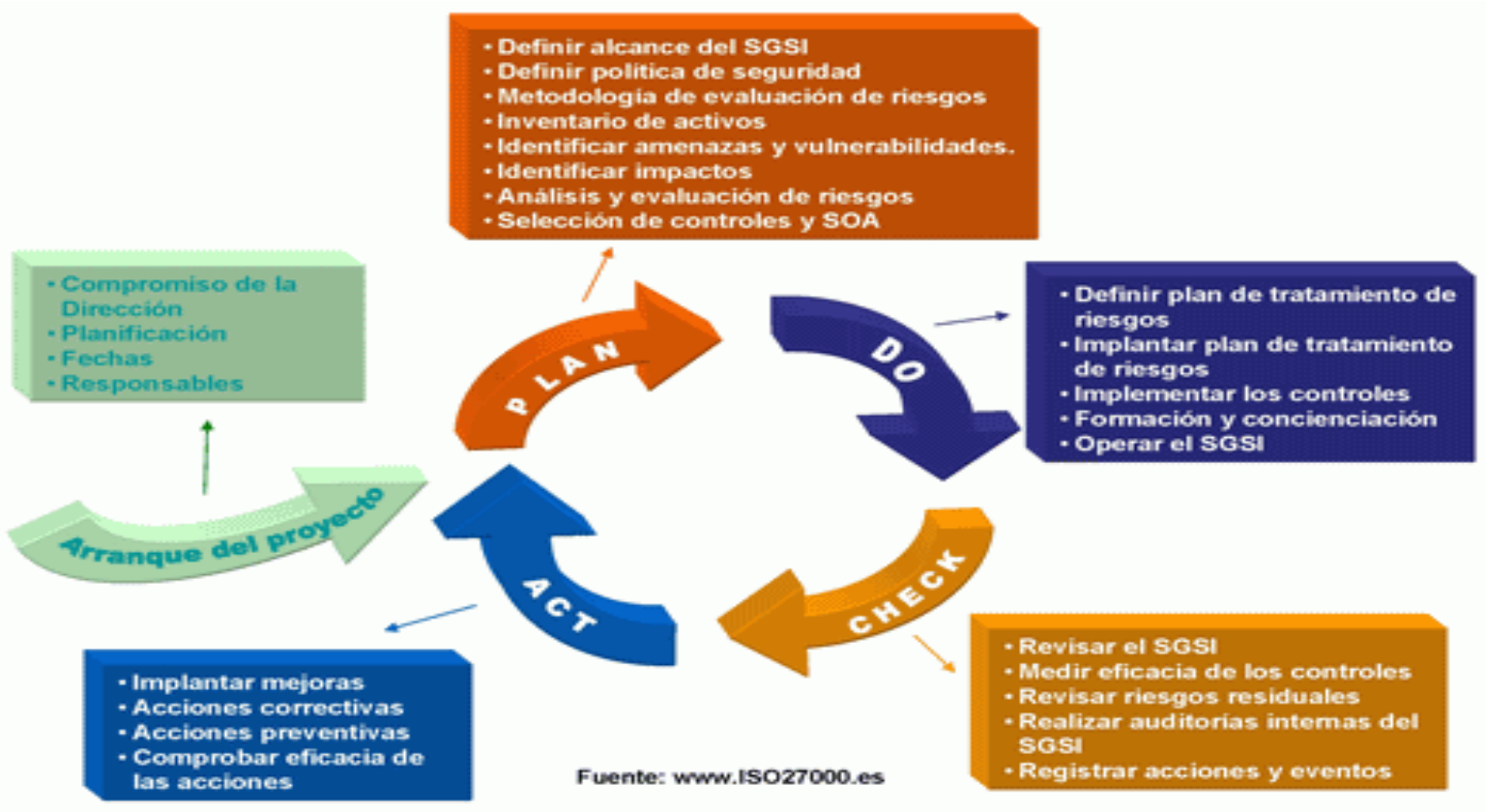
XXX
Implementación ISO 27001:2013

Informe ejecutivo

Metodología

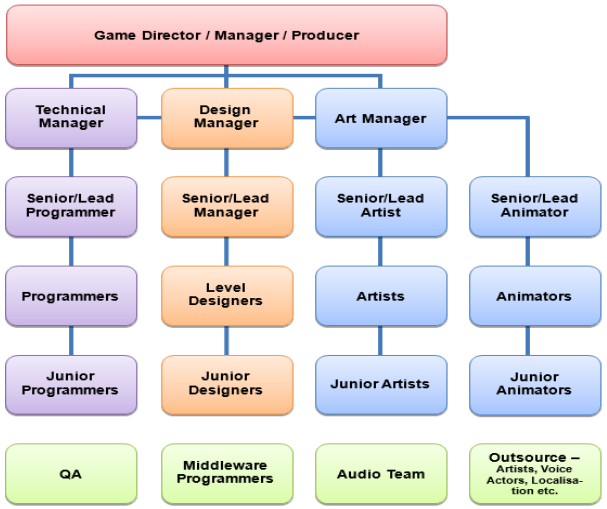


Contextualización

- Como primer paso se realiza la contextualización de la empresa a la que se va a realizar el análisis
- Necesario para conocer el contexto de la empresa y poder realizar un mejor análisis de sus necesidades.
- Características generales:
  - Empresa de videojuegos móviles
  - 3 años de vida
  - Posible pronta expansión
  - Gran interés y preocupación por parte de la dirección

Características

- 30 Empleados + Freelances
- 2 Oficinas
- Promoción del teletrabajo y BYOD
- Gran uso de [illegible] stemas/plataformas Cloud.



Alcance y objetivos

- Objetivos:
  - Identificar, calificar y hacer un tratamiento adecuado de los riesgos
  - Implementación de un equipo de seguridad proactivo
  - Mitigar lo máximo posible cualquier incidente de seguridad
  - Proteger la empresa y la información que posee
  - Dar cumplimiento a la normatividad y legislación vigente
  - Fomentar la cultura organizacional, la capacitación y toma de conciencia en seguridad informática
- Alcance: todos los procesos de negocio y de desarrollo de la empresa, así como cualquier otra actividad que resulte de la aplicación de esta auditoría

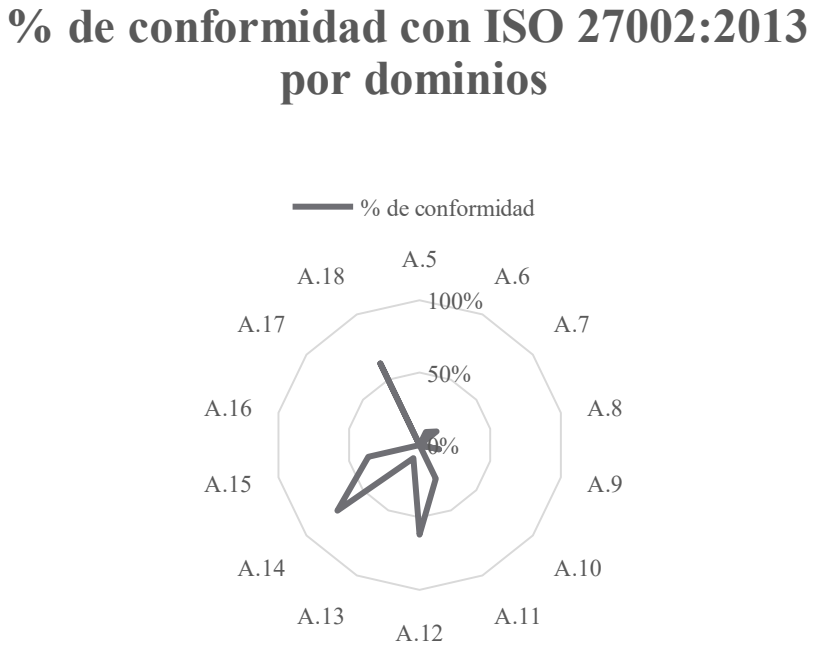
Definición de niveles de cumplimiento

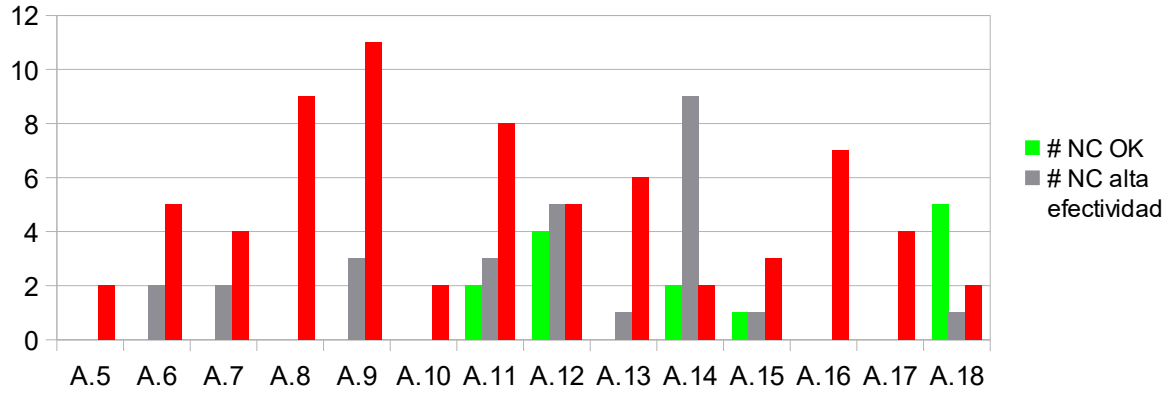
Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

Análisis diferencial 27001:2013

	Dominio	% de conformidad	# NC mayores	# NC menores	# NC OK
4	Contexto de la organización	5%	5	0	0
5	Liderazgo	1%	14	0	0
6	Planificación	0%	31	0	0
7	Soporte	10%	14	3	0
8	Funcionamiento	0%	3	0	0
9	Evaluación de Rendimiento	5%	23	0	0
10	Proceso de mejora	0%	11	0	0

Análisis diferencial 270002:2013





Política de seguridad: Objetivos y alcance

- Entender que la información en toda la organización debe ser protegida, conservando la confidencialidad, integridad y disponibilidad de la misma
- Los trabajadores deben incluir la cultura de seguridad como parte de sus funciones diarias
- Las normas definidas en la política de seguridad serán de obligado cumplimiento
- Todos los trabajadores y personal que trate con la información deberán conocer y aceptar la política de seguridad de la empresa
- La empresa tomará las medidas y acciones que considere oportunas para hacer cumplir con la política de seguridad

Definición de responsabilidades

- Se definen los siguientes comités y roles, asignándole responsabilidades específicas:
  - El Comité de Dirección
  - Comité de Seguridad de la Información (CSI)
  - Responsable de seguridad de la información (RSI)

Así mismo, se definen responsabilidades generales en los siguientes ámbitos:

- Nivel dirección
- Nivel técnico operativo
- Nivel de usuario

Definición del S.G Documental

	Definición	Obligatoriedad	Aprobado por	Divulgación
Políticas	Recogen directrices estratégicas, de alto nivel, bajo las cuales se amparará cualquier acción en materia de seguridad de la información. Todo documento de nivel inferior debiera desarrollar en base a una política	Las políticas son de obligado cumplimiento y deben ser aprobadas por la dirección	La dirección de la compañía	Todo el personal y colaboradores
Normas	Desarrollan la política a un nivel concreto y específico	De obligado cumplimiento por todo el personal y colaborador	Dirección	A quien se indique en la guía como objetivo de la misma
Guías	Proporciona una solución a un problema determinado	Buenas prácticas. No obligado cumplimiento, pero sí altamente recomendado	Comité asignado	A quien se indique en la guía como objetivo de la misma
Procedimiento	Presentan un conjunto de acciones a llevar a cabo para conseguir un determinado objetivo	De obligado cumplimiento por todo el personal y colaborador	Persona responsable del procedimiento	A quien se indique en el procedimiento como objetivo de la misma
Manuales (técnicos y de usuario)	Son listas de tareas o instrucciones detalladas para realizar determinadas acciones o utilizar herramientas concretas, se dividirán en manuales orientados a técnicos o a usuarios finales	Recomendado	Responsable	Persona que lleva a cabo la acción descrita en el manual

Nomenclatura documental

- Se procede a definir una nomenclatura común para la documentación (SGSI-XX-Título)

XX: Tipo de documento. Siendo:

- PO: Política
- NO: Norma
- GU: Guía
- PR: Procedimiento
- MU: Manual de Usuario
- MT: Manual Técnico

- De la misma manera se define una política de acceso y publicación

Procedimiento de auditorías internas

- Se define un procedimiento para la realización de auditorías internas
- Son el instrumento que se nos proporciona para comprobar que nuestro SGSI se encuentre correctamente actualizado con respecto a la norma ISO 27001:2013.
- Mediante estas auditorías se realiza un control periódico del estado de implementación de la norma ISO
- Definición de:
  - Calendario
  - Equipo
  - Procedimiento de actuación

Gestión de Indicadores

- Se definen los indicadores y sus procesos de gestión
- Necesario para comprobar el comportamiento y la eficacia de los controles de seguridad implantados dentro de un tiempo específico
- Definidos por dominios de la norma. Formato (Axx-Iyy) siendo “xx” el dominio de la noma e “yy” el numero de indicador en la misma.
- Los indicadores se actualizarán y revisarán una vez al año, se realizará una auditoría para comprobar la eficacia de cada uno de ellos y finalmente se realizará un informe que se enviará a dirección para su evaluación.

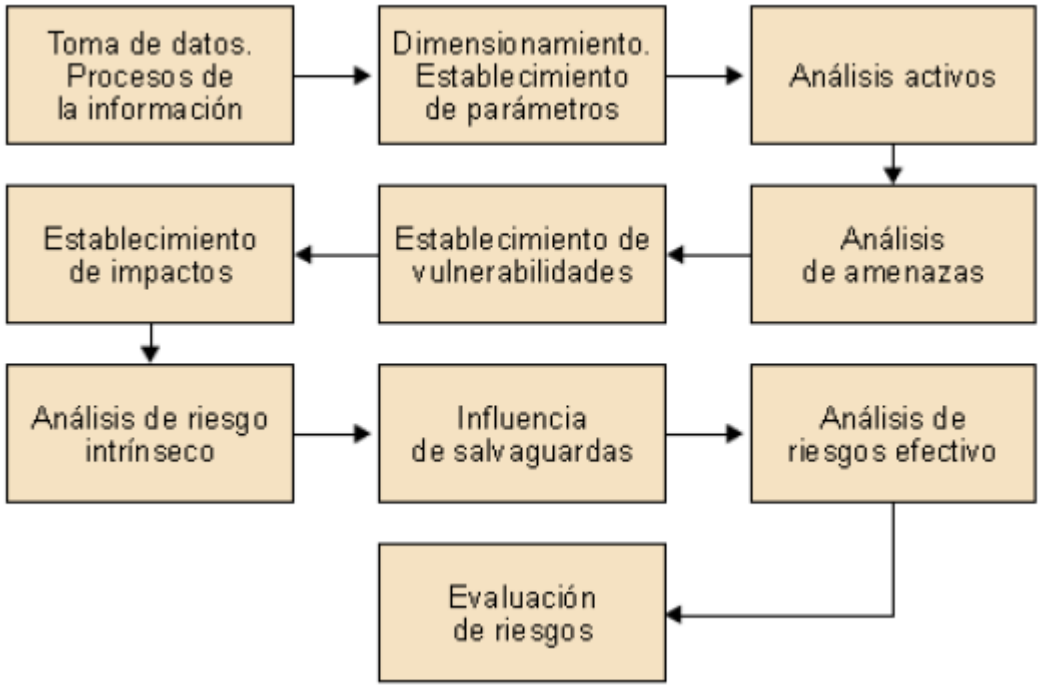
Procedimiento de revisión por dirección

- El procedimiento de revisión de dirección consiste en controlar el correcto funcionamiento del SGSI una vez este implantado.
- En caso de detectar problema, este control llevara como resultado acciones correctoras
- Se define:
  - Composición de los miembros
  - Proceso y método de convocatoria
  - Procedimiento de revisión

Declaración de aplicabilidad

- En este apartado se definen qué puntos de la norma ISO aplica para nuestra auditor
- Se proporciona una justificación del motivo por el cual aplicaría o no

Análisis de riesgos: Metodología



Análisis de riesgos: Objetivos

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Análisis de riesgos: Actividades

- Identificación de los activos.
- Identificación de los requisitos legales y de negocio que son relevantes para la identificación de los activos.
- Valoración de los activos identificados
- Identificación de las amenazas y vulnerabilidades
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgos preestablecidos.

Dimensionamiento de parámetros: Ejemplos

Valoración	Rango	Valor
Muy alto	> 250.001 Euros	300.000 Euros
Alto	Entre 100.001 y 250.000 Euros	175.000 Euros
Medio	Entre 15.001 y 100.000 Euros	60.000 Euros
Bajo	Entre 5001 y 15000 Euros	10.000 Euros
Muy bajo	<5000 Euros	2500 Euros

Probabilidad	Frecuencia	Valor
Muy Alta	Probabilidades de ocurrencia 1 vez al día	1
Alta	Probabilidades de ocurrencia 1 vez cada 2 semanas	26/365=0,071233
Media	Probabilidades de ocurrencia 1 vez cada 2 meses	6/365=0,016438
Baja	Probabilidades de ocurrencia 1 vez cada 6 meses	2/365=0,005479
Remota	Probabilidades de ocurrencia 1 vez al año	1/365=0,002739

Valoración de activos: Ejemplo

Ámbito	Activo	ID	Valor	Aspectos críticos				
				A	C	I	D	A
L	Rack principal (CPD)	[L1]	10	8	9	10	10	8
L	Archivo	[L2]	8	9	9	7	8	7
AUX	Aire acondicionado oficina	[AUX1]	2	-	-	-	7	-
AUX	Aire acondicionado CPD	[AUX2]	5	-	-	-	8	-
AUX	UPS Rack	[AUX3]	5	-	-	-	8	-
AUX	Cableado LAN	[AUX4]	7	-	-	-	9	-
AUX	Cableado Eléctrico	[AUX5]	7	-	-	-	9	-
HW	Punto de acceso WIFI	[AUX6]	5	2	7	3	6	5
HW	Switch	[AUX7]	5	4	5	7	7	5
COM	Router fibra une las sedes y da conexión a Internet	[COM1]	6	5	6	8	8	6
HW	Firewall	[HW1]	6	7	6	8	9	8
HW	Centralita IP	[HW2]	7	3	6	6	9	8
HW	FAX	[HW3]	4	2	3	3	5	3
HW	3 impresoras/Escaner red Laser	[HW4]	3	2	2	4	5	5
HW	Servidor Sistema de integración continua (linux)	[HW5]	9	9	7	9	9	7
HW	Servidor VPN	[HW6]	9	9	9	9	9	8
DATOS	Servidores CRM: Nóminas, datos de cliente y negocio	[DATOS 1]	8	9	10	10	9	6
HW	IDS	[HW7]	5	6	7	6	7	8
HW	SIEM	[HW8]	6	6	6	6	8	8
HW	Servidores de Logs	[HW9]	6	9	9	9	10	8
DATOS	Servidor Backup	[DATOS 2]	9	9	9	9	10	7
P	20 empleados	[P1]	8	-	-	-	6	-
HW	20 Portátiles empleados	[HW10]	9	6	8	7	9	4
HW	2 Portátiles para el uso interno en CPD y similar	[HW11]	7	6	7	7	7	5
HW	20 Móviles empleados	[HW12]	6	5	8	6	6	7
HW	10 tablets Android	[HW13]	6	5	8	3	3	3
HW	20 Dispositivos conexión 3G/4G	[HW14]	5	5	6	2	5	5
SW	20 Libreoffice	[SW1]	4	2	3	2	3	3
SW	20 Cliente programa VPN	[SW2]	2	8	6	7	7	6
SW	5 Photoshop	[SW3]	2	2	2	2	4	3
SW	IDE Desarrollo	[SW4]	2	3	3	3	5	6
Datos	Imágenes corporativas	[Datos3]	8	-	-	6	8	5
Datos	Recursos artísticos	[Datos4]	8	-	-	7	7	5

Identificación de amenazas: Ejemplo

ACTIVOS [DATOS]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[DATOS1] Servidores CRM: Nóminas, datos de cliente y negocio	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS2] Servidor Backup	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS3] Imagenes corporativas	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS4] Recursos artisticos	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS5] Estadísticas Juego Usuario (Amazon)	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS6] Servidor de almacenaje de código (externo)	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS7] Servidor de recursos y documentación (externo)	Alta	100,00 %	100,00%	75,00%	100,00%	
[DATOS8] Servidor de correo (Externo)	Alta	100,00 %	100,00%	75,00%	100,00%	
LISTA DE AMENAZAS						
E.1] Errores de los usuarios	Alta		25,00%	25,00%	25,00%	
[E.2] Errores del administrador	Baja		30,00%	50,00%	30,00%	
[E.15] Alteración accidental de la información	Baja			20,00%		
[E.18] Destrucción de información	Baja			25,00%		
E.19] Fugas de información	Media			25,00%		
[A.5] Suplantación de la identidad del usuario	Baja	100,00 %	50,00%	50,00%		
[A.6] Abuso de privilegios de acceso	Baja		100,00%	50,00%	100,00%	
[A.11] Acceso no autorizado	Baja			75,00%		
[A.15] Modificación deliberada de la información	Baja			50,00%		
[A.18] Destrucción de información	Remota				100,00%	
[A.19] Divulgación de información	Remota		100,00%			

Evaluación del impacto y del riesgo

- Una vez identificados y evaluados activos y amenazas procedemos a evaluar el Impacto y el riesgo potencial
- El impacto viene dado por la siguiente formula:

  Impacto Potencial = Valor Activo X Porcentaje de Impacto

- *El riesgo potencial:*

  Riesgo = Frecuencia X Impacto Potencial

Tras el cálculo se procede a realizar medidas para mitigar el riesgo que se encuentre por encima del umbral definido por dirección

Cálculo del riesgo

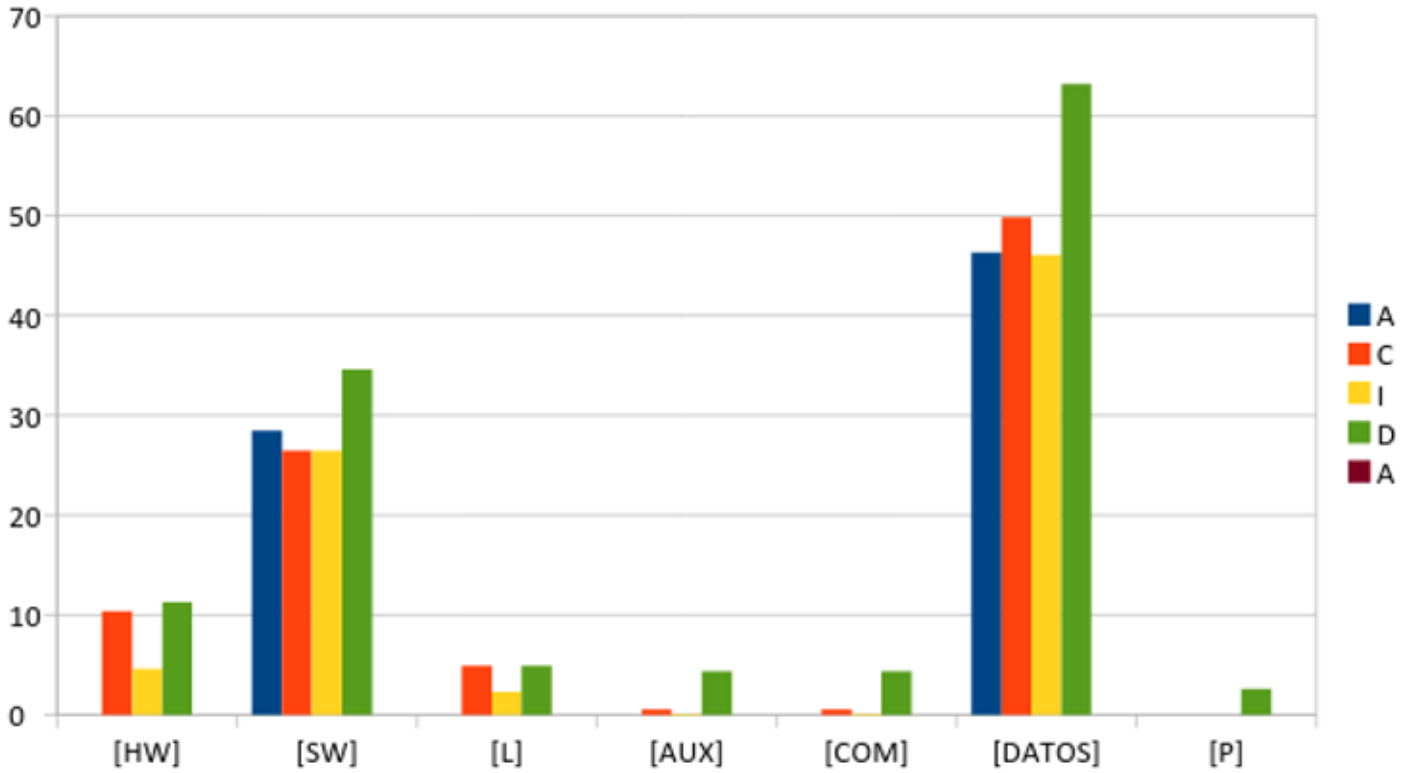


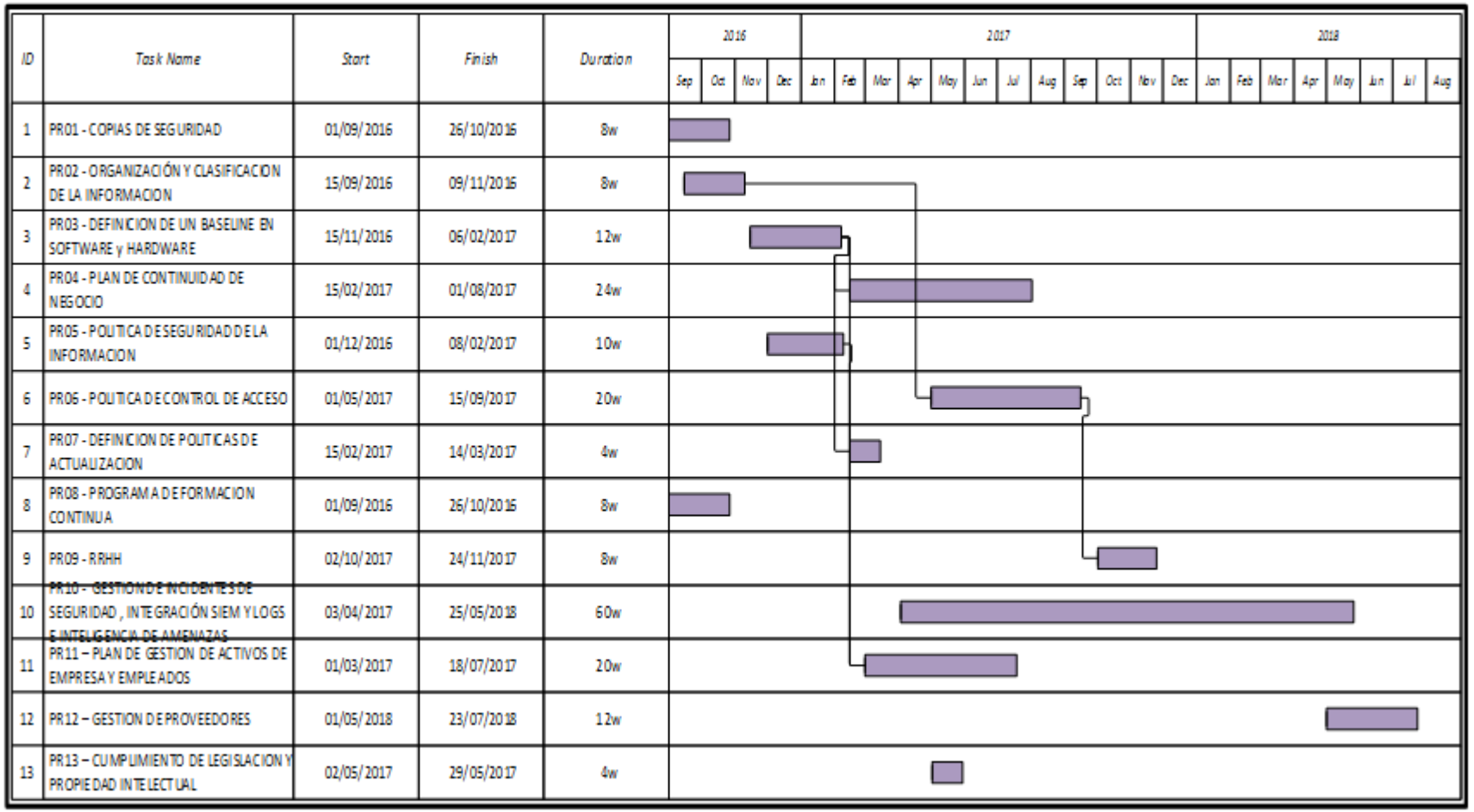
Ilustración 14 Riesgo medio para cada dimensión

Propuesta de proyectos

- Una vez conocidos los riesgos y dónde es prioritario actuar, se definen 13 proyectos que mejorarán la seguridad de la organización de una manera notable:

- PR01 – COPIAS DE SEGURIDAD
- PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION
- PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE
- PR04 - PLAN DE CONTINUIDAD DE NEGOCIO
- PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION
- PR06 - POLITICA DE CONTROL DE ACCESO
- PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION
- PR08 - PROGRAMA DE FORMACION CONTINUA
- PR09 - RRHH
- PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS
- PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS
- PR12 – GESTION DE PROVEEDORES
- PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL

Planificación temporal de proyectos

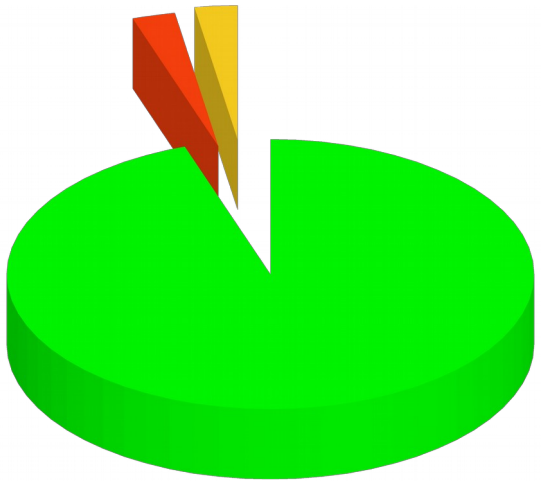


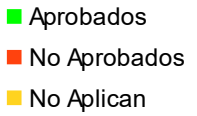
ID	Task Name	Start	Finish	Duration
1	PR01 - COPIAS DE SEGURIDAD	01/09/2016	26/10/2016	8w
2	PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION	15/09/2016	09/11/2016	8w
3	PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE	15/11/2016	06/02/2017	12w
4	PR04 - PLAN DE CONTINUIDAD DE NEGOCIO	15/02/2017	01/08/2017	24w
5	PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION	01/12/2016	08/02/2017	10w
6	PR06 - POLITICA DE CONTROL DE ACCESO	01/05/2017	15/09/2017	20w
7	PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION	15/02/2017	14/03/2017	4w
8	PR08 - PROGRAMA DE FORMACION CONTINUA	01/09/2016	26/10/2016	8w
9	PR09 - RRHH	02/10/2017	24/11/2017	8w
10	PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS	03/04/2017	25/05/2018	60w
11	PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS	01/03/2017	18/07/2017	20w
12	PR12 – GESTION DE PROVEEDORES	01/05/2018	23/07/2018	12w
13	PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL	02/05/2017	29/05/2017	4w

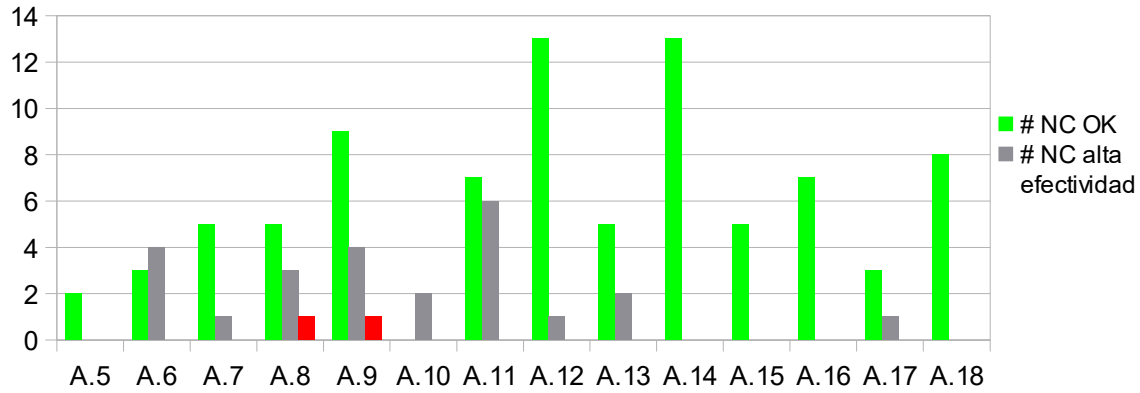
Planificación económica de proyectos

Proyecto	Coste Implementación	Coste Mantenimiento
PR01 – COPIAS DE SEGURIDAD	34.640 €	10.440 €
PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION	2.480 €	4.000 €
PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE	4.640 €	6.400 €
PR04 - PLAN DE CONTINUIDAD DE NEGOCIO	16.000 €	7.200 €
PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION	4.560 €	9.600 €
PR06 - POLITICA DE CONTROL DE ACCESO	36.200 €	6.240 €
PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION	3.200 €	4.640 €
PR08 - PROGRAMA DE FORMACION CONTINUA	27.280 €	27.280 €
PR09 – RRHH	3.200 €	4.800 €
PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS	251.000 €	69.600 €
PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS	9.600 €	8.800 €
PR12 – GESTION DE PROVEEDORES	7.360 €	6.400 €
PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL	1.600 €	1.600 €
Total	**401.760 €**	**167.000 €**

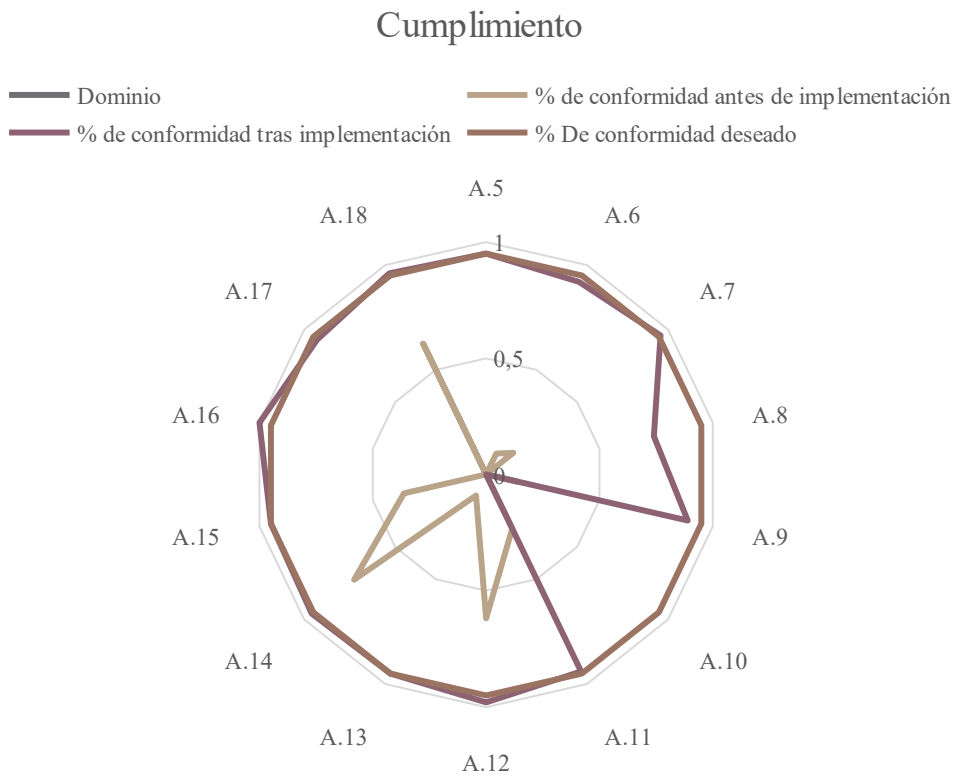
Evolución tras implantación







Auditoría del cumplimiento



Conclusiones

- Se constata una mejoría sustancial en la seguridad de la información en la organización.
- Gran mejoría en términos generales en todos los aspectos de la empresa.
- Si lo desea, la empresa podría empezar a acometer el proceso de certificación
- Se comprueba una mayor concienciación de los trabajadores con la seguridad de la información.
- La implementación de un equipo de respuesta a incidentes de seguridad y la futura integración de CTI (Cyber Threat Intelligence) en otros procesos de la inteligencia de negocio, permitirá medir el riesgo y las amenazas futuras de una manera eficiente.
- La identificación de activos y amenazas ha ayudado a la organización a ser consciente de qué posee y de qué tratamiento debe aplicar a cada uno.
- Sin embargo, que hace necesario mejorar ciertos puntos, para ello se recomienda una segunda auditoría tras concluir esta