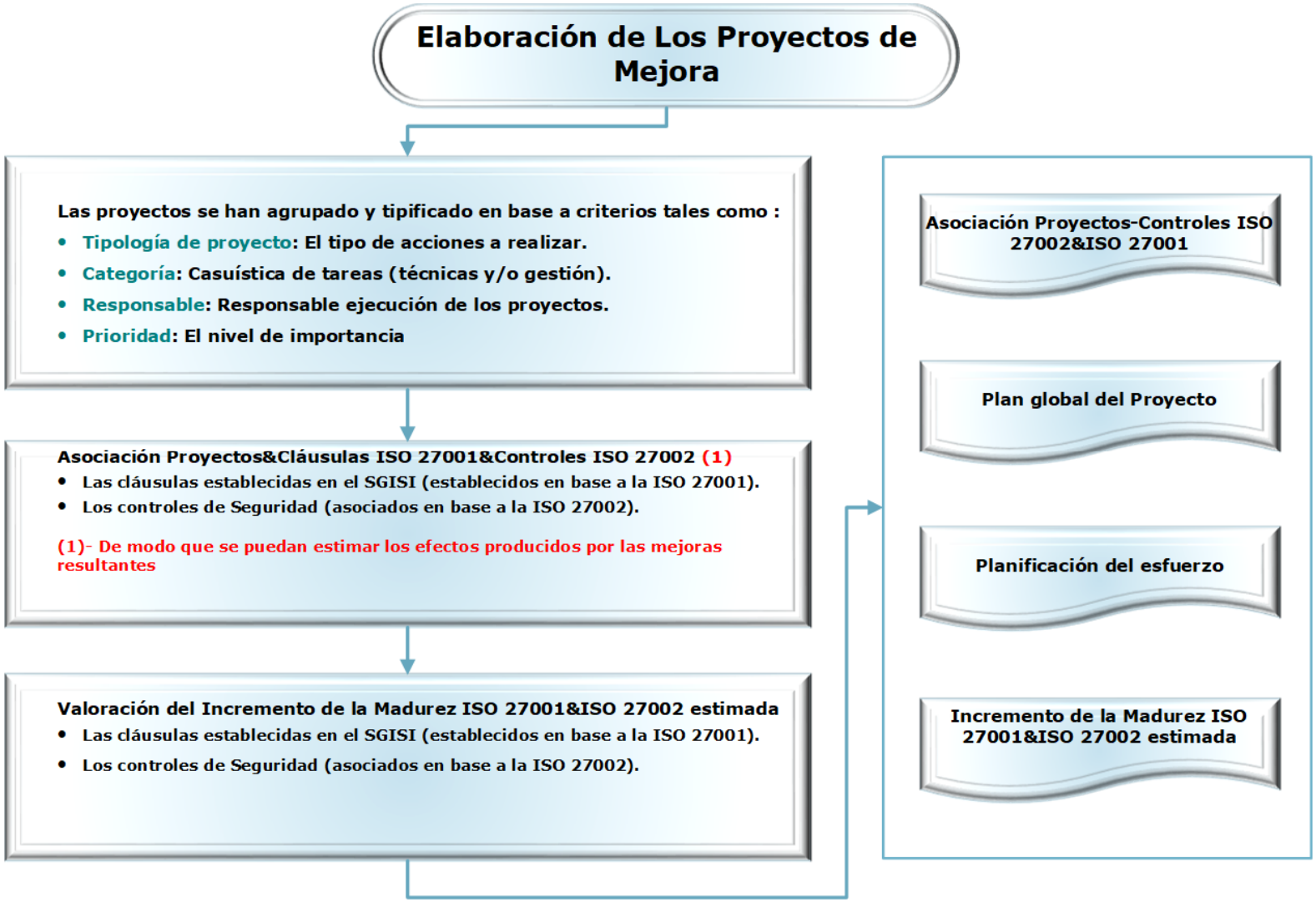
Madurez ISO 27002 en % sobre modelo CMM



Radar situación ISO 27002- inicial/objetivo



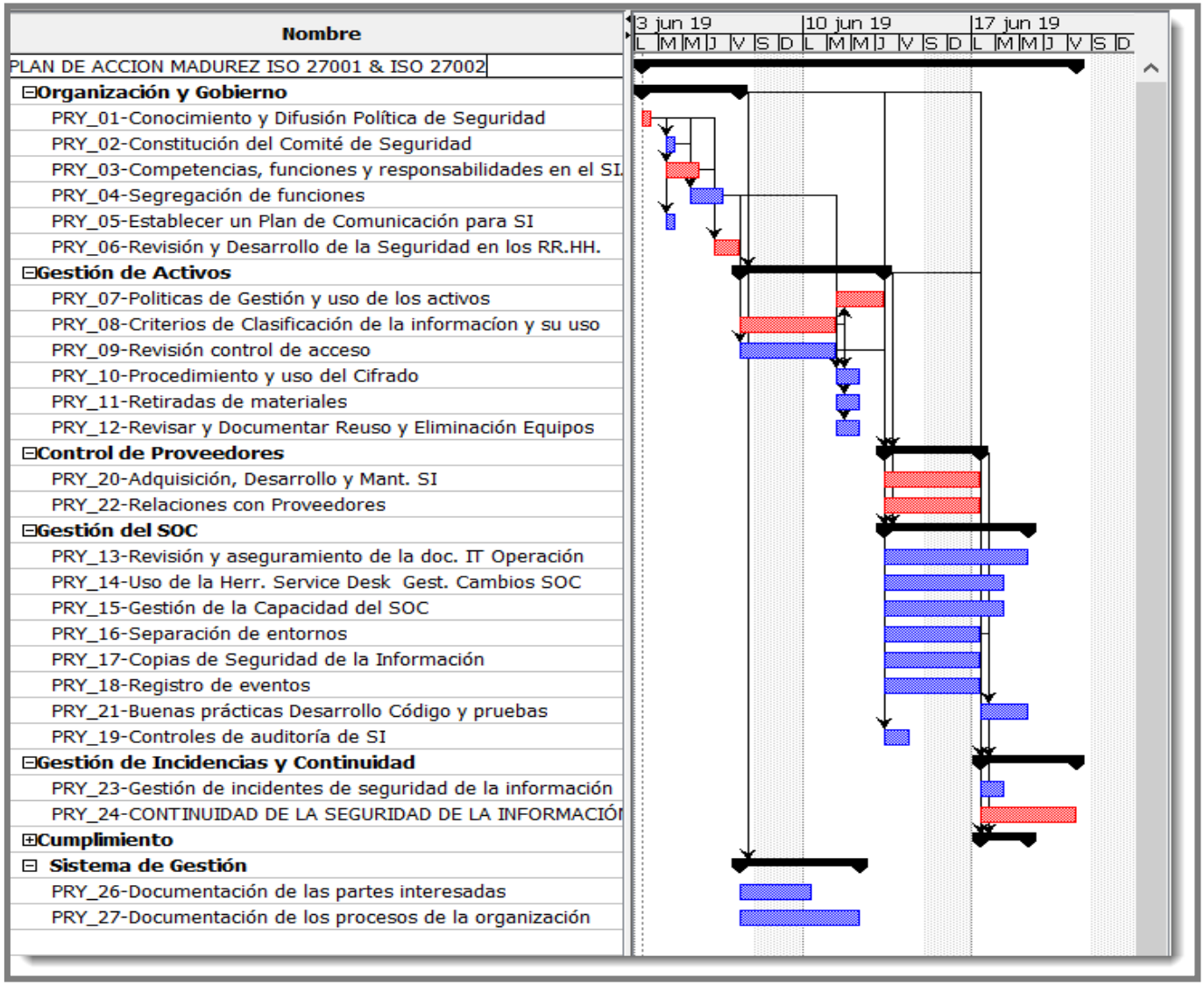
Elaboración de los Proyectos de Mejora



Elaboración de los Proyectos de Mejora-Cartera de Proyectos

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	Tipo de Proyecto	Categoría	Nombre	Proyecto	Tipo de Proyecto	Categoría	Nombre
PRY_01	Implementación y Desarrollo	Gestión	Conocimiento y Difusión de la Política de Seguridad de la Organización	PRY_14	Identificación evidencias	Gestión	Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia
PRY_02	Implementación y Desarrollo	Gestión	Constitución y Puesta en funcionamiento del Comité de Seguridad	PRY_15	Identificación y Registro	Gestión	Gestión de la Capacidad del SOC
PRY_03	Desarrollo	Gestión	Definir en detalle las competencia, funciones y responsabilidades de todos los actores que intervienen en SI.	PRY_16	Implementación y Desarrollo	Gestión	Separación de entornos
PRY_04	Identificación y Registro	Gestión	Segregación de funciones	PRY_17	Identificación y Registro	Gestión	Copias de Seguridad de la Información
PRY_05	Implementación y Desarrollo	Gestión	Establecer un Plan de Comunicación para SI	PRY_18	Definir y Desarrollar	Gestión	Registro de eventos
PRY_06	Definir y Desarrollar	Gestión	Revisión y Desarrollo de la Seguridad en los RR.HH.	PRY_19	Identificar evidencias	Gestión	Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas
PRY_07	Implementación y Desarrollo	Gestión y Tecnología (Mixto)	Políticas de Gestión y uso de los activos	PRY_20	Implementación y Desarrollo	Gestión	Adquisición, desarrollo y mantenimiento de los sistemas de información
PRY_08	Implementación y Desarrollo	Gestión	Establecer los criterios de Clasificación de la información y su uso	PRY_21	Implementación y Desarrollo	Gestión y Tecnología	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas
PRY_09	Identificación evidencias existentes	Gestión	Revisión de los mecanismos de control de acceso ya existentes	PRY_22	Implementación y Desarrollo	Gestión	Relaciones con Proveedores
PRY_10	Definir y Registrar	Gestión y Tecnología (Mixto)	Establecer procedimiento de mecanismos y uso del Cifrado en la Organización	PRY_23	Identificación y Registro	Gestión y Tecnología (Mixto)	Gestión de incidentes de seguridad de la información
PRY_11	Definir y Desarrollar	Gestión	Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)	PRY_24	Implementación y Desarrollo	Gestión	Continuidad de la Seguridad de la Información
PRY_12	Implementación y Desarrollo	Gestión	Revisar y Documentar las prácticas en Reutilizacion y Eliminación Segura de Equipos	PRY_25	Identificación y Registro	Gestión	Conformidad con los requisitos legales
PRY_13	Identificación y Registro	Gestión	Revisión y aseguramiento de la documentación Técnica del área de Operación	PRY_26	Implementación y Desarrollo	Gestión	Documentación de las partes Interesadas
PRY_27	Implementación y Desarrollo	Gestión	Documentación de los procesos de la organización				

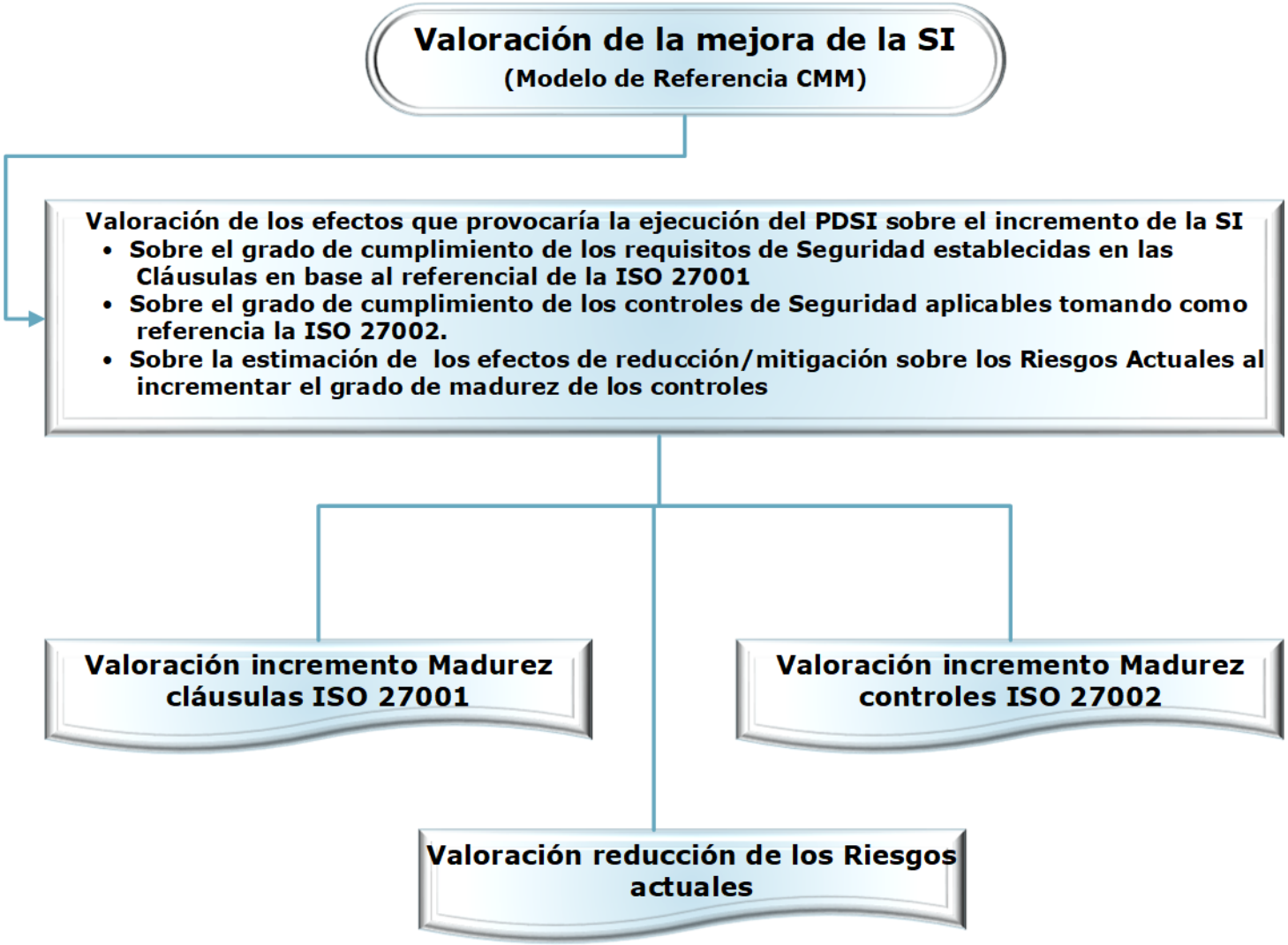
Elaboración de los Proyectos de Mejora-Planificación Global



Elaboración de los Proyectos de Mejora-Valoración esfuerzo

Planificación de Esfuerzo en Proyectos							
Proyecto	Nombre	Tiempo estimado (jornadas)	Recursos&Participación	Proyecto	Nombre	Tiempo estimado (jornadas)	Recursos&Participacíon
PRY_01	Conocimiento y Difusión de la Política de Seguridad de la Organización	2	CEO- 50%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25%	PRY_13	Revisión y aseguramiento de la documentación Técnica del área de Operación	8	DIR. OPERACIONES/DIR. IT-50%, CISO-30%, RESP. SOC-100%
PRY_02	Constitución y Puesta en funcionamiento del Comité de Seguridad	2	CEO- 10%,DIR. RR.HH. (CFO/CIO) 100%, CISO-100%	PRY_14	Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia infraestructura del SOC	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_03	Definir en detalle las competencia, funciones y responsabilidades de todos los actores que intervienen en SI.	5	DIR. RR.HH. (CFO/CIO) 100%,RESP. LEGAL-15%, DIR. OPERACIONES-50%,	PRY_15	Gestión de la Capacidad del SOC	8	DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10%,
PRY_03	Segregación de funciones	6	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15%, DIR. OPERACIONES-50%,	PRY_16	Separación de entornos	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_05	Establecer un Plan de Comunicación para SI	2	CEO-50%, DIR. MARKETING-100%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50%, DIR. OPERACIONES-50%	PRY_17	Copias de Seguridad de la Información	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_06	Revisión y Desarrollo de la Seguridad en los RR.HH.	4	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25%, DIR. OPERACIONES-25%, CISO-100%	PRY_18	Registro de eventos	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_06	Revisión y Desarrollo de la Seguridad en los RR.HH.	4	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25%	PRY_19	Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas encontradas)	3	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_07	Políticas de Gestión y uso de los activos	7	CEO-10%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-10%	PRY_20	Adquisición, desarrollo y mantenimiento de los sistemas de información	9	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50%,
PRY_08	Establecer los criterios de Clasificación de la información y su uso	7	CEO-10%, DIR. RR.HH. (CFO/CIO) 100%,RESP. LEGAL-10%, DIR. OPERACIONES/DIR. IT-	PRY_21	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	5	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_09	Revisión de los mecanismos de control de acceso ya existentes	3	CEO-10%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-10%	PRY_22	Relaciones con Proveedores	7	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50%, DIR. OPERACIONES/DIR.
PRY_10	Establecer procedimiento de mecanismos y uso del Cifrado en la Organización	3	DIR. OPERACIONES/DIR. IT-50%, CISO-100%, RESP. SOC-15%	PRY_23	Gestión de incidentes de seguridad de la información	4	DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10%, DIR. OPERACIONES/DIR.
PRY_11	Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)	3	DIR. RR.HH. (CFO/CIO) 25%, RESP. LEGAL-10%	PRY_24	Continuidad de la Seguridad de la Información	12	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15%
PRY_12	Revisar y Documentar las prácticas en Reutilización y Eliminación Segura de Equipos	10	DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10%	PRY_25	Conformidad con los requisitos legales	6	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-100%, CISO-50%
PRY_26	Documentación de las partes interesadas	5	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15%, RESP. SOC-100%	PRY_27	Documentación de los procesos de la organización	12	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15%

Valoración de la mejora de la SI



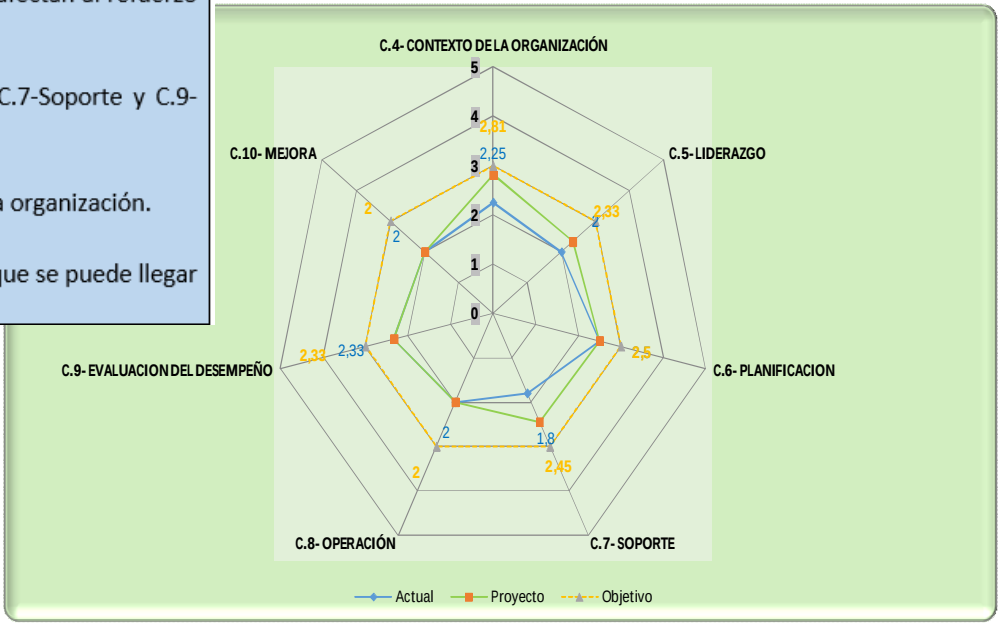
Valoración de la mejora de la SI

Resumen Estimación de la Mejora- SGSI (ISO 27001)

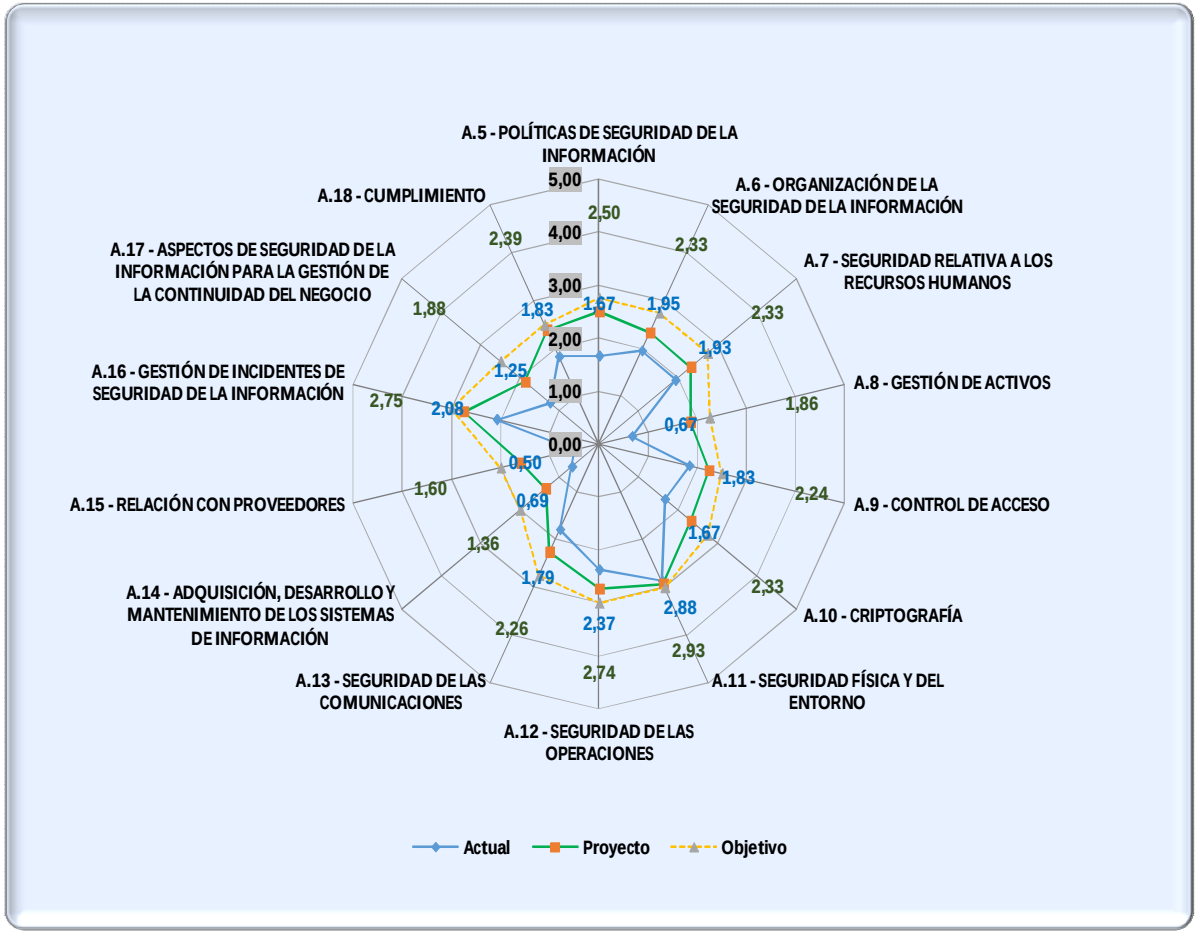
El estado **Actual** (representado en azul) es la consecuencia de la implantación del SGSI, en donde hemos establecido los componentes de base de un sistema de Gestión de la Seguridad de la Información en la organización.

El estado de Proyecto (representado en verde) es por acometer algunas acciones de mejora/refuerzo del SGSI:

- Establecer una visión de las Partes interesadas que afectan a la SI así como los mecanismos para su mantenimiento y control (4-Contexto de la Organización-C.4.2).
- Documentar los procesos y actividades que se realizan en la organización en SI.
- Refuerzo del conocimiento en base a los roles y responsabilidades de la organización (C.4.3), que afectan al refuerzo de la madurez en los requisitos del apartado 5-Liderazgo-C.5.3.
- Gestión de RR.HH. queda reforzado el cumplimiento de los requerimientos relacionados para C.7-Soporte y C.9-Evaluación del desempeño.
  - Planificación del proceso de concienciación y formación en SI dentro de la organización.
  - Valorar las necesidades en cuantos a competencias técnicas y funciones de los perfiles de la organización.
- El estado objetivo (representado en naranja) viene a representar el objetivo de madurez global al que se puede llegar en base al nivel de desarrollo, tiempo y experiencia en el SGSI del que parte la organización.



Valoración de la mejora de la SI



Dominios	Madurez Actual	Madurez Prevista
A.8 - GESTIÓN DE ACTIVOS	L1	L2
A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	L1	L2
A.15 - RELACIÓN CON PROVEEDORES	L1	L2
A.5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	L2	L3
A.6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	L2	L3
A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	L2	L3
A.9 - CONTROL DE ACCESO	L2	L3
A.10 - CRIPTOGRAFÍA	L2	L3
A.13 - SEGURIDAD DE LAS COMUNICACIONES	L2	L3
A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L2	L2
A.18 - CUMPLIMIENTO	L2	L3
A.11 - SEGURIDAD FÍSICA Y DEL ENTORNO	L3	L3
A.12 - SEGURIDAD DE LAS OPERACIONES	L3	L3
A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L3	L3

Valoración de la mejora de la SI

Resumen Estimación de la Mejora- Controles de Seguridad (ISO 27002)	
• A destacar que el establecimiento de los criterios de clasificación de la información permitirá una gestión adecuada de la seguridad de la información y de dotarla de las medidas de Seguridad apropiadas de manera focalizada y eficaz (**A8.-Gestión de Activos**). • El poder tener una gestión centralizada y ordenada de los activos de la organización permite poder tener un control sobre los activos y sus riesgos; con todo lo que esto implica en la mejora de Seguridad. (**A8.-Gestión de Activos**). • El ciclo de adquisición, desarrollo y mantenimiento de Sistemas de información quedarán establecidas pautas y procedimientos para controlar la adquisición, evaluación y control de los Sistemas de Información (Aseguramiento de especificaciones, servicios, cumplimiento de normas de seguridad, gestión de derechos y licenciamiento, etc.) que están bajo el dominio de control (A**.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**). • La gestión controlada de los proveedores permitirá tener un control sobre los mismos, sobre los servicios prestados, el cumplimiento de las especificaciones de seguridad, etc.), reflejados en el dominio (**A.15 - RELACIÓN CON PROVEEDORES**).	• Sobre la Gestión de las comunicaciones en la organización, se mejoran los aspectos de documentación de las arquitecturas y topologías de red presentes en la organización y sobre todo dejar documentado, registrado y establecidos los mecanismos de transporte e intercambio de información para mantener los niveles de seguridad deseados (transporte, correo, notificaciones internas/externas, etc.). Que quedan reflejados a través del dominio (**A.13 - SEGURIDAD DE LAS COMUNICACIONES**). • Sobre el conocimiento de los servicios críticos de la organización se tendrá una idea clara acerca de las afectaciones a negocio, de las necesidades y de los recursos necesarios para mantener la prestación de los servicios, de las necesidades de disponibilidad y de los tiempos de recuperación reales de los servicios. Es un proceso ya iniciado que habrá que seguir madurándolo progresivamente (**A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**). • Reforzar los mecanismos de seguridad a través de la planificación y seguimiento, dentro de la organización, de los aspectos de concienciación y formación en Seguridad de la Información (**A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS**).

Muchas Gracias