XXX
Implementación ISO 27001:2013

Presentación a la compañía

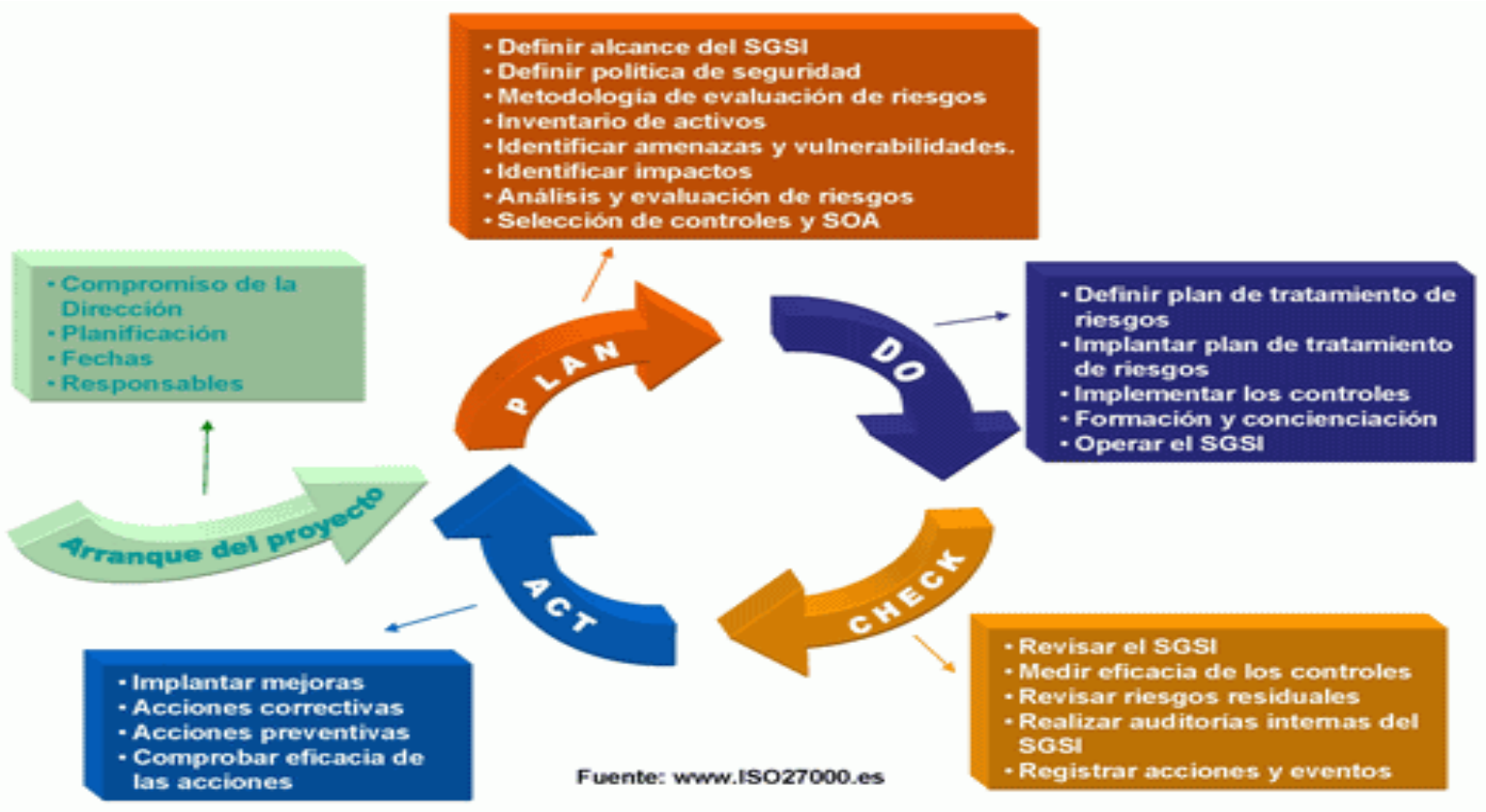
Qué es ISO 27001

- ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission
- Describe cómo gestionar la seguridad de la información en una empresa
- Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización
- Se ha convertido en la principal norma a nivel mundial para la seguridad de la información

Por qué

- 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

Cómo se ha realizado



Los dominios ISO

- ISO 27001:2013

“Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002”

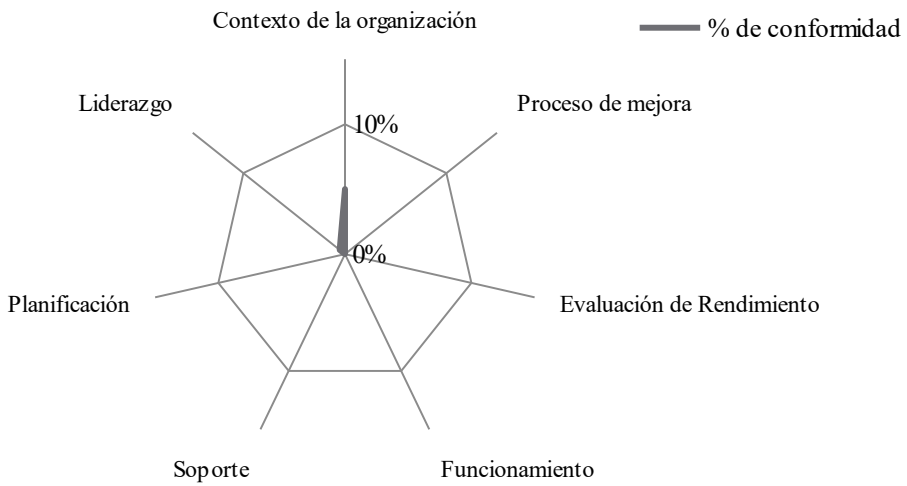
- ISO 27002:2013

“Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.”

Donde estábamos? : Indicadores

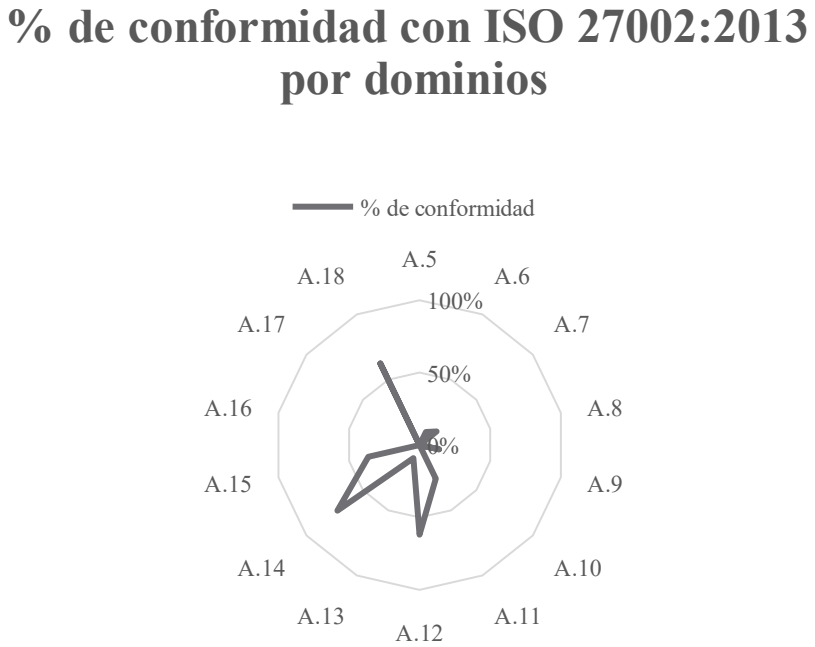
Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método 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	

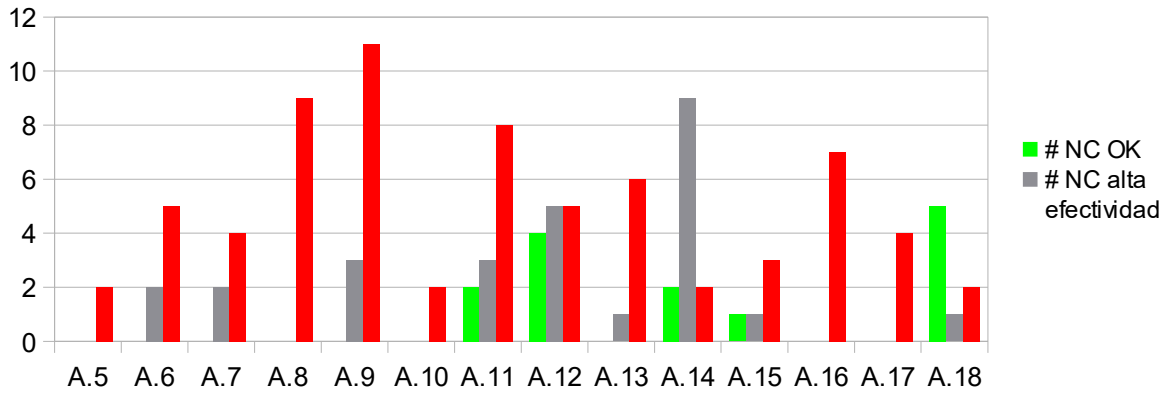
Análisis diferencial 27001:2013



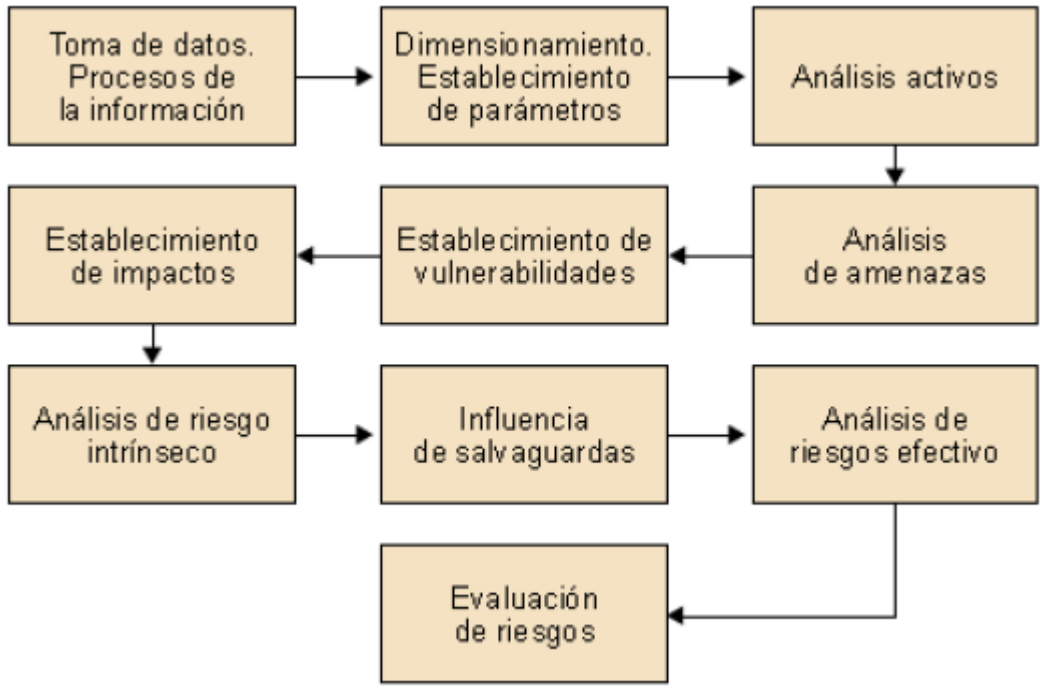
	Dominio	% de conformidad	# NC mayores	# NC menores	# NC OK
4	Contexto de la organización	5%	5	0	0
5	Liderazgo	1%	14	0	0
6	Planificación	0%	31	0	0
7	Soporte	10%	14	3	0
8	Funcionamiento	0%	3	0	0
9	Evaluación de Rendimiento	5%	23	0	0
10	Proceso de mejora	0%	11	0	0

Análisis diferencial 270002:2013





Análisis de riesgo



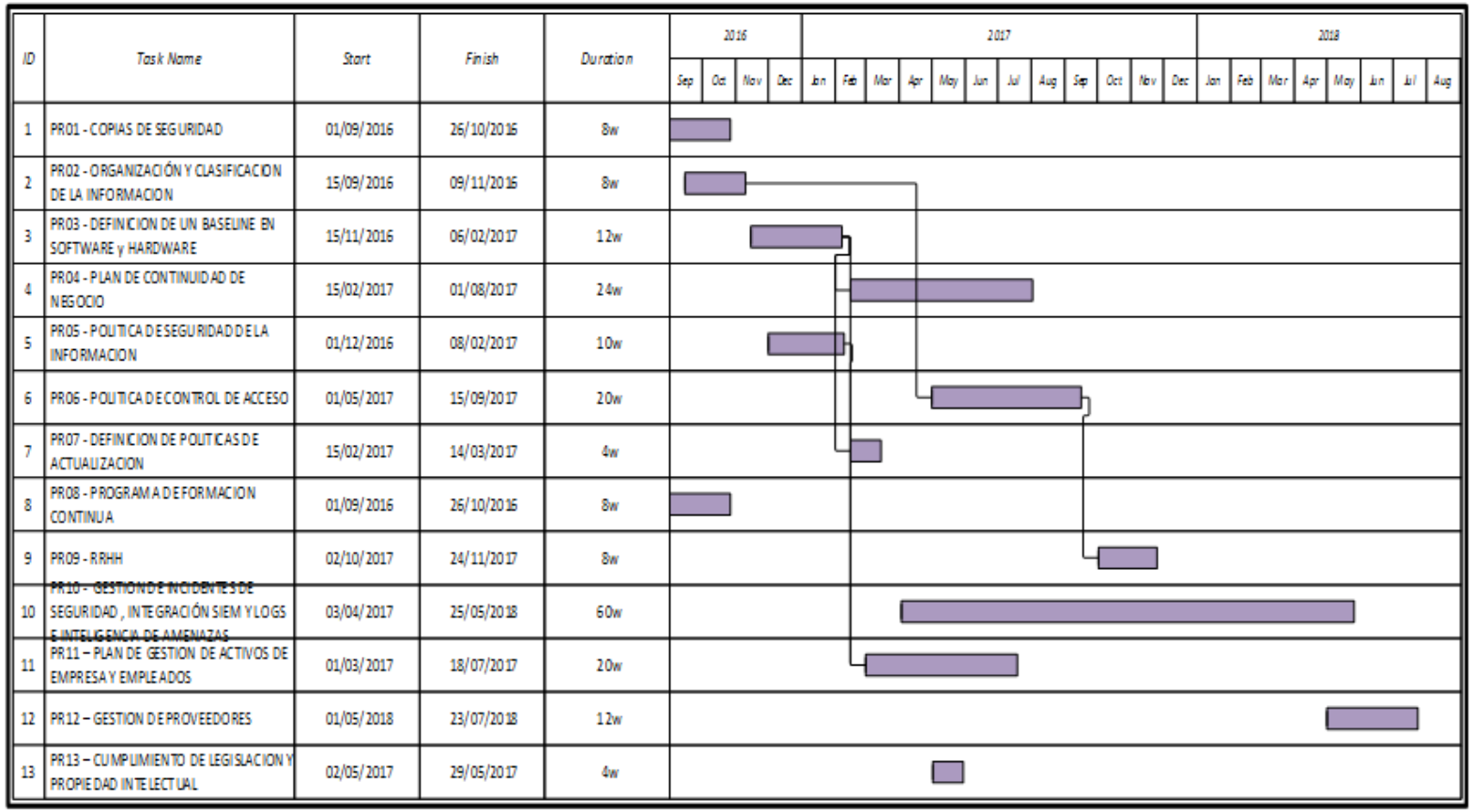
Que vamos a hacer para mejorarlo

- Propuesta de 13 proyectos para mejorar la seguridad de la organización

  - 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

Desglose temporal de proyectos

- Duración total de 24 meses, dando comienzo en Sept 2016



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

Desglose económico 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 €**

Que se ha logrado: Hitos

- Definición de roles y responsabilidades
- Definición de un sistema de gestión documental común
- Definición de política de seguridad
- Definición de proceso de auditorias internas
- Gestión de indicadores
- Definición de proceso de revisión por dirección
- Definición del proceso y realización de análisis de riesgos
- Identificación de activos y amenazas
- Calculo del impacto potencial y del riesgo para cada activo
- Propuesta de proyectos
- Ejecución de proyectos
- Auditoría de cumplimiento

Documentación desarrollada

- Política de clasificación de la información.
- Política de control de acceso.
- Política de uso adecuado de los recursos de la empresa.
- Política de acceso remoto o teletrabajo.
- Política de comunicación de información.
- Política de gestión de activos
- Política de gestión de la continuidad
- Política de gestión de incidentes
- Política de cifrado
- Política en seguridad operativa
- Política de Recursos Humanos
- Política de seguridad física y ambiental.
- Política de adquisición, desarrollo y mantenimiento de los sistemas
- Política de relación con los suministradores

Antes vs Ahora