


PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN

PRESENTADO POR: **Freddy Jara C.**

TUTOR: **Antonio José Segovia.**

JUNIO 2019

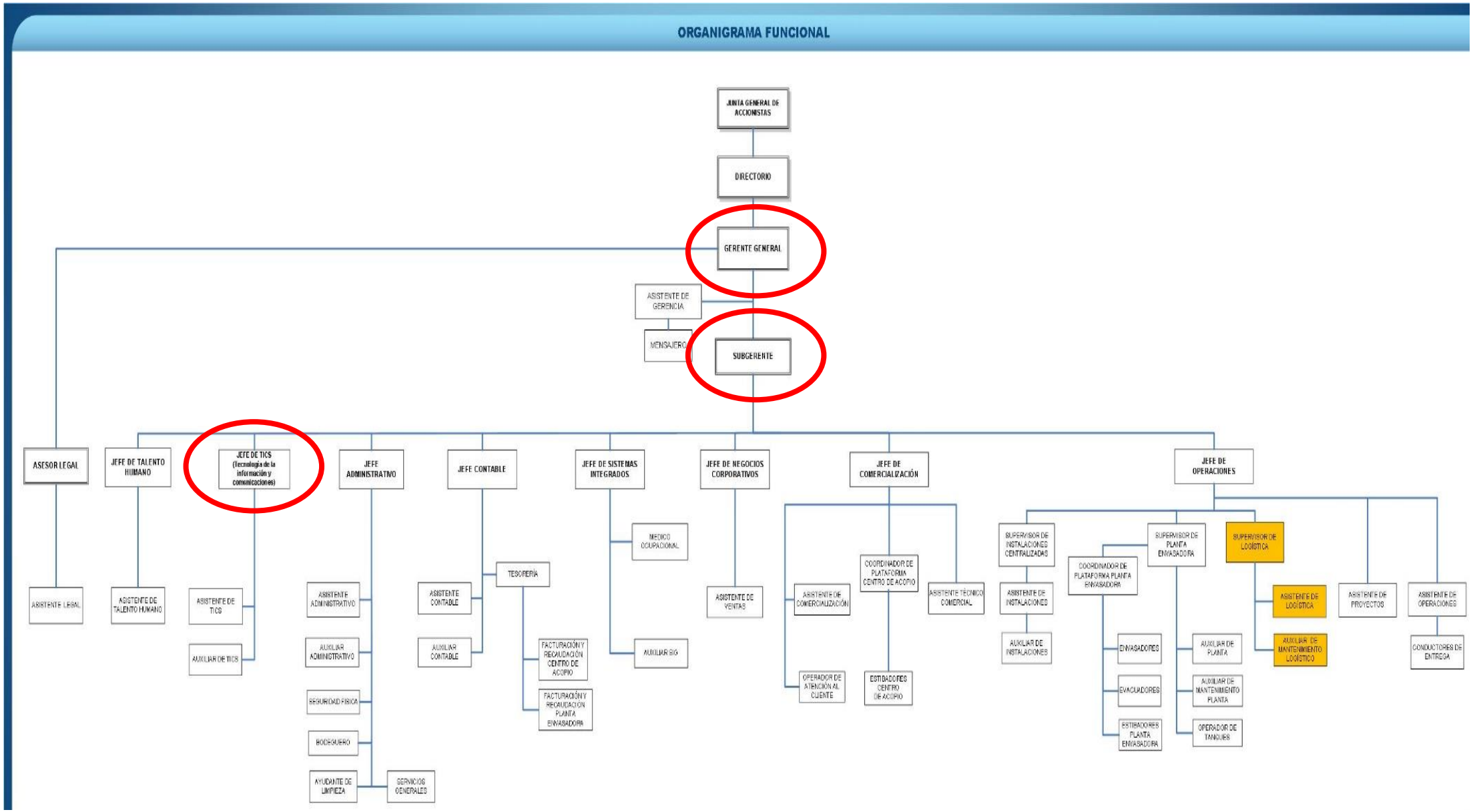
Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

AGENDA

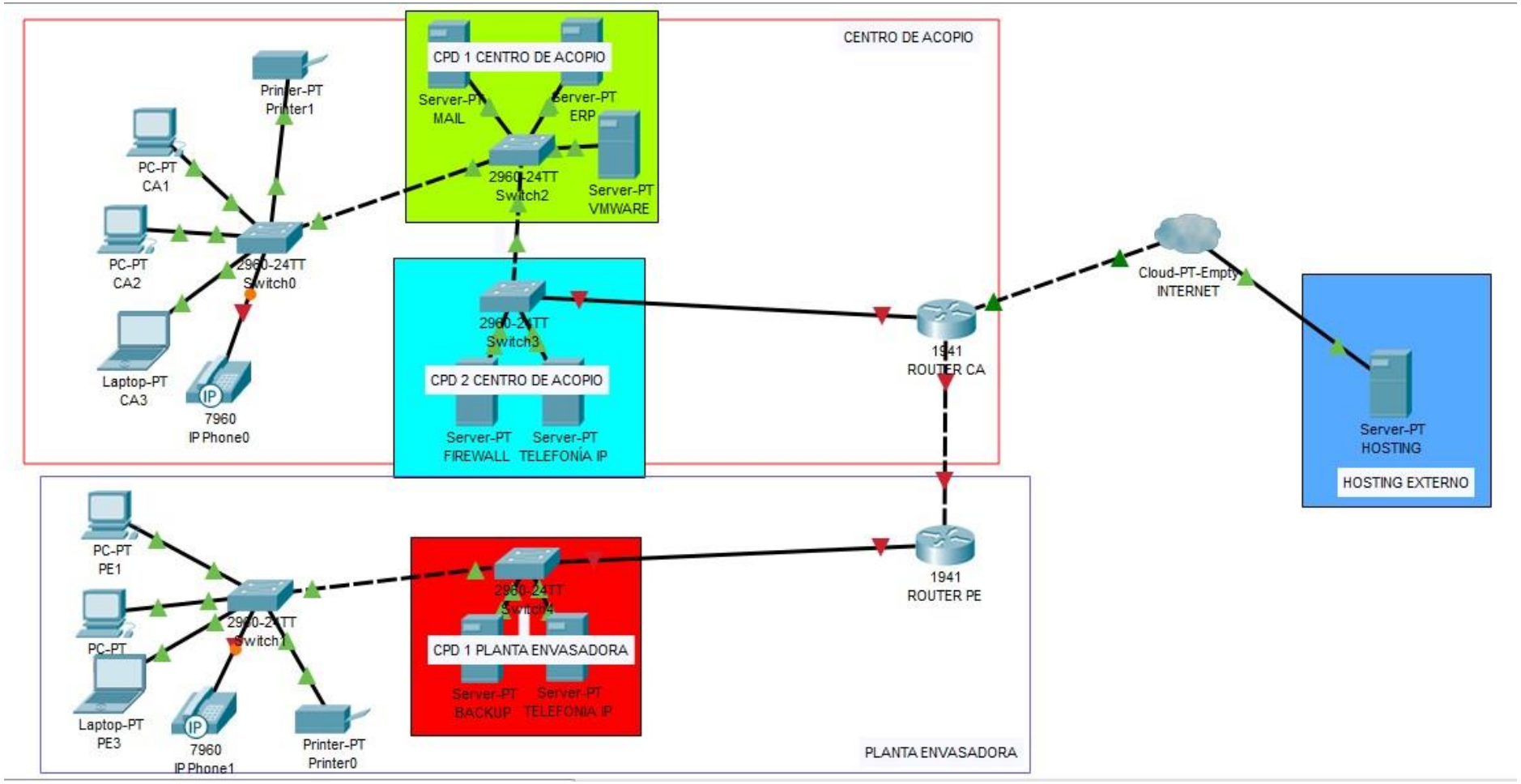
1. ¿Qué es el Plan Director de Seguridad de la Información?
2. Contexto de la Organización.
3. Objetivos.
4. ¿Cuáles son las etapas del SGSI?
5. Conclusiones.

1. ¿Qué es un Plan director de la Seguridad de la Información? PDSI

2. CONTEXTO DE LA ORGANIZACIÓN


ORGANIGRAMA FUNCIONAL
JUNTA GENERAL DE ACCIONISTAS
DIRECTORIO
GERENTE GENERAL
ASISTENTE DE GERENCIA
MENSAJERO
SUBGERENTE
ASESOR LEGAL
ASISTENTE LEGAL
JEFE DE TALENTO HUMANO
ASISTENTE DE TALENTO HUMANO
JEFE DE TICS (Tecnología de la información y comunicaciones)
ASISTENTE DE TICS
AUXILIAR DE TICS
JEFE ADMINISTRATIVO
ASISTENTE ADMINISTRATIVO
AUXILIAR ADMINISTRATIVO
SEGURIDAD FISICA
BODEGUERO
AYUDANTE DE LIMPIEZA
SERVICIOS GENERALES
JEFE CONTABLE
ASISTENTE CONTABLE
AUXILIAR CONTABLE
TESORERÍA
FACTURACIÓN Y RECAUDACIÓN CENTRO DE ACOPIO
FACTURACIÓN Y RECAUDACIÓN PLANTA ENVASADORA
JEFE DE SISTEMAS INTEGRADOS
MEDICO OCUPACIONAL
AUXILIAR SIG
JEFE DE NEGOCIOS CORPORATIVOS
ASISTENTE DE VENTAS
JEFE DE COMERCIALIZACIÓN
ASISTENTE DE COMERCIALIZACIÓN
OPERADOR DE ATENCIÓN AL CLIENTE
COORDINADOR DE PLATAFORMA CENTRO DE ACOPIO
ESTIBADORES CENTRO DE ACOPIO
ASISTENTE TÉCNICO COMERCIAL
JEFE DE OPERACIONES
SUPERVISOR DE INSTALACIONES CENTRALIZADAS
ASISTENTE DE INSTALACIONES
AUXILIAR DE INSTALACIONES
COORDINADOR DE PLATAFORMA PLANTA ENVASADORA
ENVASADORES
EVACUADORES
ESTIBADORES PLANTA ENVASADORA
SUPERVISOR DE PLANTA ENVASADORA
AUXILIAR DE PLANTA
AUXILIAR DE MANTENIMIENTO PLANTA
OPERADOR DE TANQUES
SUPERVISOR DE LOGÍSTICA
ASISTENTE DE LOGÍSTICA
AUXILIAR DE MANTENIMIENTO LOGÍSTICO
ASISTENTE DE PROYECTOS
ASISTENTE DE OPERACIONES
CONDUCTORES DE ENTREGA

2. Diagrama Lógico



3. OBJETIVOS DEL PLAN DIRECTOR

Objetivo General

El principal objetivo del presente proyecto es diseñar el plan director de seguridad e implementación de un SGSI para la empresa bajo estudio, que permita establecer las directrices y estándares ISO/IEC 27001-27002.

Como metodología de análisis y gestión de riesgos se usará MAGERIT

3. OBJETIVOS DEL PLAN DIRECTOR

Objetivos Específicos

- Asegurar la disponibilidad, confidencialidad e integridad de los activos de información críticos de la empresa.
- Reducir los riesgos a niveles aceptables en materia de la seguridad de la información a los que está expuesta la empresa.
- Definir y planificar los planes de acción a realizar, a corto, mediano y largo plazo.
- Conocer y planificar las inversiones y costos necesarios para alcanzar el nivel de seguridad adecuado.
- Mejorar los niveles de seguridad de la información al fomentar una cultura de seguridad de la información en los empleados de la empresa.

3. ALCANCE

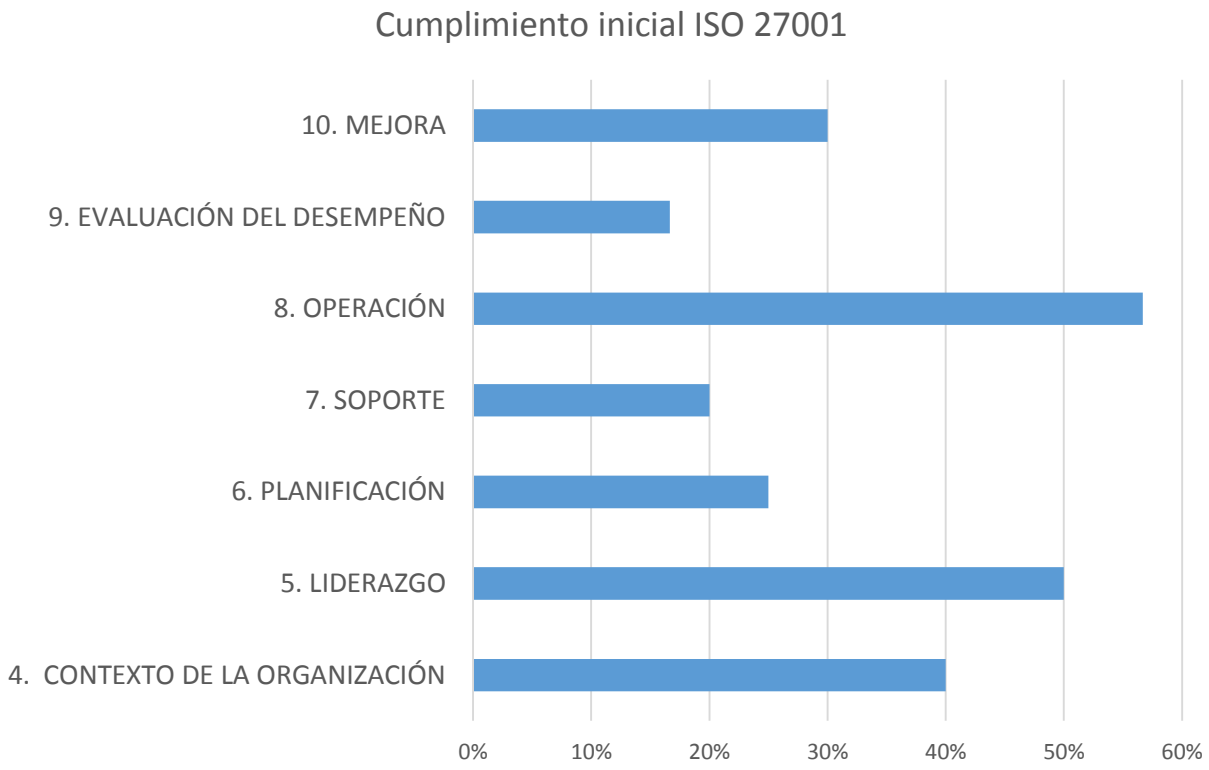
La gestión de la seguridad de la información que cubra todas las actividades asociadas con los CPD de la empresa que dan soporte a los siguientes procesos críticos

- Servicios públicos accesibles desde la red pública (Internet), pretendiendo que los clientes y empleados tengan acceso a los mismos sin la necesidad de entrar a la red interna.
- Servicios privados accesibles desde la red pública (Internet).
- Red Interna , específicamente a los CPD que cuentan con distintos servidores físicos y virtualizados tales como, bases de datos, ERP, sistema de facturación, consolas de gestión de seguridad de red, mesas de ayuda, servidores espejos, sistemas de video conferencia.

4. ¿Cuáles son las etapas del SGSI?

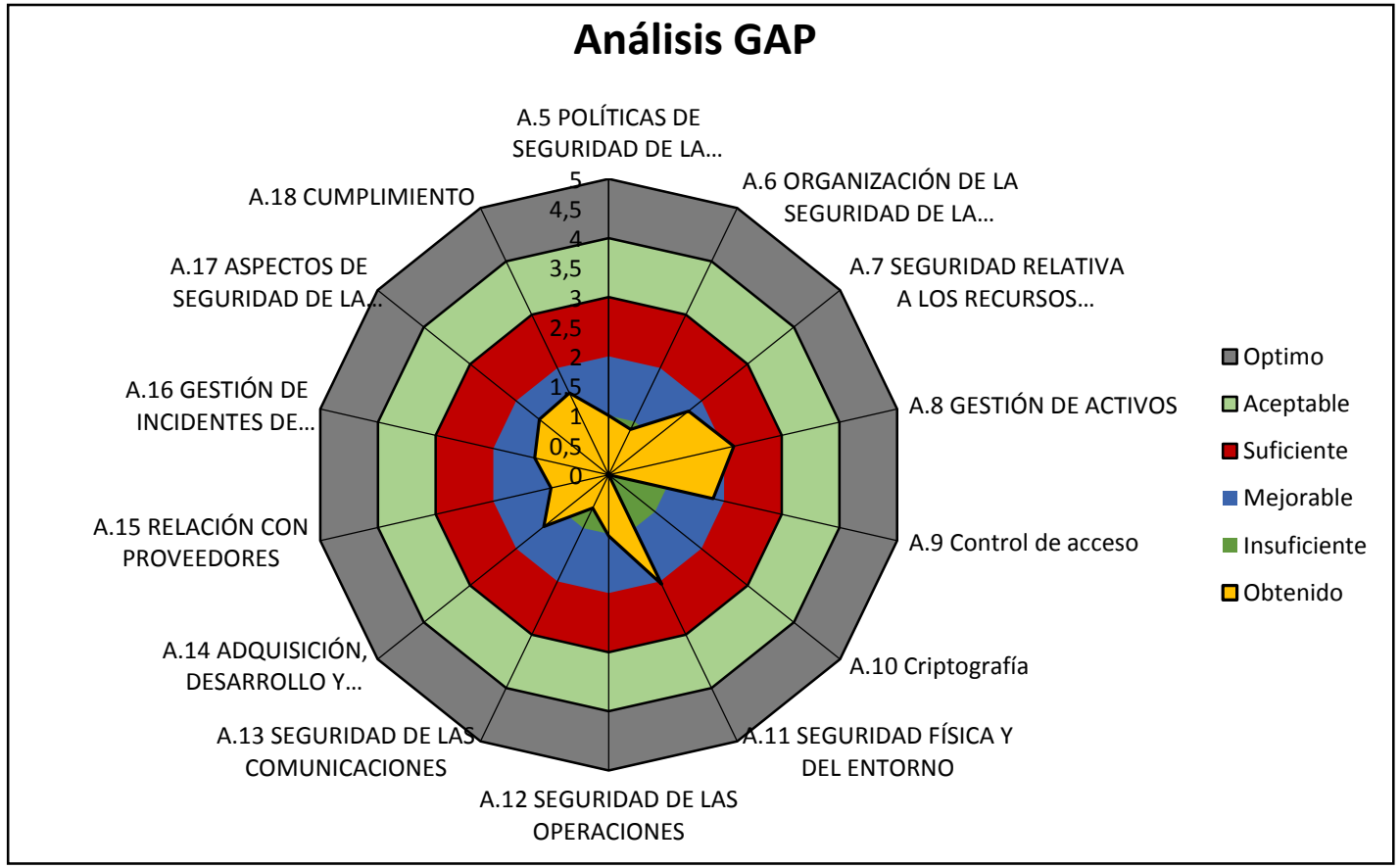
4.1 ANÁLISIS DE LA SITUACIÓN ACTUAL ISO 27001:2013

REQUISITOS	Nivel Inicial
4. CONTEXTO DE LA ORGANIZACIÓN	40%
5. LIDERAZGO	50%
6. PLANIFICACIÓN	25%
7. SOPORTE	20%
8. OPERACIÓN	57%
9. EVALUACIÓN DEL DESEMPEÑO	17%
10. MEJORA	30%



4.1 ANÁLISIS DE LA SITUACIÓN ACTUAL ISO 27002:2013

Dominios ISO/ IEC 27002:2013	Valor
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	1
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0,85
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	1,72
A.8 GESTIÓN DE ACTIVOS	2,17
A.9 Control de acceso	1,81
A.10 Criptografía	0
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	2,06
A.12 SEGURIDAD DE LAS OPERACIONES	1,04
A.13 SEGURIDAD DE LAS COMUNICACIONES	0,63
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. DE INFORMACIÓN	1,41
A.15 RELACIÓN CON PROVEEDORES	1
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	1,29
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	1,5
A.18 CUMPLIMIENTO	1,53



4.2 FASE 2. SISTEMA DE GESTIÓN DOCUMENTAL

- Políticas de la seguridad de la información
- Procedimiento de auditoria interna
- Gestión de Indicadores
- Procedimiento de revisión por la dirección
- Gestión de roles y responsabilidades
- Metodología de análisis de Riesgo
- Declaración de la aplicabilidad

4.3 ANÁLISIS DE RIESGO

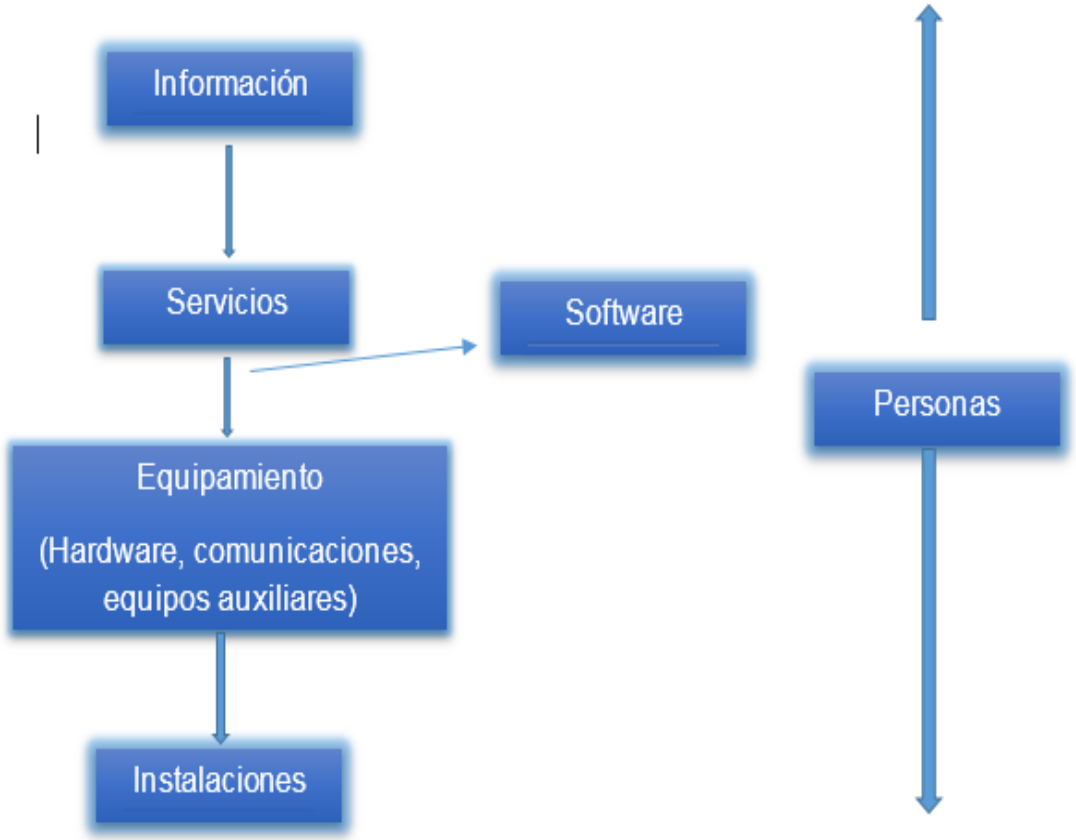
4.3.1 IDENTIFICACIÓN DE ACTIVOS

Se identificaron un total de 95 activos repartidos en 10 ámbitos

AMBITOS	Cantidad
[INS] INSTALACIONES	3
[HW] EQUIMAMIENTO INFORMÁTICO	20
[SW]APLICACIONES INFORMÁTICAS	34
[DI] DATOS/INFORMACIÓN	13
[COM] REDES DE COMUNICACIÓN	6
[SER] SERVICIOS	7
[EA] EQUIPAMINETO AUXILIAR	6
[PE] PERSONAL	3
[CC] CLAVES CRIPTOGRAFICAS	1
[MEDIA] SOPORTE DE INFORMACIÓN	2
TOTAL	95

4.3 ANÁLISIS DE RIESGO

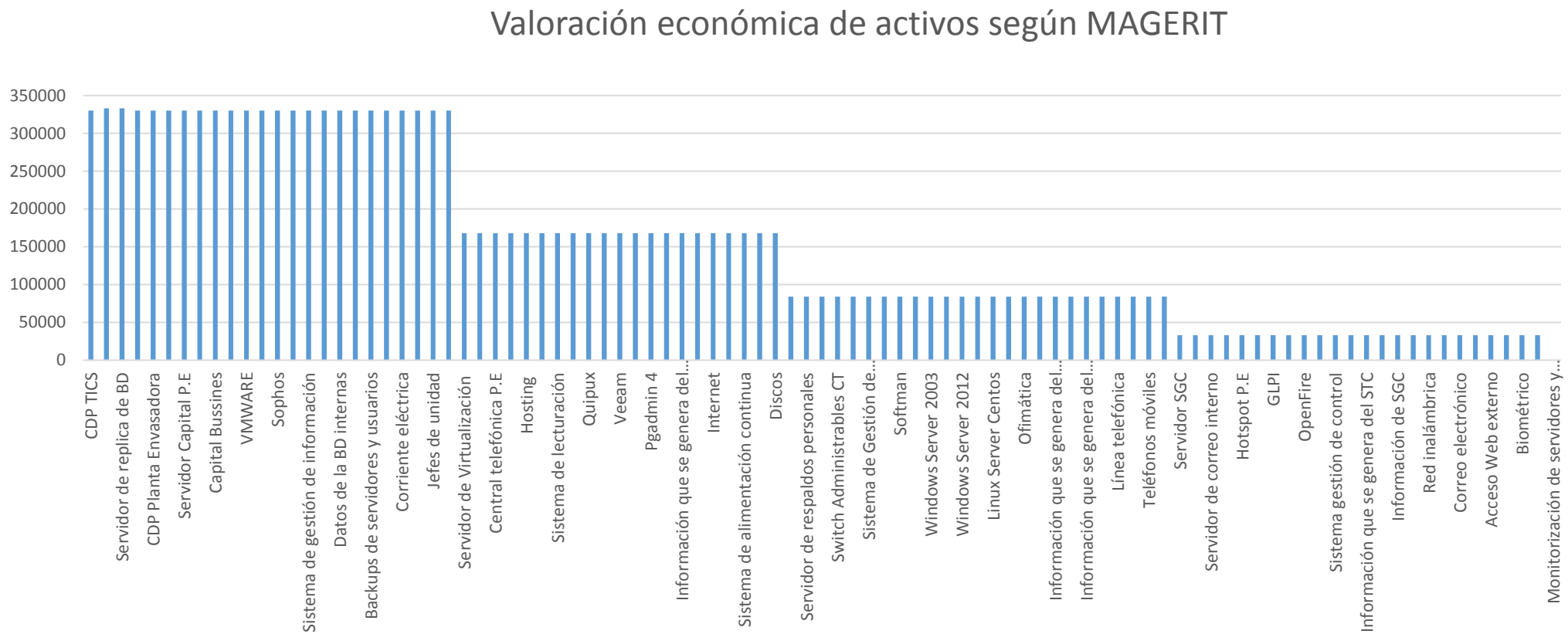
4.3.2 DEPENDENCIA ENTRE ACTIVOS



4.3 ANÁLISIS DE RIESGO

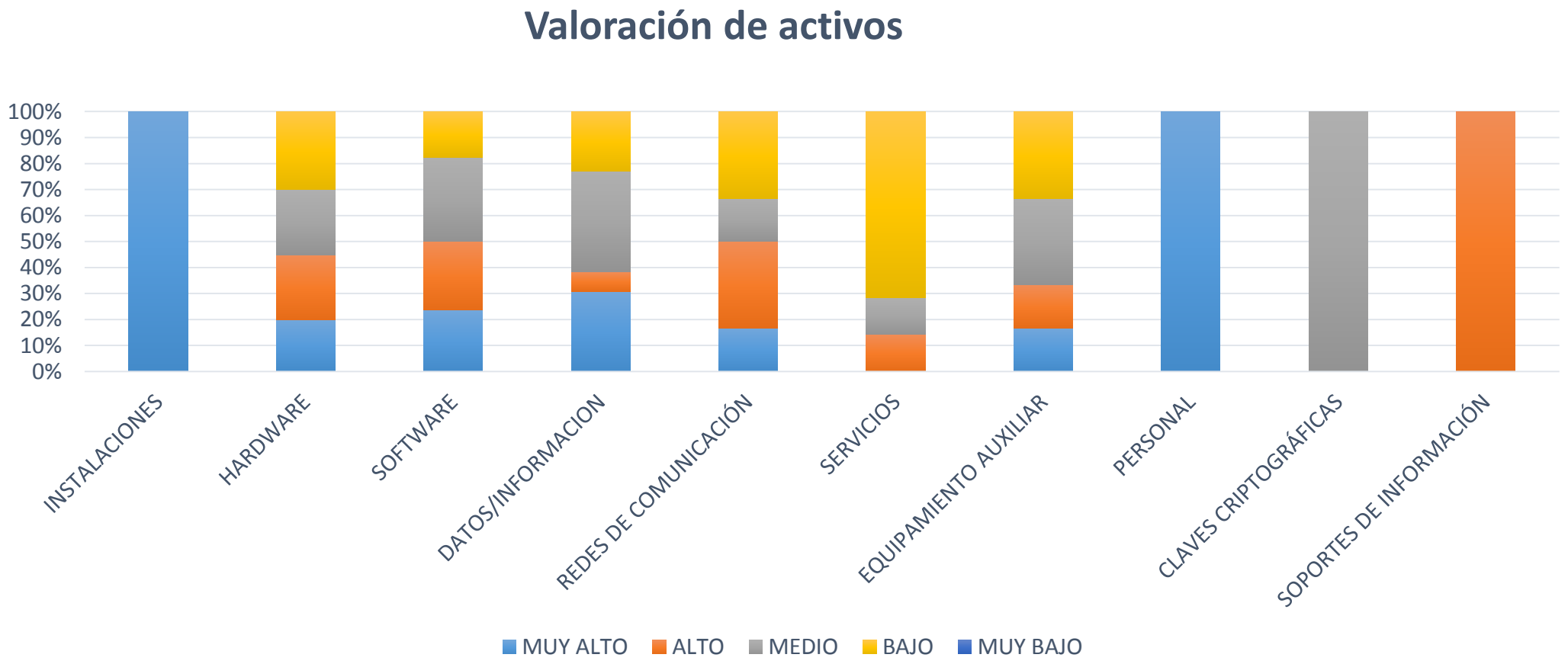
4.3.3 Valoración de Activos

La valoración económica estimada es de: 14.346.000 USD



4.3 ANÁLISIS DE RIESGO

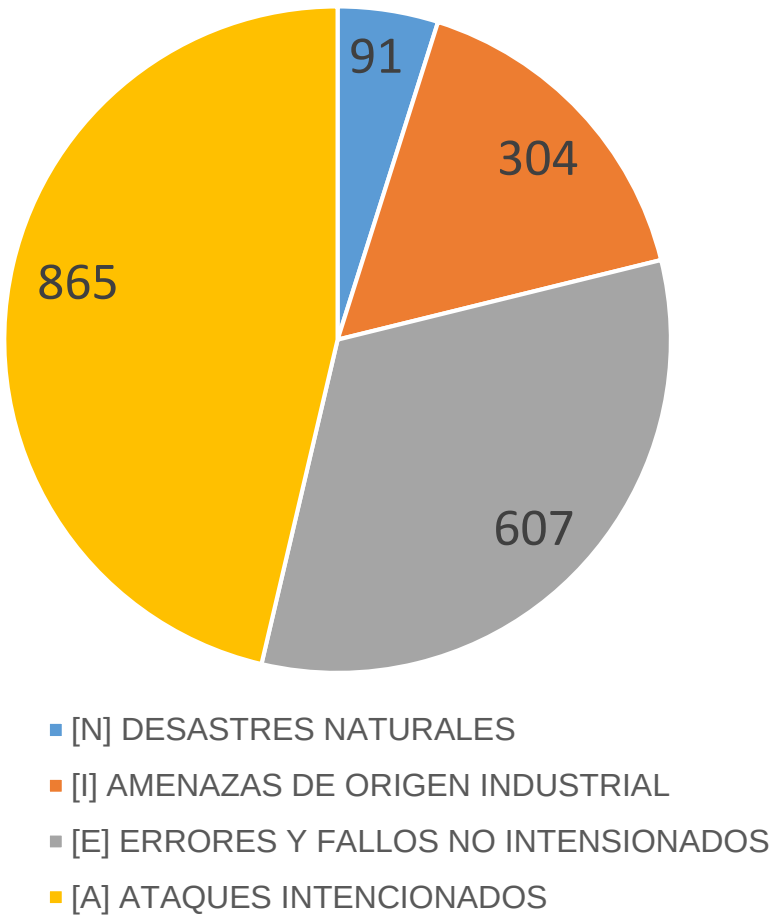
4.3.4 Valoración de Cualitativa



4.3 ANÁLISIS DE RIESGO

4.3.5 VALORACIÓN DE AMENAZAS

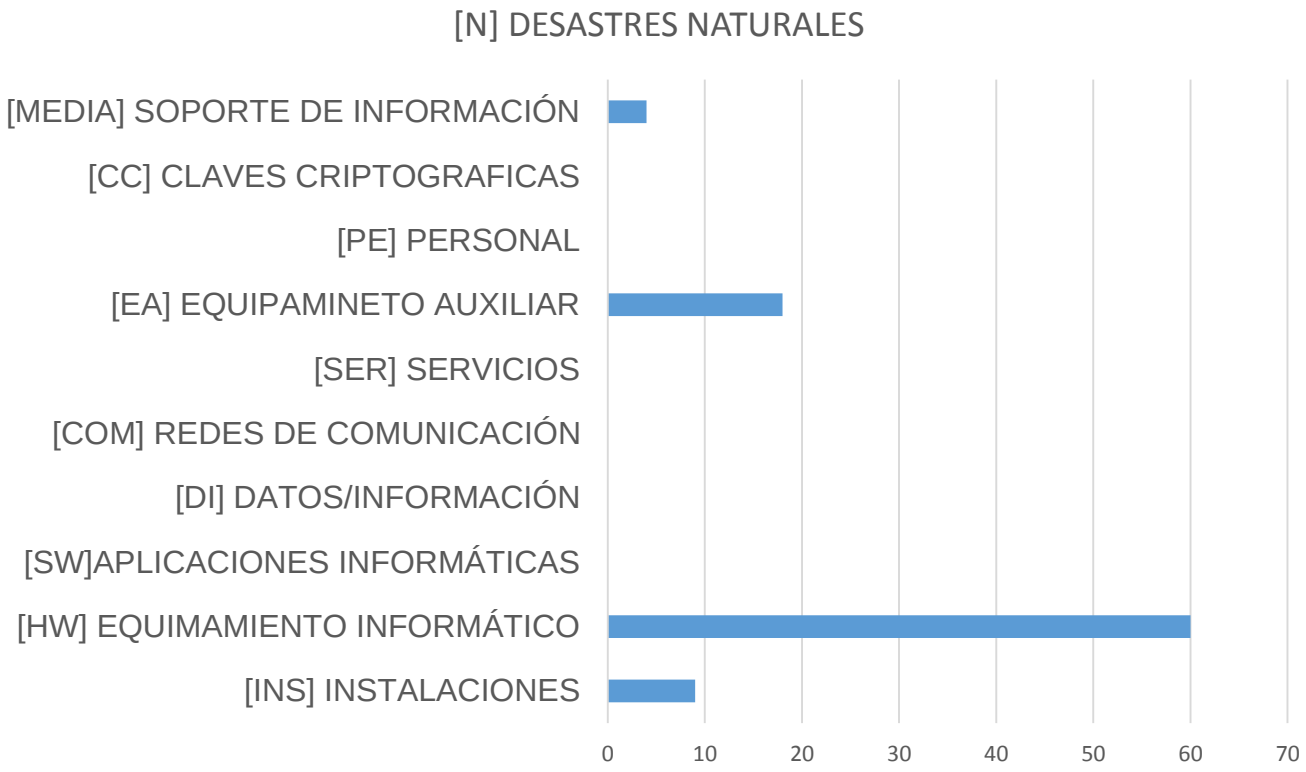
[N] DESASTRES NATURALES	91
[I] AMENAZAS DE ORIGEN INDUSTRIAL	304
[E] ERRORES Y FALLOS NO INTENSIONADOS	607
[A] ATAQUES INTENCIONADOS	865
TOTAL	1867



4.3 ANÁLISIS DE RIESGO

4.3.5 VALORACIÓN DE AMENAZAS

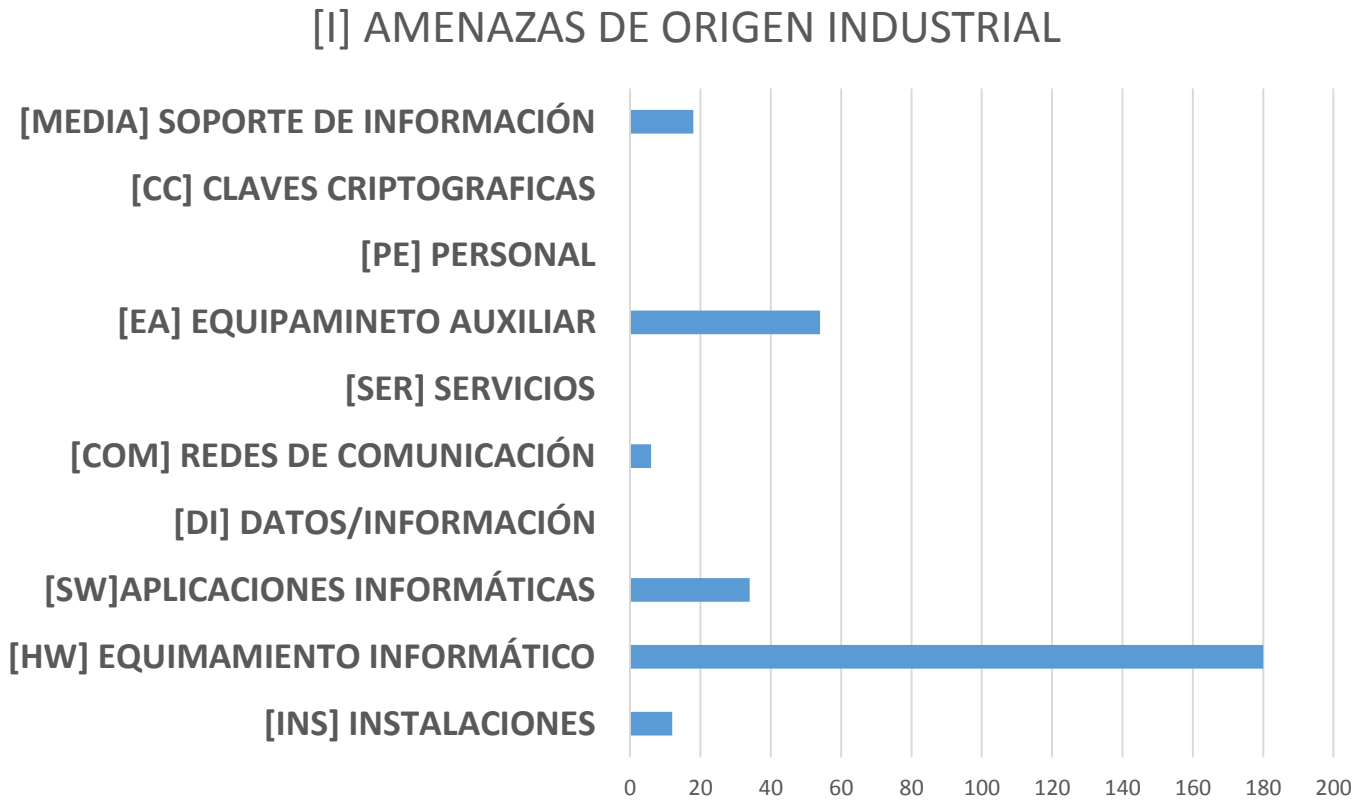
[N] DESASTRES NATURALES	
[INS] INSTALACIONES	9
[HW] EQUIMAMIENTO INFORMÁTICO	60
[SW]APLICACIONES INFORMÁTICAS	0
[DI] DATOS/INFORMACIÓN	0
[COM] REDES DE COMUNICACIÓN	0
[SER] SERVICIOS	0
[EA] EQUIPAMINETO AUXILIAR	18
[PE] PERSONAL	0
[CC] CLAVES CRIPTOGRAFICAS	0
[MEDIA] SOPORTE DE INFORMACIÓN	4
TOTAL	91



4.3 ANÁLISIS DE RIESGO

4.3.5 VALORACIÓN DE AMENAZAS

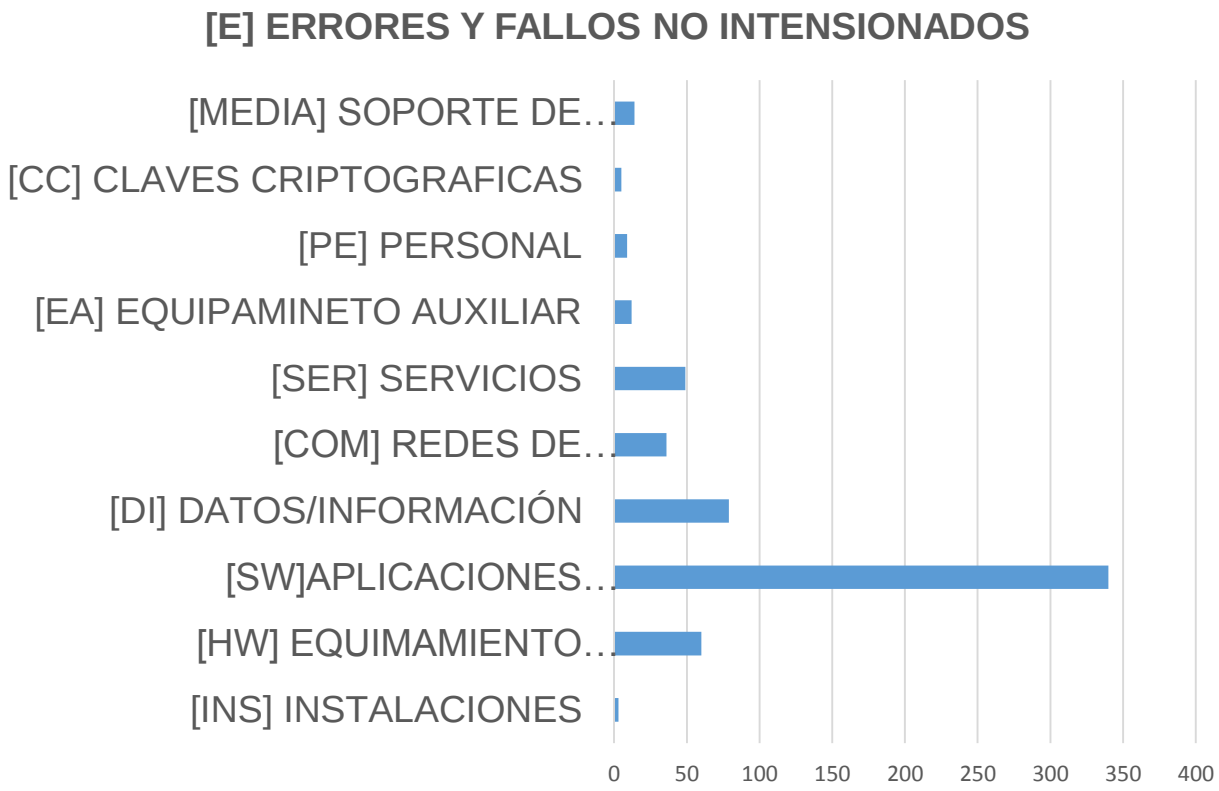
[I] AMENAZAS DE ORIGEN INDUSTRIAL	
[INS] INSTALACIONES	12
[HW] EQUIMAMIENTO INFORMÁTICO	180
[SW]APLICACIONES INFORMÁTICAS	34
[DI] DATOS/INFORMACIÓN	0
[COM] REDES DE COMUNICACIÓN	6
[SER] SERVICIOS	0
[EA] EQUIPAMINETO AUXILIAR	54
[PE] PERSONAL	0
[CC] CLAVES CRIPTOGRAFICAS	0
[MEDIA] SOPORTE DE INFORMACIÓN	18
TOTAL	304



4.3 ANÁLISIS DE RIESGO

4.3.5 VALORACIÓN DE AMENAZAS

[E] ERRORES Y FALLOS NO INTENSIONADOS	
[INS] INSTALACIONES	3
[HW] EQUIMAMIENTO INFORMÁTICO	60
[SW]APLICACIONES INFORMÁTICAS	340
[DI] DATOS/INFORMACIÓN	79
[COM] REDES DE COMUNICACIÓN	36
[SER] SERVICIOS	49
[EA] EQUIPAMINETO AUXILIAR	12
[PE] PERSONAL	9
[CC] CLAVES CRIPTOGRAFICAS	5
[MEDIA] SOPORTE DE INFORMACIÓN	14
TOTAL	607



4.3 ANÁLISIS DE RIESGO

4.3.5 VALORACIÓN DE AMENAZAS

AMENAZAS	CANTIDAD DE AMENAZAS POR ACTIVOS
[A.11] ACCESO NO AUTORIZADO	92
[E.2] ERRORES DEL ADMINISTRADOR	83
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	81
[A.7] USO NO PREVISTO	78
[A.15] MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	75
[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	72
[E.19] FUGAS DE INFORMACIÓN	69
[A.19] DIVULGACIÓN DE LA INFORMACIÓN	66
[E.15] ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	63
[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	63

4.3 ANÁLISIS DE RIESGO

4.3.6 NIVEL DE RIESGO ACEPTABLE Y RESIDUAL

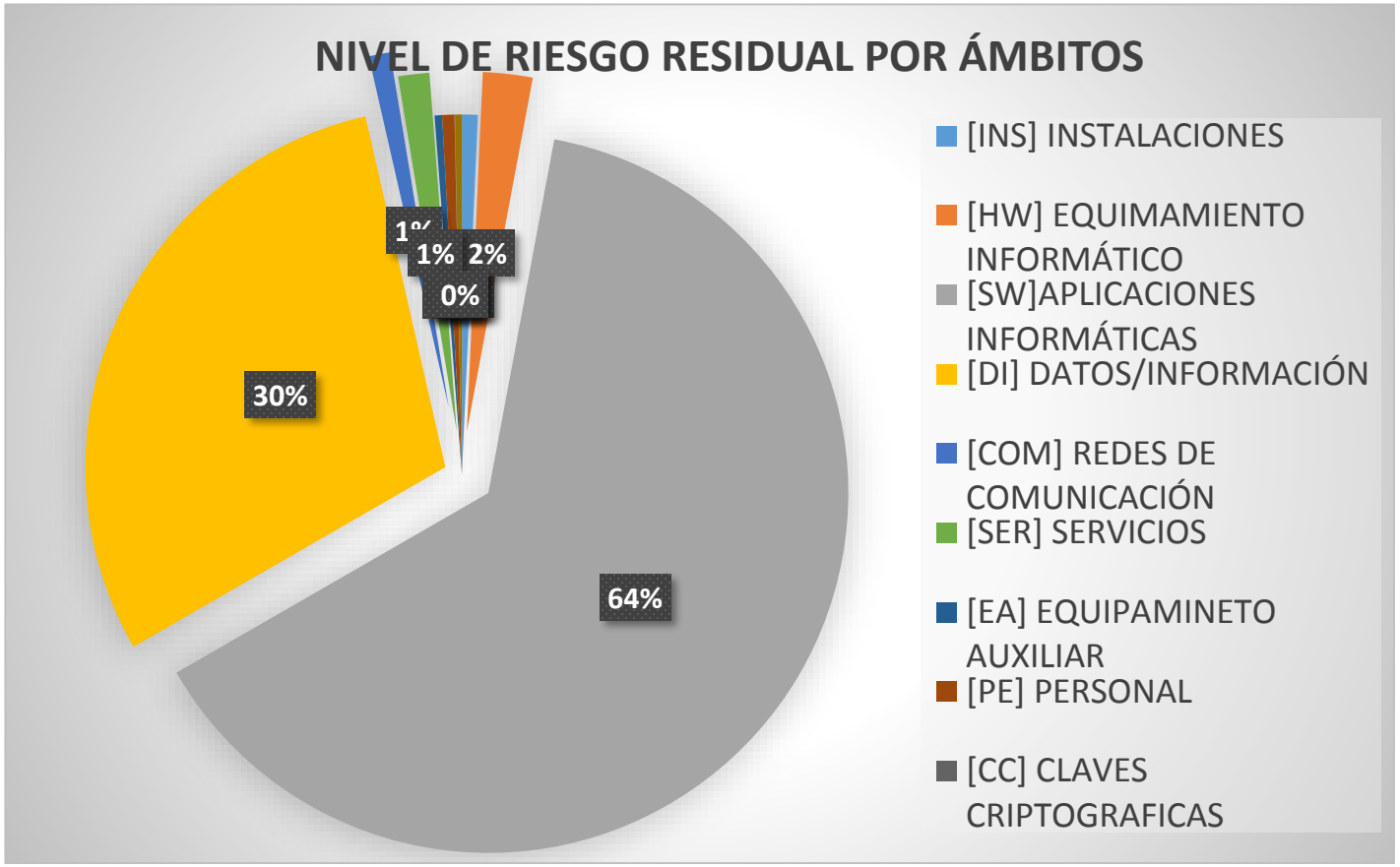
El nivel de riesgo aceptable debe ser aprobado por la dirección de la organización y se deben definir los criterios para establecer el nivel de riesgo.

El valor que la dirección asumido establecer como umbral (RIESGO ACEPTABLE) es 500, siendo este valor el que determinará la necesidad de acometer proyectos de mejora. Hasta el valor de riesgo 500 la empresa ha decidido asumir el riesgo.

4.3 ANÁLISIS DE RIESGO

4.3.7 Cálculo del nivel de Riesgo

ÁMBITO	VALOR DE RIESGO
[INS] INSTALACIONES	8700
[HW] EQUIMAMIENTO INFORMÁTICO	27400
[SW]APLICACIONES INFORMÁTICAS	784100
[DI] DATOS/INFORMACIÓN	366000
[COM] REDES DE COMUNICACIÓN	11800
[SER] SERVICIOS	17175
[EA] EQUIPAMINETO AUXILIAR	4100
[PE] PERSONAL	6750
[CC] CLAVES CRIPTOGRAFICAS	250
[MEDIA] SOPORTE DE INFORMACIÓN	3800



4.3 ANÁLISIS DE RIESGO

4.3.8 Activos que superan el nivel de riesgo aceptable

4.3 ANÁLISIS DE RIESGO

4.3.9 RESULTADOS

Se ha dividido en dos grupos:

Primero con un valor de riesgo mayores a 1000, que son los que tienen prioridad urgente para mitigar el riesgo de los activos, y

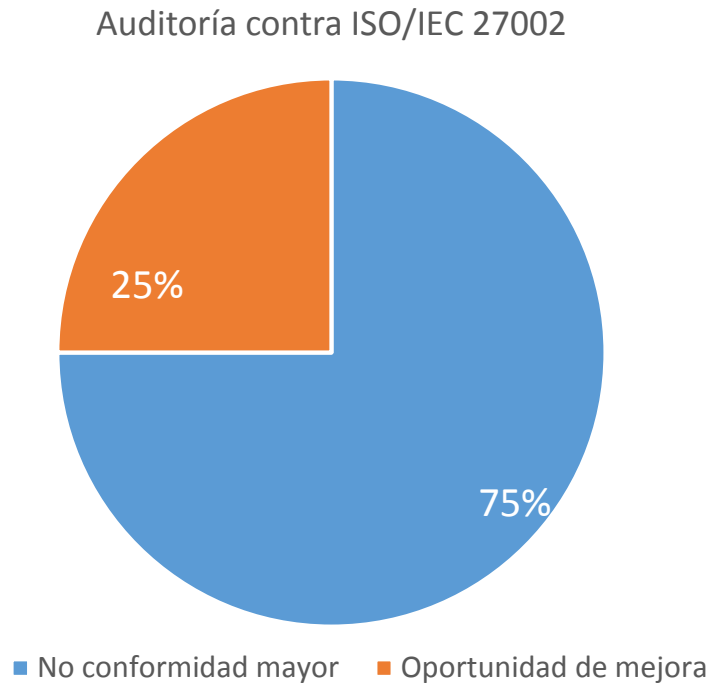
Segundo con un valor de riesgo en un intervalo que va de 500 a 1000, que posteriormente se realizarán las gestiones para mitigar el riesgo.

4.4 PROPUESTA DE PROYECTOS

PROYECTO	COSTE USD		TEMPORALIDAD	
PROJ01: Plan de continuidad del Negocio	35000	46500	1 año	1 Año
PROJ02: Política de Backups y recuperación	5000		6 meses	
PROJ03: Plan de clasificación y tratamiento de la información	3000		6 meses	
PROJ04: Acceso seguro a la información externa/interna	1500		2 meses	
PROJ05: Formaciones continuas en temas de seguridad.	2000		1 año	
PROJ06: Procedimiento de destrucción de soportes	500	169900	1 mes	1 Año
PROJ07: Implantación de políticas de la seguridad de la información	14400		1 año	
PROJ08: Gestión de activos.	0		1 mes	
PROJ09: Alta disponibilidad para aplicaciones que soporta la empresa.	150000		1 año	
PROJ10: Plan de mejora de la seguridad del CPDS	5000		6 meses	
PROJ11: Gestión de incidentes de seguridad	0		2 meses	

4.5 AUDITORIA DE CUMPLIMIENTO

4.5 AUDITORIA DE CUMPLIMIENTO



6. CONCLUSIONES

- Partimos con un estado inicial de la empresa en el que la mayoría de requerimientos de la ISO/IEC 27001 y controles de la ISO/IEC 27002 estaban en un nivel inexistente e inicial. La implantación del presente SGSI dota a la empresa de las medidas de seguridad necesarias para gestionar y mitigar las amenazas detectadas en el presente proyecto, permitiendo una reducción considerable de los riesgos que están expuestos los activos.
- Se levantó un inventario y valoración de activos que permitieron realizar una evaluación y valoración de las posibles amenazas que podrían materializarse en los activos, con esta información permitió realizar el cálculo del impacto en las diferentes dimensiones de seguridad y nivel de riesgo que tienen cada uno de los activos de la empresa

6. CONCLUSIONES

- Se analizaron los resultados anteriores permitiendo el planteamiento de varias Propuestas de Proyectos que tienen como objetivo mejorar la seguridad de la información incluyendo coste estimado de implementación, tiempo de ejecución y puntos de control.
- Se realiza una evaluación de la madurez de los requerimientos y controles establecidos en la ISO/IEC 27001 -27002, mediante una auditoría de cumplimiento. Dando como resultado “no conformidades” que deben ser resueltas en plazos establecidos.
- Tras la realización de todas las fases mencionadas anteriormente se ha logrado mejorar el estado inicial de la seguridad de la información a demás se ha logrado la concienciación y colaboración de los empleados en materia de la seguridad de la información.

6. CONCLUSIONES

- Finalmente existe un compromiso por parte de la alta dirección de revisar y monitorear el SGSI, permitiendo retroalimentar el Ciclo de Demming, asegurando que los controles o salvaguardas sigan siendo efectivas y no se produzcan desviaciones, nuevas amenazas o cambios en el contexto o en los objetivos de la empresa.

GRACIAS