INFORME EJECUTIVO

PLAN DIRECTOR DE SEGURIDAD PARA EL GRUPO ASD

Presentado por:
RICARDO ALBERTO DUITAMA LEAL

UNIVERSIDAD OBERTA DE CATALUNYA
MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES
BARCELONA, ESPAÑA
2013

INFORME EJECUTIVO

PLAN DIRECTOR DE SEGURIDAD PARA EL GRUPO ASD

Presentado por:
RICARDO ALBERTO DUITAMA LEAL

Tutor Asignado:
Antonio Jose Segovia Henares

UNIVERSIDAD OBERTA DE CATALUNYA
MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES
BARCELONA, ESPAÑA
2013

TABLA DE CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

1. MOTIVACION DEL PROYECTO

GRUPO ASD, la cual es la entidad de más alto nivel de planeamiento y dirección estratégica para las instituciones castrenses de Colombia, se encuentra en un proceso de mejoramiento y alineación de sus procesos de negocio que garanticen que funcionan de forma Eficiente y cumpliendo estándares internacionales (asociados s temas de calidad y de seguridad de la información).

De esta iniciativa general surgió la necesidad de Definir el Plan Director de Seguridad de la Información para el area de TI, 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.

Tal como se contemplo el proyecto se espera que se definan:

- Alcance del TFM y caracterización de la empresa: El objetivo es caracterizar la organización y definir el o los procesos sobre los cuales se desarrollara el presente proyecto.

- Identificación de Activos de Información: Una vez identificados el o los procesos a evaluar, se procederá a identificar cuáles son los activos de información que los soportan.

- Análisis de Riesgos: El análisis de riesgos permitirá identificar la situación actual de la organización y definir los controles para mantener un nivel de riesgo aceptable en la organización

- Definición del Plan Director de Seguridad: Este plan definirá la estrategia de toda la organización a corto, mediano y largo plazo.

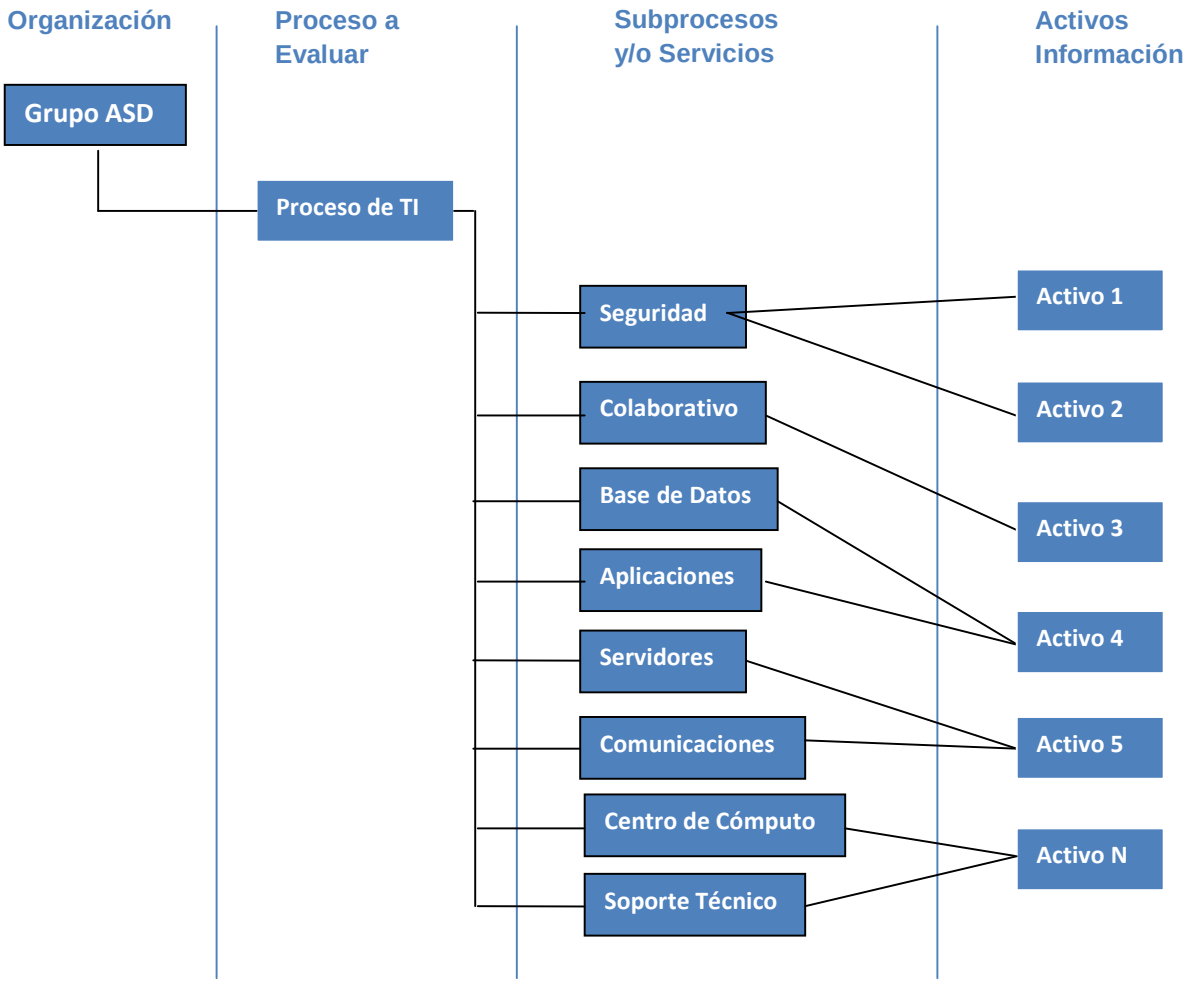
- Presentación de informes: Una vez realizado un diagnóstico del estado actual de seguridad y de definir el Plan Director de Seguridad, se procede a presentar los resultados a la alta dirección y a los diferentes sponsors para garantizar así el apoyo en todo los niveles de la organización.

2. ENFOQUE DEL PROYECTO

El presente proyecto definió el Plan Director de seguridad para GRUPO ASD, el cual estará alineado bajo los estándares ISO 27001 e ISO 27002 y la metodología de análisis de riesgos MARGERIT.

El alcance que se le darán serán los procesos más importantes del área de Tecnología de la información (TI) del GRUPO ASD. Es por ello que a continuación se mencionan los servicios y/o subprocesos que fueron analizados en el presente proyecto:

Figura 1. Alcance Análisis de Riesgos y SGSI



.

Las actividades estuvieron enfocadas en:

- Identificación de Activos Críticos para el proceso y subprocesos a evaluar.
- Realizar un proceso de análisis de riesgos bajo una metodología de riesgos identificando los riesgos y amenazas en cada uno de los activos de información.
- Realizar un análisis de Brecha para evaluar la situación actual de seguridad de la GRUPO ASD respecto a un estándar de buenas practica como lo es ISO 27002.
- Definición del Pan director para la organización teniendo como referencia el análisis de riesgo efectuado sobre los activos de información.
- 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.

3. CONCLUSIONES

Una vez se han llevado a cabo las diferentes actividades contempladas para definir el Plan Director de Seguridad de la Información, se mencionan las principales conclusiones de acuerdo a la actividad realizada.

3.1 Esquema General Plan Director de Seguridad de la Información

El PDSI se definió teniendo en cuenta los siguientes cuatro elementos

Figura 2. Esquema Plan director de Seguridad

- Situación Actual: Se realizo un análisis del estado actual de seguridad de la organización. Para ello el análisis de riesgo evaluó el nivel actual de seguridad de la organización, luego se definió a dónde quiere llegar la organización y se determinaron las actividades necesarias para cerrar esa brecha.

- Marco de Seguridad: Se Redefinieron los aspectos organizativos y se creo un marco normativo suficiente para regular la seguridad de la organización.

- Plan: Se elaboraron los planes de Acción necesarios para gestionar los riesgos detectados. De estos planes se definieron los proyectos que deberán ser gestionados para cumplir con el PDSI.

- Implementación y Seguimiento: Se realizar un seguimiento a la implementación del PDS para establecer la efectividad del plan trazado y reaccionar ante desviaciones que impacten en el negocio.

3.2 Análisis de Riesgos

- Se evaluaron 50 Activos de información los cuales se enuncian a continuación de acuerdo al servicio y modulo donde se encuentran funcionando:

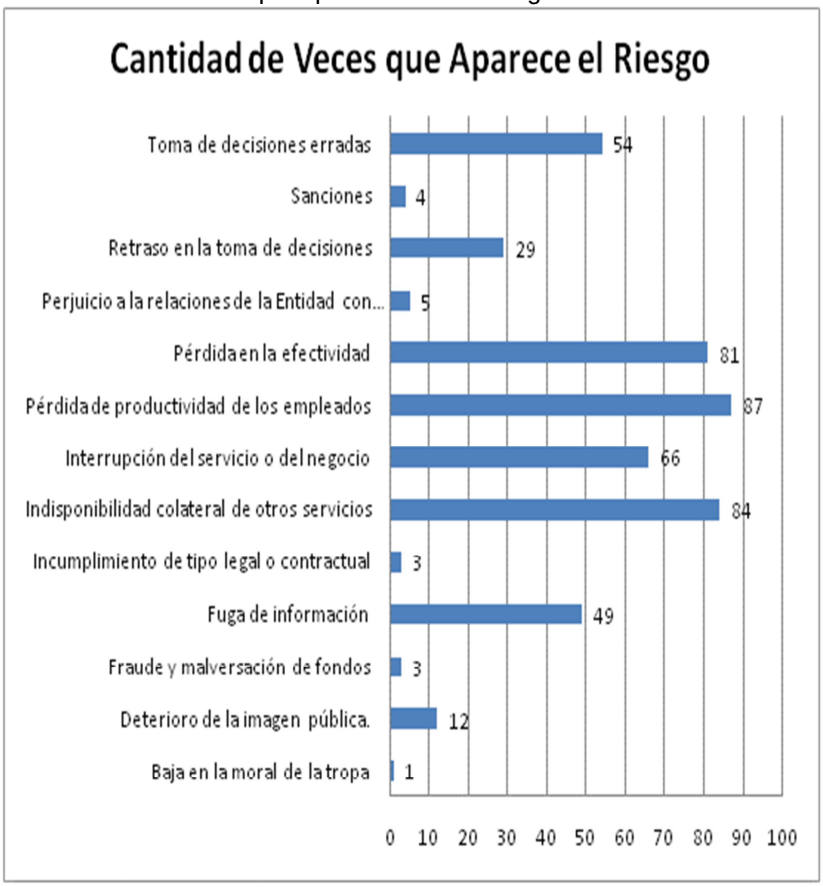
Tabla 1. Activos de Información

Proceso	Servicio	Módulo	Activos
Gestión de Tecnología Informática	Administración de seguridad	Administración Seguridad - Infraestructura	ASI-Firewall
			ASI-Switch Core de Seguridad
			ASI-IDS
			ASI-Encripcion Medios
			ASI-Antivirus
			ASI-AV Correo Interno
		Administración Seguridad - Gestión de SI	ASI-Gestión de SI
	Centro de Cómputo	Centro de Cómputo	Centro de Cómputo - Control de Acceso
			Centro de Cómputo – Instalaciones
			Centro de Cómputo – Cableado
			Centro de Cómputo - Control climático
			Centro de Cómputo – Comunicaciones
			Centro de Cómputo - Energía eléctrica
			Centro de Cómputo - Control del fuego
			Centro de Cómputo – Autenticación
			Centro de Cómputo – Ambiente
	Administración de comunicaciones	Comunicaciones - Infraestructura	Red-Switch Core
			Red-Router Internet
			Red-SW de Gestión
			Red-Switch de piso
		Comunicaciones - Gestión de Comunicaciones	Red-Gestión de Comunicaciones
	Soporte Técnico	Soporte Técnico - Infraestructura	ST–DMS
			ST–Analistas de soporte
			ST–Equipos PC portátiles

			ST –Equipos de escritorio
		Soporte Técnico - Gestión de Soporte	ST - Gestión de Soporte
	Desarrollo y mantenimiento de aplicaciones	Aplicaciones - Infraestructura	AP-Bodega de datos
			AP-APP1
	Administración de Servidores	Servidores - infraestructura	SRV-NAS 4000
			SRV-SAN
			SRV – Producción
			SRV – Pruebas
			SRV-OAS
			SRV - Controladores de dominio
			SRV - Correo electrónico
			SRV – NOMIFIN
			SRV – FINANCIERO
			SRV – APLICACIONES
			SRV – INTRANET
		Servidores – Gestión de Servidores	SRV - Gestion de servidores
	Administración de Bases de Datos	BD – infraestructura	BD - Base de datos de producción
		BD - Gestión de BD	BD - Outsourcing de DBA
			BD - Gestion de Base de datos
	Servicios de colaboración	Colaborativos - Infraestructura	COLABORATIVOS - Aplicativo Proxy
			COLABORATIVOS - Controlador Dominio
			COLABORATIVOS - Correo Electronico
			COLABORATIVOS - Portal Web
			COLABORATIVOS - Pagina Web
			COLABORATIVOS–Intranet
		Colaborativos – Gestión IT	COLABORATIVOS-Gestion Colaborativos

- Los riesgos que más fueron mencionados durante el análisis de riesgo fueron la Perdida de productividad de los empleados, Indisponibilidad colateral de servicios y Perdida en la efectividad. A continuación se muestra por riesgo la cantidad de veces que apareció durante el análisis de riesgos:

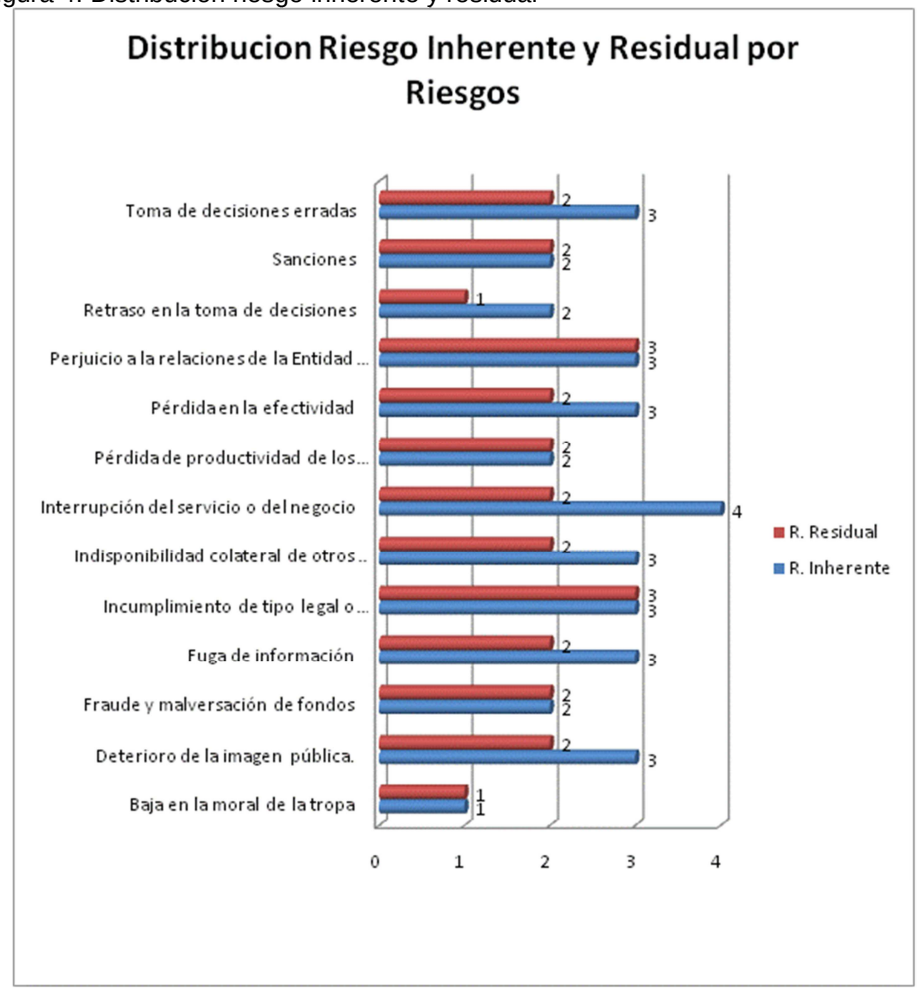
Figura 3. Número de veces que aparecieron los riesgos



- Otro factor a tener en cuenta es el nivel de riesgo inherente y residual, de esto podemos concluir que los riesgos con un mayor nivel de Riesgo Inherente (riesgo antes de implementar los controles) son:

  - Interrupción del servicio o del Negocio
  - Toma de decisiones erradas
  - Perjuicio a las relaciones de la entidad
  - Perdida en la efectividad
  - Indisponibilidad colateral de otros servicios
  - Incumplimiento de tipo legal o contractual
  - Fuga de información
  - Deterioro de la imagen pública.

Figura 4. Distribución riesgo inherente y residual



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

Una vez implementados los controles referidos en el plan de tratamiento de riesgos, se observa que los riesgos con un nivel de riesgo residual más alto son los siguientes:

- Perjuicio a las relaciones de la entidad
- Incumplimiento de tipo legal o contractual

3.3. Análisis de Brecha ISO 27001

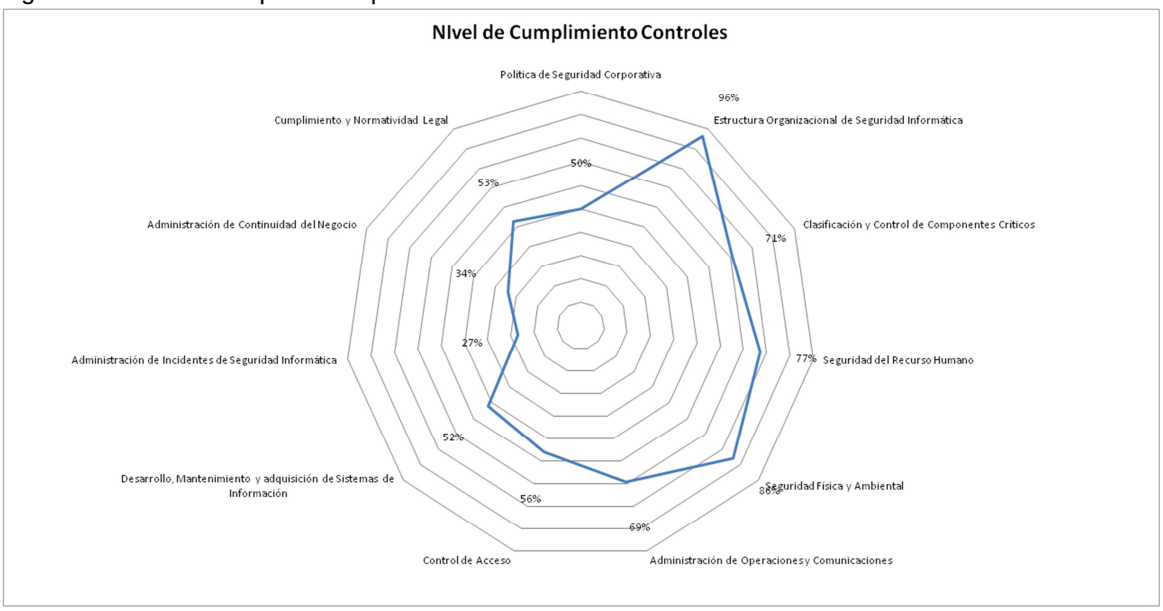
A continuación se describe los controles implementados y el porcentaje de cumplimiento por cada dominio:

Tabla 2. Porcentaje de Cumplimiento Controles

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%

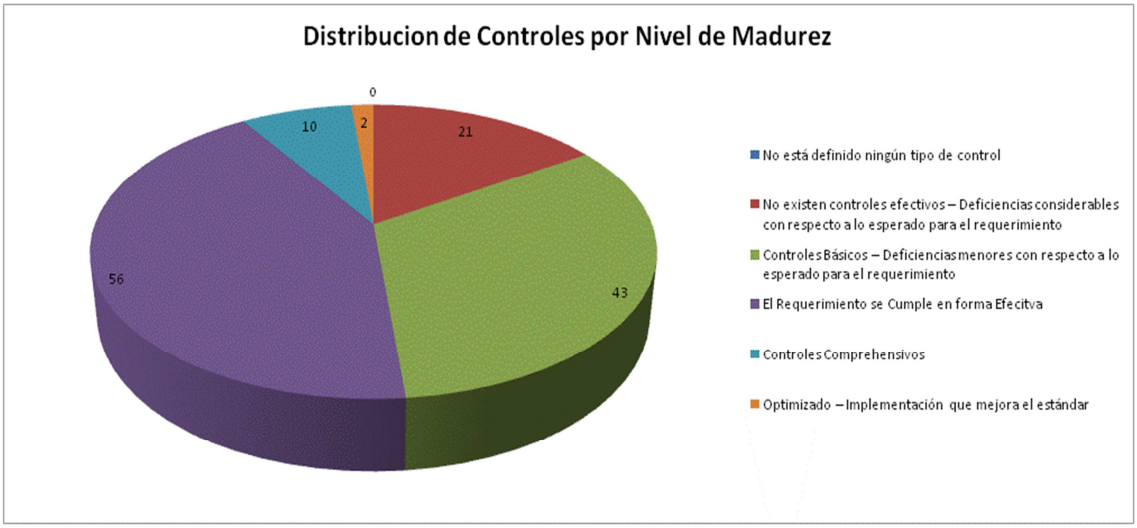
Observando el nivel de cumplimiento por dominio tenemos la siguiente grafica:

Figura 5. Nivel de cumplimiento por dominios



Si se evalúa por nivel de madurez, observamos que la mayora de controles se encuentran implementados de forma efectiva (L3) seguido de controles básicos (L2). Esto indica que hay un nivel aceptable de implementación de los controles planteados en la ISO 27002.

Figura 6. Controles por niveles de madurez



3.4. 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.

- 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
    - Control de cambios
    - Firewall interno / segmentación de redes
    - Sitio alterno
    - Organización del Área de Seguridad de la Información
    - Implementación de SGSI
    - Clasificación de la información
    - Endurecimiento
    - Ambientes independientes de: producción, desarrollo y pruebas
    - Protección de datos de desarrollo
    - Cuentas locales con privilegios de administración
    - Implementación de solución de Gestión de Identidad.
    - Cuentas de acceso
    - Controles varios – Centro de Cómputo
    - Rack de piso

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

    - Puntos únicos de falla
    - Logs de auditoría
    - Cuentas genéricas
    - Conexiones remotas
    - Documentación de procedimientos

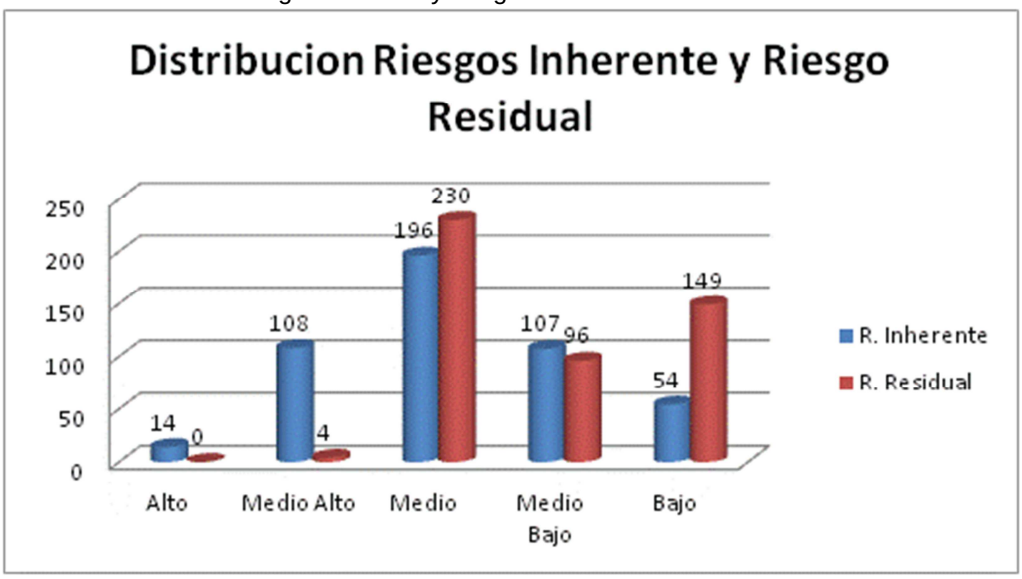
- Baja: Son controles que ayudan a evitar vulnerabilidades para situaciones particulares.

    - Servidor de archivos
    - Herramientas de gestión
    - Consola de gestión de red

3.5. Análisis Impacto Implementación Controles

Una vez finalizada la fase de definición de proyectos e identificando los controles a ser implementados, se hace necesario realizar un análisis del impacto que van a tener estos proyectos en el esquema de gestión de riesgos y en la política de cumplimiento respecto a la ISO 27002.

Figura 7. Distribución de Riesgo Inherente y riesgo Residual



Podemos observar como una vez se implementen los controles propuestos y se ejecuten los proyectos definidos, los niveles de riesgos tienden a varias considerablemente. Para la categoría de riesgos Altos se pasa de 14 riesgos identificados a 0; para los Medio Altos se pasa de 108 a 4; para los riesgos Medios se pasa de 196 a 230; aquí observamos un aumento el cual esta justificado porque mucho de los riesgos de la categoría de alto y medio altos debieron reducirse y caen en esta categoría.

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. A continuación se presenta el porcentaje de cumplimiento o nivel de madurez por dominio actual y el que se espera obtener una vez se han implementado los controles y proyectos de seguridad:

Figura 8. Comparativo Niveles Madurez