GRUPO ASD

PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACION

GRUPO ASD

Presentado por: Ricardo Alberto Duitama Leal

Tutor: Antonio José Segovia

Máster Interinstitucional en Seguridad de la información y Telecomunicaciones

Barcelona España 2013

Introducción

- Definir un Plan Director de Seguridad para GRUPO ASD, el cual permitirá definir las bases de mejora continua a nivel de seguridad de la información permitiendo conocer el estado actual y definir las acciones necesarias para mitigar los riesgos que se presentan en los activos de información de la organización.

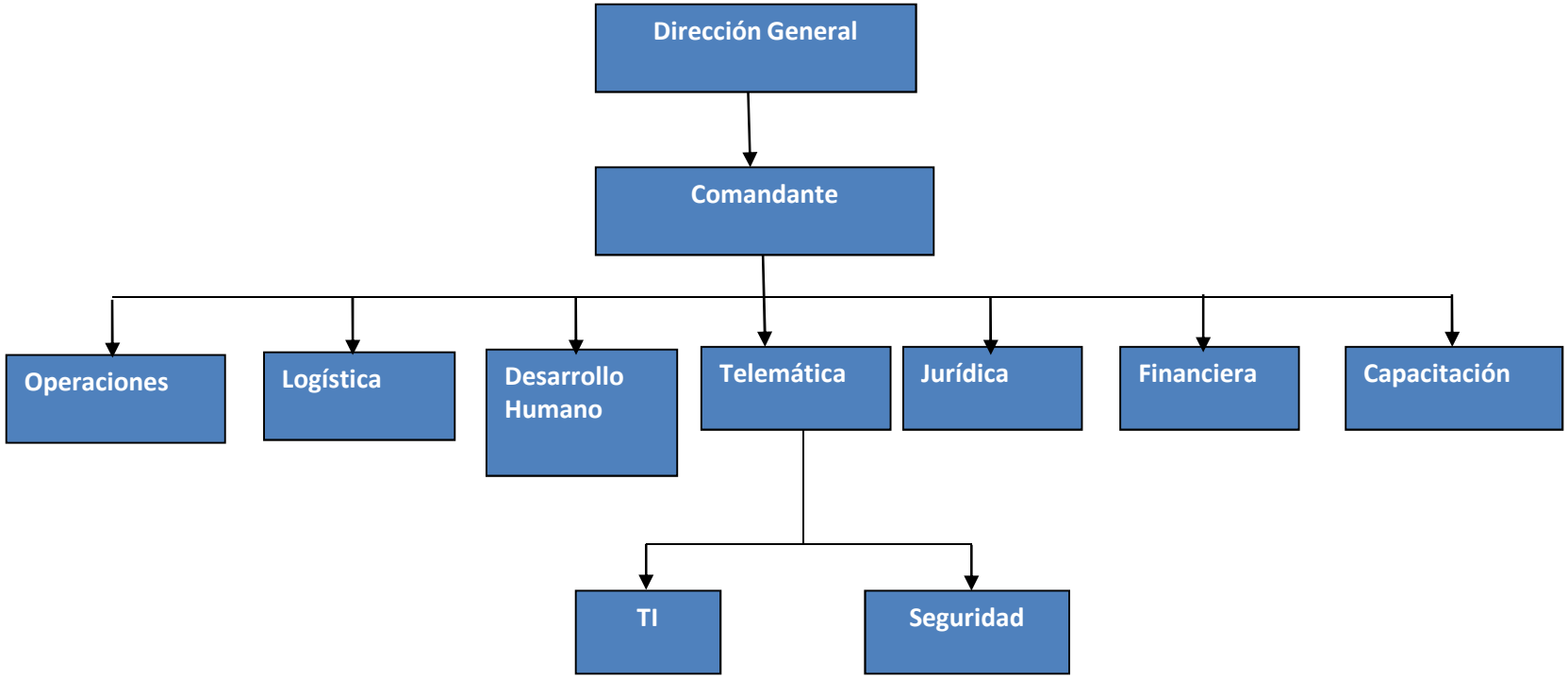
Objetivos

Dentro de los objetivos que se pretende alcanzar con este proyecto están:

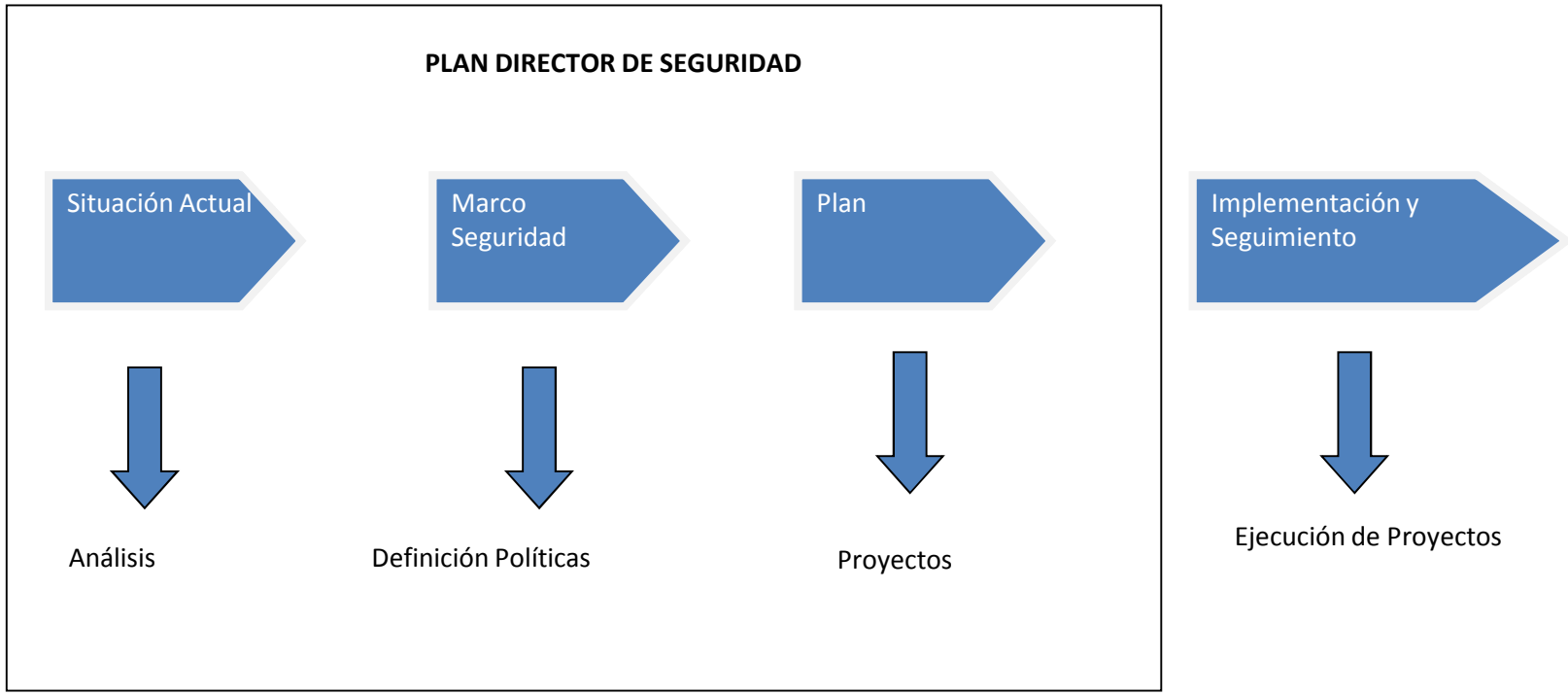
- Identificación de Activos Críticos para el proceso y subprocesos a evaluar.
- Realizar un proceso de análisis de riesgos bajo una metodología de riesgos
- Realizar un análisis de Brecha ISO 27002.
- Definición del Plan director para la organización
- Optimizar las inversiones en seguridad de la información al ejecutar planes de acción que apoyen la consecución de los objetivos de la organización.
- Mejorar los niveles de Seguridad de la Información al fomentar la adopción de una cultura de seguridad de la información a todos los niveles.

Selección Empresa

- El presente proyecto se pretende desarrollar en el GRUPO ASD, la cual es la entidad de más alto nivel de planeamiento y dirección estratégica para las instituciones castrenses de Colombia. Bajo su égida y faro están el Ejército Nacional, la Armada y la Fuerza Aérea.



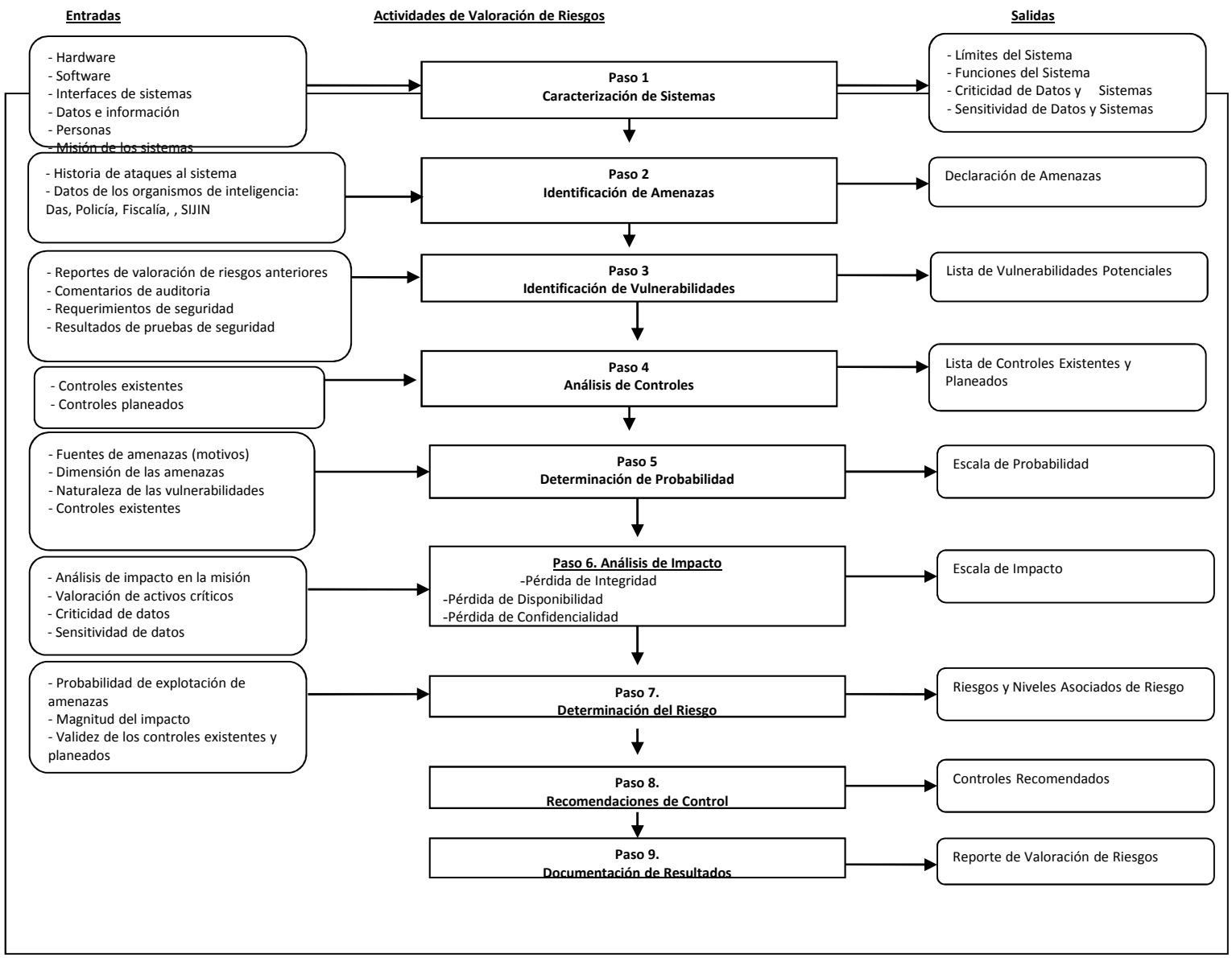
Esquema Plan Director de Seguridad



SITUACION ACTUAL

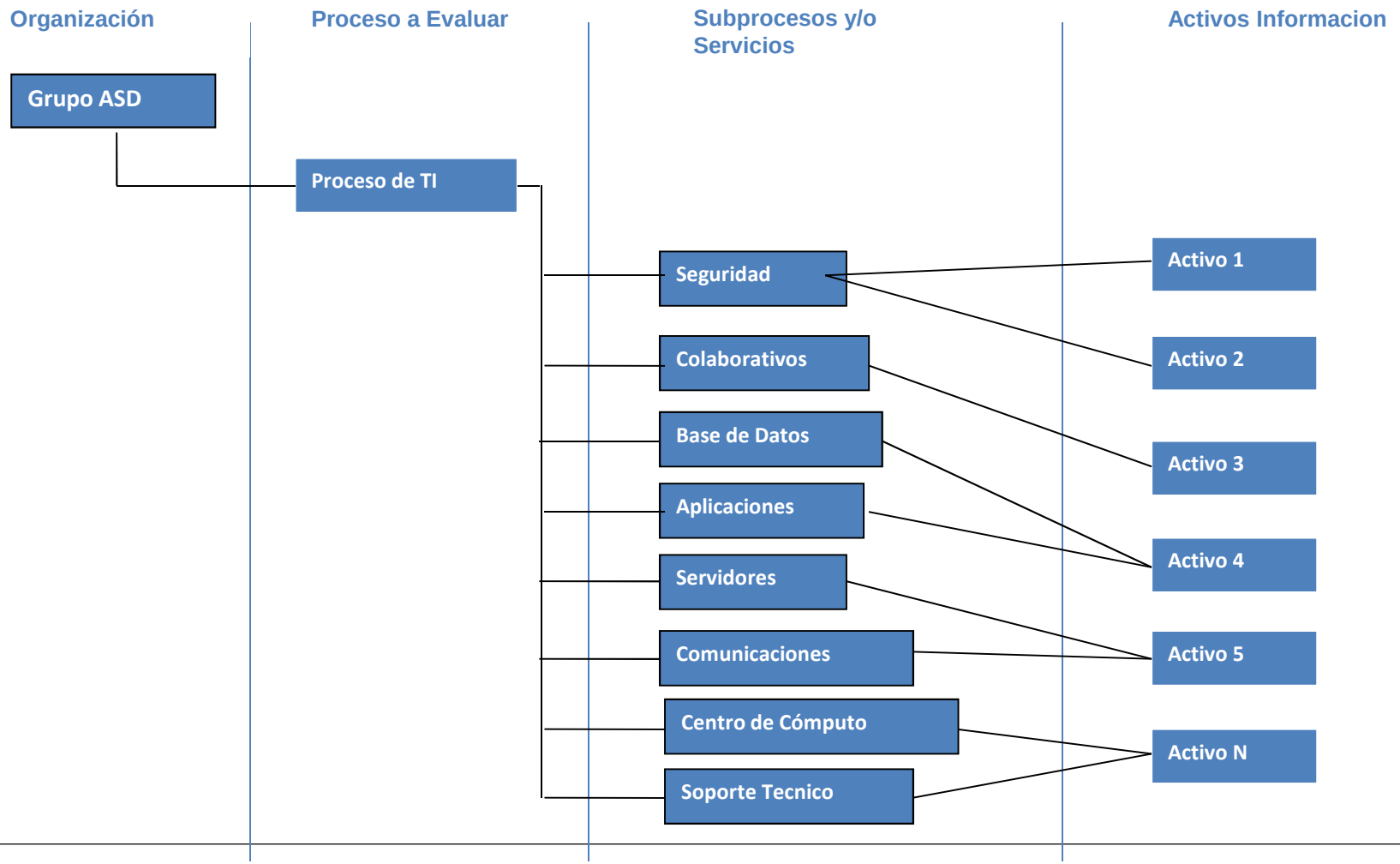
Análisis de Riesgos

Metodología ANZ 43660

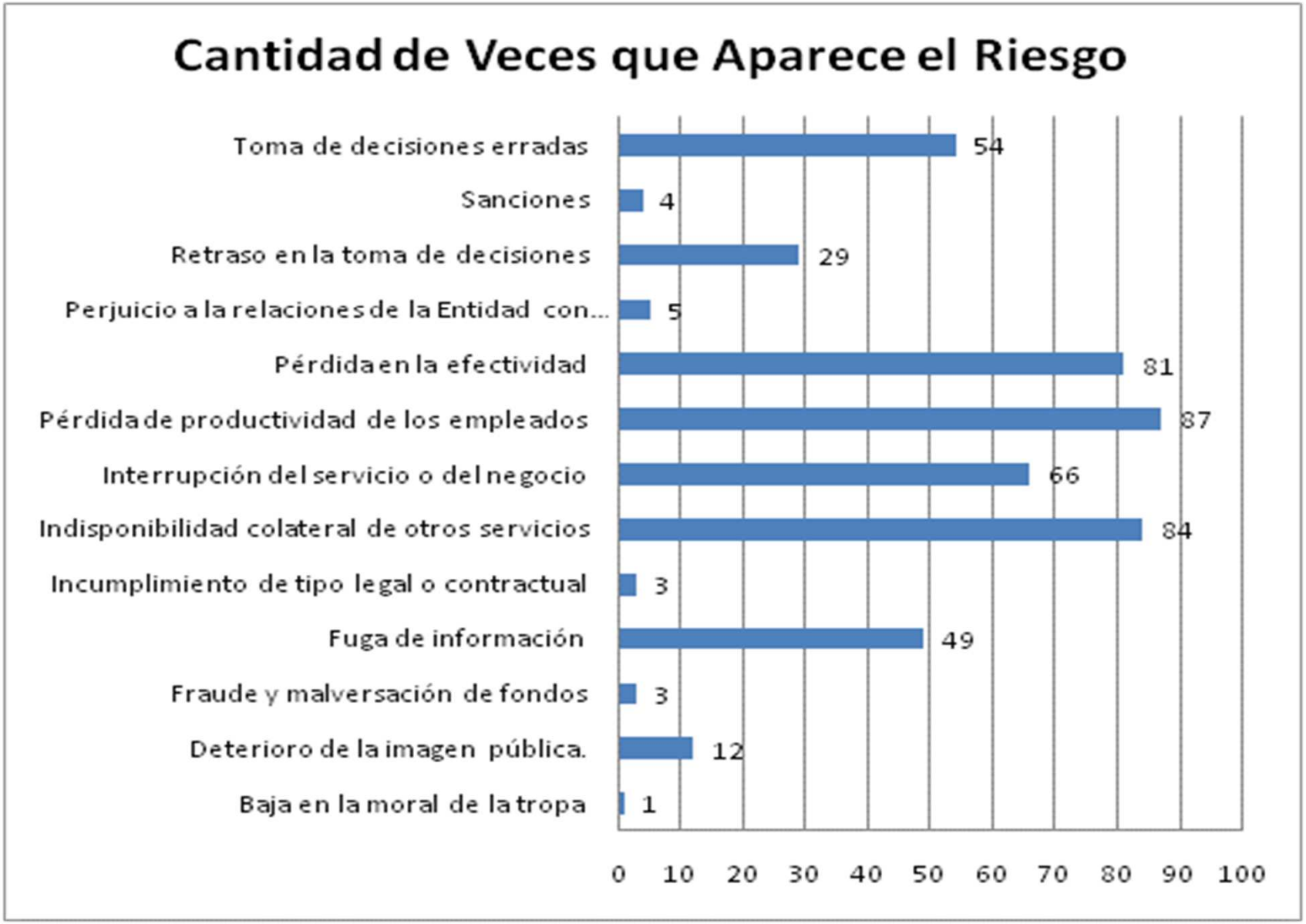


Identificación de Activos

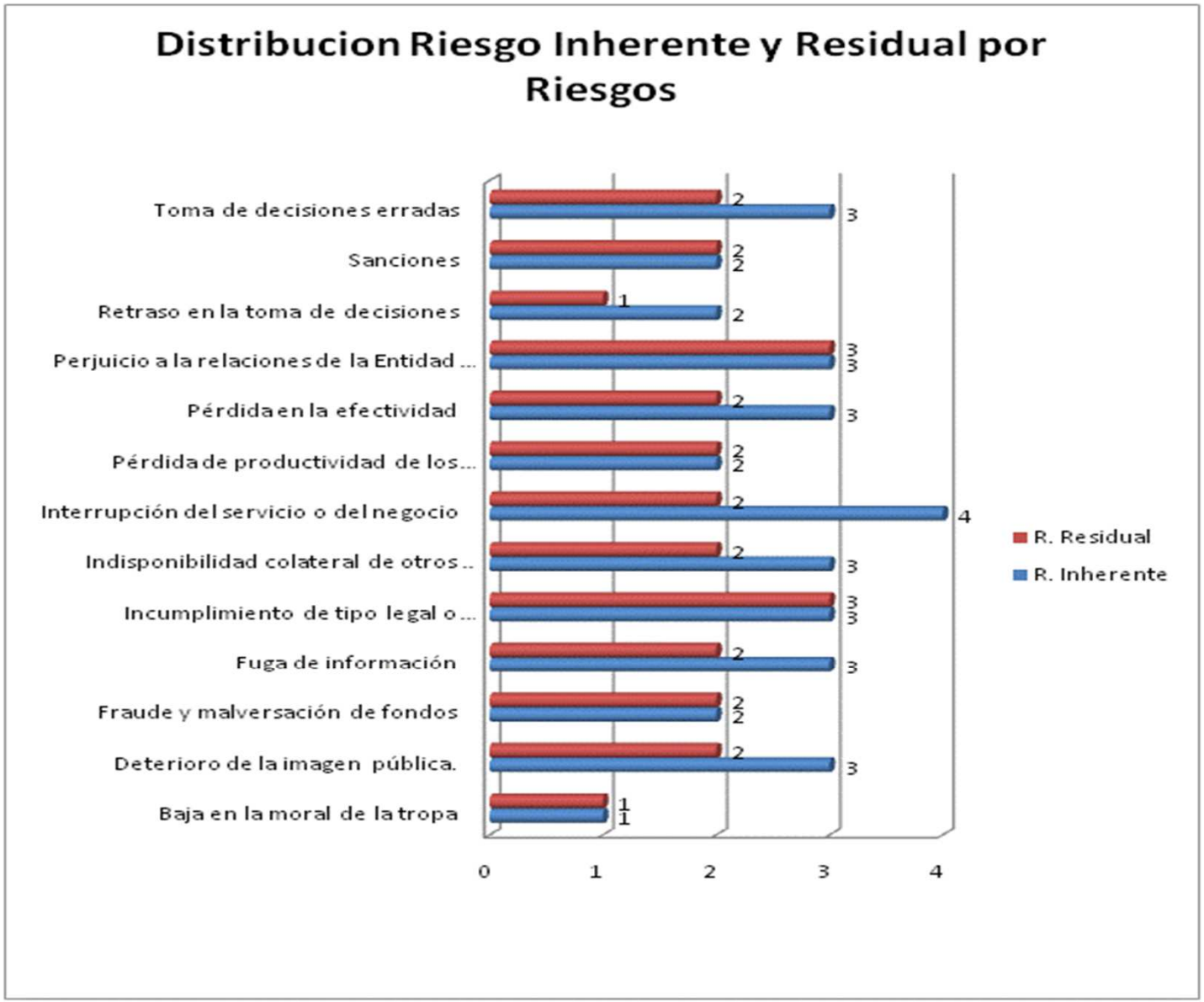
Se Evaluaron 50 Activos de información los cuales se encuentran clasificados bajo el siguiente esquema



Resultados Análisis de Riesgos



Resultados Análisis de Riesgos



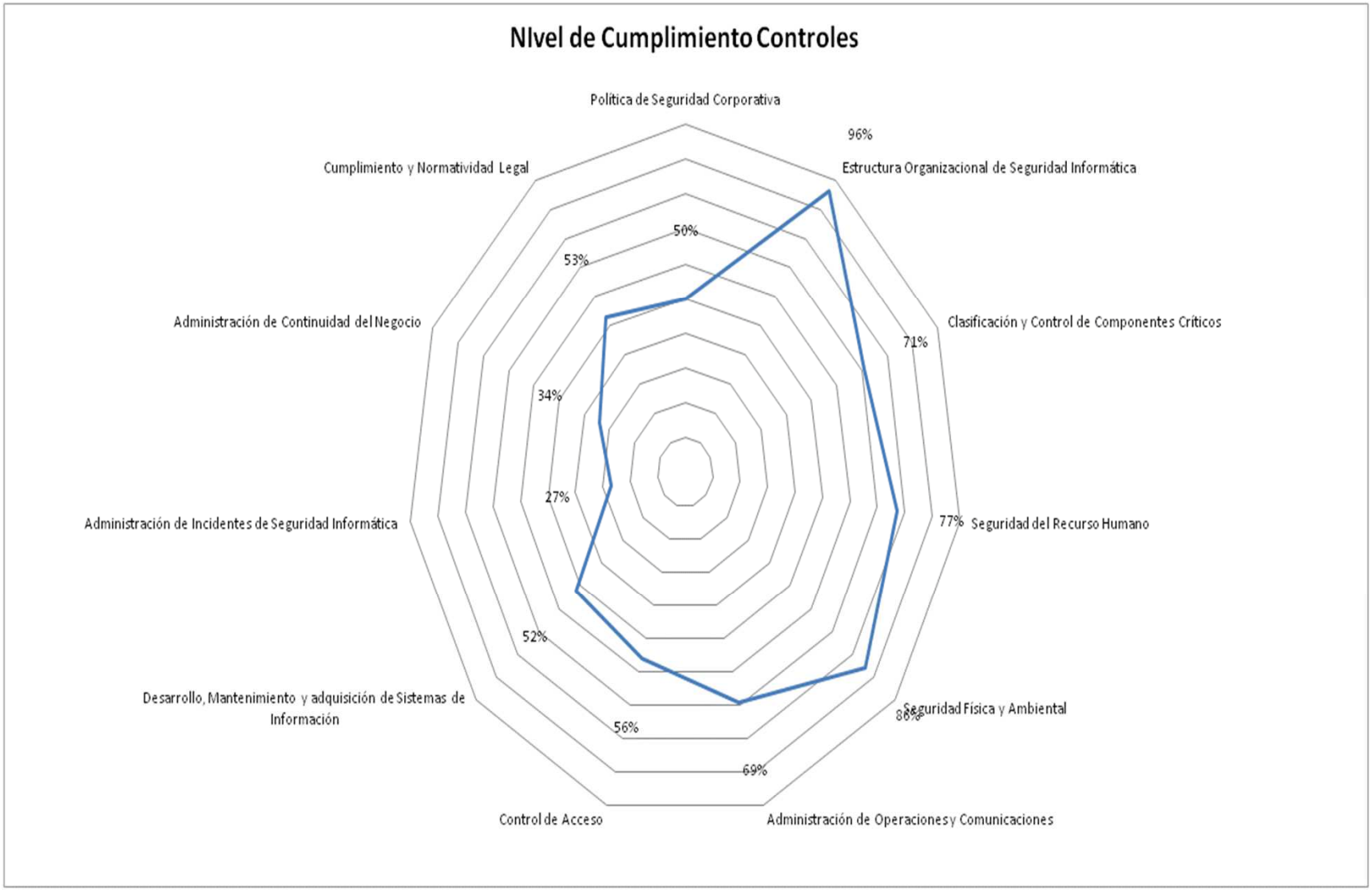
Nivel	Escala	
Bajo	B	1
Medio Bajo	M-	2
Medio	M	3
Medio Alto	M+	4
Alto	A	5

ANALISIS BRECHA ISO 27000

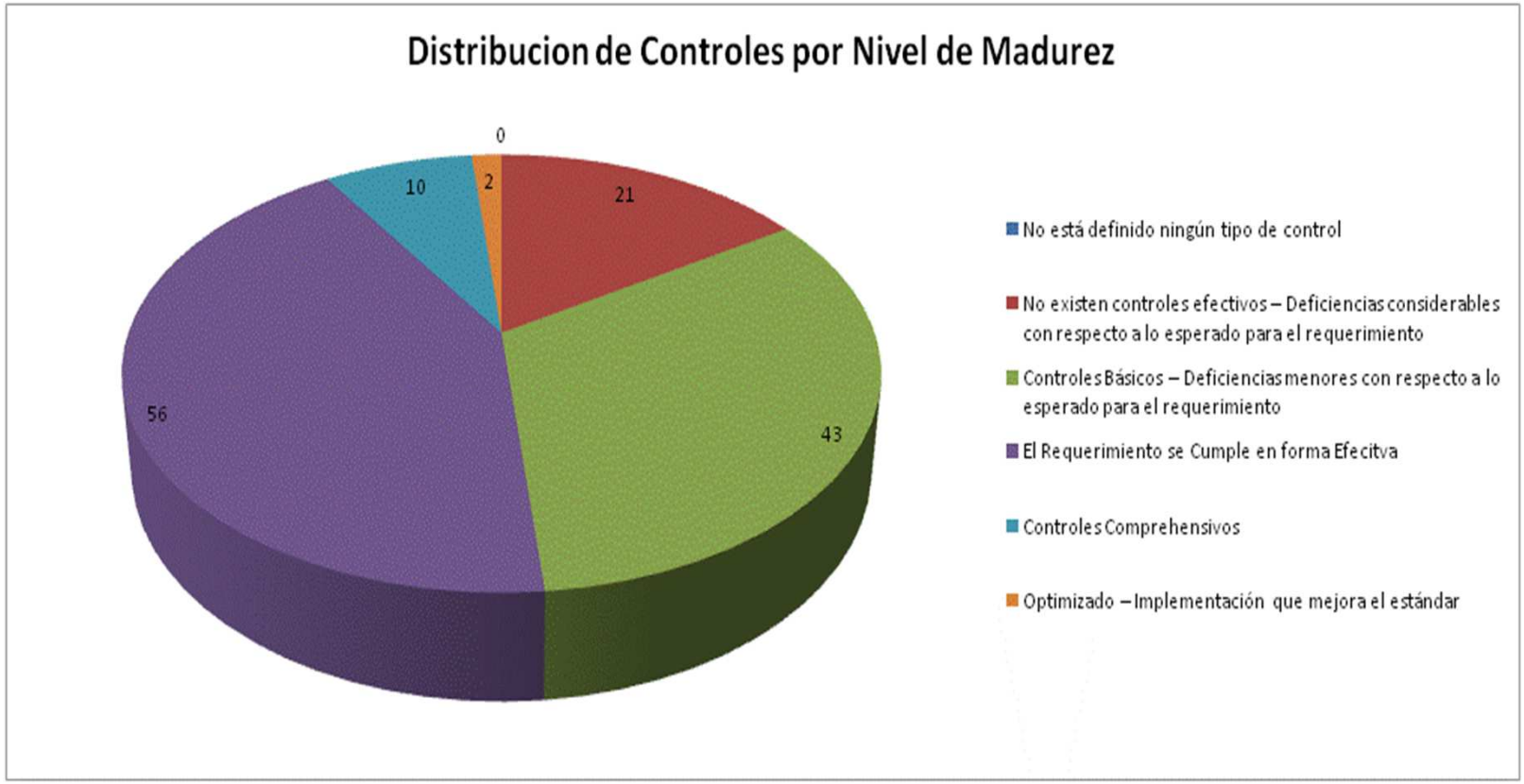
Porcentaje de Cumplimiento

Dominio	Aprobados	NO Aprobados	Porcentaje Cumplimiento
Política de Seguridad Corporativa	2	0	50%
Estructura Organizacional de Seguridad Informática	11	0	96%
Clasificación y Control de Componentes Críticos	5	0	71%
Seguridad del Recurso Humano	9	0	77%
Seguridad Física y Ambiental	13	0	86%
Administración de Operaciones y Comunicaciones	29	2	69%
Control de Acceso	25	0	56%
Desarrollo, Mantenimiento y adquisición de Sistemas de Información	16	0	52%
Administración de Incidentes de Seguridad Informática	5	0	27%
Administración de Continuidad del Negocio	5	0	34%
Cumplimiento y Normatividad Legal	10	0	53%

Porcentaje de Cumplimiento



Niveles de Madurez



PLANES DE ACCION

Planes de Acción

Comprenden las actividades que se recomendaron para reducir los riesgos significativos y que contribuyen a la implementación del SGSI.

El plan se ha clasificado de acuerdo a la prioridad con la cual los controles ayudan a reducir el nivel de riesgo inherente.

Prioridad Alta

Son controles que contribuyen de una forma más efectiva para evitar que las vulnerabilidades sean explotadas. La protección tiene un cubrimiento sobre múltiples vulnerabilidades. Dentro de las acciones a realizar en esta categoría están:

•Plan Estratégico de tecnología de Información: Duración 2 años. Costo por establecer

•Control de cambios: Duración 1 mes y estima en 160 Hora por un valor de 3.000.000 millones de pesos.

•Firewall interno / segmentación de redes: Duración 1 mes. Licenciamiento por un valor de $2.363.971 Pesos, implementación del firewall y de la segmentación de redes se estima en 4.000.000 con una duración de 4 meses trabajando medio tiempo.

•Sitio alterno: Duración 6 meses. Mensualmente se cobrara un valor de 5.000.000 (cinco millones de pesos) por el arrendamiento de servidores y canales de comunicación

Prioridad Alta

•Organización del Área de Seguridad de la Información: Definición (Duración 20 horas con un costo de 1 millón de pesos).

•Implementación de SGSI: Duración 6 meses y un Valor de 80.000.000

•Clasificación de la información: Duración 6 meses y un Valor de 4.000.000

•Endurecimiento: Duración 4 meses. Valor de 1.000.000 por servidor

•Ambientes independientes de producción, desarrollo y pruebas: Duración 4 meses por un valor de 3.949.003 por servidor (Valor total 7.898.006 pesos).

•Protección de datos de desarrollo: Duración 4 meses y los costos se cargaran al area de TI.

•Cuentas locales con privilegios de administración: Duración 1 mes por un valor de 1.500.000

Prioridad Alta

•Implementación de solución de Gestión de Identidad: Adquisición de la solución por 20.000.000 y un valor de licenciamiento anual de 4.000.00

•Cuentas de acceso: Duración de 1 mes y se utilizara una herramienta Open Source

•Controles varios – Centro de Cómputo: Duración de 1 mes por valor de 30.000.000

•Rack de piso: Duración de 1 mes por valor de 70.000.000.

Prioridad Media

Son controles complementarios que ayudan a elevar la efectividad de los controles y optimizar el nivel de protección.

•Puntos únicos de falla: Duración de 6 meses. El valor del Switch de Core (Catalyst 6500 4-Port 10 GigaBit) es de 31.228.900 millones y el switch de Core LAN (Cisco Catalyst 3750X-48P-L) es de 14.792.375 millones.

•Logs de auditoría: Duración 6 meses. Se usara una aplicación abierta para la centralización de Logs.

•Cuentas genéricas: Duración 2 meses. El costo de esta actividad se estima en 1.500.000

•Conexiones remotas: Duración 8 Meses. Los costos se asociaran al area de TI.

•Documentación de procedimientos: Duración de 2 Meses. Los costos se asociaran al recurso asignado por el area de calidad.

Prioridad Baja

Son controles que ayudan a evitar vulnerabilidades para situaciones particulares.

•Servidor de archivos: Duración de 12 meses. El valor es de 3.949.003 por servidor

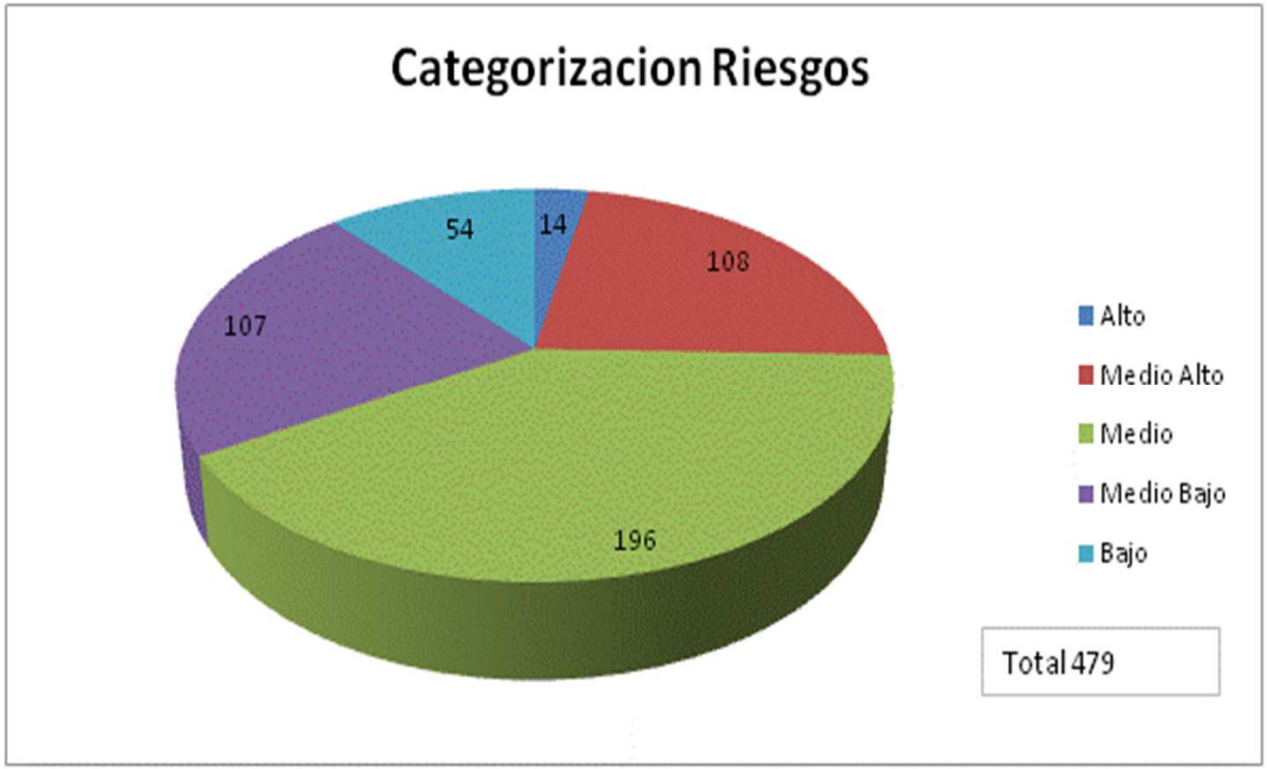
•Herramientas de gestión: Duración de 12 meses. El valor es de 3.949.003 por servidor

•Consola de gestión de red: Duración de 12 meses. El valor es de 3.949.003 por servidor

IMPACTO DE LAS IMPLEMENTACIONES

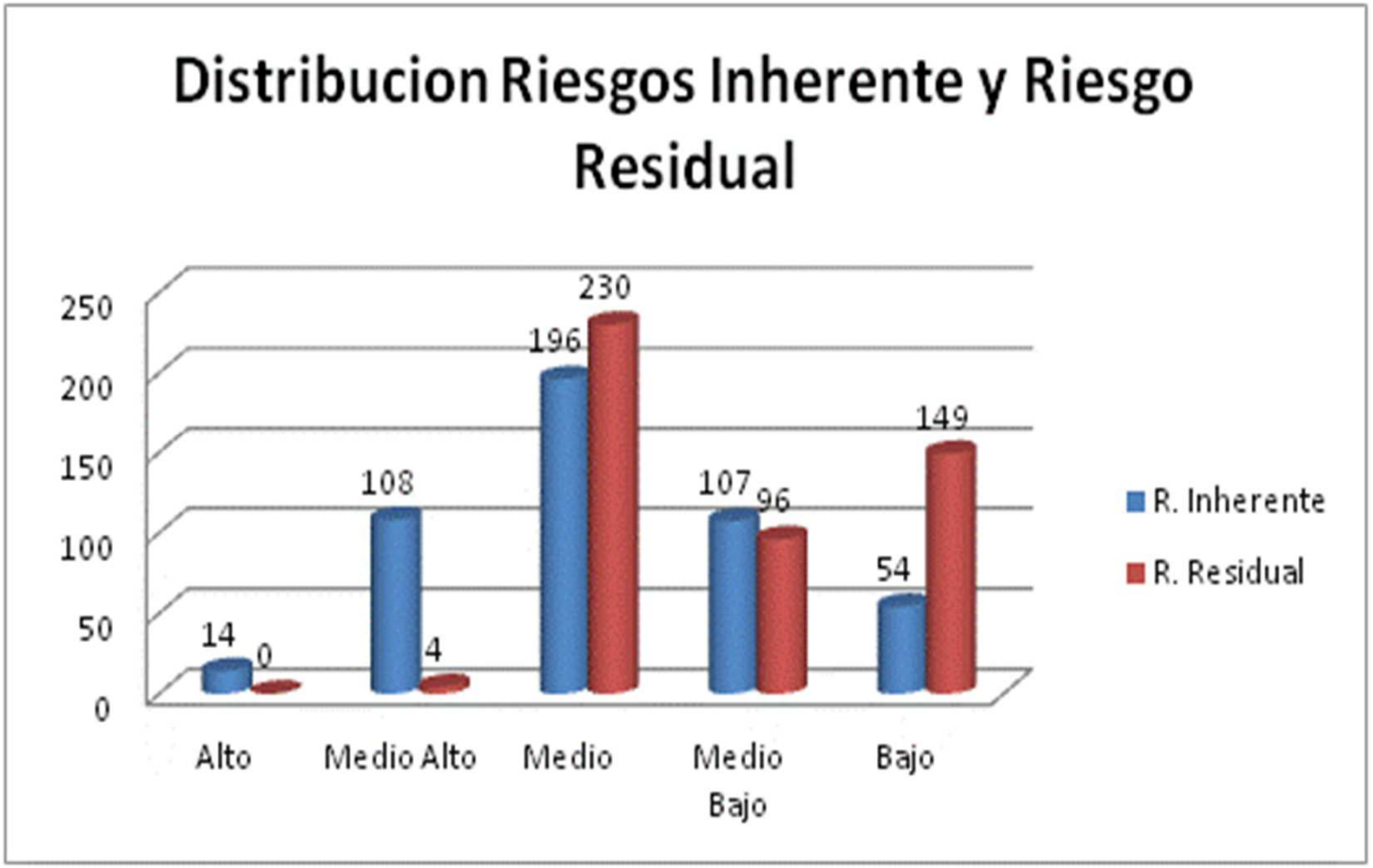
Riesgos

Del total de activos reportados, se identificaron 479 riesgos Inherentes (nivel de riesgo sin tener en cuenta la implementación de controles de seguridad) categorizados de la siguiente forma:



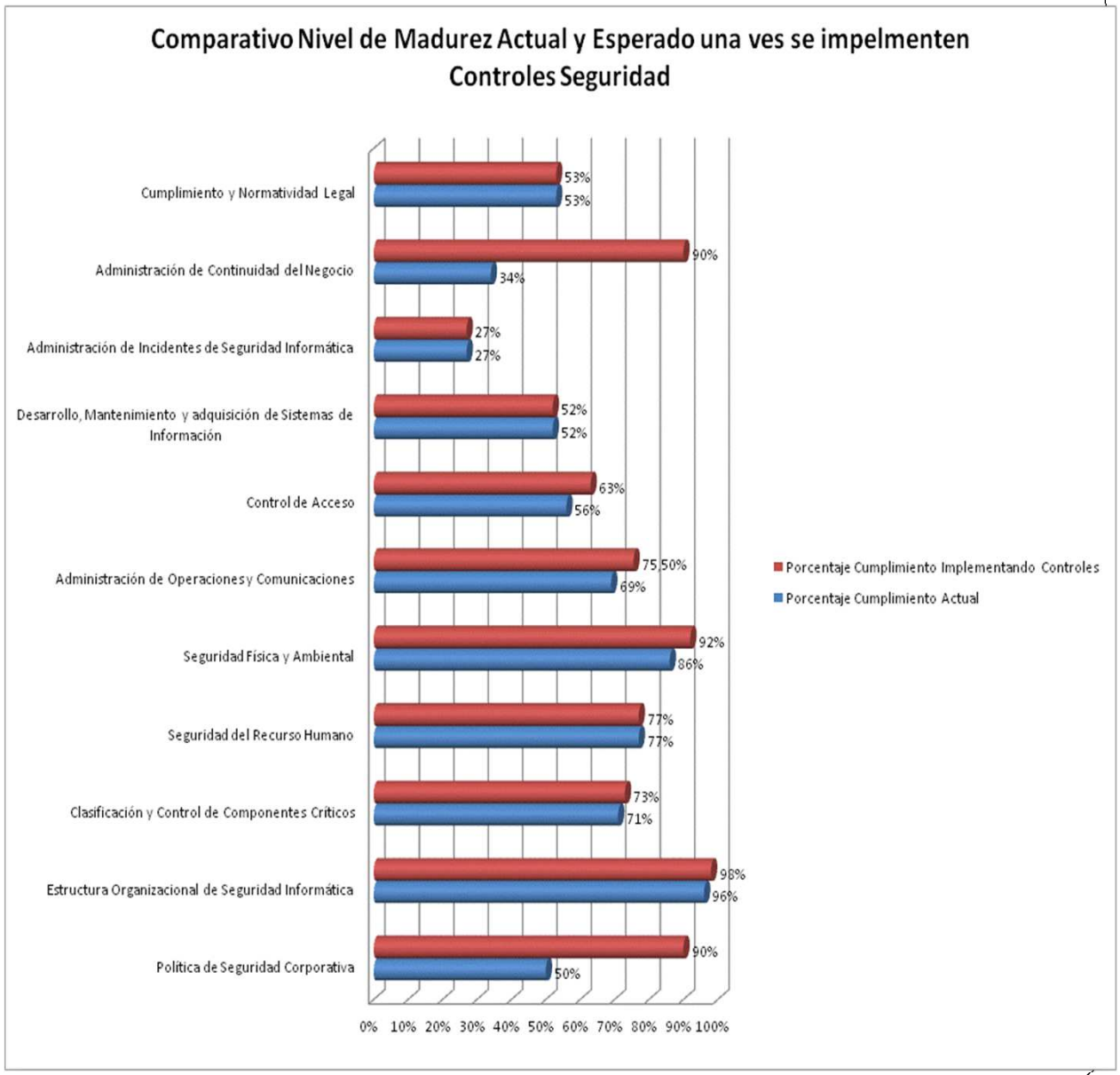
Riesgos

Podemos observar como una vez se implementen los controles propuestos y se ejecuten los proyectos definidos, los niveles de riesgos tienden a varias considerablemente.



Controles Seguridad

El otro enfoque para evaluar el impacto de los proyectos y controles de seguridad a implementar se da en los niveles de madurez en cada uno de los dominios definidos del estándar ISO 27002.



PREGUNTAS