Universitat Autònoma de Barcelona

www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC
(MISTIC)

PLAN DE SEGURIDAD DE LA INFORMACION

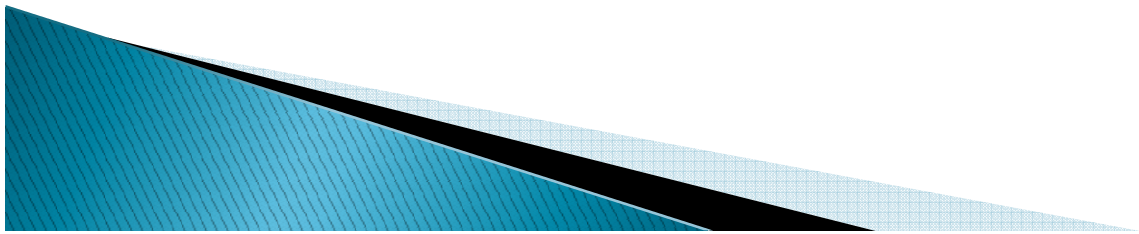
Preparado por:

Luis Alejandro Bautista Torres

16-12-2012

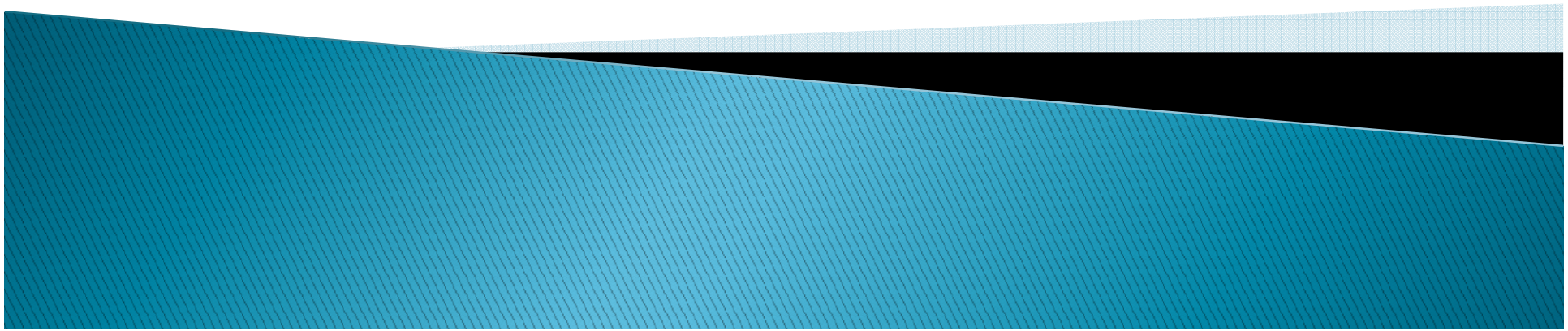
Agenda

- ✓ Objeto del Proyecto
- ✓ Fases del Proyecto
- ✓ Resultados por Fase
- ✓ Entregables



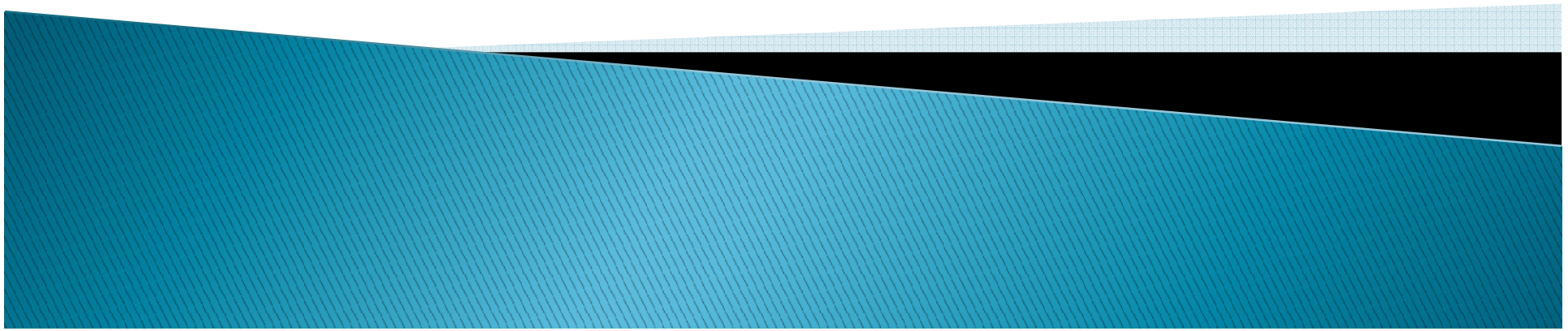
Objetivo

Generación del Plan Director de Seguridad para XYZ Soluciones



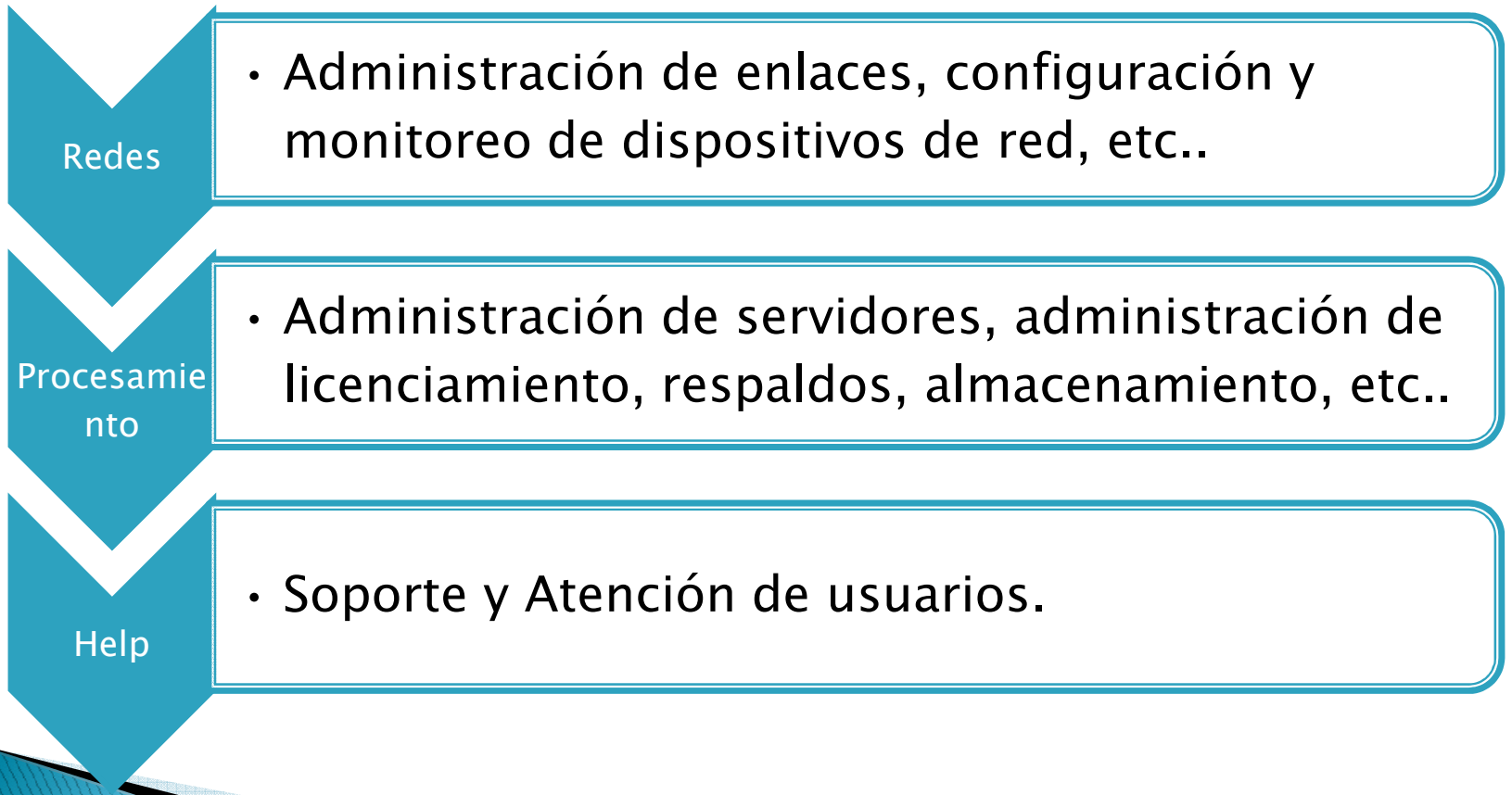
Fases del Proyecto

- FASE I → Identificación de la Metodología
- FASE II → Objetivos del Plan
- FASE III → Identificación y Valoración de Activos
- FASE IV → Auditoria de Cumplimiento
- FASE V → Propuestas de Proyectos
- FASE VI → Entrega de Resultados



Fase I: Metodología

Dependencias de XYZ Soluciones



Fase I: Metodología

Dependencias de XYZ Soluciones

Bases de Datos

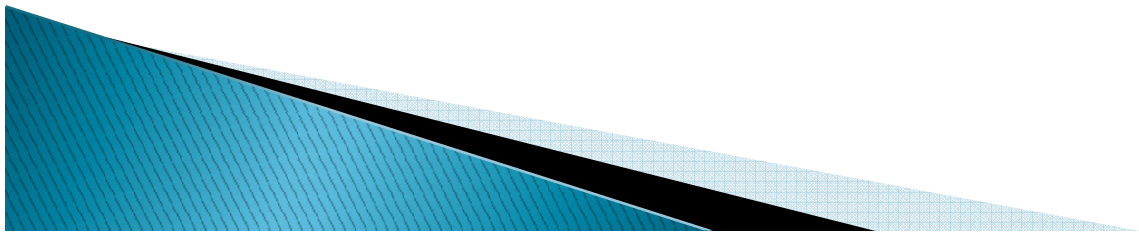
- Mantenimiento de las bases de datos, gestión y administración de capacidad de bases de datos, etc.

Seguridad Informática

- Gestión de antivirus, administración de firewall, control de contenido perimetral, administración de circuito cerrado de televisión, etc..

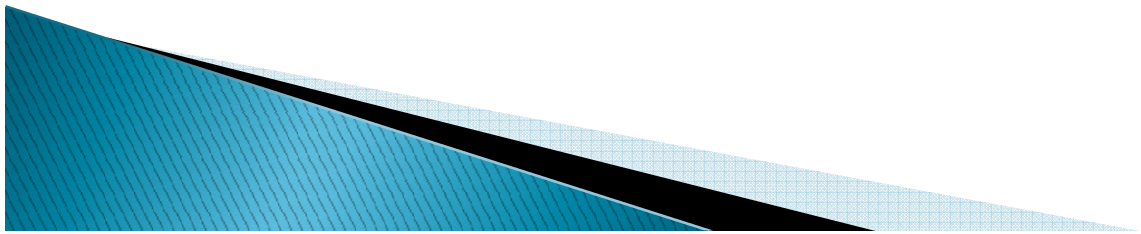
Fase I: Metodología

- Paso 1 → Caracterización del Contexto Evaluado
- Paso 2 → Definir Criterios de Evaluación
- Paso 3 → Identificación de Activos
- Paso 4 → Identificación de amenazas
- Paso 5 → Identificación de vulnerabilidades
- Paso 6 → Análisis de controles



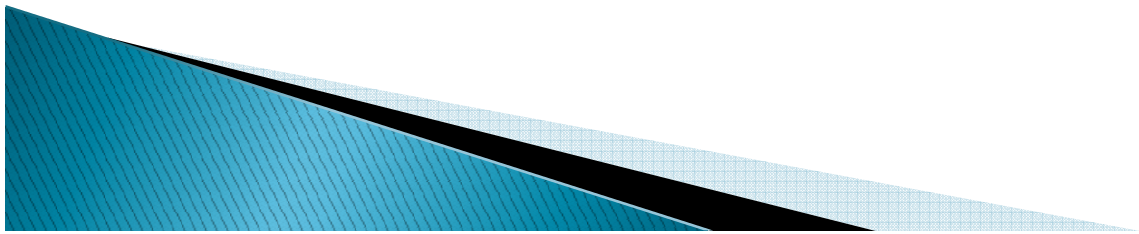
Fase I: Metodología

- Paso 7 → Determinación de probabilidades
- Paso 8 → Análisis de impacto
- Paso 9 → Determinación de riesgos
- Paso 10 → Identificación de controles
- Paso 11 → Otros factores de evaluación
- Paso 12 → Resultados Documentados



Fase I: Metodología

- Técnicas de recolección de la Información
  - → Cuestionarios
  - → Entrevistas
  - → Revisión de Documentos
  - → Uso de tecnologías para escaneo



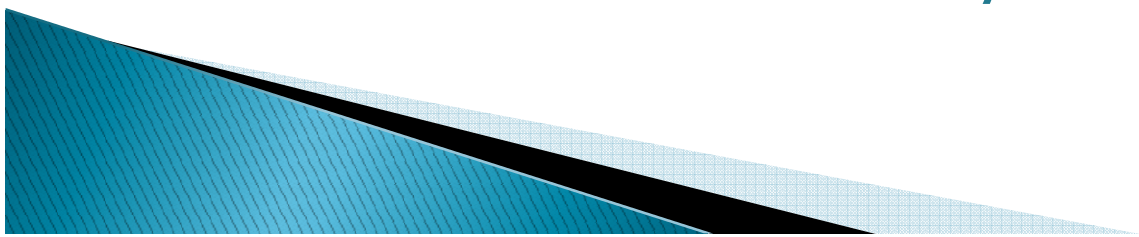
Fase I: Metodología

Entregable: F01 – Metodologia.pdf

- Contextualización de la Organización
- Metodología
  - Propósito
  - Técnicas de Recolección
  - Valoración de Riesgos
  - Criterios de Evaluación
  - Identificación de Controles
  - Implementación de buenas practicas

Fase II : Objetivos del Plan

- → Generar Mapa de Ruta para S.I.
- → Sugerir estructura Organizacional
- → Identificación de Responsabilidades
  - Operadores y usuarios
  - Propietarios o Dueños de la información
  - Administradores y Coordinadores de áreas o dependencias
  - Analista de monitoreo e incidentes
  - Oficial de Seguridad de la Información
  - Comité de Seguridad de la Información
  - Alta Dirección
- → Identificar Proyectos



Fase II : Objetivos del Plan

Entregable: F02 – Objetivos del Plan.pdf

- Objetivo Principal del Plan
- Objetivos de Infraestructura Organizacional
- Objetivos alineados con ISO 27002
- Concienciación de la Alta Dirección
- Estructura Ideal para un SGSI

Fase III : Valoración de Activos

Activos Bases de Datos

PROPIETARIO	NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS	AUTEN.	CONF.	INTEG.	DISP.	TRAZA
BASES DE DATOS	EIXYZSOL34	Aplicación	CAPA 3	8	8	6	6	8
BASES DE DATOS	EIXYZSOL22	Datos	CAPA 4	10	8	8	6	10
BASES DE DATOS	EIXYZSOL49	Datos	CAPA 4	10	8	8	6	10
BASES DE DATOS	EIXYZSOL50	Datos	CAPA 4	10	8	8	6	10
BASES DE DATOS	EIXYZSOL53	Datos	CAPA 4	10	8	8	6	10

Fase III : Valoración de Activos

Activos Help

PROPIETARIO	NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS	AUTEN.	CONF.	INTEG.	DISP.	TRAZA
HELP	EIXYZSOL21	Aplicación	CAPA 3	6	6	6	1	6
HELP	EIXYZSOL45	Aplicación	CAPA 3	8	8	6	6	8
HELP	EIXYZSOL46	Aplicación	CAPA 3	8	8	6	6	8
HELP	EIXYZSOL48	Datos	CAPA 4	10	8	8	6	10
HELP	EIXYZSOL70	Personal	CAPA 4	8	8	6	6	8

Fase III : Valoración de Activos

Activos Procesamiento de la Información

PROPIETARIO	NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS	AUTEN.	CONF.	INTEG.	DISP.	TRAZA
PROCESAMIENTO DE INF.	EIXYZSOL25	Aplicación	CAPA 3	8	8	6	6	8
PROCESAMIENTO DE INF.	EIXYZSOL28	Hardware	CAPA 3	10	8	8	6	10
PROCESAMIENTO DE INF.	EIXYZSOL32	Hardware	CAPA 3	10	8	8	6	10
PROCESAMIENTO DE INF.	EIXYZSOL35	Hardware	CAPA 3	10	8	8	6	10
PROCESAMIENTO DE INF.	EIXYZSOL36	Hardware	CAPA 3	10	8	8	6	10
PROCESAMIENTO DE INF.	EIXYZSOL33	Datos	CAPA 4	10	8	8	6	10
PROCESAMIENTO DE INF.	EIXYZSOL40	Personal	CAPA 4	10	8	8	6	10

Fase III : Valoración de Activos

Activos Red

PROPIETARIO	NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS	AUTEN.	CONF.	INTEG.	DISP.	TRAZA
RED	EIXYZSOL17	Instalaciones	CAPA 1	10	8	8	10	10
RED	EIXYZSOL19	Soporte	CAPA 1	10	8	8	10	10
RED	EIXYZSOL73	Red	CAPA 1	10	8	8	10	10
RED	EIXYZSOL14	Hardware	CAPA 2	10	8	8	6	10
RED	EIXYZSOL15	Hardware	CAPA 2	10	8	8	6	10
RED	EIXYZSOL16	Hardware	CAPA 2	10	8	8	6	10
RED	EIXYZSOL18	Hardware	CAPA 2	8	8	6	2	8

Fase III : Valoración de Activos

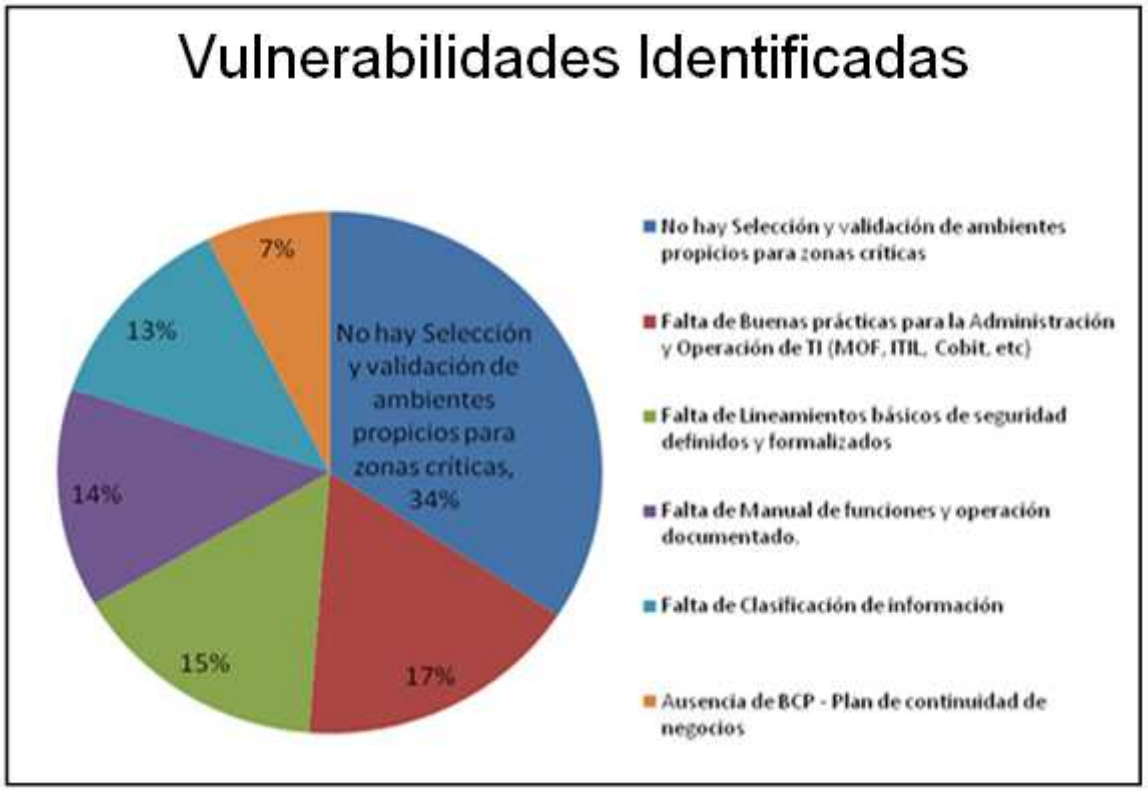
Activos Seguridad Informática

PROPIETARIO	NOMBRE ACTIVO	TIPIFICACION	JERARQUIAS	AUTEN.	CONF.	INTEG.	DISP.	TRAZA
SEGURIDAD INFORMATICA	EIXYZSOL08	Hardware	CAPA 2	10	8	8	10	10
SEGURIDAD INFORMATICA	EIXYZSOL12	Hardware	CAPA 2	6	8	6	6	8
SEGURIDAD INFORMATICA	EIXYZSOL04	Aplicación	CAPA 3	6	8	6	4	6
SEGURIDAD INFORMATICA	EIXYZSOL05	Aplicación	CAPA 3	8	8	6	6	8
SEGURIDAD INFORMATICA	EIXYZSOL11	Servicios	CAPA 4	6	8	6	4	6

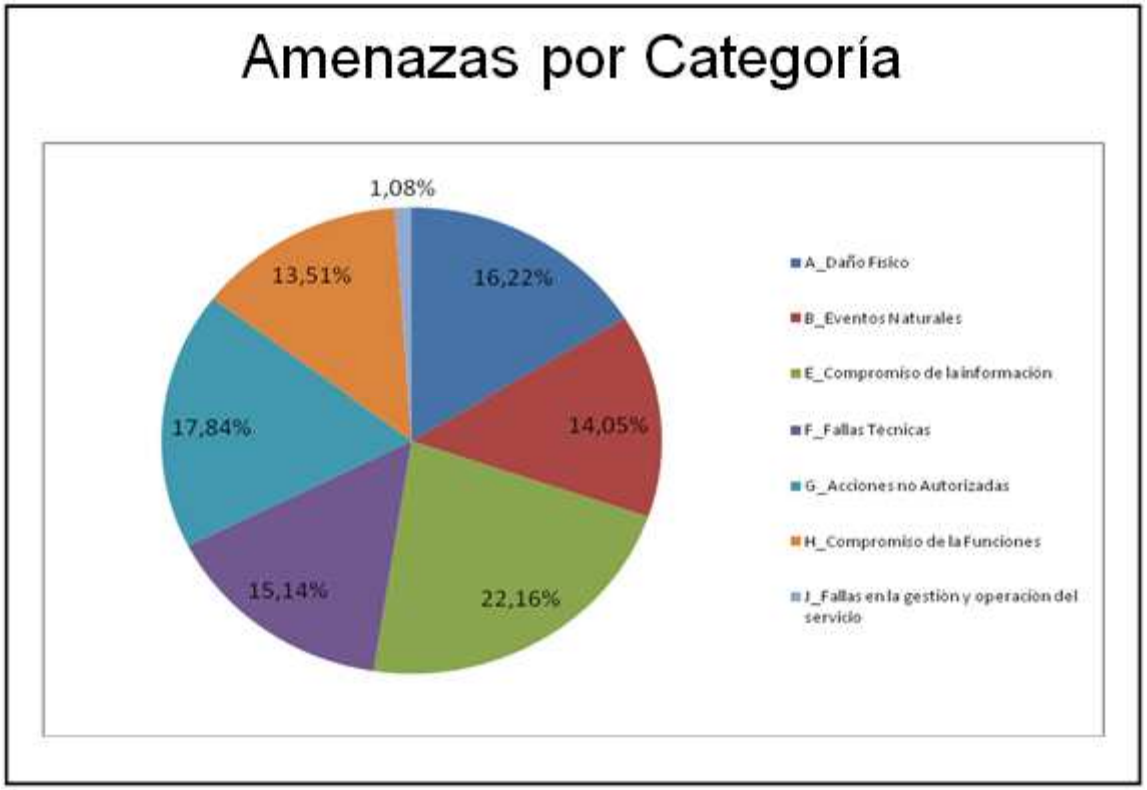
Fase III : Valoración de Activos

HERENCIAS				
ACTIVOS	CAPA 1	CAPA 2 Y 3	CAPA 4	CAPA 5
CAPA 1	1,2,3	N/A	N/A	N/A
CAPA 2 Y 3	4 al 20	4 al 20	N/A	N/A
CAPA 4	21,22,24 y 26 al 29	21,22,24 y 26 al 29	21,22,24 y 26 al 29	N/A
CAPA 5	N/A	N/A	N/A	N/A

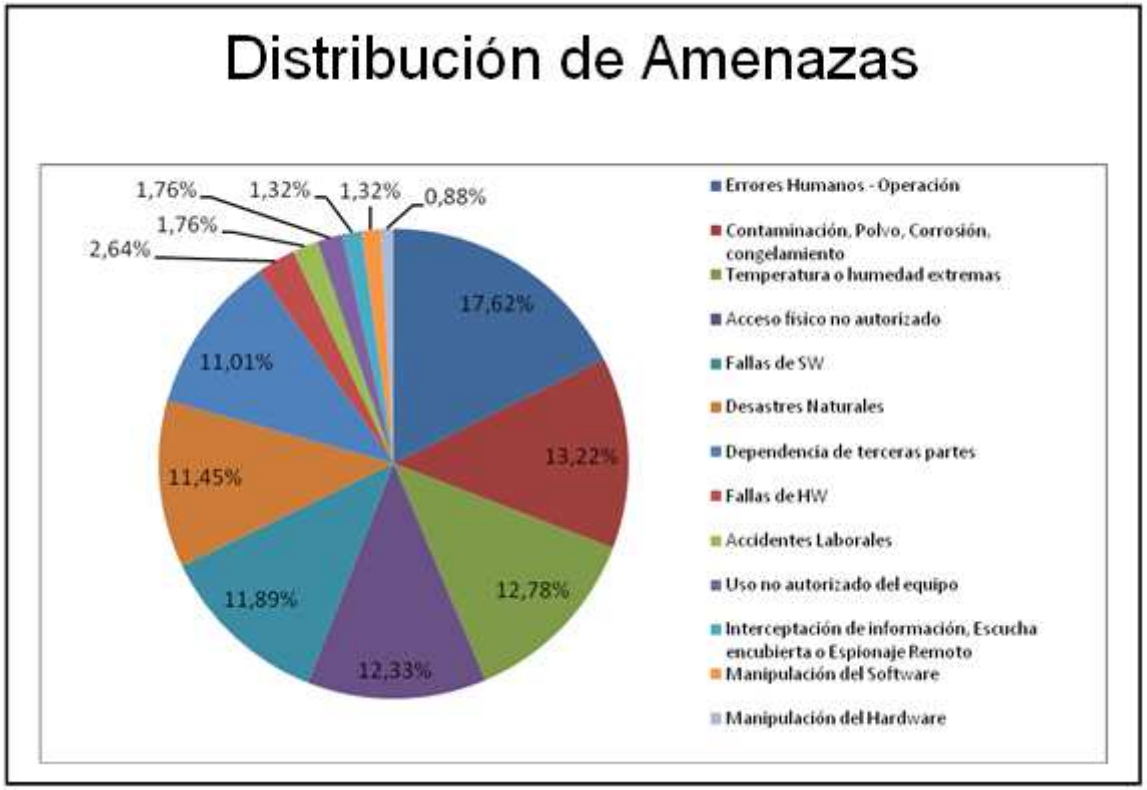
Fase III : Valoración de Activos



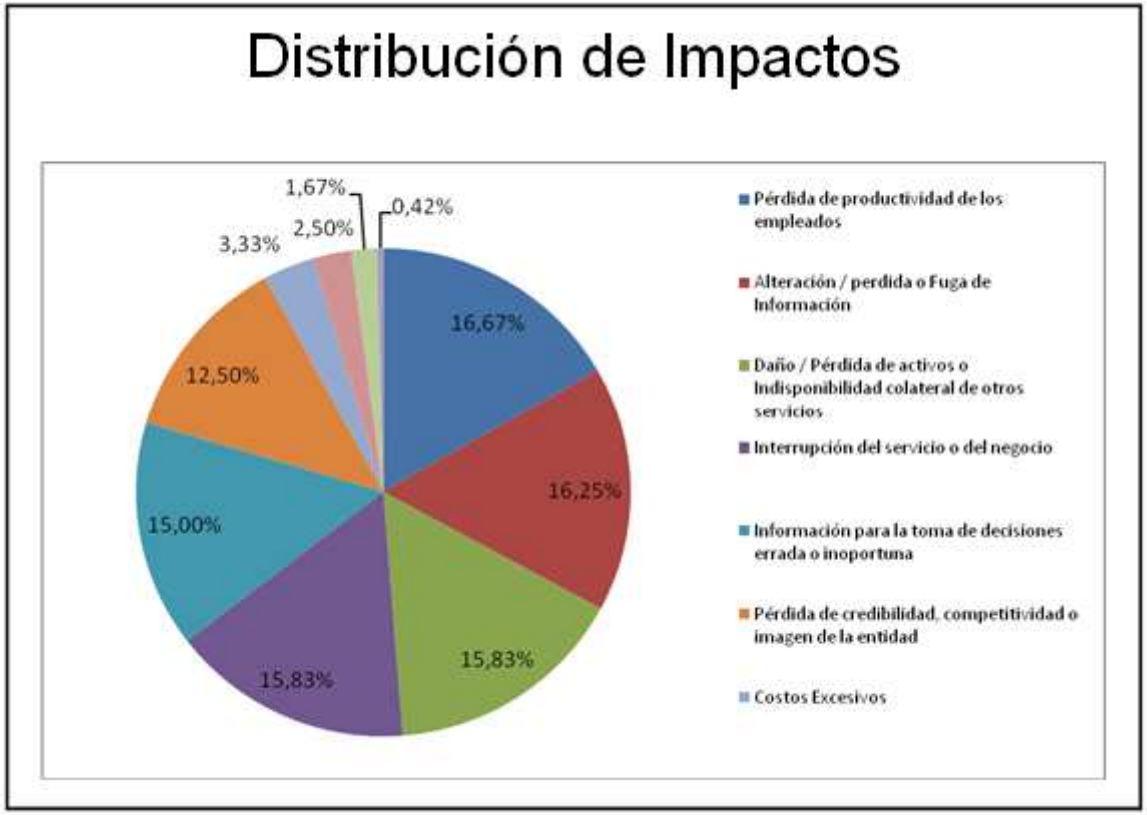
Fase III : Valoración de Activos



Fase III : Valoración de Activos



Fase III : Valoración de Activos

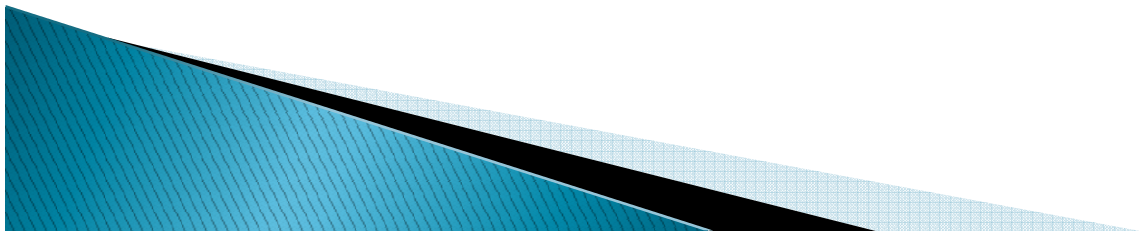


Fase III : Valoración de Activos

Fase III : Valoración de Activos

Entregable: F03 – Valoración de Activos.pdf

- Criterios de Identificación de Activos
- Caracterización y Tipificación
- Inventario de activos
- Herencias
- Amenazas
- Riesgo y Probabilidad
- Efectividad de los Controles



Fase III : Valoración de Activos

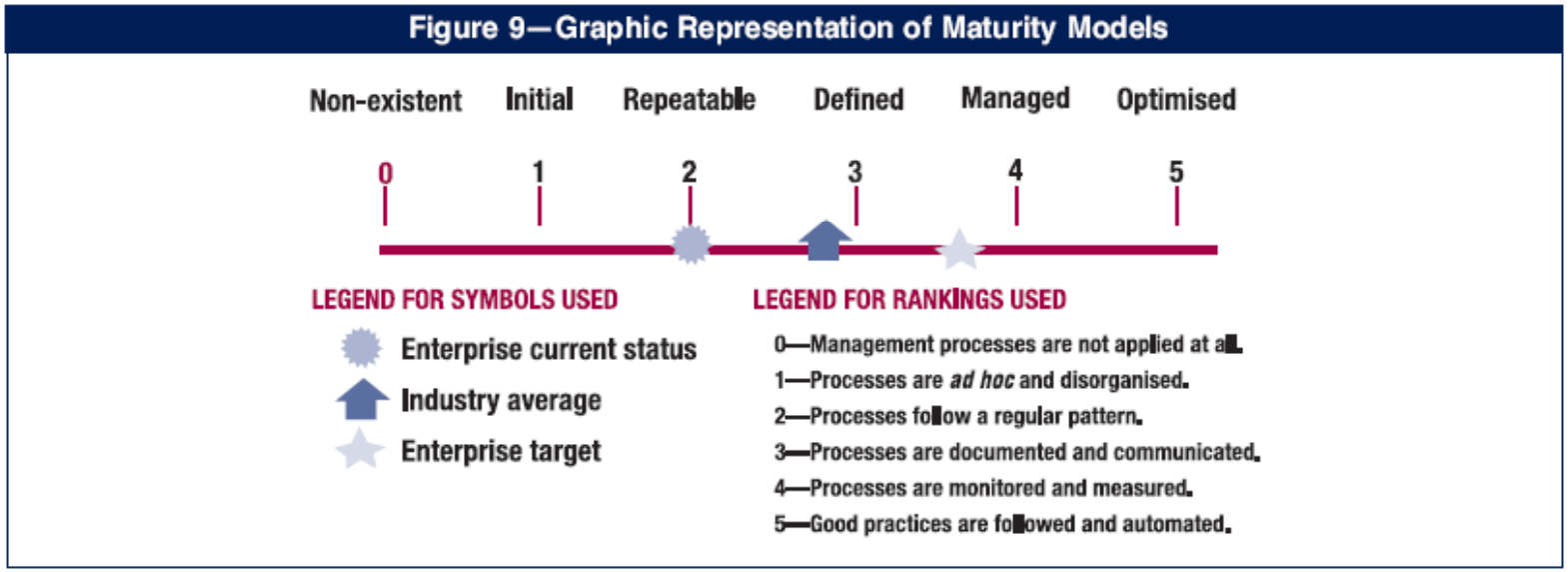
Entregable: F03 – Act-Consolidado.pdf

- Memoria de la Caracterización y Tipificación
- Inventario de activos
- Herencias

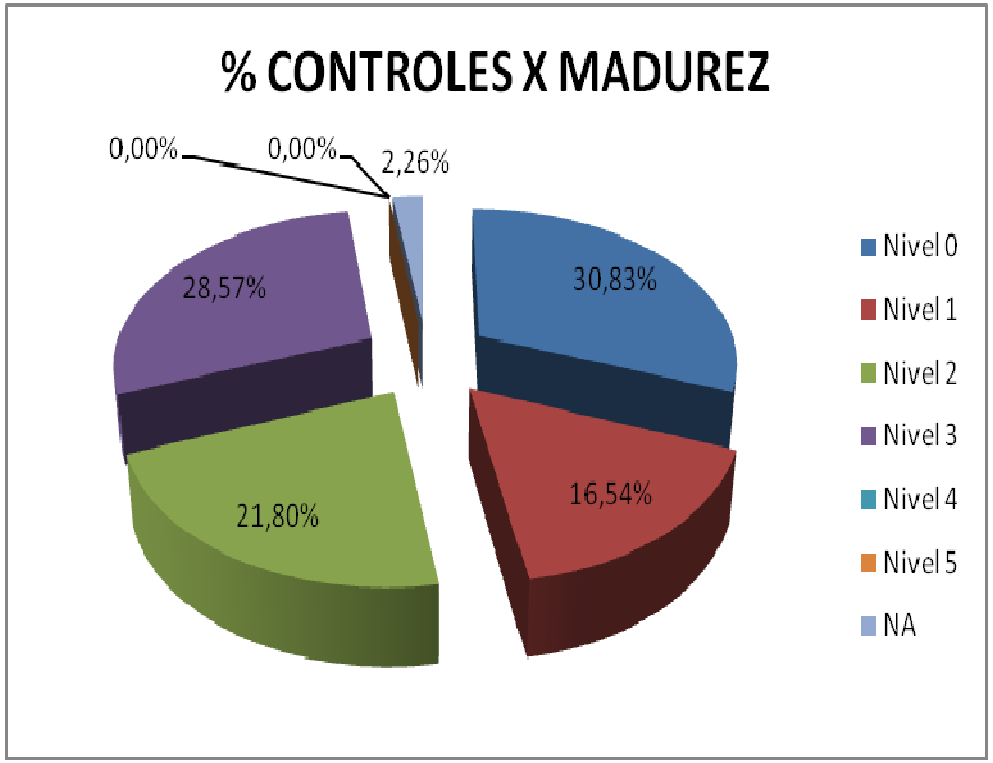
Fase IV : Auditoria de Cumplimiento

Modelo CMM

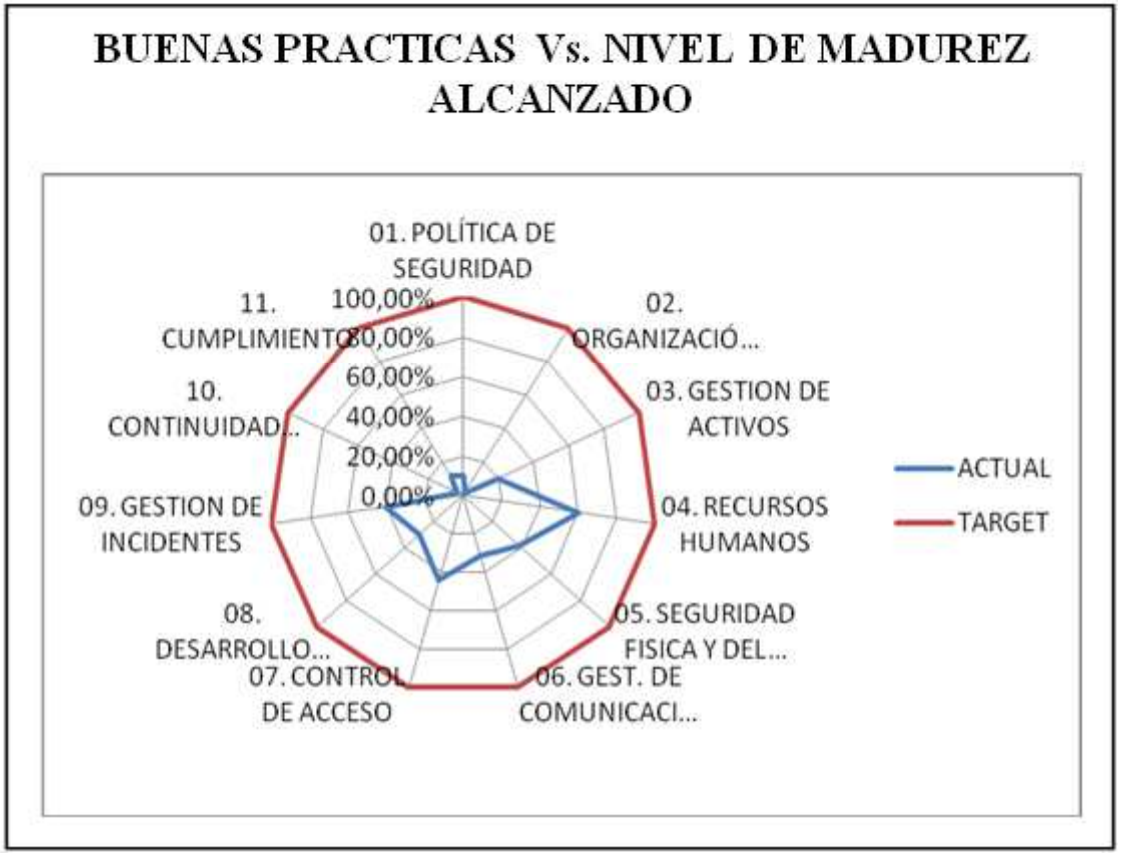
Figure 9—Graphic Representation of Maturity Models



Fase IV : Auditoria de Cumplimiento



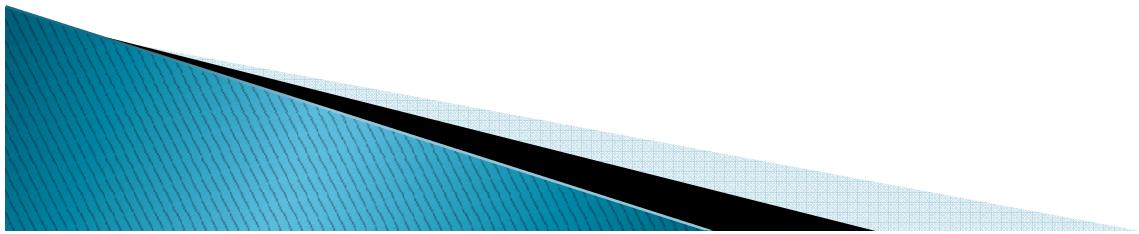
Fase IV : Auditoria de Cumplimiento



Fase IV : Auditoria de Cumplimiento

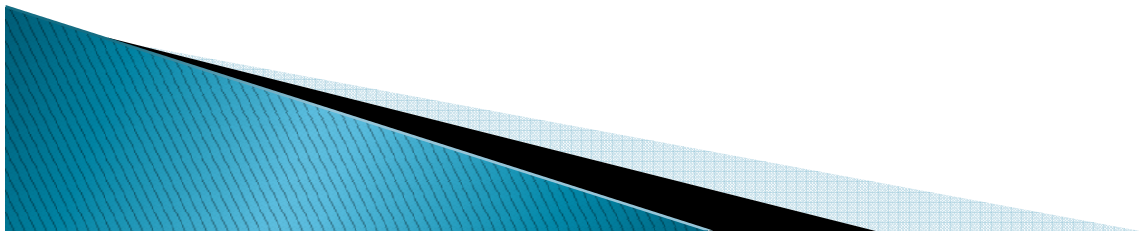
Entregable: F04 – Auditoria de Cumplimiento.pdf

- Escalas de Evaluación CMM
- Estado actual de los Controles
- Estado actual frente a ISO 27002
- Nivel de madurez alcanzado



Fase V : Propuestas de Proyectos

PROYECTOS Y ACTIVIDADES SUGERIDAS.	
01	Implementación del SGSI (1 año)
02	Implementación del PCN (1 año)
03	Clasificación de la Información. (1 - 6 meses)
04	Implementación Marco de Trabajo Estándar (1 año)
05	Concienciación en Seguridad de la Información
06	Renovación Acuerdos de Confidencialidad
07	Control de acceso a recursos



Fase V : Propuestas de Proyectos

	2013				2014	
ACTIV.	Nov	Dic	Jul	Dic	Ene	Jun
1	Corto plazo					
2						
3			Mediano plazo			
4					Largo plazo	
5	Actividades Permanentes					
6						
7						

Ilustración 38. Roadmap de implementación

Fase V : Propuestas de Proyectos

<table>
<tr><td></td><td colspan="2">2013</td><td>2014</td></tr>
<tr><td>ACTIV.</td><td>US$150000</td><td>US$100000</td><td>US$50000</td></tr>
<tr><td>1</td><td rowspan="2">Corto plazo</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>2</td></tr>
<tr><td>3</td><td rowspan="2"></td><td>Mediano plazo</td><td rowspan="2"></td></tr>
<tr><td>4</td><td>Largo plazo</td></tr>
<tr><td>5</td><td colspan="3" rowspan="3">ACT < US$30000</td></tr>
<tr><td>6</td></tr>
<tr><td>7</td></tr>
</table>

Ilustración 39. Costos de implementación

Fase V : Propuestas de Proyectos

Entregable: F05 – Propuestas de Proyectos.pdf

- Proyectos de Seguridad
- Acciones Rápidas y Permanentes
- RoadMap de Proyectos
- Prioridades
- Costos Estimados