



**Adhoc
Security**

**ORGANIZANDO UN
PLAN DIRECTOR DE SEGURIDAD**

Qué es un Plan Director de Seguridad



Adhoc
Security

Conjunto de actuaciones sistematizadas, coherentes y organizadas, dirigidas a abordar la seguridad de una organización, en base a un ideal de seguridad definido por la Dirección de la empresa.

Objetivos de un Plan Director de Seguridad

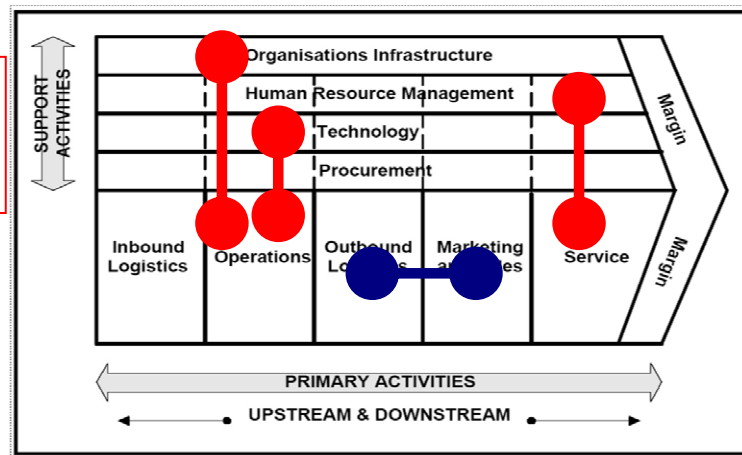


Adhoc
Security

Realizar un análisis de riesgos relacionado con la seguridad de los sistemas de información para identificar un Plan de Acción en base a la diferencia entre la situación actual de la empresa y el objetivo de seguridad

Causas en las
dependencias

Porter's Value Chain Analysis.



La información está relacionada con la informática e infraestructuras mediante dependencias horizontales y verticales

Consecuencias en los procesos

¡RIESGOS!

¡ACCIONES!



Adhoc Security

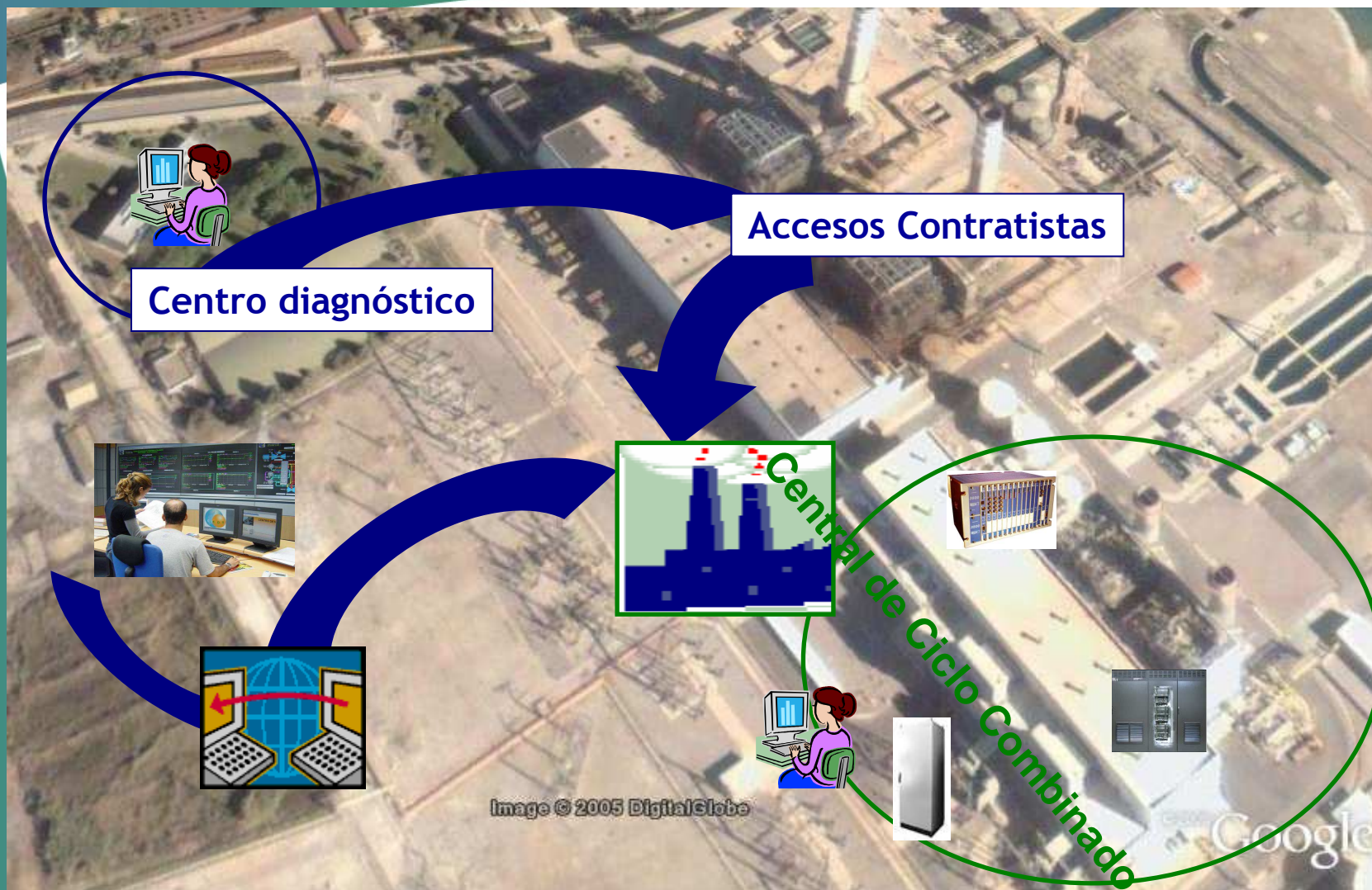
**Cómo llegar a un Plan Director de
Seguridad**

**Caso práctico: Central eléctrica de ciclo
combinado de potencia media de unos
400MW**

Centrales eléctricas de ciclo combinado



Adhoc
Security



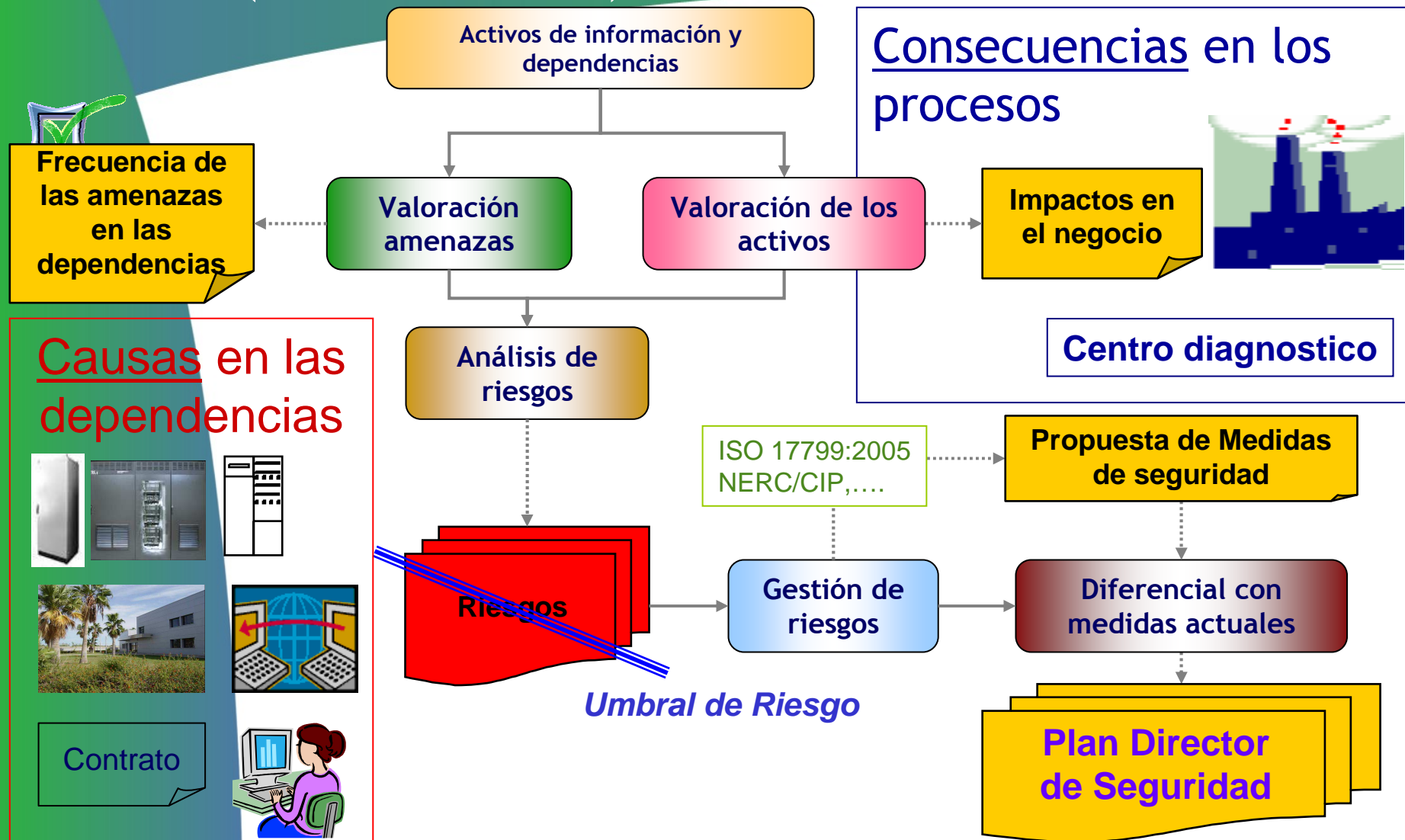
Marco de actuaciones y referencias (requisitos de seguridad)



Adhoc
Security

- ✓ **ISO Estándares Prácticas de Análisis y Gestión de Riesgos para una seguridad proporcional:**
 - ISO 17799 Catálogo de 133 controles de seguridad
 - ISO 27001 Sistema de Gestión certificable (línea ISO27xxx)
 - ISO 17776 Guidelines on tools and techniques for hazard identification and risk assessment
- ✓ **NERC: Critical Infrastructure Protección**
CIP02-09 (Draft 4) de 182 Requerimientos de protección
Physical and Cyber Alarm at YELLOW level since 2004 (ESISAC)
- ✓ **CEE: European Program for Critical Infrastructure Protection**
Instalaciones de producción de electricidad reconocidas como CI
EPCIP Policy
- ✓ **CIWIN Critical Infrastructure Warning Information Network**
- ✓ **EPRI:**
EIS Program 86: Energy Information Security.
EPRI PowerSec Initiative: Cyber Security Vulnerability Assessment
Conferencias SANS (SCADA Security meeting) y otros.
- ✓ **Normativa u obligaciones legales propias de cualquier organización**
- ✓ **Códigos deontológicos de la empresa**

Métodología: cómo llegar hasta un P.D.S (Plan de Acción)



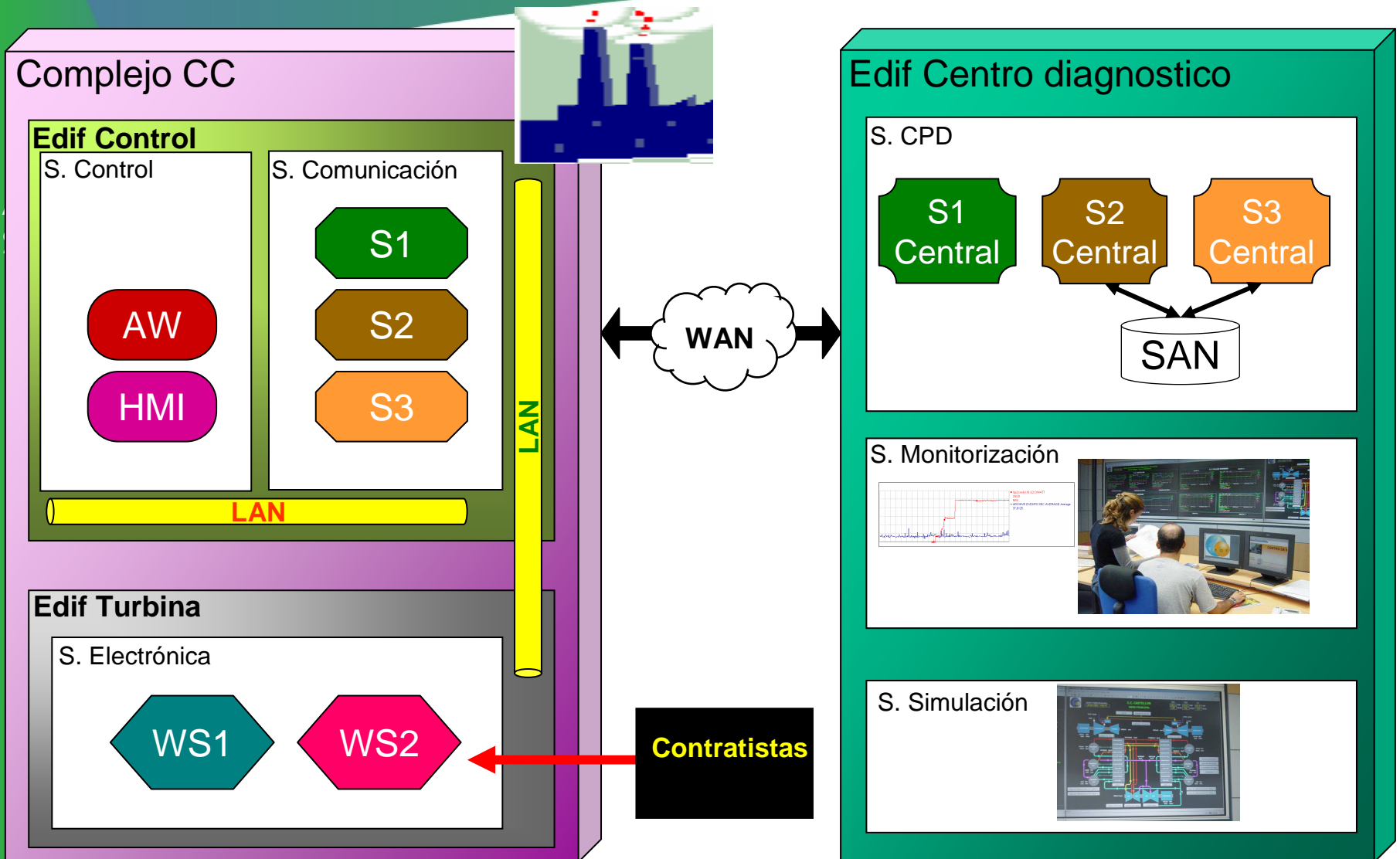
Búsqueda de ACTIVOS de INFORMACIÓN



Adhoc
Security

Activo de Información	Descripción
Operaciones	Información operativa para la explotación de la central
Mantenimiento	Información de mantenimiento de la central
Seguimiento	Información en tiempo real de la actividad de las plantas
Diagnóstico	Información de diagnóstico de la central para recomendaciones de operaciones y mantenimiento
Información medioambiental	Información medioambiental de niveles de emisión, inmisión, vertidos ...
Entrenamiento	Información para la formación de los operadores

Esquema de DEPENDENCIAS



VALORACIÓN de ACTIVOS: 26 criterios de valoración (*)



Adhoc
Security

	Información no disponible		Intercambio inadecuado de información
15mn	durante 15mn	IN	inserción de mensajes falsos, tal como petición inadecuada
1h	durante 1 hora	RO	repudio de Origen: mensaje rechazado por quien lo mandó
3h	durante 3 horas	RC	repudio de Destino : el destinatario niega haberlo recibido
12h	durante 12 horas	Nd	NO entrega: una petición no llega a su destino de forma accidental o intencionada
1d	durante 1 día entero	Rp	Duplicación de la petición
2d	durante 2 días	Mr	Destinatario equivocado
1s	durante 1 semana	TM	Monitorización de tráfico: se conoce el volumen y los interlocutores sin conocer el contenido
2s	durante 2 semanas	OS	Orden equivocado en los procesos
1m	durante 1 mes		
2m	durante 2 meses ó mas		
	Dstrucción de la información		
DP	perdida parcial desde el ultimo backup		
DT	perdida total con backup induidos		
	Revelación de la Información		
DI	a personas internas de [redacted] pero no autorizadas a ver los datos		
DCSP	a personas externas de empresas contratadas con acceso a sistemas y redes pero no a los datos		
DO	a cualquier persona externa a [redacted]		
	Modificación de la información		
SE	error puntual o accidental de entrada, tedado, etc.		
WE	error generalizado en toda la información por ejemplo debido a un fallo en la programación		
DM	error deliberado debido a una mala intención		

1-3

4-6

7-10

Los escenarios se valoran en una escala de 1 a 10

*Fuente: CRAMM

VALORACIÓN de ACTIVOS (II): Impactos de los activos aplican a las dependencias

Pérdida de Disponibilidad

Impactos en los activos



Adhoc
Security

	máximo	2	2	3	4	5	6	7	7	8	8	3	8
Descripción	15mn	1h	3h	12h	1d	2d	1s	2s	1m	2m+		Destruc. Parcial	Destruc. Total
Data Asset:			3	4	5	6	7	7	8	8		3	6
Data Asset:			2	2	3	3	5	5	5	5		1	5
Data Asset:	2	2	3	3	3	3	3	4	4	5		1	2
Data Asset:							3	3	4	6		1	8
Data Asset:								1	2	3		2	2
Data Asset:								1	1	1		1	1
Data Asset:													

UBICACIONES

Elementos HW

	máximo	8	2	2	3	4	5	6	7	7	8	8	3	8
Descripción	Destruc. Física	15mn	1h	3h	12h	1d	2d	1s	2s	1m	2m+		Destruc. Parcial	Destruc. Total
Location Asset	8			3	4	5	6	7	7	8	8		3	6
Location Asset	5			3	4	5	6	7	7	8	8		3	6
Location Asset	2			3	4	5	6	7	7	8	8		3	6
Location Asset	5	2	2	3	3	3	3	3	4	5	6		1	8
Location Asset	3	2	2	3	3	3	3	3	4	5	6		1	8
Location Asset	6			2	2	3	3	5	5	5	5		1	5
Location Asset	1								1	2	3		2	2

Adhoc Security

ANALISIS de RIESGOS



Adhoc
Security

Método de cálculo del valor del riesgo para cada escenario

Valor amenaza/vulnerabilidad

Amenaza Vulnerabilidad	VL			L			M			H			VH		
	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Impacto															
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3

Valor impacto

Valor riesgo

Propuesta de CONTRAMEDIDAS (I): según apartados de la ISO17799

ISO 17799:2005 → 133 Controles con +de 1000 medidas de implantación



Adhoc
Security



		1	2	3	4	5	6	Total general
5	POLÍTICA DE SEGURIDAD					1	16	17
6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			3	2	16	34	55
7	GESTIÓN DE ACTIVOS		4	15	6	44	30	99
8	SEGURIDAD LIGADA AL PERSONAL			1	5	1	41	48
9	SEGURIDAD FÍSICA	5	27	181	98	438	319	1068
10	GESTIÓN DE COMUNICACIONES Y OPERACIONES	3	39	192	183	479	607	1503
11	CONTROL DE ACCESO			81	83	188	706	1058
12	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE II		48	21	160	190	215	634
13	GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN			5	6	9	65	85
14	GESTIÓN DE LA CONTINUIDAD DE NEGOCIO			26	53	26	30	135
15	CONFORMIDAD			22	86	70	169	347
	Total general	8	118	547	682	1462	2232	5049

Propuesta de CONTRAMEDIDAS (II): según CIP y nivel de riesgo gestionado



Adhoc
Security

CIP002 Critical Cyber Assets

CIP003 Security Management controls

CIP004 Personnel and Training

CIP005 Electronic security

CIP006 Physical security

CIP007 Systems Security Management

CIP008 Incident reporting & Response planning

CIP009 Recovery Plans for Critical Cyber Assets

Codigo CIP	6	5	4	3	2	1	Total general
CIP-002	9	5	4	3			21
CIP-003	213	111	68	34	27		453
CIP-004	51	45	15	8			119
CIP-005	261	141	19	63	11		495
CIP-006	190	14	58	5			267
CIP-007	716	525	272	207	17		1737
CIP-008	94	14	7	5			120
CIP-009	171	114	82	62	4	3	436
NO CIP	527	493	157	160	59	5	1401
Total general	2232	1462	682	547	118	8	5049

GESTIÓN de los RIESGOS

Umbral Riesgos → Obligaciones →
de gestión

Adhoc
Security

>5

3-Necesario

*Estado
Contramedida
“objetivo”*

A-Auditado

4 - 5

2-Recomendado

I-Implementado

<4

1-Informativo

D-Definido

S-Sin definir

Amenaza Vulnerabilidad	VL			L			M			H			VH		
	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Impacto															
10	5	5	6	5	5	6	6	6	6	6	7	7	7	7	7
9	4	5	5	5	6	6	5	6	6	6	6	7	7	7	7
8	4	4	5	4	5	5	5	5	6	6	6	6	6	6	7
7	3	4	4	4	4	5	4	5	5	5	5	5	5	6	6
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
4	2	2	3	2	3	3	3	3	3	4	3	4	4	4	5
3	1	2	2	2	3	2	3	3	3	3	3	4	3	4	4
2	1	1	2	1	2	2	2	3	2	3	3	3	3	3	4
1	1	1	1	1	1	1	1	2	1	2	2	2	2	2	3

Madurez de las medidas

MÉTRICA de NIVELES de SEGURIDAD



Riesgos

Ac
Se

3-Necesario



3

2-Recomendado



2

1-Informativo



1

N1

“objetivo”

**Estado
Contramedida**

N2

“real”

A-Auditado

3

I-Implementado

2

D-Definido

1

S-Sin definir

0

Nivel adecuado → 0 → Objetivo conseguido

Nivel de seguridad de un subconjunto= $\sum (N2-N1)$ sumatoria para todas las propuestas de CM

Generación de Propuesta de Contramedidas (D.S.C): Evaluación del estado de las Contramedidas



Adhoc
Security

P.O.S					Max		5		
Detalles					Min		4		
					UMBRALES RIESGO				
Generado por la Herramienta CRAMM					VALORES EXTRAIDOS DEL GAP CM				
Codi go	Grupo CM	Subgrupo CM	Descripción CM	Elemento	NdR	Obj	Solución er	Estado actual	NIVS EC
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled	ELT1 ELT2 ELT3 ...	5	2	Procedimiento Personas Mantenimiento (pero actualmente	1-Definida	-1
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		4	2		0-Sin definir	-2
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled		5	2	Procedimiento Personas Mantenimiento (pero actualmente	1-Definida	-1
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1		0-Sin definir	-1
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1	Procedimiento Personas Mantenimiento (pero actualmente	1-Definida	0
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		4	2		0-Sin definir	-2
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1		0-Sin definir	-1
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1		0-Sin definir	-1
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1	Procedimiento Personas Mantenimiento (pero actualmente	1-Definida	0
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		4	2	Estudiar si existe Clausulas de seguridad fisica en el contrato de	0-Sin definir	-2
270.	270. Hardware	430. Supervision of Hardware	Access by maintenance staff should be controlled		4	2		0-Sin definir	-2
430.1.	Maintenance	430. Supervision of Hardware	Access by maintenance staff should be controlled		3	1		0-Sin definir	-1

Contramedida

Elemento T.I

Situación de las CMS

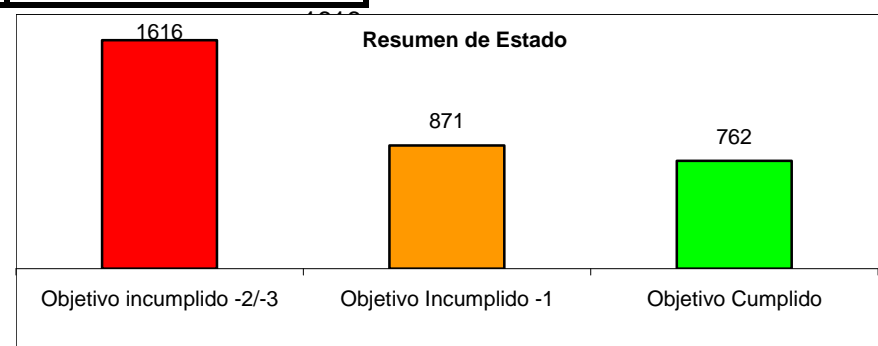
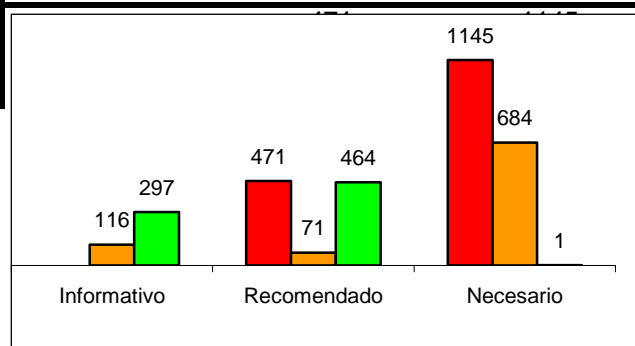
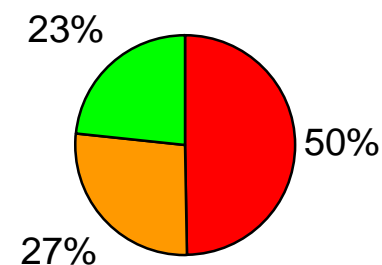
Diferencial con Objetivo de Seguridad

Seguimiento de la implantación de las CMS



Adhoc
Security

Estado CM				3341
No aplica	1	14	77	92
0-Sin definir	28%	47%	44%	Objetivo incumplido -2/-3
1-Definida	19%	7%	18%	
2-Implementada	53%	46%	37%	
3-Auditada	0%	0%	0%	Objetivo Incumplido -1
Estado valorado	100%	100%	100%	Objetivo Cumplido
	413	1006	1830	3249

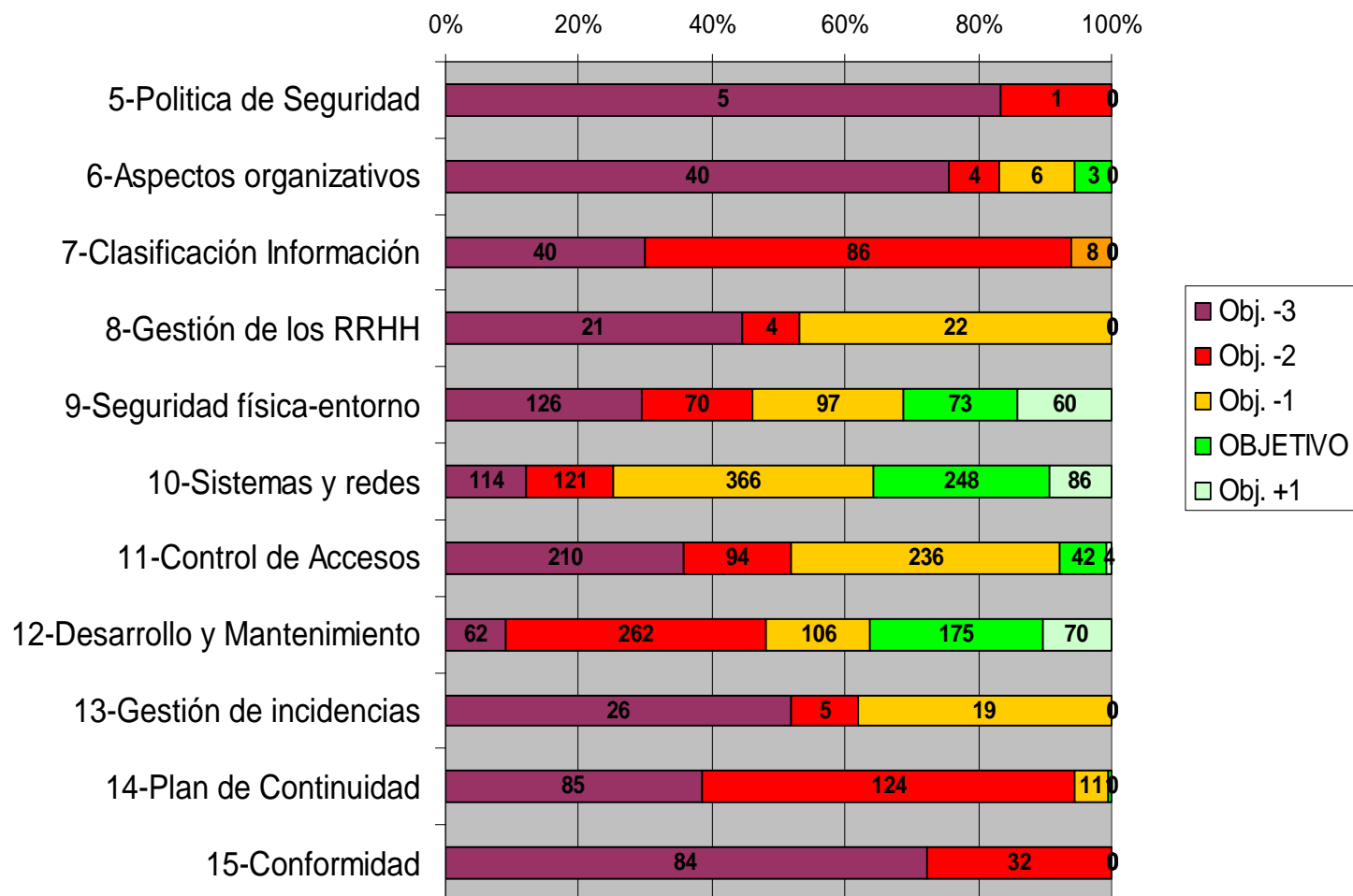


Diferencial con la ISO17799



Adhoc
Security

Diferencial con el objetivo de los Controles por áreas de la ISO 17799

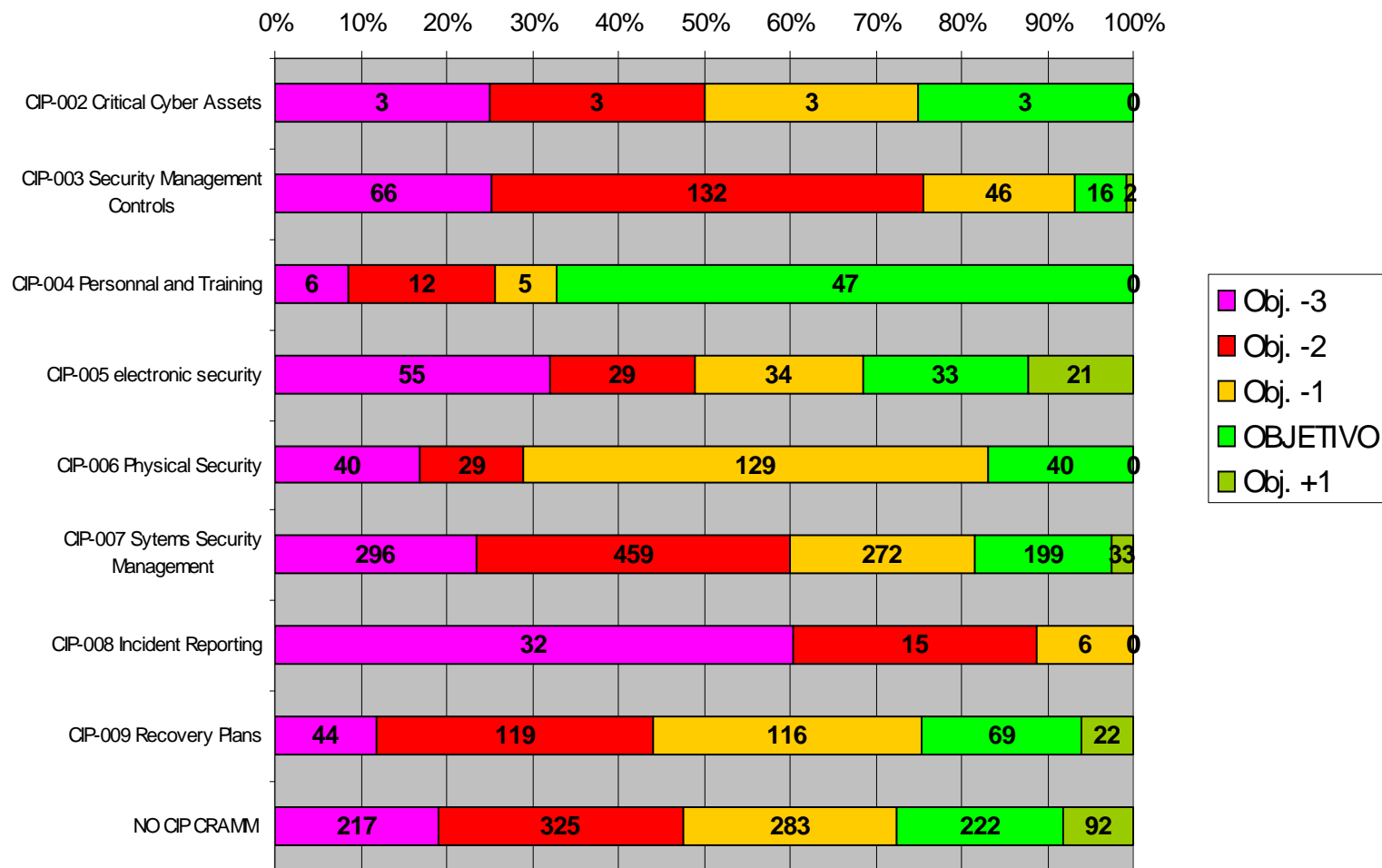


NIVSEC Diferencial NERC/CIP



Adhoc
Security

Diferencial con el objetivo de los Controles por áreas del CIP



Líneas de trabajo (I): Propuesta 1 de estructura de proyectos de seguridad



Adhoc
Security

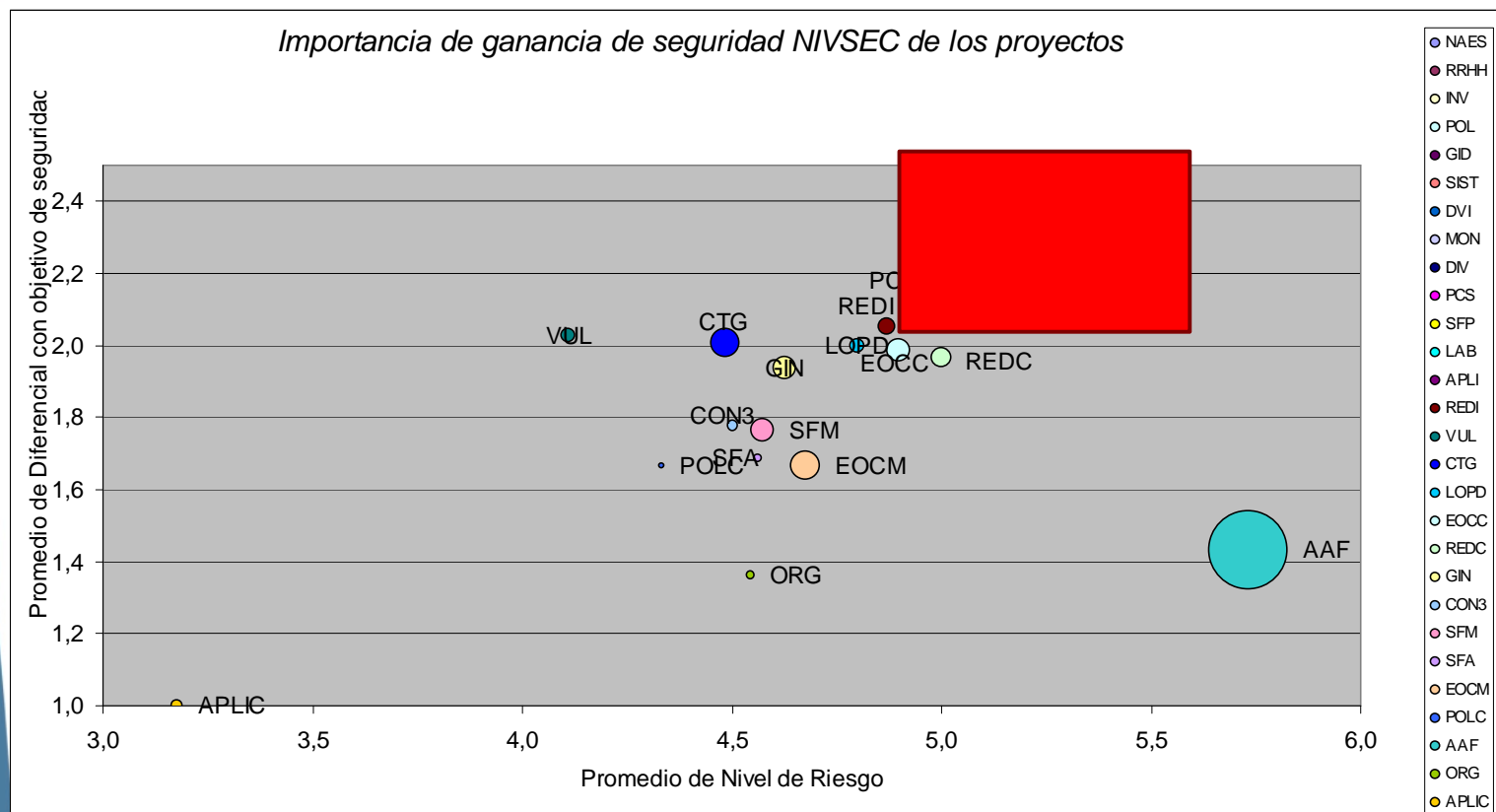
Agrupación de líneas de trabajo según relación CMS/puntos de la norma ISO 17799

Código	Descripción Proyecto	Servicio Responsable	NIVSEC	NIVEL	Nº CM	Efectividad media	Coste medio	NdR Medio
ADA	Adecuación Desarrollo Aplicaciones	Desarrollo/ Propietario	-1,8	-44	25	2,4	2,0	3,6
ARED	Arquitectura de red segura	Comunicaciones	-1,4	-7	5	3,0	2,4	5,4
ASR	Administración Segura de la Red	Comunicaciones	-2,9	-96	33	3,0	3,0	6,0
AUD	Plan de auditoría	Control Interno/CGA	-1,1	-768	714	2,6	2,0	6,0
CAL	Manual de calidad	Gerencia	-1,4	-11	8	2,0	1,4	4,0
CAM	Gestión de cambios en Sistemas y Redes	Servicios Informáticos	-2,0	-403	204	2,6	1,7	5,3
CLA	Clasificación de la información	Servicios Informáticos	-2,4	-308	129	2,3	2,6	5,3
COM	Intercambio y Comercio electrónico seguro	Servicios Informáticos	-1,9	-31	16	2,9	3,0	5,8
CONR	Aspectos contractuales de Externalización de red	Servicios Informáticos	-2,7	-60	22	2,1	2,2	5,9
CTG	Plan de contingencias	Servicios Informáticos	-2,4	-498	210	2,3	2,2	5,1
DES	Estándares de desarrollo	Desarrollo	-2,1	-312	152	3,0	2,4	4,5
DIV	Divulgación de la seguridad	RRHH / SSII	-2,8	-151	53	2,3	1,4	5,8
DVI	Detección de Virus en Servidores	Seguridad informática	-1,8	-44	25	2,8	2,0	5,7
GID	Gestión de identidad	Servicios Informáticos	-2,3	-539	230	2,6	2,4	5,9
GIN	Gestión de incidencias	Servicios Informáticos	-2,4	-230	97	2,8	2,8	5,5
INV	Gestión de inventario	Servicios Informáticos	-2,6	-111	43	2,0	3,0	5,9
JUR	Aspectos jurídicos: Obligaciones legales, RRHH y contratos	Asesora jurídica	-2,6	-45	17	2,0	1,9	6,4
LOPD	Temas de tratamiento de información de carácter personal	Asesora jurídica LOPD RRHH	-2,8	-336	120	1,3	1,3	5,8
MON	Monitorización y revisión	Servicios Informáticos	-1,5	-83	55	2,9	2,9	3,7
MSPC	Mejora Seguridad Puesto Trabajo (Virus e Intrusión)	SSII/Puesto Trabajo	-2,0	-47	24	2,4	2,6	5,5
NAP	No aplican		0,0	0	94	2,0	1,8	5,8
ORG	Organización y gestión de la seguridad	Gerencia/Seguridad	-3,0	-6	2	2,5	1,5	6,0
OSP	Operaciones de seguridad puntuales	Servicios Informáticos	-2,8	-11	4	3,0	2,0	5,8
POL	Normas y procedimientos de seguridad	Servicios Informáticos	-2,7	-241	88	2,0	2,1	5,7
RED	Redes y comunicaciones	Comunicaciones	-2,0	-60	30	2,0	2,1	5,5
SFA	Control de acceso Físico	Infraestructura y servicios	-2,7	-126	47	2,5	1,8	6,1
SFM	Material y mercancías	Infraestructura y servicios	-2,7	-69	26	2,7	2,2	5,8
SFO	Prevención Operacional	Infraestructura y servicios	-2,3	-90	40	2,9	2,6	5,3
SFP	Seguridad Perimetral	Infraestructura y servicios	-2,6	-103	39	2,7	2,6	6,2
VUL	Análisis de vulnerabilidades	Seguridad informática	-2,0	-73	36	2,0	2,9	6,0

Nivel de PRIORIDAD de proyectos de seguridad



Adhoc
Security



Solo para CM con NIVSEC < 0 y NO IMPLEMENTADO

Líneas de trabajo (II): Propuesta 2 de estructura de proyectos de seguridad

5 líneas de actuación



Adhoc
Security

Gestión



Gestión, organización, divulgación
y evaluación de la seguridad



Ciberwall



Proteger los elementos tecnológicos de las CC

CARE



Centro de Alerta, Respuesta y Emergencias



PIC



Protección del acceso y entorno operativo
de las Infraestructuras Críticas



Integración

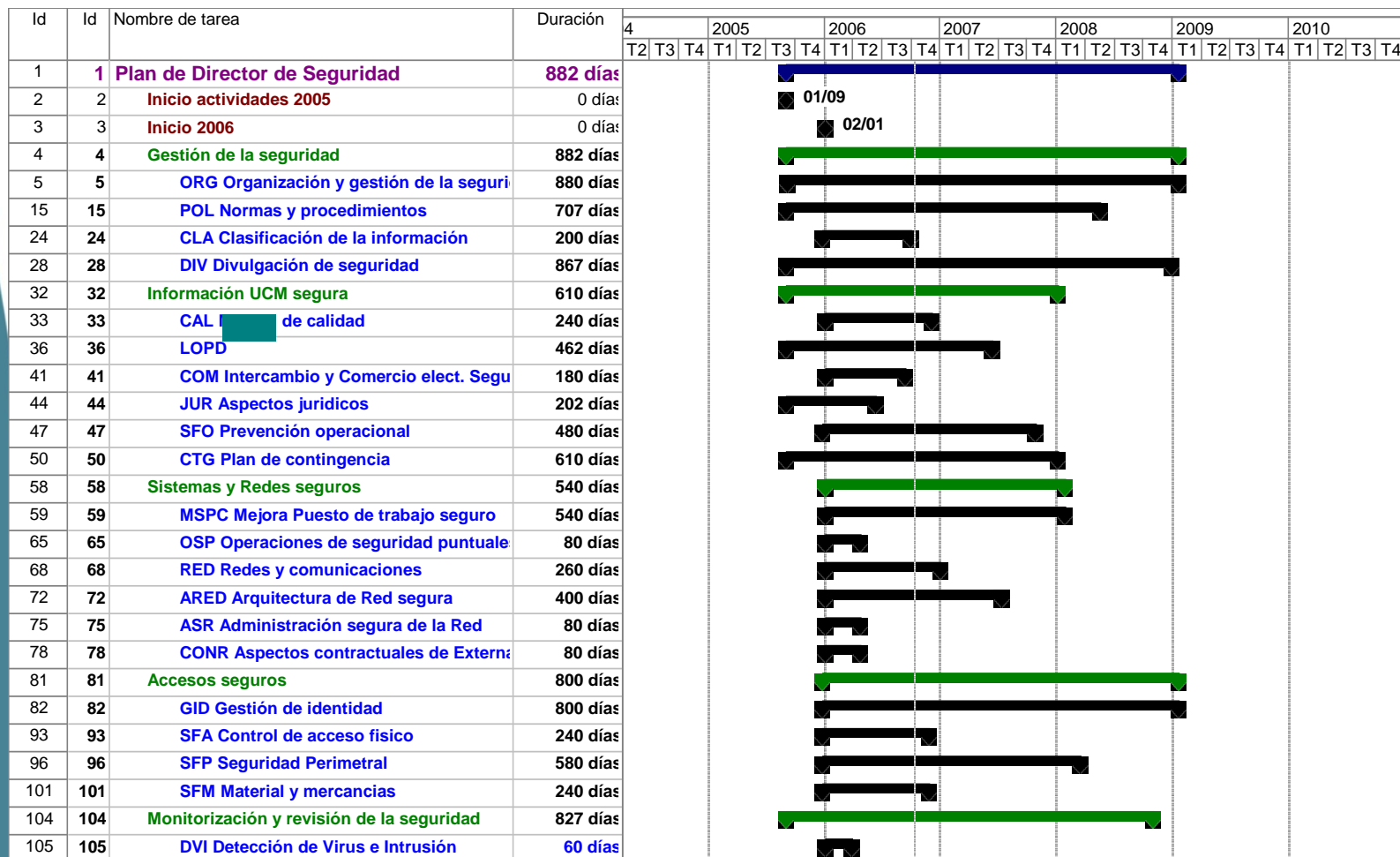


Integración con
procesos corporativos

Líneas de trabajo (III): Planificación de proyectos de seguridad en el tiempo



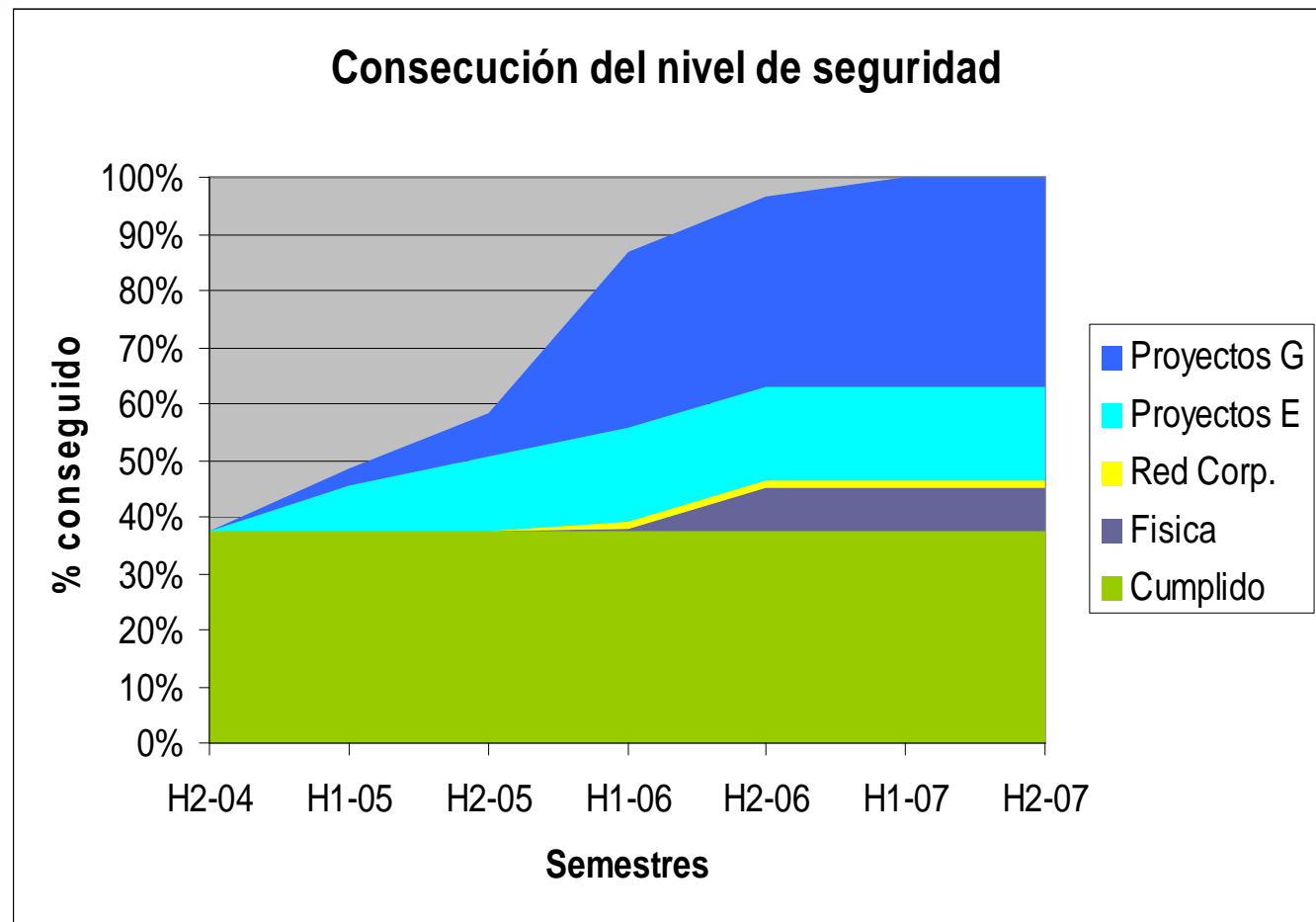
Adhoc
Security



Seguimiento de consecución objetivos de seguridad en la gestión de riesgos según planificación prevista



Adhoc
Security



100% = 10.985 Contramedidas identificadas en su Nivel de seguridad

Presupuesto de los proyectos de seguridad



Adhoc
Security

- ✓ Evaluación de costes:
- HW, SW para inmovilizado
 - Servicios
 - Costes recurrentes

												Nº Pax * Dias* 8				Servicios	
												Tarifa Media Externo/hora				HW+SW	
												60 €				15% anual	

SUBTOTAL												HW	SW	Servicios	h.int	Costes Rec.
												1.337.800 €	738.400 €	1.256.770 €	8248,5	485.185 €
												anual				

XXX														
YYY	10 prioritarios													

LINEA	Código	Desc.	ACTIVIDADES	Servicio Responsabl e	NIVSE C	NdR Medio	HW	SW	Servicios	h.int	Costes recurrentes anuales	HW	SW	Servicios	H.int	Costes recurrentes anuales
GESTIÓN	ORG	ORG Organización y gesti			-0,3	4,6	- €	25.000 €	204.480 €	176	150.760 €					
			Definición de la organización											4.800 €	32	
			Documentar, implantar el SGSI (con un SW de apoyo)										15.000 €	38.400 €	32	1.000 €
			Cuadro de mando: diseño e implantación										10.000 €		16	
			Oficina de seguridad-Administración y seguimiento de la seguridad											149.760 €	96	149.760 €
GESTIÓN	POL	POL Normas y procedimie			-2,2	5,092	- €	- €	28.800 €	16	- €					
			Marco normativo en CC-CMDS											19.200 €	8	
			Guías para usuarios											9.600 €	8	
GESTIÓN	DIV	DIV Divulgación de segur			-1,6	5,152	15.000 €	15.000 €	31.200 €	88	14.100 €					
			Diseño del Plan de concienciación											4.800 €	16	
			Selección y adecuación Plataforma: CD-Rom, CBT,...									15.000 €	15.000 €	4.800 €	16	4.500 €
			Diseño de contenido: Virus, Incidentes,...											9.600 €	16	9.600 €
			Formación en seguridad											12.000 €	40	