
Quito
DISTRITO METROPOLITANO

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

CENTRO DE POSTGRADOS
(MEVAST)

PREVIO A LA OBTENCION DEL TITULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

Tema: “Modelo de Evaluación y Monitoreo del cumplimiento de controles de gestión tecnológico para el Municipio del Distrito Metropolitano de Quito”

Autores:

Ing. Jacqueline Lala G.

Ing. Luis Daniel López

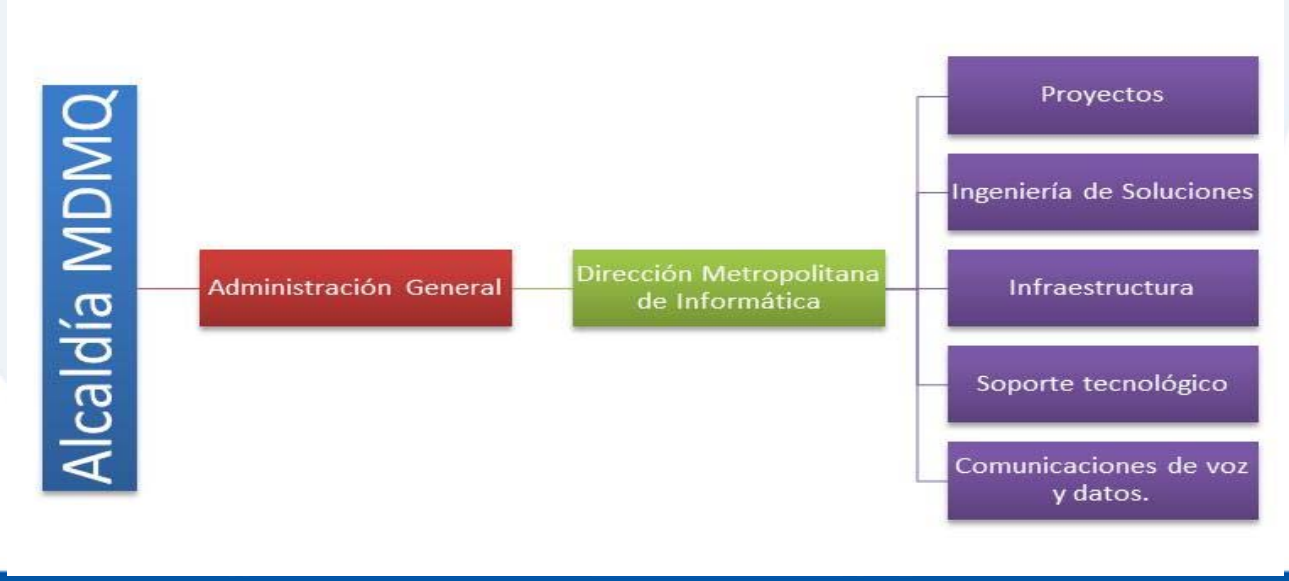
Sangolquí – Ecuador

2014

INDICE

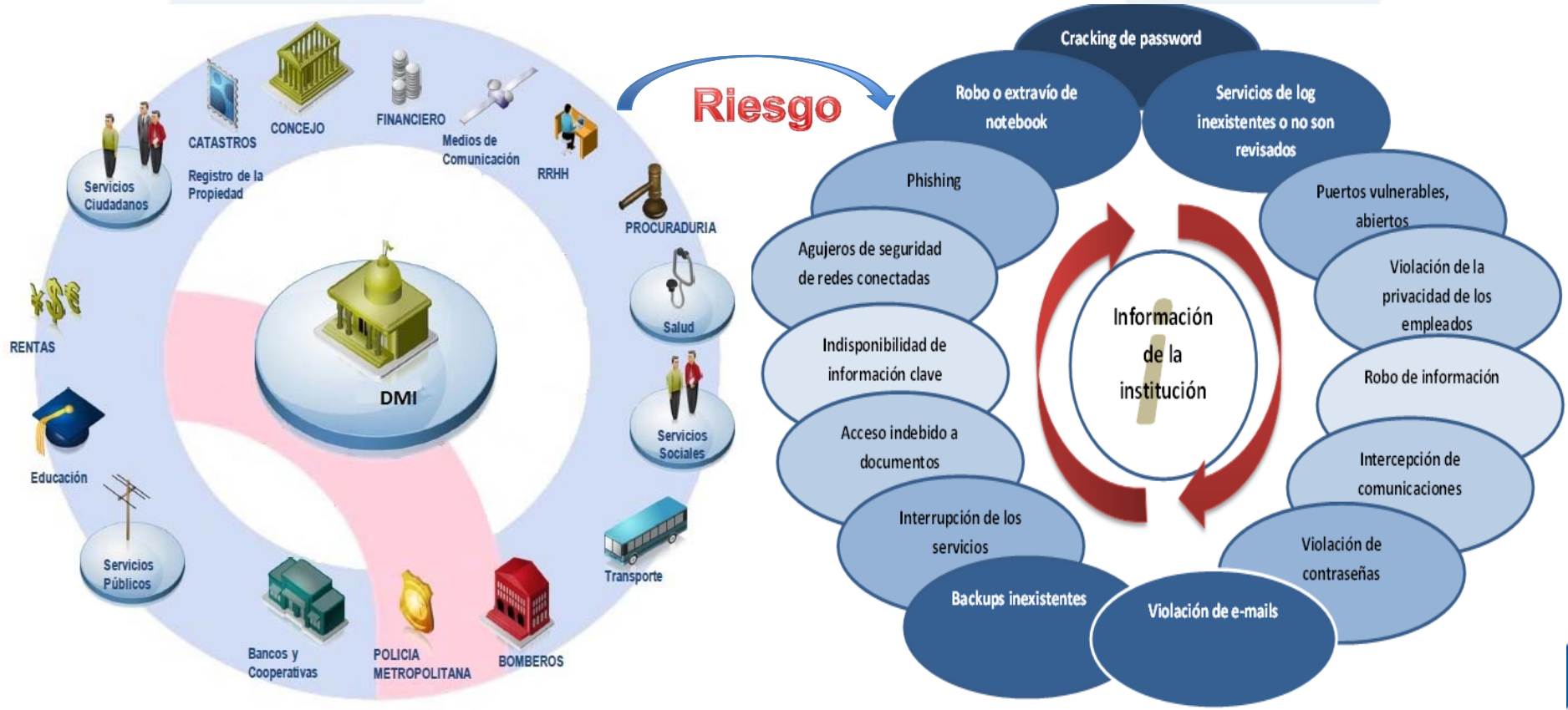
Antecedentes

- El Municipio del Distrito Metropolitano de Quito establece a la Dirección Metropolita de Informática como ente rector para emitir políticas que apoyen a la Gestión Tecnológica.
- La Dirección Metropolitana de Informática alinea al Plan Estratégico de Tecnologías de Información con el Plan de Gobierno Municipal y con las Normas de Control Interno.
- La Dirección Metropolitana de Informática apoyo a la gestión de gobierno local, por lo tanto, existe la necesidad de contar con un modelo de Evaluación y monitoreo estándar que permita la aplicación y monitoreo de cumplimiento de controles de forma continua.



Planteamiento del Problema

Hoy por hoy en la Dirección Metropolitana de Informática existen amenazas latentes que afectan a la seguridad y control tecnológico generando un conjunto de problemas.



Objetivo General

Crear un modelo de Evaluación y monitoreo del cumplimiento de los controles de gestión Tecnológica en el Municipio del Distrito Metropolitano de Quito MDMQ, a fin de establecer un marco de referencias estándar para la aplicación de controles de gestión tecnológica en sus dependencias.

Objetivos Específicos

- Analizar la normativa vigente donde se establezcan estándares de control interno y seguimiento de Gestión de TI, para evaluar la eficacia de los controles aplicados en la gestión e tecnología.
- Realizar el diagnóstico de la situación actual de la DMI y de los ejes estratégicos institucionales, referente al cumplimiento de las políticas para determinar el nivel de madurez utilizando la normativa vigente aplicando métodos de investigación de campo.
- Definir un modelo de control tecnológico que permita estandarizar los controles proactivos en las dependencias de la Municipalidad.
- Establecer experimentos y métodos que permitan validar el modelo sobre una muestra.

Hipótesis

Disminuir los niveles de riesgo de los controles en la mayoría de los casos tecnológicos establecidos por la DMI en el MDMQ, a través de un modelo de evaluación y monitoreo del cumplimiento de controles de gestión Tecnológica adaptado a la realidad municipal.

Marco Teórico

- Permita a las organizaciones mejorar las practicas de control interno.
- Evalúa la efectividad, eficiencia operacional y confiabilidad de la información financiera.

COSO

- Marco de referencia para la dirección TI
- Logro de objetivos del negocio

COBIT

- Conjunto de conceptos y prácticas para la gestión de servicios

ITIL

- Metodología de análisis y gestión de riesgos de la seguridad de la información
- Estudia los riesgos que soporta un determinado sistema de información y el entorno asociado.

MAGERIT

- Estándares de gestión de seguridad de la información
- Mejores practicas sobre la gestión

ISO 27000

ISO-27000

Norma	Título
ISO/IEC 27000:2009	Norma que explica cómo implantar un **Sistema de Gestión de Seguridad de la Información** en una empresa
ISO/IEC 27001:2005	Enfoque basado en procesos y especifica los requisitos
ISO/IEC 27002:2005	Guía de buenas prácticas, describe los objetivos de control y controles de seguridad de la información, contiene 133 controles, 39 objetivos de control agrupados en 11 dominios.
ISO/IEC 27003:2010	Guía que se encarga de aspectos críticos necesarios para el diseño e implementación de un SGSI
ISO/IEC 27004:2009	Guía para el desarrollo y utilización de métricas y técnicas de medida que determina la eficacia de un SGSI
ISO/IEC 27005:2011	Directrices para la gestión del riesgo en la Seguridad de la Información
ISO/IEC 27006:2011	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Diagnóstico

Metodología

Análisis y valoración

Identificar activos

- Servicios
- Datos
- Aplicaciones
- Equipos Informáticos
- Redes de comunicaciones
- Soporte de información
- Instalaciones

Análisis de riesgos

Mapa de riesgo basado en la ISO 27005:2012.

Riesgo= Probabilidad X Impacto.

La escala de Riesgo se define con los niveles: Alto, Medio Alto, Medio Bajo, Medio Bajo, Bajo.

Análisis de impacto

- Integridad
- Disponibilidad
- Confidencialidad

Determinar probabilidad

De acuerdo a la ISO 27002, el porcentaje de riesgos identificado, se evalúa como :

- Alta
- Media alta
- Medio
- Medio bajo
- Bajo

Tamaño de la muestra

- Secretarías (27)
- Administraciones zonales (27)
- Dependencias (20)
- Áreas de la DMI (30)

Diagnóstico

Activos de información

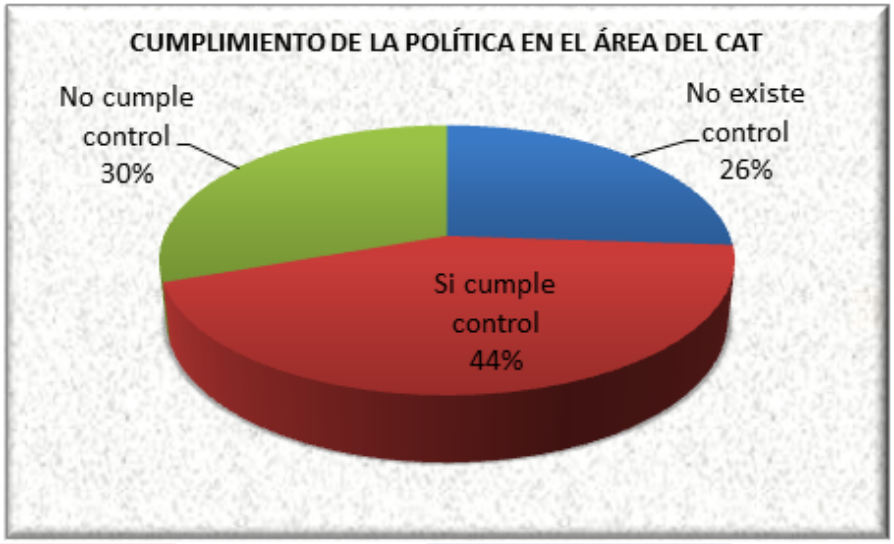
Activos	Escala Cualitativa	Escala cuantitativa	Descripción	Impacto
Servicios	Alto	5	Más de $32.000.001 mensuales	5
Datos/ información	Medio Alto	4	de $ 24.000.001 - $32.000.000	5
Aplicaciones	Medio	3	de $16.000.0001 - $24.000.000	5
Equipos	Medio Bajo	2	Hasta $16.000.001	4
Redes de comunicacio nes	Bajo	1	Hasta $800.000	4
Soporte de información				4
Equipamient o auxiliar				5
				3

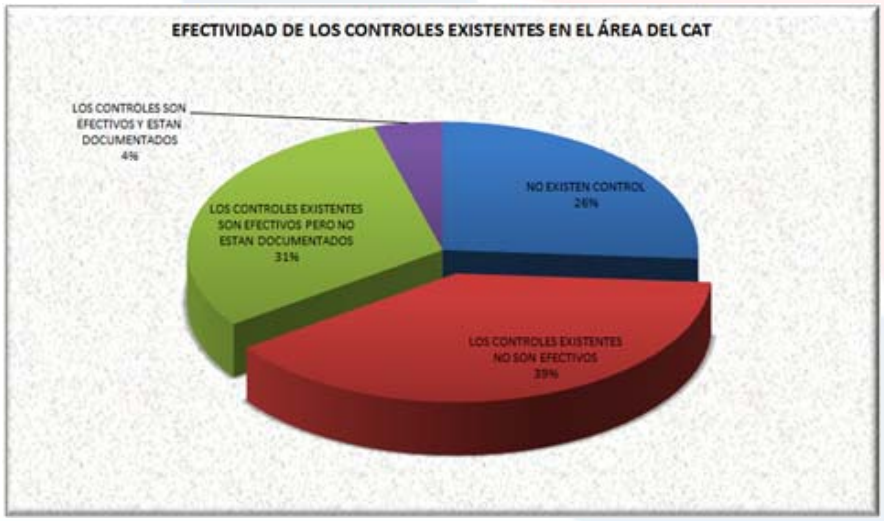
Total (Valor estimado) = $64.700.000

Diagnóstico

Área de Centro de Atención Tecnológica

	Vulnerabilidad del Area CAT
Zona inaceptable	Pérdidas de activos físicos y lógicos
Zona moderada	Falta de control en la determinación de IP públicas
	Ausencia de documentación para actualizacion del Hardware
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de documentación para actualizacion e inventario del Hardware
	Ausencia de un eficiente control de cambios en la configuración y adquisición de hardware
	Ausencia de promocion y repositorio de manuales técnicas
Zona tolerable	Incumplimiento en el mantenimiento del cableado
	Ausenia de Inventario de la parte interna del equipo
	Ausencia de politicas para el uso correcto de internet y mensajeria
	Ausencia de acuerdos de niveles de servicio, o insuficiencia de los mismos
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Existencia de código malicioso (virus, troyano)
Zona aceptable	Ausencia de documentaciòn para actualización de manuales técnicos





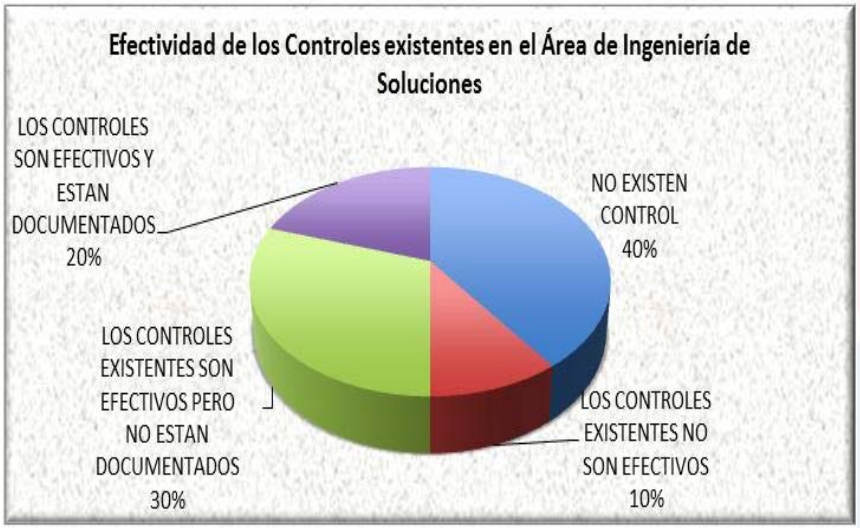
	Amenanzas del área CAT
Zona inaceptable	Destrucción de equipos o de medios.
	Ausencia de procedimiento formal para el registro y retiro de usuarios
Zona moderada	Falta de actualizaciones al Software
	Acceso forzado al sistema
	Error en el uso
	Abuso de derechos
Zona tolerable	Pérdida de equipos
	Incumplimiento en el mantenimiento del sistema de informaciòn
	Falta de difusion de los conocimiento
	Uso no autorizado del equipo
Zona Aceptable	Falta de actualizaciones al Hardware

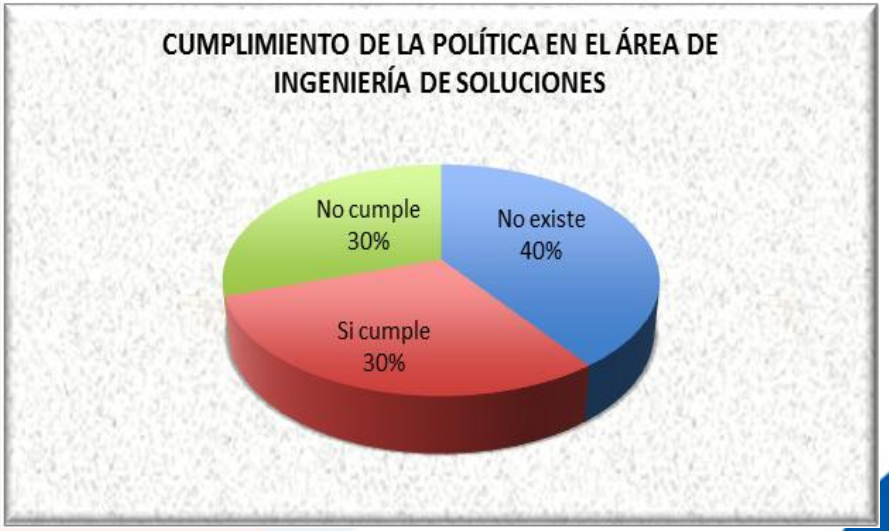
Diagnóstico

Área de Ingeniería de Soluciones

	Vulnerabilidades de Ing, Soluciones
ZONA INACEPTABLE	Inexsistencia de procedimiento y proceso para rendimiento de software
	Incumplimiento en el mantenimiento de los SI
	Ausencia de procedimientos de control de cambios
ZONA MODERADA	Ausencia de procedimiento para aceptar el software
	Ausencia de promocion de manuales técnicas
	Inexsistencia de procedimiento para tener los derechos de autor
	Ausencia de procedimiento para la encriptación de información
ZONA TOLERABLE	Ausencia de procedimiento de para desarrollo de software
	Ausencia de procedimiento de para la arquitectura de software
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario

	Amenazas de Ing.Soluciones
ZONA INACEPTABLE	Mal funcionamiento del software
	Abuso de derechos
ZONA TOLERABLE	Falta de difusion de los conocimiento
	Falsificación de derechos



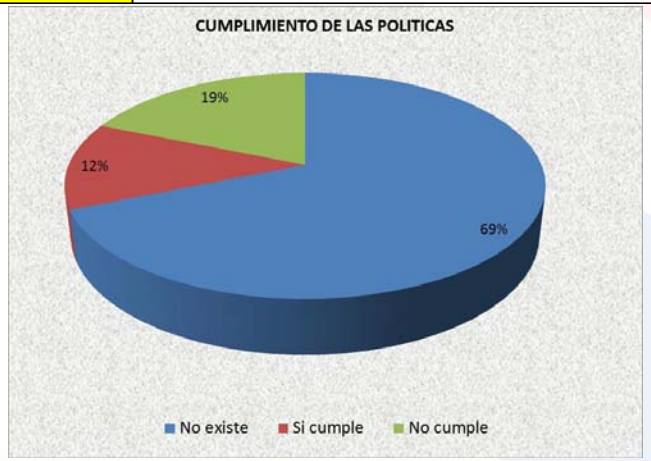


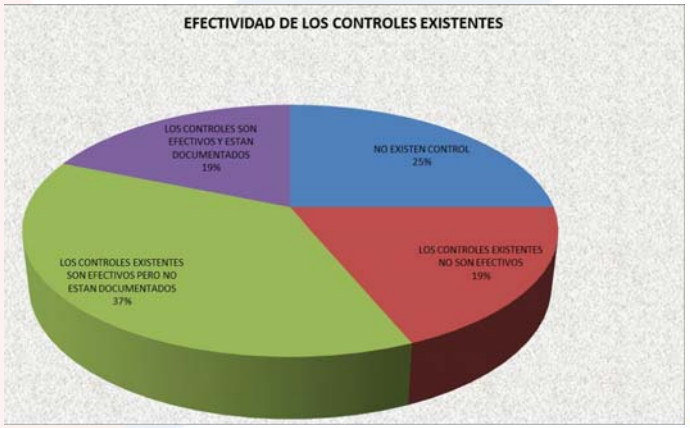
Diagnóstico

Área de Redes

REDES	Vulnerabilidad
ZONA INACEPTABLE	Falta de control en la depuración de IP públicas
	Contraseñas sin protección dispositivos de seguridad perimetral y de red
	Ausencia de cambio regulares en las Contraseñas de los dispositivos de seguridad perimetral y de red
	Ausencia de procedimientos para manterner la seguridad de los medios físicos en movimiento.
ZONA MODERADA	Ausencia de procedimientos para administración de incindentes
	Ausencia de procedimientos para la recolección de evidencia de los incidentes de los SI
	Ausencia de procedimientos que detallen debilidades de seguridad de incidentes
	Ausencia de promocion de manuales técnicas
	Gestión inadecuado de la red (tolerancia a fallas en el enrutamiento)

Redes	Amenazas
Zona inaceptable	Falsificación de derechos
	Espionaje remoto, abuso de derechos.
	Abuso de derechos
Zona moderada	Falta de difusion de los conocimiento
	Saturación del sistema de información





Diagnóstico

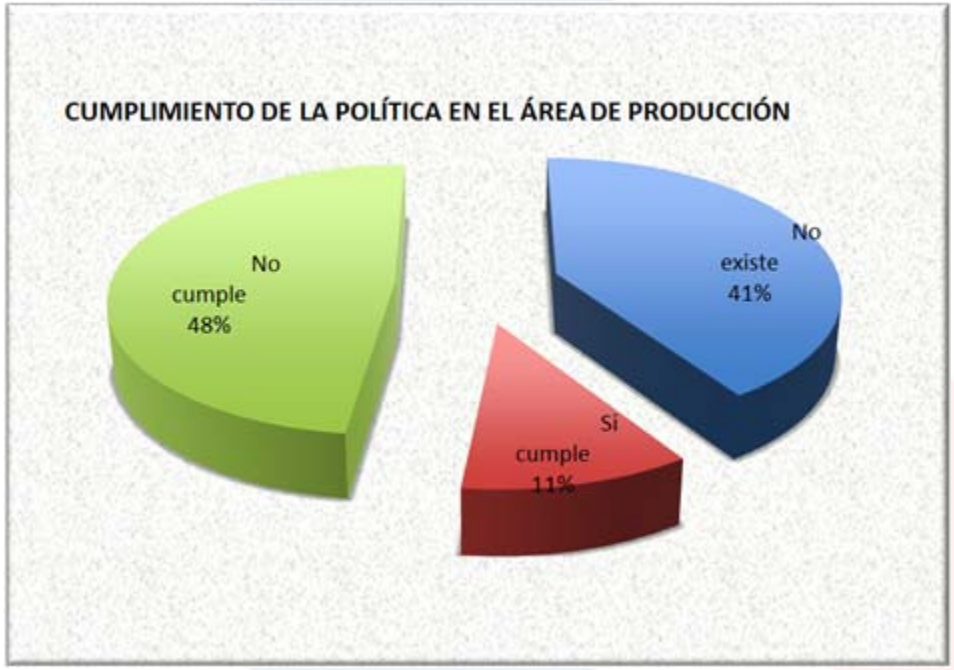
Área de Infraestructra

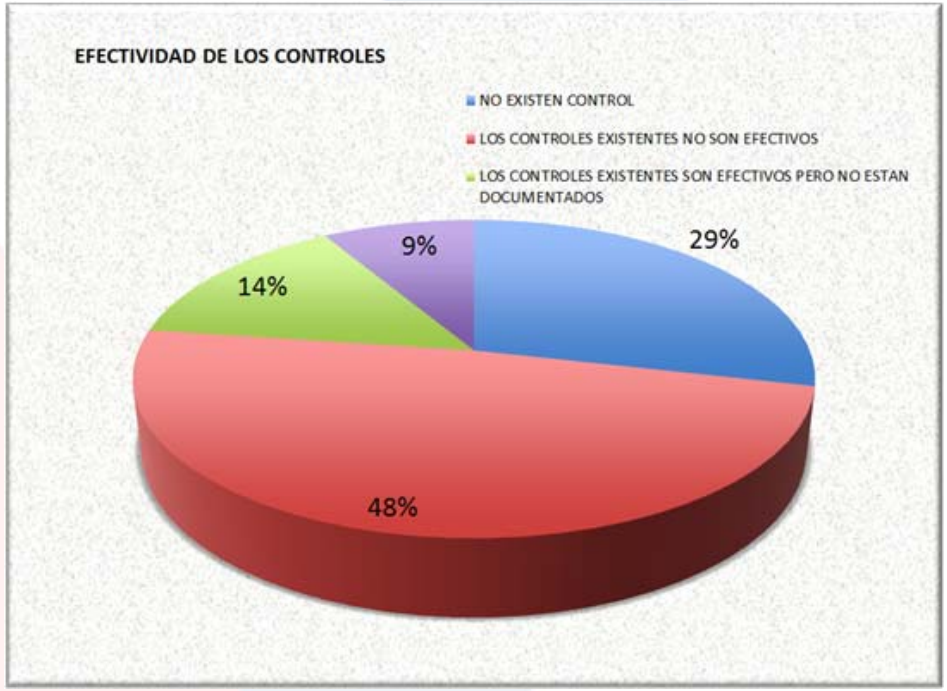
PRODUCCIÓN	Vulnerabilidad
Zona inaceptable	Ausencia de plan de continuidad (sitio alterno)
	Ausencia de documentación para actualizacion e inventario del Hardware
	Ausencia de auditorías (supervisiones) regulares
Zona Moderada	Ausencia de respaldo de informacion
	Ausencia de bitacoras o registro de las claves entregadas
	Ausencia de control de cambios en los aplicativos
	Ausencia de respaldo de las bases de datos
	Ausencia de mecanismos de autorizacion de acceso y carda de datos a las Bases de datos
	Ausencia de respaldo de la configuración de la virtualización
Zona Tolerable	Ausencia de procedimientos para disponibilidad de servicio
	Ausencia de procedimientos para el ingreso de áreas sensibles
	Ausencia de documentación para la actualizacion y pruebas del Software
	Ausencia de procedimientos de seguridad que controlen la fuga de información
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Ausencia de procedimientos seguridad para el control de la clasificacion de informacion
	Almacenamiento sin protección
	Ausencia de disponibilidad de servicio
	Tabla de contraseña sin proteccion
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de promocion de manuales técnicas
	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de documentación para mantener la seguridad en el suministro de electricidad
	Ausencia de procedimientos para proteger los sistemas operativos

PRODUCCIÓN	Amenazas
Zona inaceptable	Falta de actualizaciones al Hardware
	Falla en los sistemas
Zona Moderada	Abuso de derechos
	Falta de actualizaciones al Software
	Pérdida de las bases de datosdatos
	Hurto de medios o documentos
	Perdida de la configuración de virtualización
	Mal funcionamiento del software(aplicativo)
	Ingreso de persona no autorizado
Zona Tolerable	Manipulacion de los equipos por personal no autorizado
	Subir bases de datos con errores
	Pérdida de información
	Uso no autorizado de la informacion
	error en el uso
	Falta de difusion de los conocimiento
	No existe disponibilidad en los servicios de la institución.
	corrupcion de datos, inexsistencia de encriptación

Diagnóstico

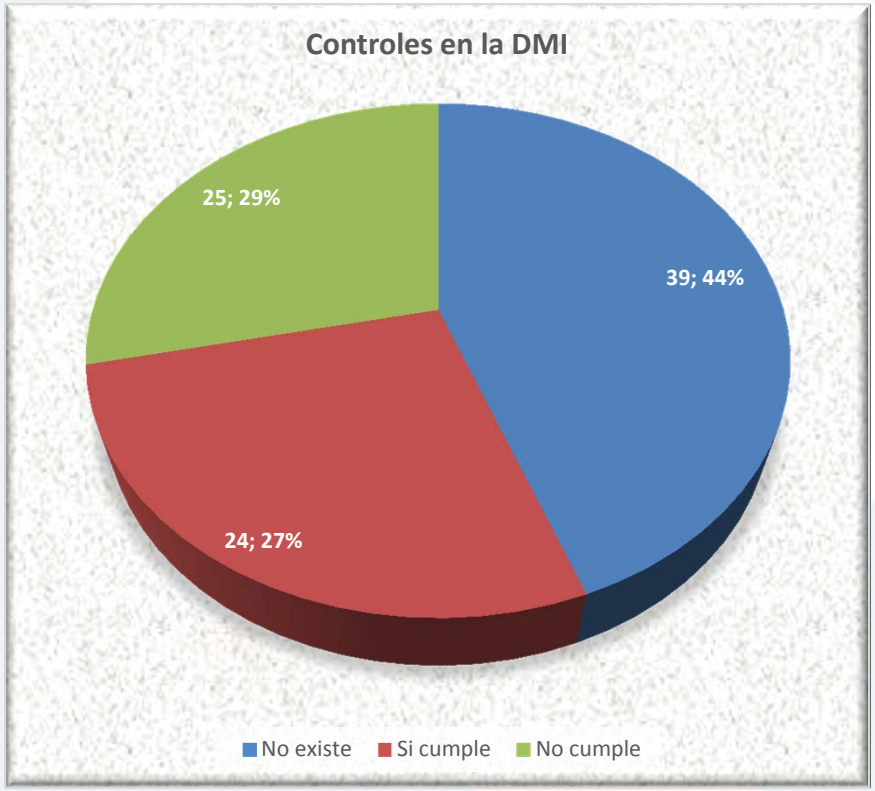
Área de Infraestructra





Diagnóstico

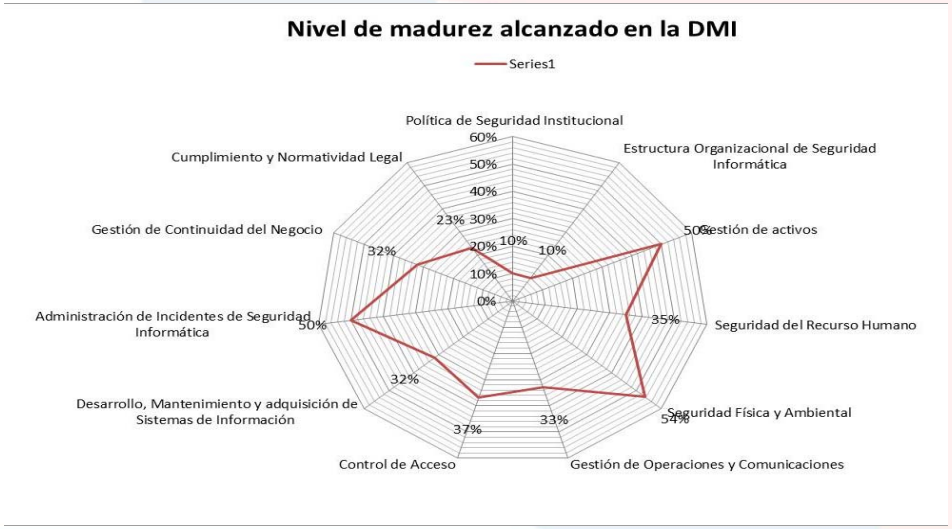
Efectividad de los controles en la DMI

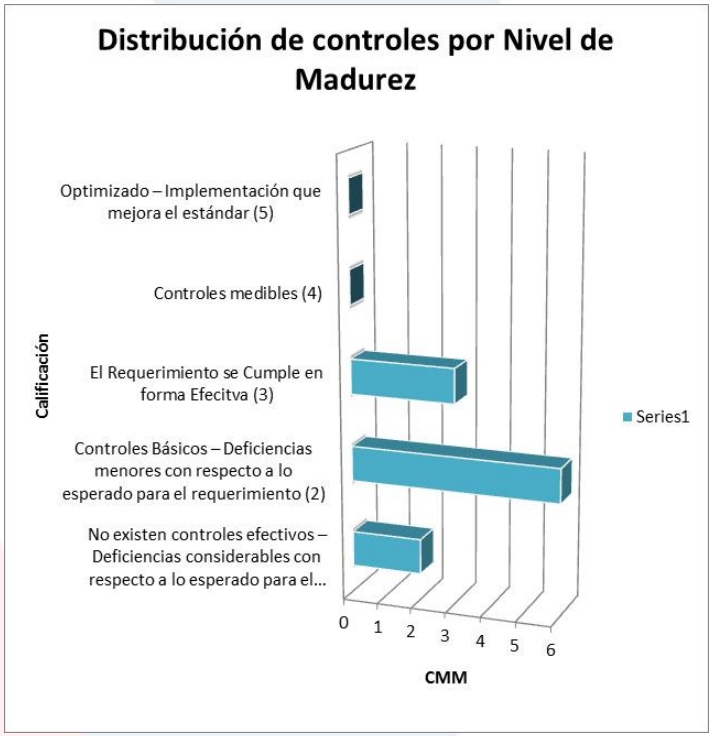


Diagnóstico

Nivel de Madurez de la DMI

Dominio	Nivel de madurez	Controles existentes	Controles no existentes	Porcentaje Cumplimiento
Política de Seguridad Institucional	1	2	0	10%
Estructura Organizacional de Seguridad Informática	1	10	1	10%
Gestión de activos	3	5	0	50%
Seguridad del Recurso Humano	2	8	1	23%
Seguridad Física y Ambiental	3	11	2	54%
Gestión de Operaciones y Comunicaciones	2	26	9	33%
Control de Acceso	2	14	11	37%
Desarrollo, Mantenimiento y adquisición de Sistemas de Información	2	16	0	32%
Administración de Incidentes de Seguridad Informática	3	5	0	50%
Gestión de Continuidad del Negocio	2	5	0	32%
Cumplimiento y Normatividad Legal	2	10	0	23%





Diagnóstico

Riesgo de la DMI

La línea de base de la madurez de la DMI se define por:

- El Impacto por dominio se obtiene del promedio de los impactos obtenidos para cada control.
- El Indicador por dominio se obtiene de la media ponderada del impacto y el indicador de cada control.
- El riesgo % es el valor del porcentual del riesgo de cada dominio.

Dominio de la ISO 27002	Impacto por dominio	Indicador por dominio	Riesgo	Riesgo %
1.- Política de Seguridad	5,00	5,00	25,00	100,00
2.- Estructura Organizacional de Seguridad Informática	5,00	5,00	25,00	100,00
3. - Gestión de activos	4,20	2,93	12,30	49,20
4.- Seguridad del Recurso Humano	3,00	4,44	13,33	53,33
5.- Seguridad Física y Ambiental	4,37	2,14	9,33	37,33
6.- Gestión de comunicaciones y operaciones	4,63	3,12	14,44	57,78
7.- Control de Acceso	4,71	3,42	16,13	64,50
8.- Desarrollo, Mantenimiento y adquisición de Sistemas de Información	4,80	3,24	15,53	62,13
9 - Administración de Incidentes de Seguridad Informática	4,60	3,00	13,80	55,20
10. - Administración de Continuidad del Negocio	5,00	2,80	14,00	56,00
11 - Cumplimiento y Normatividad Legal	4,10	3,09	12,67	50,67
Riesgo total				**60,44 %**

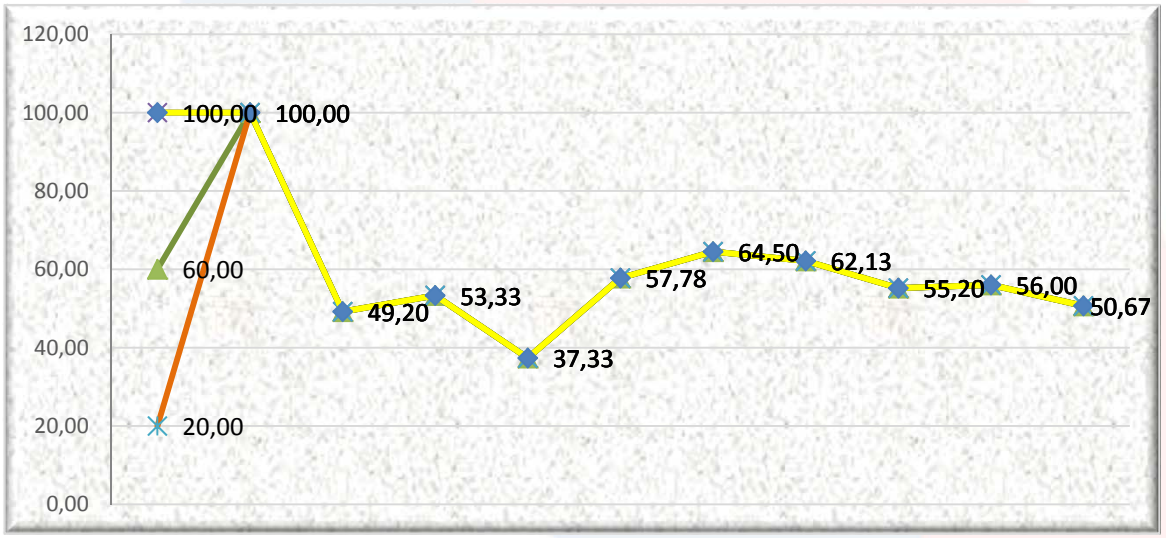
Modelo

Experimentación D1

1.- Política de Seguridad (D1)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
5	5	25	100	1	5	20	3	15	60	5	25	100

Riesgo por nivel de exposición	
Línea base	60,44 %
Al minimizar	53,17 %
Medio	56,18 %
Al maximizar	60,44 %

Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%

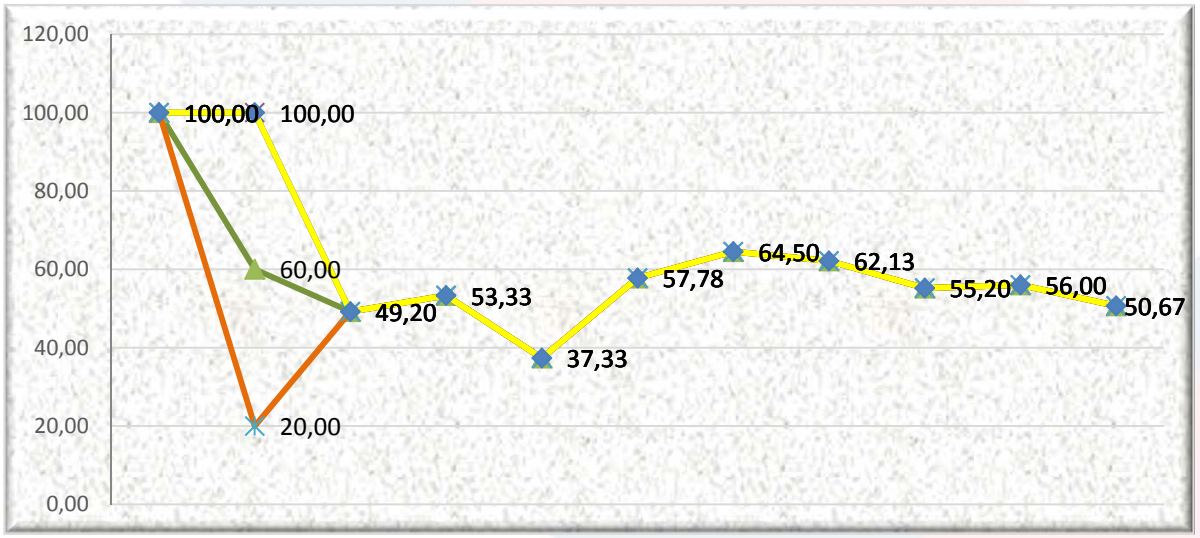


Modelo

Experimentación D2

2.- Estructura Organizacional de SI (D2)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
5	5	25	100	1	5	20	3	15	60	5	25	100
Riesgo por nivel de exposición	Línea base					60,44 %						
	Al minimizar					53,17 %						
	Medio					56,18 %						
	Al maximizar					60,44 %						

Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%

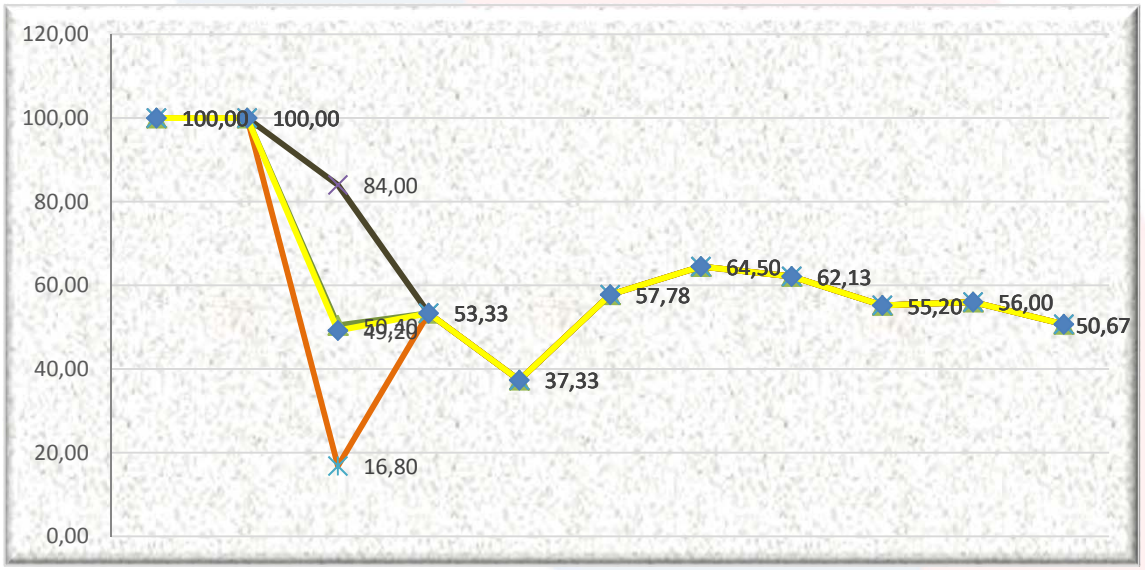


Modelo

Experimentación D3

3.- Gestión de activos (D3)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,2	2,9	12,3	49,2	1	4	16,8	3	12,6	50,4	5	21	84
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					57,50 %			
				Medio					60,55 %			
				Al maximizar					63,61 %			

Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%

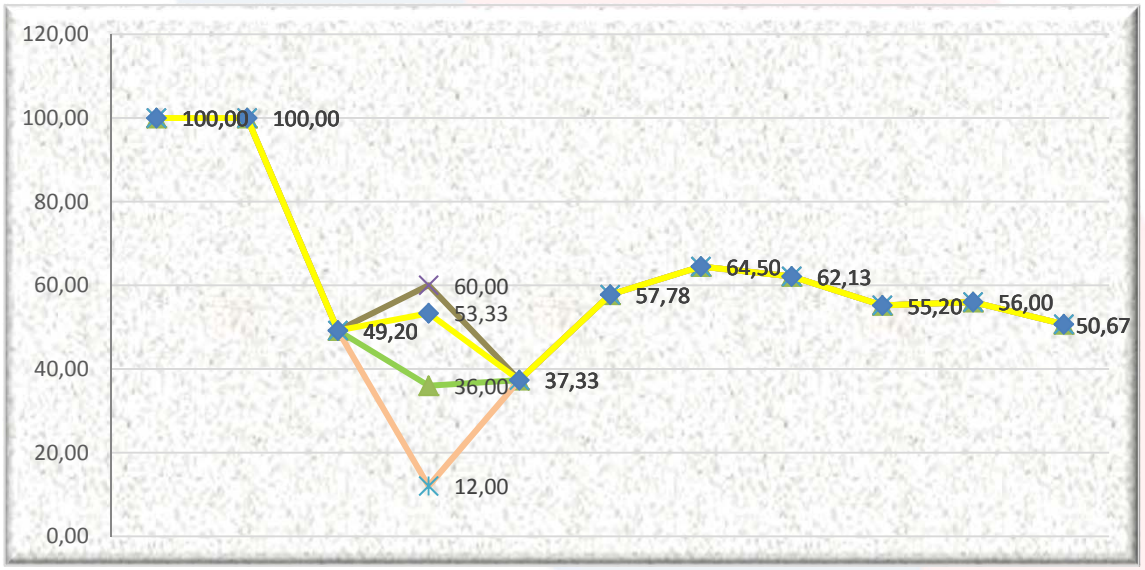


Modelo

Experimentación D4

4.- Seguridad de Recurso Humano (D4)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
3	4,4	13,3	53,3	1	3	12	3	9	36	5	15	60
Riesgo por nivel de exposición	Línea base								60,44 %			
	Al minimizar								56.69 %			
	Medio								58,87 %			
	Al maximizar								61,05 %			

Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%

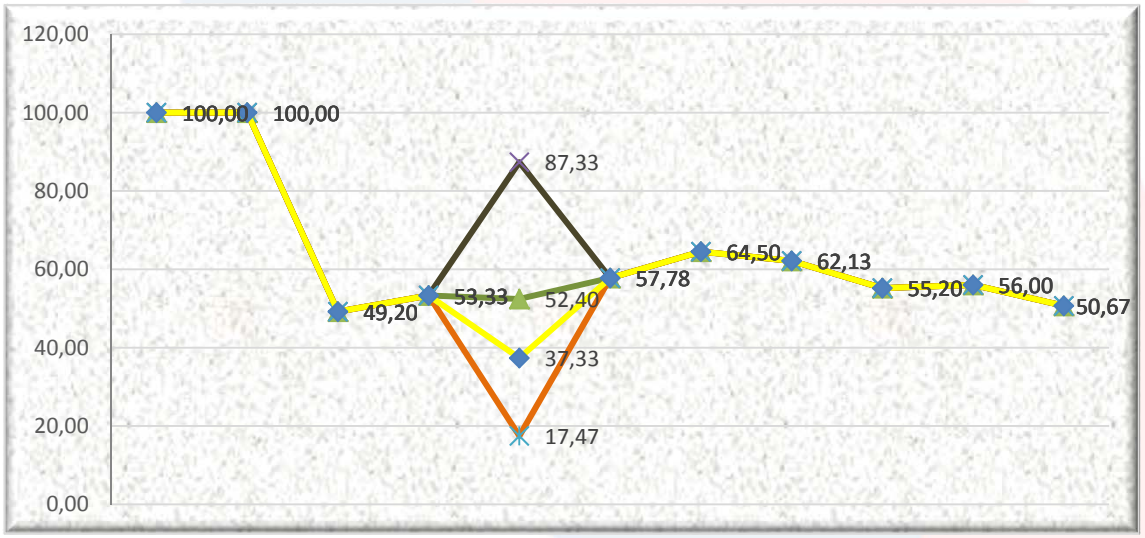


Modelo

Experimentación D5

5.- Seguridad Física y Ambiental (D5)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,37	1,9	8,3	37,3	1	4,4	17,5	3	13,1	52,4	5	21,8	87,3
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					59,00 %			
				Medio					62,18 %			
				Al maximizar					65,35 %			

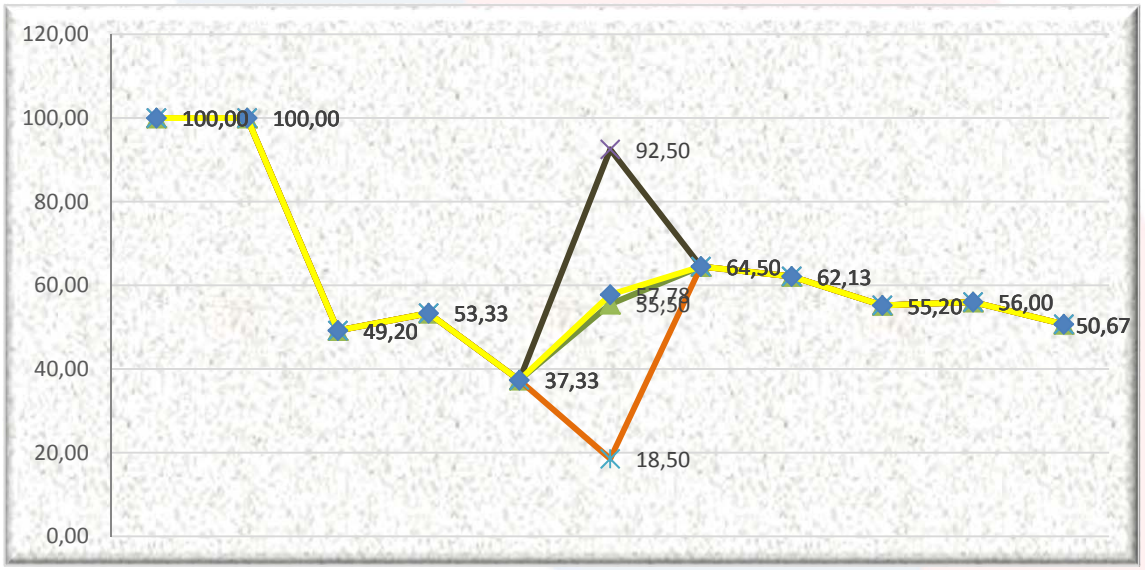
Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%



Modelo

Experimentación D6

6.- Dominio de Gestión de Comunicaciones (D6)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,63	3	14	57,7	1	4,6	18,5	3	13,8	55,5	5	23,1	92,5
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					57,02 %			
				Medio					60,39 %			
				Al maximizar					63,75 %			

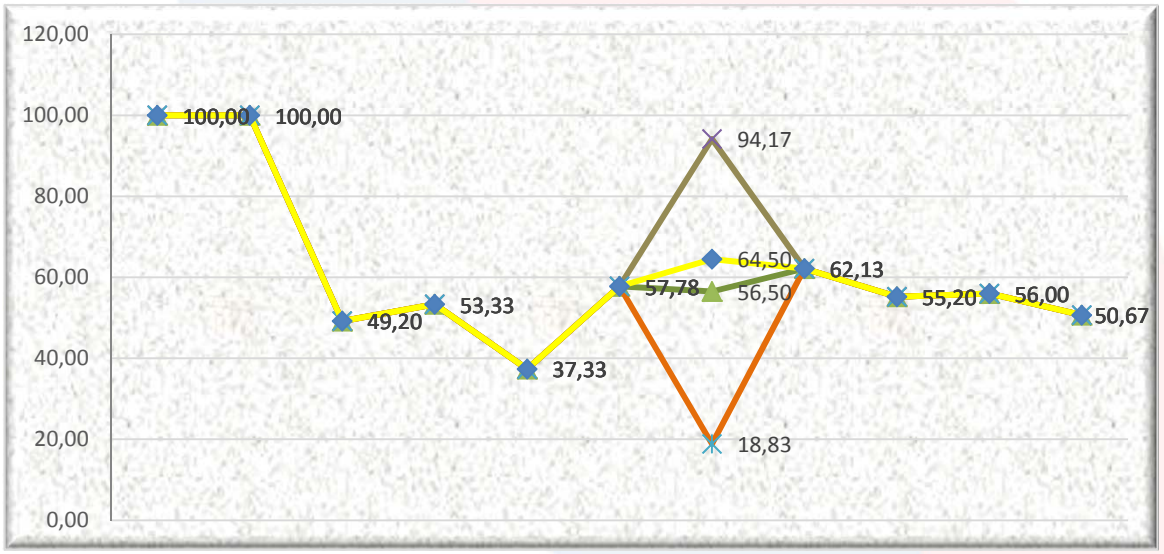


Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,78%	18,5%	55,5%	92,5%

Modelo

Experimentación D7

7.- Dominio de Control de acceso (D7)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,71	3,4	3	64,5	1	4,7	18,3	3	14,1	56,5	5	23,5	94,1
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					56,29 %			
				Medio					59,72 %			
				Al maximizar					63,14 %			

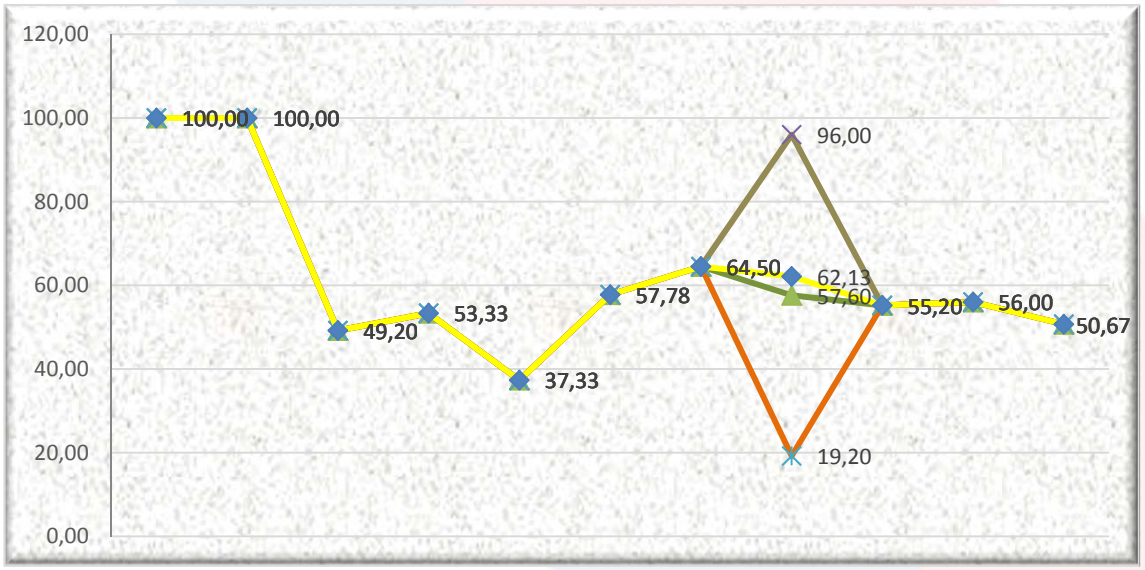


Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%

Modelo

Experimentación D8

8.- Desarrollo, Mantenimiento y adquisición de Sistemas de Información (D8)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,8	3,2	15,5	62,1	1	4,8	19,2	3	14,4	57,6	5	24	96
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					56,54 %			
				Medio					60,03 %			
				Al maximizar					63,52 %			

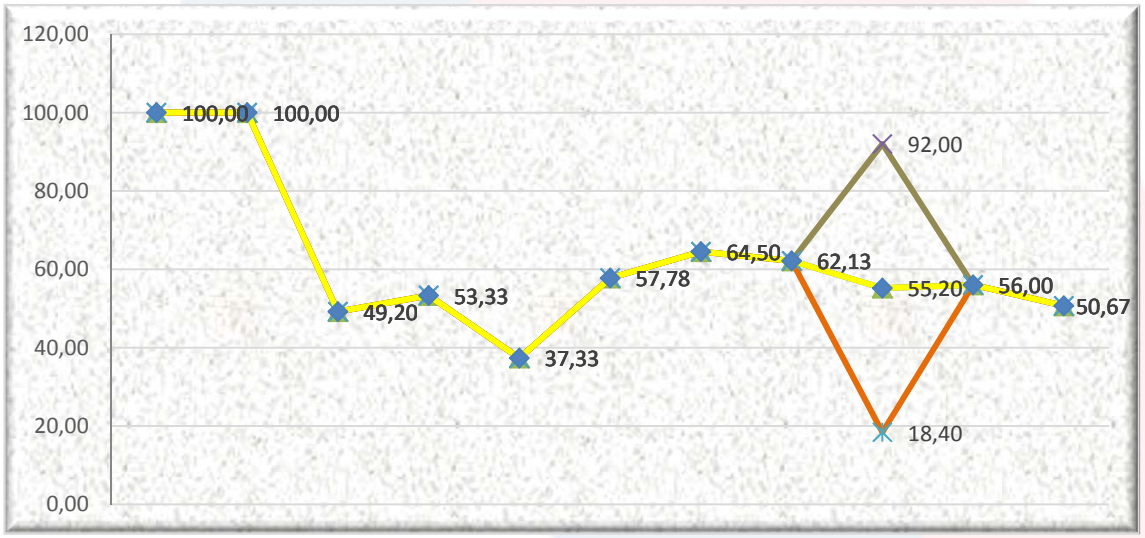


Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%
D8	62,1%	19,2%	57,8%	96%

Modelo

Experimentación D9

9.- Administración de Incidentes de Seguridad (D9)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,6	3	13,8	55,2	1	4,6	18,4	3	13,8	55,2	5	23	92
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					58,04 %			
				Medio					61,39 %			
				Al maximizar					65,73%			

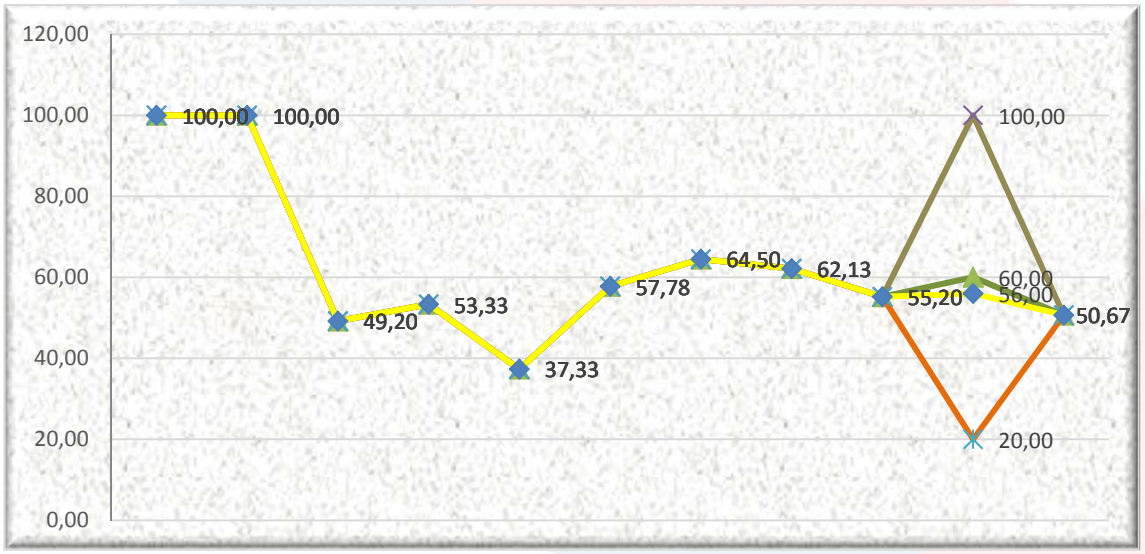


Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%
D8	62,1%	19,2%	57,8%	96%
D9	55,2%	18,4%	55,2%	92%

Modelo

Experimentación D10

10.- Administración de Continuidad del Negocio (D10)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
5	2,8	14	56	1	5	20	3	15	60	5	25	100
Riesgo por nivel de exposición	Línea base								60,44 %			
	Al minimizar								59,10 %			
	Medio								63,74 %			
	Al maximizar								66,38%			

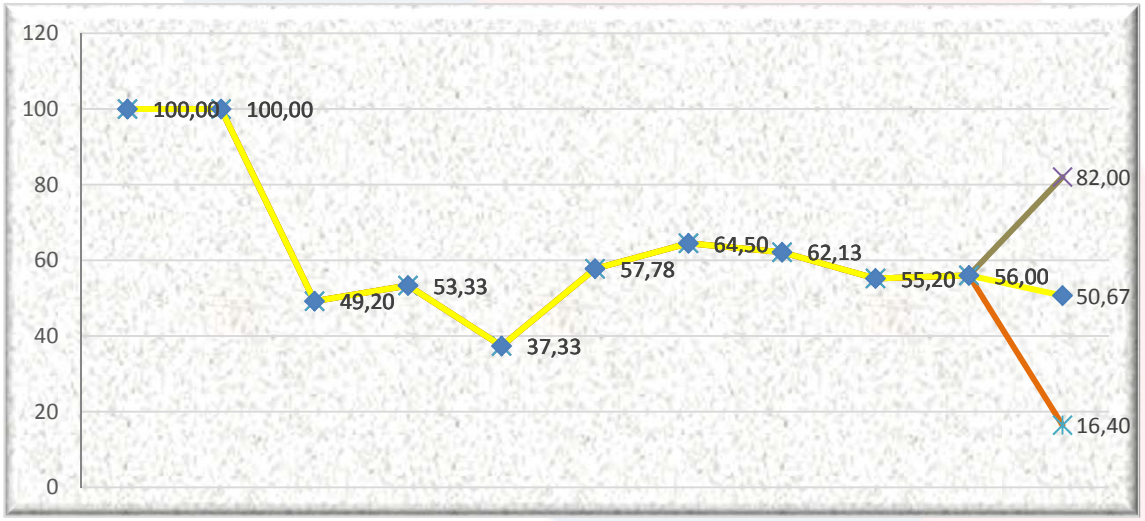


Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%
D8	62,1%	19,2%	57,8%	96%
D9	55,2%	18,4%	55,2%	92%
D10	56%	20%	60%	100%

Modelo

Experimentación D11

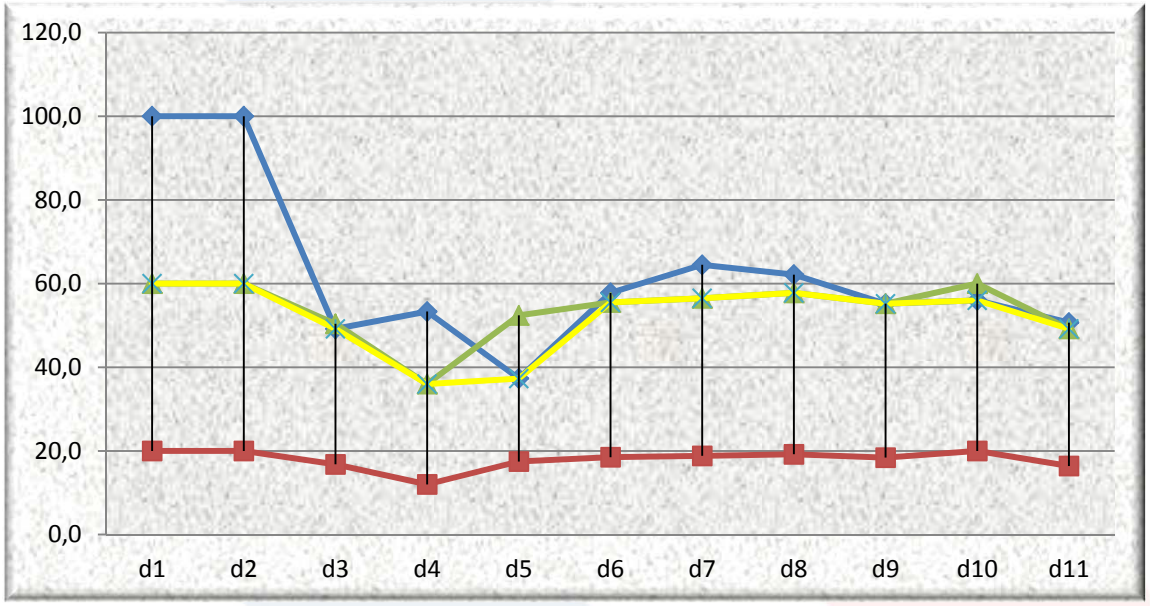
11.- Cumplimiento y Normativa legal (D11)												
Impacto por dominio	Valor línea Base			Valor de exposición = 1			Valor de exposición = 3			Valor de exposición = 5		
	InD	R	RP%	InD	R	RP%	InD	R	RP%	InD	R	RP%
4,1	3	12,7	50,7	1	4,1	16,4	3	12,3	49,2	5	20,5	82
Riesgo por nivel de exposición				Línea base					60,44 %			
				Al minimizar					59,26 %			
				Medio					62,24 %			
				Al maximizar					65,23%			



Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%
D8	62,1%	19,2%	57,8%	96%
D9	55,2%	18,4%	55,2%	92%
D10	56%	20%	60%	100%
D11	50,7%	16,4%	49,2%	82%

Modelo

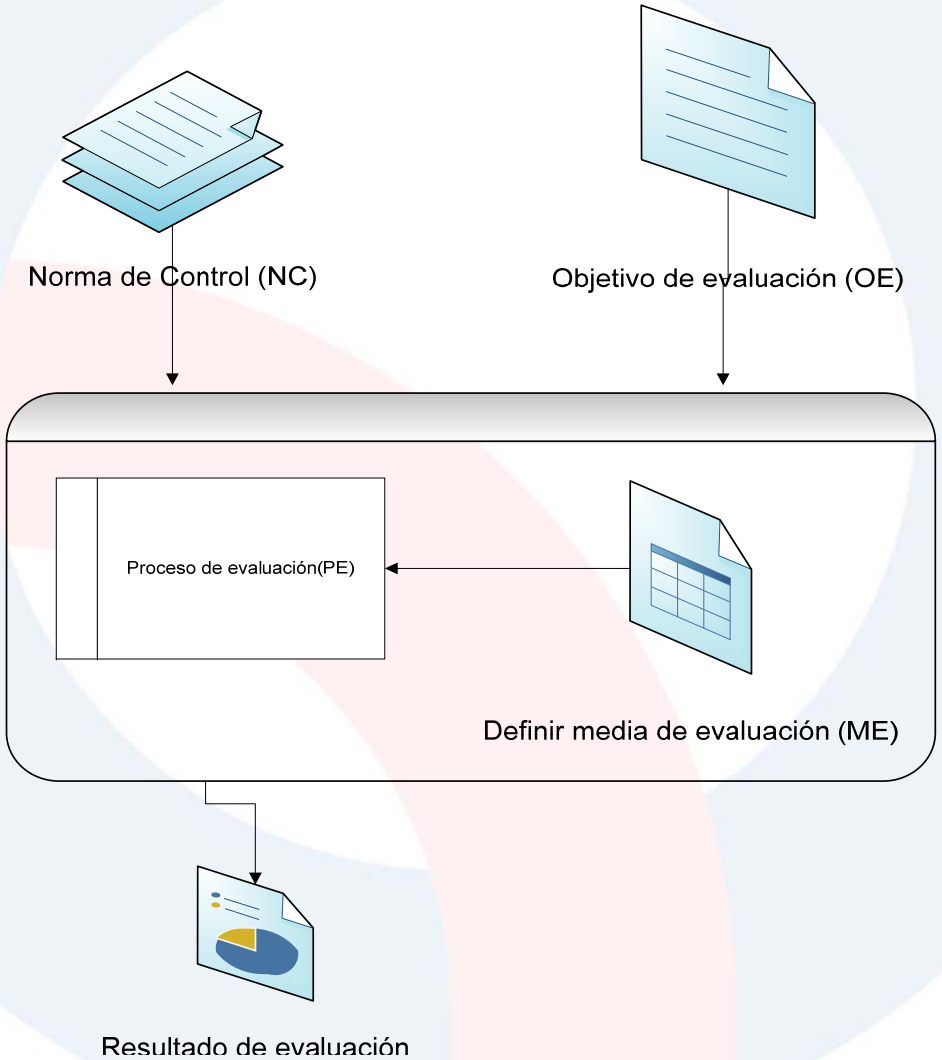
Resumen de experimentación



Dominio	Línea Base	Experimentos del riesgo		
		Riesgo bajo = 1	Riesgo medio = 3	Riesgo alto = 5
D1	100%	20%	60%	100%
D2	100%	20%	60%	100%
D3	49,2%	16,8%	50,4%	84%
D4	53,3%	12%	36%	60%
D5	37,3%	17,5%	52,4%	87,3%
D6	57,18%	18,5%	55,5%	92,5%
D7	64,5%	18,8%	56,5%	94,2%
D8	62,1%	19,2%	57,8%	96%
D9	55,2%	18,4%	55,2%	92%
D10	56%	20%	60%	100%
D11	50,7%	16,4%	49,2%	82%
Riesgo total	**60,44%**	**18%**	**53,9%**	**89,8%**

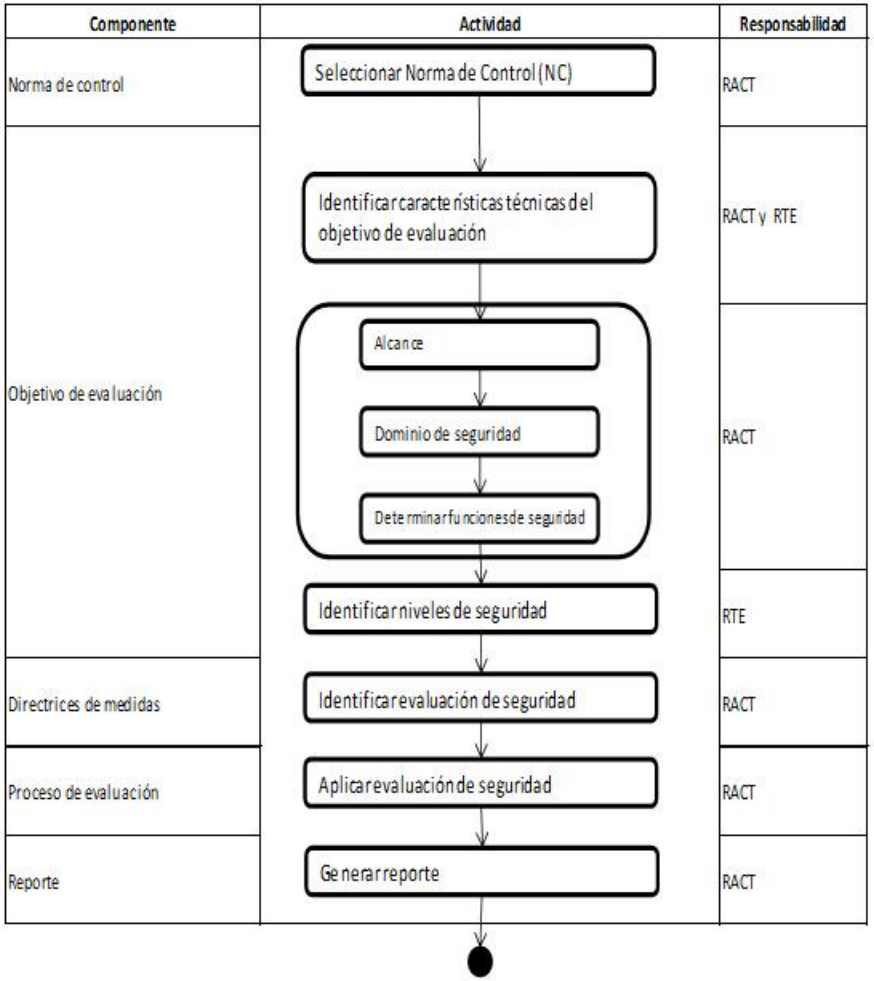
Modelo

Componente del Modelo de Evaluación



Modelo

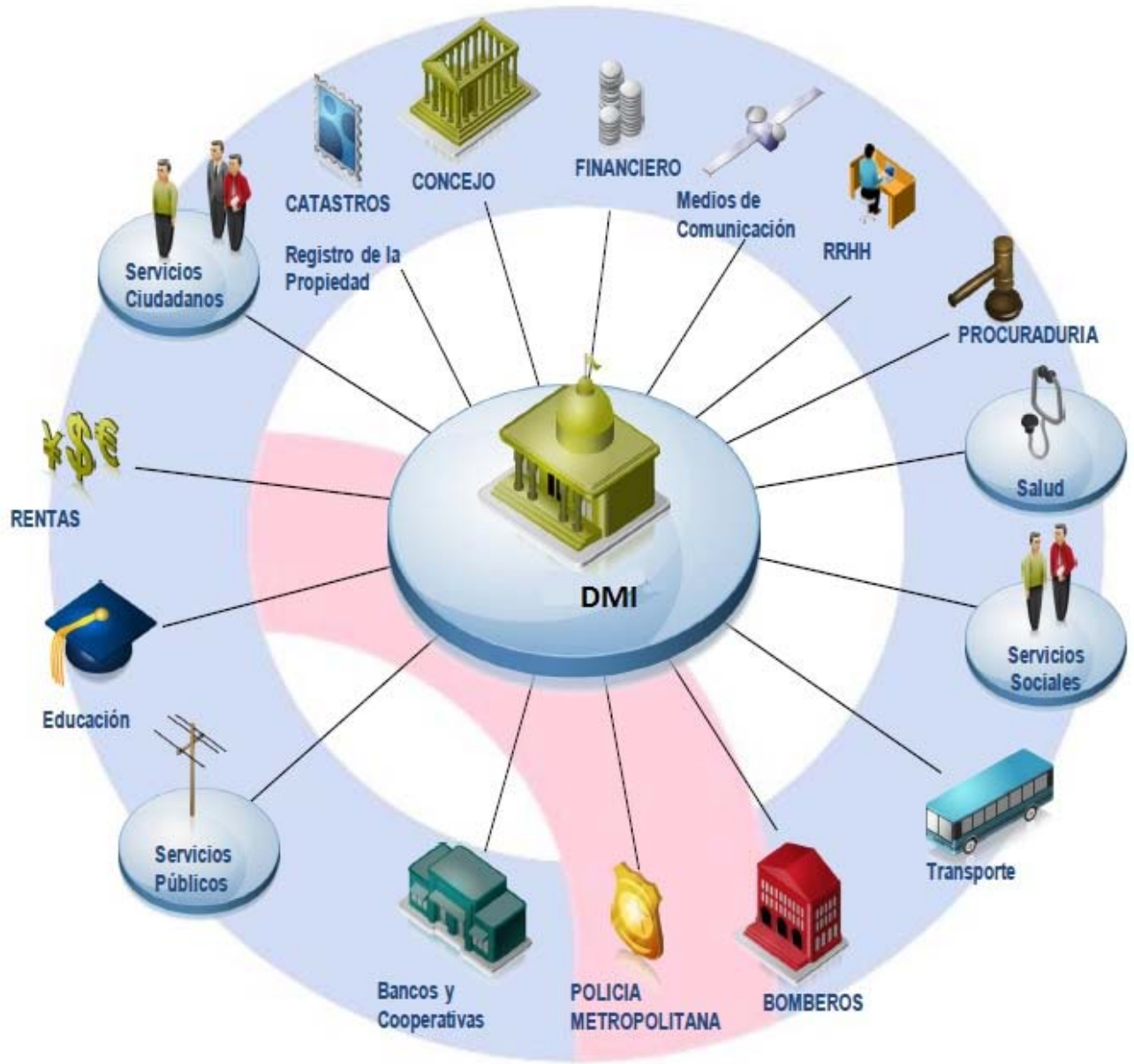
Diagrama de actividades



Nombre	Rol
Responsable tecnológico de las entidades (RTE)	Responsable de las dependencias municipales a quien se aplicará el modelo y se evaluará.
Responsable del área de Control Tecnológico (RACT)	Responsable de evaluar de acuerdo a directrices identificadas por la norma

Modelo

Metodología de implementación


CATASTROS
CONCEJO
FINANCIERO
Medios de Comunicación
RRHH
Servicios Ciudadanos
Registro de la Propiedad
PROCURADURIA
RENTAS
Salud
DMI
Educación
Servicios Sociales
Servicios Públicos
Transporte
Bancos y Cooperativas
POLICIA METROPOLITANA
BOMBEROS

Conclusiones

- Actualmente la Dirección Metropolitana de Informática dentro de su modelo de gestión aplicado no presenta el área de Seguridad que apoye los objetivos tecnológicos.
- El levantamiento de información realizado en las dependencias desconcentradas de la Municipalidad, permite realizar un análisis de riesgo apoyados en la ISO 27002 obteniendo el resultado por dominio y determinando un riesgo total del 60.44%, equivalente a un riesgo medio alto.
- El problema que la institución municipal presente un alto riesgo tecnológico, no se soluciona completamente con la implementación de procedimientos, normas o modelos, debido a que la decisión del usuario que opera es el que define en gran medida si ejecuta o no el control.
- El modelo propuesto se basó en 33 experimentos agrupados por dominio, utilizando valores de exposición que permitieron disminuir el riesgo total al 18% equivalente a riesgo bajo.
- El modelo de Evaluación y Monitoreo propuesto permitirá identificar los controles, procesos que tiene la institución y los que requieren mayor atención para mejorar la eficacia y disminuir el riesgo.

Recomendaciones

- La creación del área de coordinación de Seguridad Informática con la involucración de los jefes de áreas en la administración de la seguridad para la ejecución del modelo
- Realizar evaluaciones a las dependencias municipales utilizando la normas técnica Ecuatorianas NTE INEN – ISO/IEC 27000 para la gestión de la seguridad.
- Realizar evaluaciones periódicas a las dependencias municipales, que permitan identificar el cumplimiento de controles, amenazas y vulnerabilidades que afecten al core del negocio de la institución.
- Para la mejora de las políticas en la institución se recomienda implementar el modelo propuesto que permite evaluar los controles existentes, implementar nuevos controles el nivel de madurez en la gestión de seguridad de la institución.
- Concientizar a los funcionarios municipales que la responsabilidad de la seguridad de la información es responsabilidad de todos.

Gracias

DISTRITO METROPOLITANO