Sistema de Gestión de la Seguridad de la Información.

Estudiante: Francisco Antonio Lievano Cos.
Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC).
Consultor: Arsenio Tortajada Gallego.
Centro: Universitat Oberta de Catalunya.
Entrega: Junio de 2016.

Contenidos (1/2)

1. Introducción.
    1. Objetivos.
    2. Descripción de la organización.
    3. Análisis del cumplimiento inicial.

2. Sistema de gestión documental.
    1. Política de Seguridad.
    2. Auditorías internas.
    3. Gestión de indicadores.
    4. Revisión por la Dirección.
    5. Roles y responsabilidades.
    6. Declaración de aplicabilidad.

3. Análisis de riesgos.
    1. Identificación de activos.
    2. Valoración de activos.
    3. Análisis de amenazas y vulnerabilidades.

Autor: Francisco Antonio Lievano Cos.

Contenidos (2/2)

4. Propuestas de proyectos.
5. Auditoría de cumplimiento.
6. Conclusiones.

Autor: Francisco Antonio Lievano Cos.

1.1. Objetivos

El presente Trabajo Final de Máster tiene como objetivo analizar en profundidad los Sistemas de la Información de una determinada empresa, en base a normativas y estándares internacionales (como ISO27002:2013) y proponer acciones a modo de proyectos para mejorar la seguridad en base a este sistema de gestión.

En cualquier organización, sea del tamaño que sea, es completamente necesario conocer el estado de los Sistemas y Tecnologías de la Información, para determinar si son adecuados y seguros para llevar a cabo la actividad de la empresa de forma satisfactoria.

El Plan Director de la Seguridad tiene que ir de la mano o dirigido por los objetivos de la empresa, ya que por sí mismo no tiene ningún interés: ha de estar alineado con objetivos estratégicos.

Autor: Francisco Antonio Lievano Cos.

1.2. Descripción de la organización (1/3)

- Empresa dedicada al desarrollo de software de simulación y de modelado 3D.
- Dimensión de entre 60 y 70 empleados ubicados en una misma oficina.
- Ubicada en Madrid y tiene colaboradores (freelance) que trabajan desde Barcelona (una persona), Canarias (una persona) y China (una persona).
- Oficinas centrales en un único edificio con CPD en el sótano.
- Todas las zonas de la oficina están protegidas mediante un sistema de control de acceso utilizando tarjetas de proximidad.
- Sólo pueden acceder al CPD el CEO de la empresa y el responsable de Sistemas e IT.


Multilight


Real light

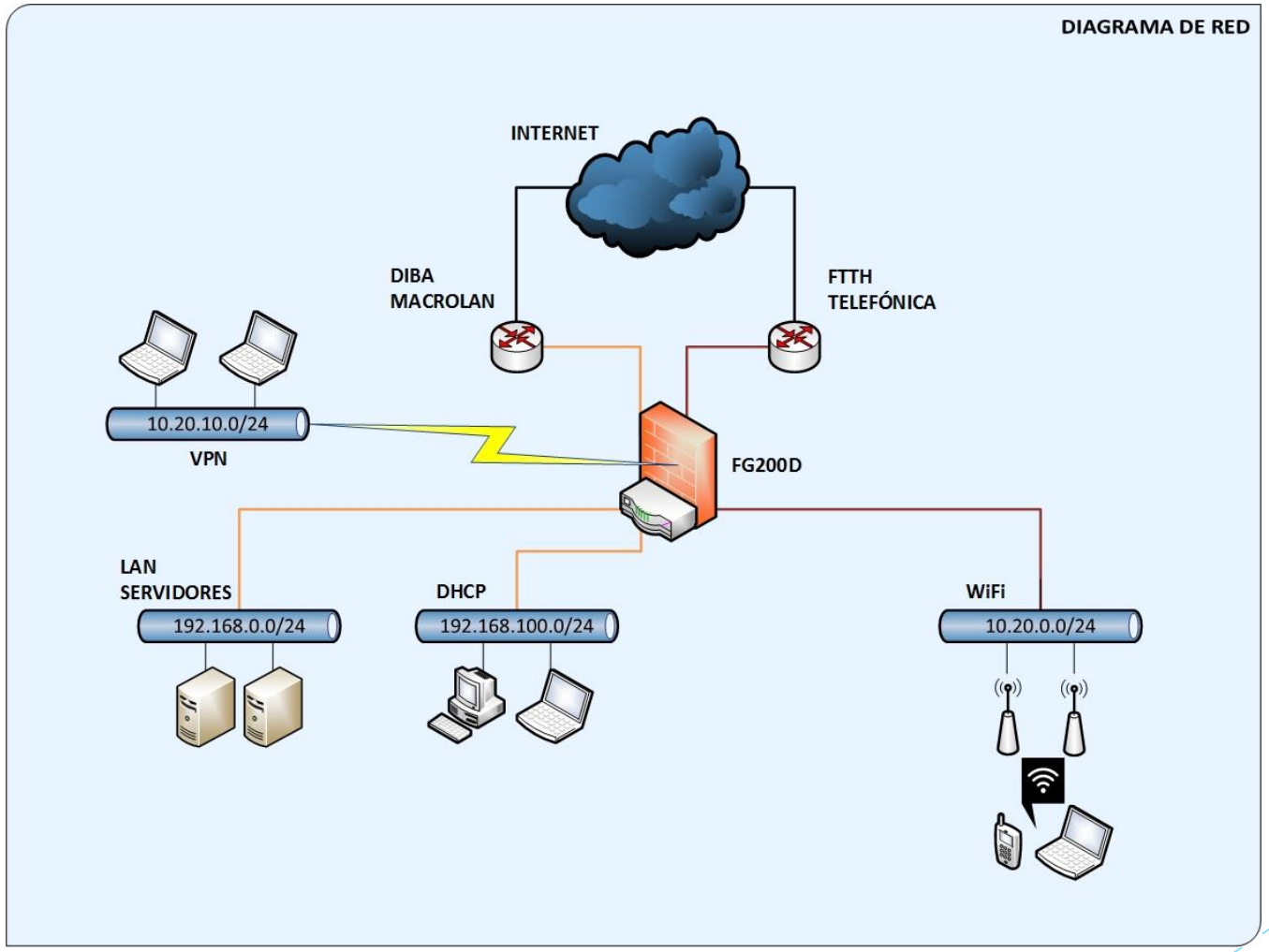

Realistic Camera Model

Autor: Francisco Antonio Lievano Cos.

1.2. Descripción de la organización (2/3)

- Sistemas utilizados en la empresa:
  - Correo electrónico: Postfix alojado en proveedor externo.
  - Repositorio de código: GIT, SVN y Mercurial In-House.
  - Intercambio de ficheros: servidor Fedora con Samba.
  - Helpdesk interno: GLPI In-House.
  - Gestión de proyectos: Jira In-House.
  - Helpdesk externo: Freshdesk en servidor cloud.

1.2. Descripción de la organización (3/3)



Autor: Francisco Antonio Lievano Cos.

1.3. Análisis del cumplimiento inicial (1/2)

Cumplimiento inicial por dominios de la seguridad:

- 5. Políticas de seguridad: 40%.
- 6. Aspectos organizativos de la seguridad de la información: 55%.
- 7. Seguridad ligada a los recursos humanos: 63.3%.
- 8. Gestión de activos: 68,6%.
- 9. Control de accesos: 70.2%.
- 10. Cifrado: 60%.
- 11. Seguridad física y ambiental: 74,7%.
- 12. Seguridad en la operativa: 56,4%.
- 13. Seguridad en las telecomunicaciones: 55,8%.

Autor: Francisco Antonio Lievano Cos.

1.3. Análisis del cumplimiento inicial (2/2)

- 14. Adquisición, desarrollo y mantenimiento de los sistemas de la información: 65,1%.
- 15. Relaciones con suministradores: 60%.
- 16. Gestión de incidentes en la seguridad de la información: 62,8%.
- 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio: 65%.
- 18. Cumplimiento: 71%.

En la mayoría de dominios no se obtiene una valoración superior a 75%.

En el momento inicial, antes de aplicar un sistema de gestión de la seguridad, la empresa no cumple correctamente los controles de seguridad estipulados en la normativa.

Autor: Francisco Antonio Lievano Cos.

2.1. Política de Seguridad

Regulación de la organización en los siguientes aspectos:

- Hardware y software: compra, duplicación y transferencia.
- Acceso a Internet y redes de comunicación.
- Sistema de correo electrónico.

Consideraciones referentes a:

- Principios de la seguridad de la información.
- Monitorización.
- Incumplimiento.

Autor: Francisco Antonio Lievano Cos.

2.2. Auditorías internas (1/2)

- Proceso para realizar un correcto mantenimiento continuado en el tiempo y evolutivo del Sistema de Gestión de la Seguridad de la Información.

- El encargado de realizar las auditorías internas es el auditor interno, que tiene las siguientes funciones específicas:

  - Preparar las auditorías.
  - Comunicar y establecer los requisitos de la auditoría.
  - Conocer y analizar los resultados de las auditorías anteriores, en caso de haber.
  - Dirigir el proceso de auditoría en el período planificado.
  - Recoger evidencias objetivas del área auditada, mediante entrevistas, observación de actividades y revisión de registros.
  - Verificar que el SGSI es conforme con la norma y se mantiene vigente y eficaz.
  - Informar de forma eficaz a los implicados los hallazgos obtenidos durante la auditoría.
  - Documentar de forma adecuada las observaciones y no conformidades.
  - Elaborar y presentara el informe de auditoría.

Autor: Francisco Antonio Lievano Cos.

2.2. Auditorías internas (2/2)

- Planificación inicial de auditorías de seguridad:

	Auditoría	Programación (mes)											
Nº	Área	01	02	03	04	05	06	07	08	09	10	11	12
1	Políticas de seguridad			X									
2	Aspectos organizativos de la seguridad de la información			X									
3	Seguridad ligada a los recursos humanos			X									
4	Gestión de activos			X									
5	Control de accesos			X									
6	Cifrado							X					
7	Seguridad física y ambiental							X					
8	Seguridad de la operativa							X					
9	Seguridad en las telecomunicaciones							X					
10	Adquisición, desarrollo y mantenimiento de los sistemas de información							X					
11	Relaciones con suministradores											X	
12	Gestión de incidentes en la seguridad de la información											X	
13	Aspectos de seguridad de la información en la gestión de la continuidad del negocio											X	
14	Cumplimiento											X	

Autor: Francisco Antonio Lievano Cos.

2.3. Gestión de indicadores (1/2)

- Los indicadores siguientes son los que se utilizarán para la evaluación agrupada de distintos controles especificados por la normativa:

ID indicador	IND-01
Nombre	Control de repositorio de código
Descripción	Comprobar salud de repositorio de código
Control de seguridad	6.1.5; 8.1.3; 8.2.3; 9.1.1; 12.1.4
Medida	Errores y advertencias de seguridad
Unidad de medida	Incidencias
Frecuencia	1 vez a la semana
Valor objetivo	0
Valor límite	0,2
Responsable	Responsable de SITIC

ID indicador	IND-02
Nombre	Control de webs
Descripción	Comprobar estado de páginas webs de información, soporte y venta online
Control de seguridad	9.1.2; 12.1.1; 13.2.1; 14.1.3
Medida	Fallos / monitorizaciones efectuadas
Unidad de medida	Chequeo / chequeo
Frecuencia	1 chequeo cada 30 minutos
Valor objetivo	0,05
Valor límite	Superior a 0,1
Responsable	Responsable de SITIC

Autor: Francisco Antonio Lievano Cos.

2.3. Gestión de indicadores (2/2)

ID indicador	IND-03
Nombre	Control de soporte y satisfacción de clientes
Descripción	Comprobar incidencias y comentarios de usuarios en foros
Control de seguridad	9.1.2; 12.1.1; 13.2.1; 14.1.3
Medida	Comentarios negativos / comentarios
Unidad de medida	Comentarios
Frecuencia	1 vez al día
Valor objetivo	0,1
Valor límite	Superior a 0,5
Responsable	Responsable de Marketing y Soporte

ID indicador	IND-04
Nombre	Control de contabilidad
Descripción	Comprobar salud de sistema de contabilidad
Control de seguridad	9.1.2; 12.1.1; 13.2.1; 14.1.3
Medida	Errores y advertencias de seguridad
Unidad de medida	Incidencias
Frecuencia	1 vez a la semana
Valor objetivo	0
Valor límite	0,2
Responsable	Responsable de SITIC

ID indicador	IND-05
Nombre	Control de equipos informáticos
Descripción	Comprobar el estado del parque informático
Control de seguridad	9.1.2; 11.1.2; 11.2.2; 12.1.1; 13.2.1; 14.1.3
Medida	Virus+Malware / comprobaciones
Unidad de medida	Fallos / comprobaciones
Frecuencia	1 vez al mes
Valor objetivo	0,1
Valor límite	Superior a 0,3
Responsable	Responsable de SITIC

ID indicador	IND-06
Nombre	Control de cumplimiento de normativa
Descripción	Comprobar la normativa referente a LOPD, LSSI y otras normas que apliquen
Control de seguridad	15 (completo); 18 (completo)
Medida	No conformidades
Unidad de medida	No conformidades
Frecuencia	Según frecuencia de auditorías internas
Valor objetivo	0
Valor límite	Superior a 3
Responsable	Responsable de SITIC

UOC Universitat Oberta de Catalunya www.uoc.edu
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili

Autor: Francisco Antonio Lievano Cos.

2.4. Revisión por la Dirección (1/2)

Revisiones periódicas con la Dirección de la empresa para analizar la evolución y cumplimiento de los siguientes puntos:

- Las Políticas de calidad y seguridad de la información.
- El cumplimiento de los objetivos de calidad y seguridad de la información.
- El desempeño de los procesos y conformidad de los productos, incluyendo la retroalimentación de las partes interesadas.
- Los resultados de las auditorías internas y externas.
- Las acciones correctivas y preventivas necesarias para el mejoramiento del SGSI.
- Las acciones de seguimiento de las revisiones por la Dirección previas en caso de existir.
- Cumplimiento de la implementación de los planes de tratamiento definidos para los riesgos identificados.
- Resultados de las mediciones de eficacia del SGSI.

Autor: Francisco Antonio Lievano Cos.

2.4. Revisión por la Dirección (2/2)

- Cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.
- Resultados de la gestión de riesgos corporativos, incluyendo vulnerabilidades o amenazas.

Planificación de revisiones de Dirección:

	Auditoría	Programación (mes)											
Nº	Área	01	02	03	04	05	06	07	08	09	10	11	12
1	Políticas de seguridad			X									
2	Aspectos organizativos de la seguridad de la información			X									
3	Seguridad ligada a los recursos humanos			X									
4	Gestión de activos			X									
5	Control de accesos			X									
6	Cifrado							X					
7	Seguridad física y ambiental							X					
8	Seguridad de la operativa							X					
9	Seguridad en las telecomunicaciones							X					
10	Adquisición, desarrollo y mantenimiento de los sistemas de información							X					
11	Relaciones con suministradores											X	
12	Gestión de incidentes en la seguridad de la información											X	
13	Aspectos de seguridad de la información en la gestión de la continuidad del negocio											X	
14	Cumplimiento											X	

Autor: Francisco Antonio Lievano Cos.

2.5. Roles y responsabilidades (1/3)

La Dirección de la empresa ha distribuido las distintas responsabilidades que implican el mantenimiento del Sistema de Gestión de la Seguridad de la Información en distintos grados, en función de los siguientes roles

- Responsabilidades generales:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Dirección.

- Gestión de cumplimiento de normativa:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Administración y Legal.

- Gestión de riesgos:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Dirección.

- Revisión y medición del SGSI:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Auditor interno.

Autor: Francisco Antonio Lievano Cos.

2.5. Roles y responsabilidades (2/3)

- Gestión de activos:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Departamento de Sistemas y TI.

- Gestión de incidencias:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Departamento de Sistemas y TI.

- Gestión de la cultura y comunicación:
  - Departamento: todos los afectados por el SGSI.
  - Responsable: Dirección.

Autor: Francisco Antonio Lievano Cos.

2.5. Roles y responsabilidades (3/3)

Roles dentro de la organización:

Autor: Francisco Antonio Lievano Cos.

2.6. Declaración de aplicabilidad

En la normativa ISO 27001 se establece que la aplicabilidad de los controles puede deberse por una obligación contractual, por un requerimiento regulatorio o por un requerimiento del negocio. De igual modo, se estipula que alguno de los controles puede ser excluido de la aplicabilidad de la norma. En el caso concreto de la empresa objeto de este estudio no hay ningún control que escape de la aplicabilidad de la normativa.

En el caso objeto del presente estudio, todos los dominios y controles de las seguridad son aplicables, por lo que todos ellos han de estar analizados. El estado de madurez inicial de cada dominio y control dentro de la organización es distinto.

3.1. Identificación de activos (1/2)

Antes de empezar a valorar activos y sus amenazas y vulnerabilidades, debemos identificar los activos, objeto del Sistema de Seguridad de los Sistemas de la Información, dentro de la empresa. Los activos identificados son:

Redes de comunicación			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Cableado de datos para puestos de trabajo	80	Cat6	Edificio completo
Cableado de datos para servidores	30	Cat6	CPD
Cableado de datos entre dispositivos de red	110	Cat6	Edificio completo
Switch	8	HP ProCurve	Edificio completo
Access Points	3	FortiAP 221C	Plantas Baja, 1, 2 y 3
Firewalls	1	FortiGate 200D	CPD
Routers	2	Cisco Catalyst	CPD

Hardware (PCs, servidores, consumo)			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
PCs	73	Dell	Plantas Baja, 1, 2 y 3
Portátiles	5	Dell Latitude	Plantas Baja, 1, 2 y 3
Impresoras	7	Brother	Plantas Baja, 1, 2 y 3
Teléfonos	8	Huawei	Plantas Baja, 1, 2 y 3
Lectores de tarjetas de proximidad	4	Propietario	Plantas Baja, 1, 2 y 3
Servidores	20	Dell PowerEdge	CPD
Ratones (stock)	5	Logitech	Almacén
Teclados (stock)	5	Logitech	Almacén
Pantallas (stock)	2	Dell	Almacén

Autor: Francisco Antonio Lievano Cos.

3.1. Identificación de activos (2/2)

Software			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Ofimática	80	Microsoft Office	Plantas Baja, 1, 2 y 3
Aplicaciones de desarrollo	40	Microsoft	Plantas Baja, 1, 2 y 3
Aplicaciones de administración	10	No aplica	Planta Baja
Motores de bases de datos	1	Microsoft	CPD

Datos			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Repositorio de código	3	GIT, SVN, HG	CPD
Base de datos de clientes	1	No aplica	AWS
Base de datos de proveedores	1	No aplica	CPD
Base de datos de recursos humanos	1	No aplica	AWS

Aplicaciones			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Webs	6	No aplica	AWS
Servidor de licencias	2	RLM	AWS

Personal			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Empleados	77	No aplica	Plantas Baja, 1 y 2
Socios directivos	2	No aplica	Plana Baja

Intangibles			
Nombre	**Cantidad**	**Tipo**	**Ubicación**
Satisfacción de clientes	No aplica	No aplica	No aplica
Imagen corporativa de la empresa	No aplica	No aplica	No aplica

Autor: Francisco Antonio Lievano Cos.

3.2. Valoración de activos (1/3)

Antes de aplicar una valoración a cada activo, necesitamos una escala que nos permita crear grupos según el valor de cada activo:

Valoración de activos	
Valoración	**Rango (en €)**
Muy alta	Entre 300.000 y 100.000
Alta	Entre 99.999 y 50.000
Media	Entre 49.000 y 10.000
Baja	Entre 9.999 y 1.000
Muy baja	Entre 999 y 1

En base a esta escala, valoramos cada uno de los activos identificados:

Autor: Francisco Antonio Lievano Cos.

3.2. Valoración de activos (2/3)

Valoración de activos						
Nombre	Valoración	Criticidad				
		A	C	I	D	T
Redes de comunicación						
Cableado de datos para puestos de trabajo	Baja	8	8	5	10	8
Cableado de datos para servidores	Baja	8	8	5	10	8
Cableado de datos entre dispositivos de red	Baja	8	8	5	10	8
Switch	Media	8	8	5	10	8
Access Points	Baja	8	8	5	10	8
Firewalls	Media	8	10	8	10	10
Routers	Media	2	4	2	8	2
Hardware (PCs, servidores, consumo)						
PCs	Alta	2	2	1	1	5
Portátiles	Media	2	2	1	1	5
Impresoras	Media	0	2	0	0	4
Teléfonos	Baja	1	3	0	0	2
Lectores de tarjetas de proximidad	Baja	3	4	3	0	7
Servidores	Alta	8	8	7	9	7
Ratones (stock)	Muy baja	0	0	0	0	0
Teclados (stock)	Muy baja	0	0	0	0	0
Pantallas (stock)	Muy baja	0	0	0	0	0
Software						
Ofimática	Media	2	1	5	1	5
Aplicaciones de desarrollo	Media	2	1	5	1	5
Aplicaciones de administración	Media	2	5	5	5	5
Motores de bases de datos	Media	7	7	7	7	10

Autor: Francisco Antonio Lievano Cos.

3.2. Valoración de activos (3/3)

Aplicaciones						
Webs	Alta	8	10	10	10	8
Servidor de licencias	Media	8	7	7	7	7
Datos						
Repositorio de código	Muy alta	10	8	10	10	10
Base de datos de clientes	Muy alta	7	8	10	8	8
Base de datos de proveedores	Muy alta	7	8	10	8	8
Base de datos de recursos humanos	Muy alta	7	8	10	8	8
Personal						
Empleados	Muy alta	5	0	0	5	5
Socios directivos	Muy alta	5	0	0	5	5
Intangibles						
Satisfacción de clientes	Muy alta	8	8	8	0	0
Imagen corporativa de la empresa	Muy alta	8	8	0	0	0

Autor: Francisco Antonio Lievano Cos.

3.3. Análisis de amenazas y vulnerabilidades (1/3)

Al igual que hemos hecho en el apartado anterior, es necesario definir escalas para agrupar vulnerabilidades y amenazas:

- **Clasificación de vulnerabilidades:** se toma como máximo el valor 1, que quiere decir que la vulnerabilidad está presente el 100% de días del año (365 días). Partiendo de esto, se crea la siguiente escala:

Clasificación de vulnerabilidades		
Valoración	**Rango (en iteraciones)**	**Código**
Muy alta	1 (cada día)	F-1
Alta	0,0712 (cada 2 semanas)	F-2
Media	0,0164 (cada 2 meses)	F-3
Baja	0,0054 (cada semestre)	F-4
Muy baja	0,0027 (cada año)	F-5

- **Escala de valoración del impacto:** se toma como máximo 100%, que corresponde a que impacta a la totalidad de activos de la empresa. Partiendo de esto, se crea la siguiente escala:

Valoración del impacto	
Valoración	**Rango (en %)**
Muy alto	Entre 100 y 75
Alto	Entre 74 y 50
Medio	Entre 49 y 25
Bajo	Entre 25 y 5
Muy bajo	Entre 4 y 1

Autor: Francisco Antonio Lievano Cos.

3.3. Análisis de amenazas y vulnerabilidades (2/3)

- **Dimensiones de seguridad:** a continuación, se presenta la escala con la que se mide la criticidad de las amenazas a las cinco dimensiones de la seguridad:

Dimensiones de la seguridad	
Valoración	**Criterio / daño**
10	Muy grave
9 - 7	Grave
6 - 4	Importante o considerable
3 - 1	Menor
0	Irrelevante

- Clasificación de amenazas por origen:

Clasificación de amenazas		
Origen	**Amenaza**	**Identificación**
Natural	Inundación	A-NAT1
Natural	Tormenta eléctrica	A-NAT2
Natural	Incendio	A-NAT3
Industrial	Baja médica	A-IND1
Industrial	Bajo rendimiento	A-IND2
No intencionado	Accidente laboral	A-NOINT1
No intencionado	Avería	A-NOINT2
No intencionado	Pérdida / hurto	A-NOINT3
Intencionado	Ataque SQL / DoS	A-INT1
Intencionado	Robo	A-INT2
Intencionado	Intrusión	A-INT3

Autor: Francisco Antonio Lievano Cos.

3.3. Análisis de amenazas y vulnerabilidades (3/3)

En cuanto al impacto potencial, para determinar el coste que implicaría a la empresa que se materialicen las amenazas, se realiza la siguiente estimación, a partir de la escala de valores definida en el documento de metodología de análisis de riesgos:

Valoración de activos	
Nombre	**Valoración**
Redes de comunicación	
Cableado de datos para puestos de trabajo	Baja
Cableado de datos para servidores	Baja
Cableado de datos entre dispositivos de red	Baja
Switch	Media
Access Points	Baja
Firewalls	Media
Routers	Media
Hardware (PCs, servidores, consumo)	
PCs	Alta
Portátiles	Media
Impresoras	Media
Teléfonos	Baja
Lectores de tarjetas de proximidad	Baja
Servidores	Alta
Ratones (stock)	Muy baja
Teclados (stock)	Muy baja
Pantallas (stock)	Muy baja
Software	
Ofimática	Media
Aplicaciones de desarrollo	Media
Aplicaciones de administración	Media
Motores de bases de datos	Media
Aplicaciones	
Webs	Alta
Servidor de licencias	Media

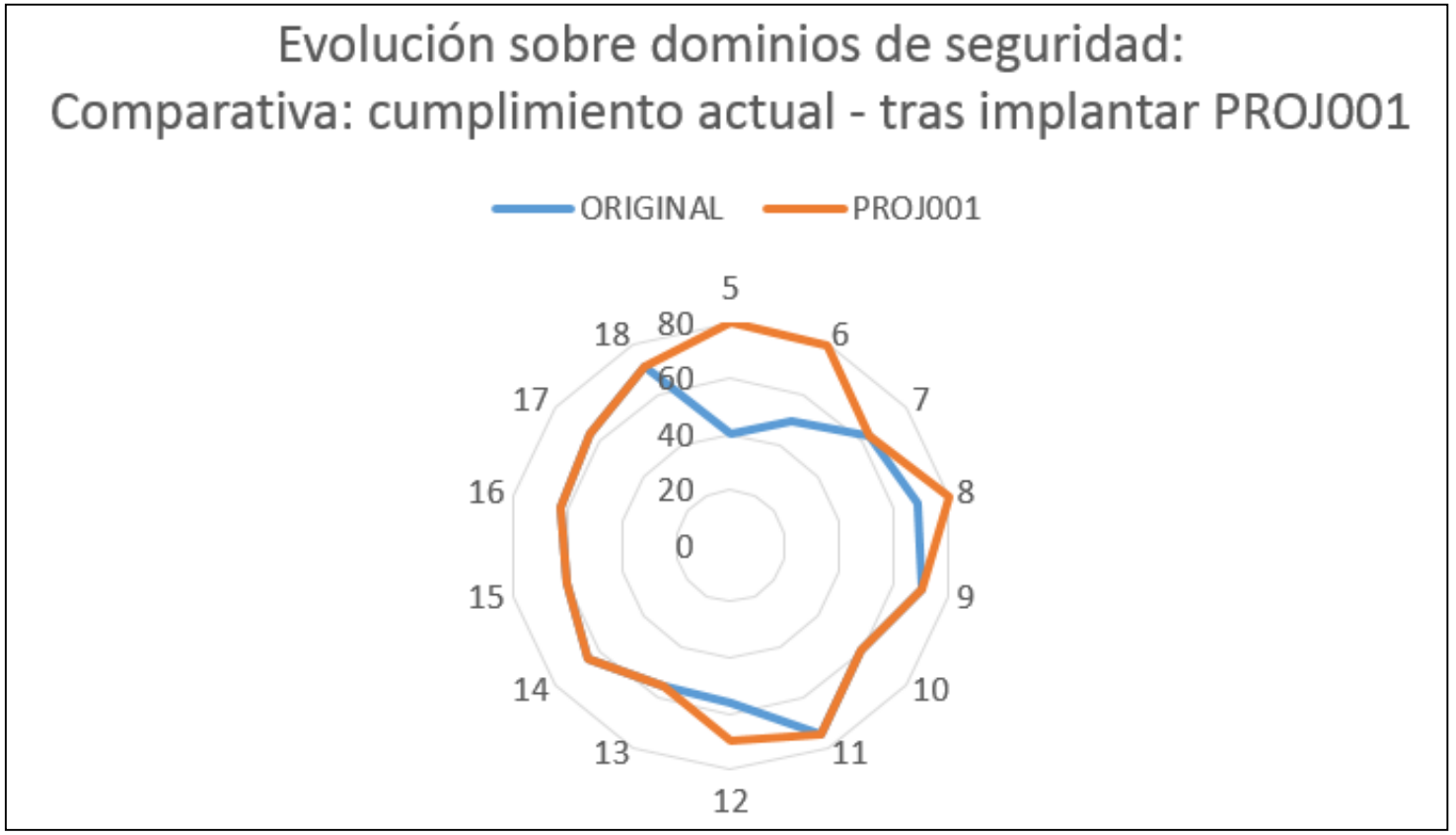
Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (1/12)

Los proyectos propuestos se pretenden aparcar a lo largo de un año entero, hasta el momento en que se haga una revisión completa al SGSI. Los proyectos son los siguientes (de forma esquemática y resumida):

- **Código del proyecto:** PROJ001
- **Nombre del proyecto:** Implantación de políticas de seguridad de la información.
- **Dominios afectados:** Políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad en la operativa.
- **Objetivo:** Crear e implantar un conjunto de normas y directrices que conformen la política de seguridad de la información que rija el comportamiento de la organización como conjunto, para el cumplimiento del Sistema de Gestión de la Seguridad de la Información.
- **Responsable:** Dirección de la organización y responsable de sistemas y tecnologías de la información (Comité de Seguridad de la Información).
- **Riesgo a mitigar:** intrusiones intencionadas (amenaza A-INT3) sobre los datos, robo intencionado (A-INT2) sobre los datos y hardware, pérdida / hurto (A-NOINT3) del hardware, averías no intencionadas (A-NOINT2) sobre el hardware.

4. Propuestas de proyectos (2/12)



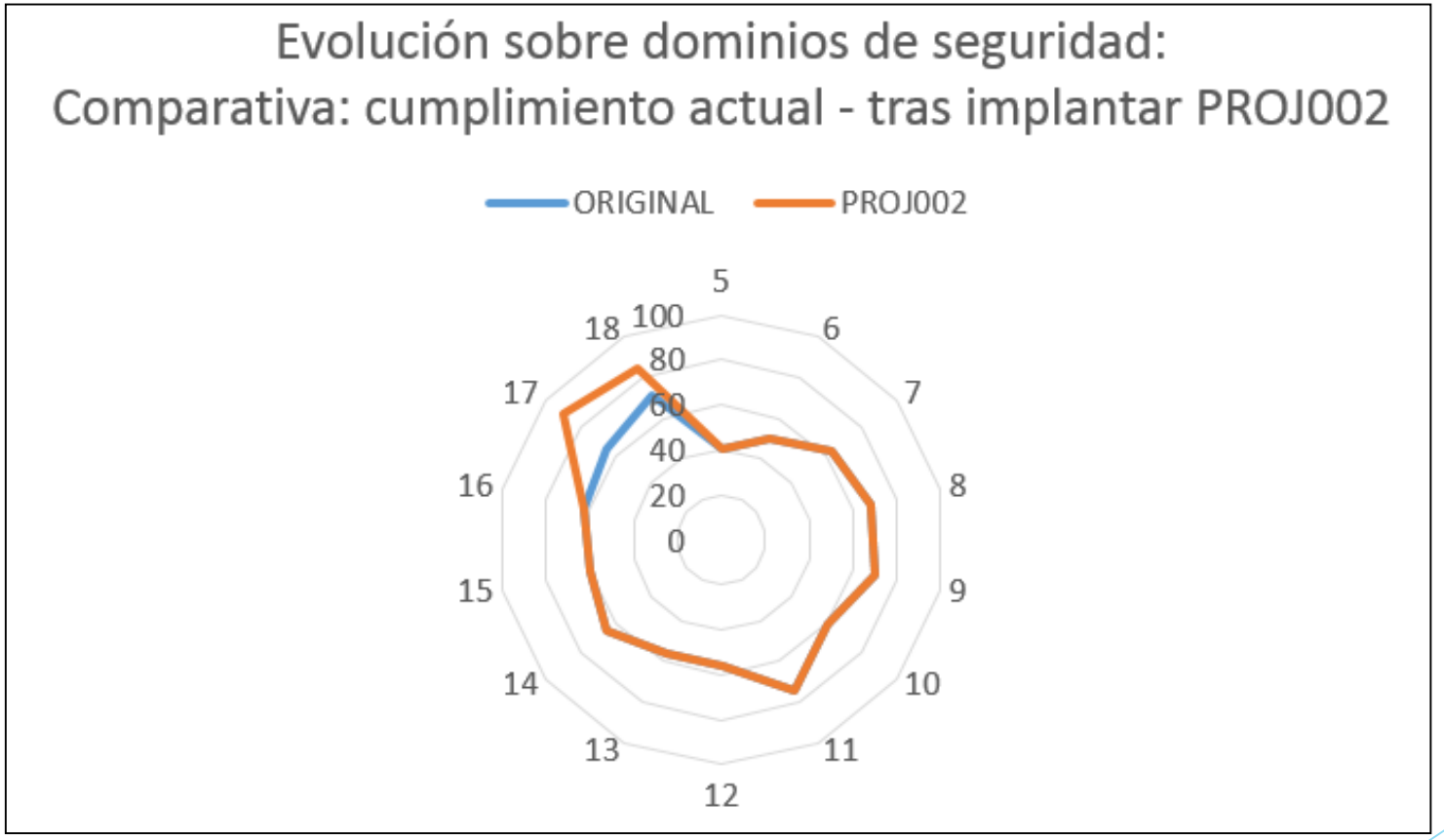
Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (3/12)

- **Código del proyecto:** PROJ002
- **Nombre del proyecto:** Instalación de un sistema de backup y recuperación.
- **Dominios afectados:** Políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad en la operativa.
- **Objetivo:** Implementar un sistema centralizado de gestión de tareas de creación, recuperación y almacenamiento de copias de seguridad, tanto de servidores, como de carpetas compartidas y de aplicaciones de negocio (web corporativa, bases de datos, aplicación de contabilidad).
- **Responsable:** Responsable de sistemas y tecnologías de la información.
- **Riesgo a mitigar:** robo intencionado (A-INT2) sobre los datos y hardware, pérdida / hurto (A-NOINT3) del hardware, ataques y DoS (A-INT1) sobre las aplicaciones, averías no intencionadas (A-NOINT2) sobre el hardware.

Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (4/12)



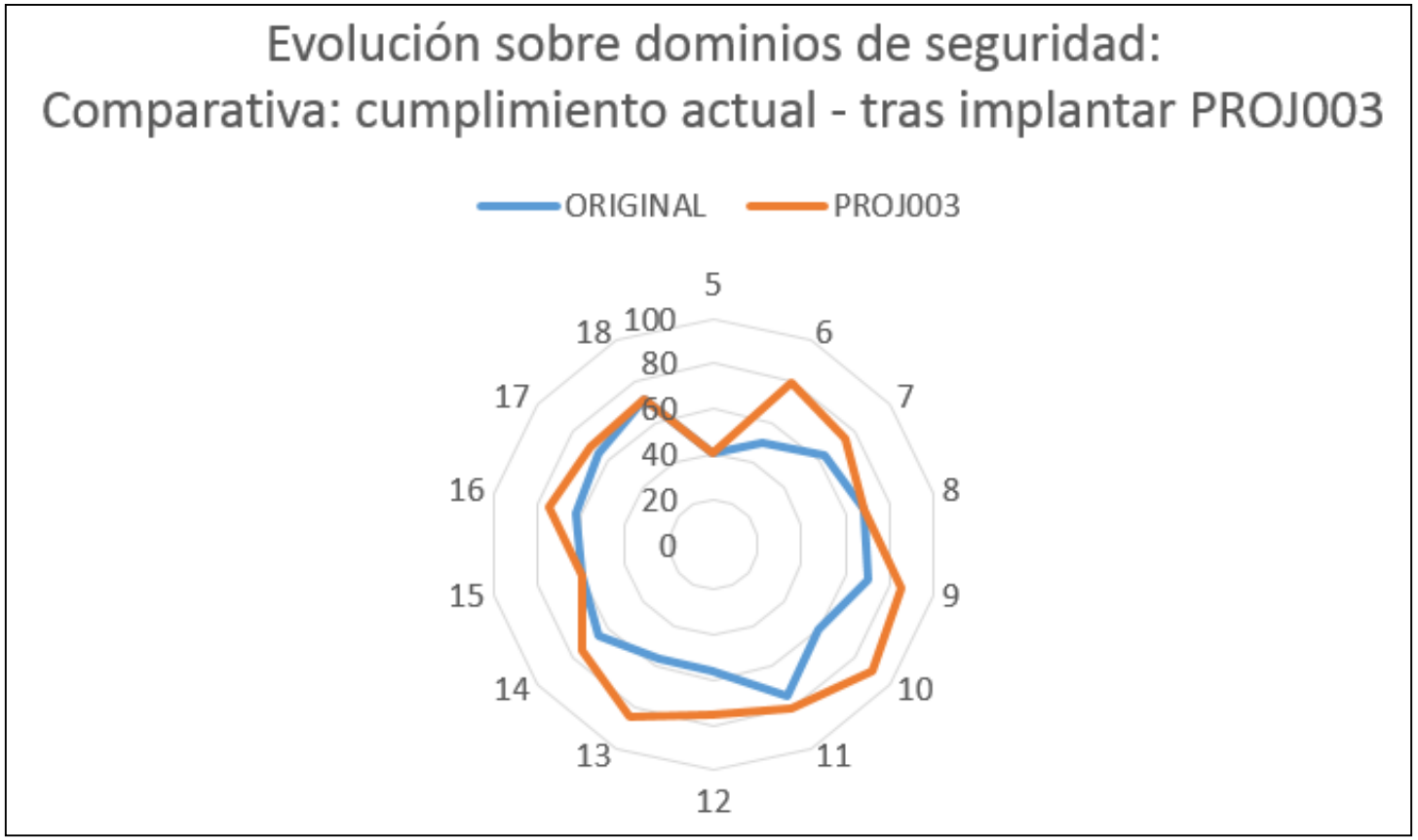
Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (5/12)

- **Código del proyecto:** PROJ003
- **Nombre del proyecto:** Migración de dispositivos de seguridad de red (router y firewall).
- **Dominios afectados:** Aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, control de accesos, cifrado, seguridad física y ambiental, seguridad en la operativa, seguridad en las telecomunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes en la seguridad de la información, aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- **Objetivo:** Migrar el router/firewall actual debido a que no ofrece las funcionalidades de seguridad y prestaciones necesarias para dar servicio a todo el personal que trabaja en la oficina.
- **Responsable:** Responsable de sistemas y tecnologías de la información.
- **Riesgo a mitigar:** intrusiones intencionadas (amenaza A-INT3) sobre los datos, robo intencionado (A-INT2) sobre los datos, ataques SQL o DoS (A-INT1) intencionados a las aplicaciones y servidores, intrusión intencionada (A-INT3) sobre los sistemas de la compañía.

Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (6/12)

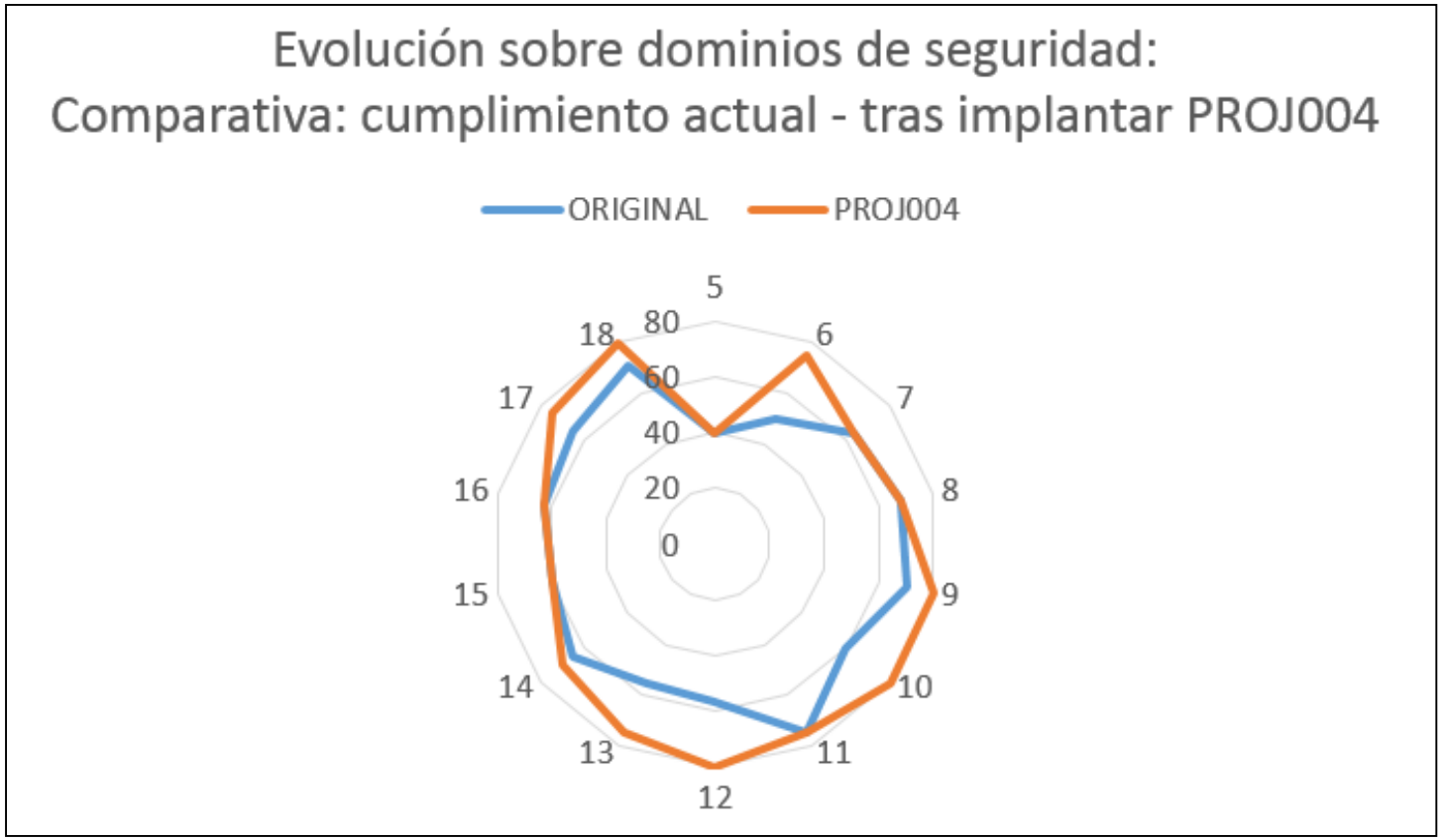


Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (7/12)

- **Código del proyecto:** PROJ004
- **Nombre del proyecto:** Migración del servicio de correo electrónico.
- **Dominios afectados:** Aspectos organizativos de la seguridad de la información, control de accesos, cifrado, seguridad en la operativa, seguridad en las telecomunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información, aspectos de seguridad de la información en la gestión de la continuidad del negocio, cumplimiento.
- **Objetivo:** Migrar el servicio de correo electrónico a un servicio en la nube.
- **Responsable:** Responsable de sistemas y tecnologías de la información.
- **Riesgo a mitigar:** intrusiones intencionadas (amenaza A-INT3) sobre los datos, robo intencionado (A-INT2) sobre los datos, ataques SQL o DoS (A-INT1) intencionados sobre el sistema de correo electrónico, intrusión intencionada (A-INT3) sobre los buzones de correo electrónico.

4. Propuestas de proyectos (8/12)

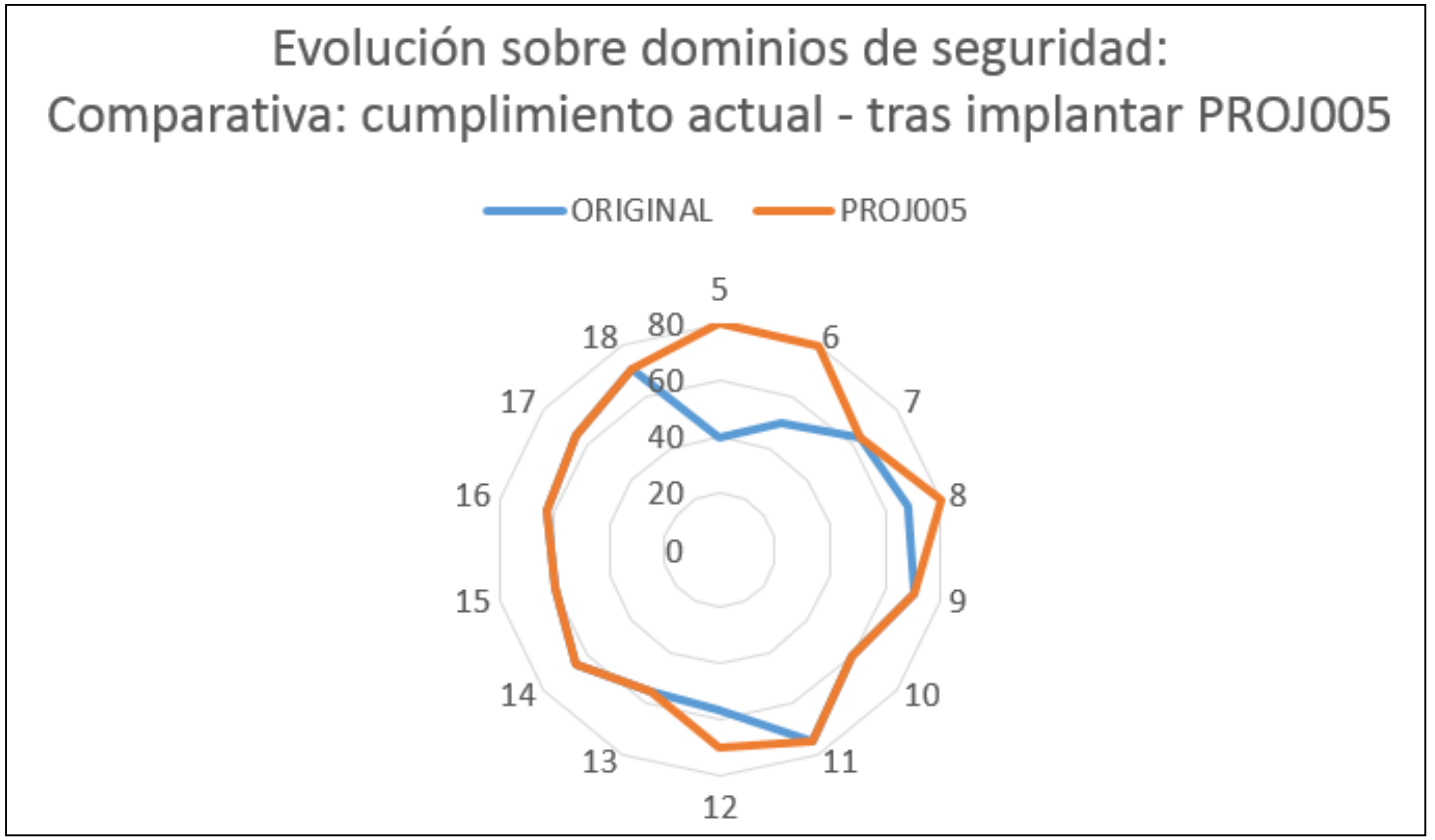


Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (9/12)

- **Código del proyecto:** PROJ005
- **Nombre del proyecto:** Implantación de sistema de Helpdesk y tratamiento de incidencias de Sistemas y Tecnologías de la información.
- **Dominios afectados:** Aspectos organizativos de la seguridad de la información, gestión de activos, seguridad física y ambiental, seguridad en la operativa, adquisición, desarrollo y mantenimiento de los sistemas de información, relaciones con suministradores, gestión de incidentes en la seguridad de la información, aspectos de seguridad de la información en la gestión de la continuidad del negocio, cumplimiento.
- **Objetivo:** Implementar un sistema Helpdesk o de tratamiento de incidencias y peticiones de servicio para el departamento de Sistemas y Tecnologías de la Información y de la Comunicaciones.
- **Responsable:** Responsable de sistemas y tecnologías de la información.
- **Riesgo a mitigar:** intrusiones intencionadas (amenaza A-INT3) sobre los datos y hardware, robo intencionado (A-INT2) sobre los datos y hardware, pérdida / hurto sobre el hardware de la compañía.

4. Propuestas de proyectos (10/12)



Autor: Francisco Antonio Lievano Cos.

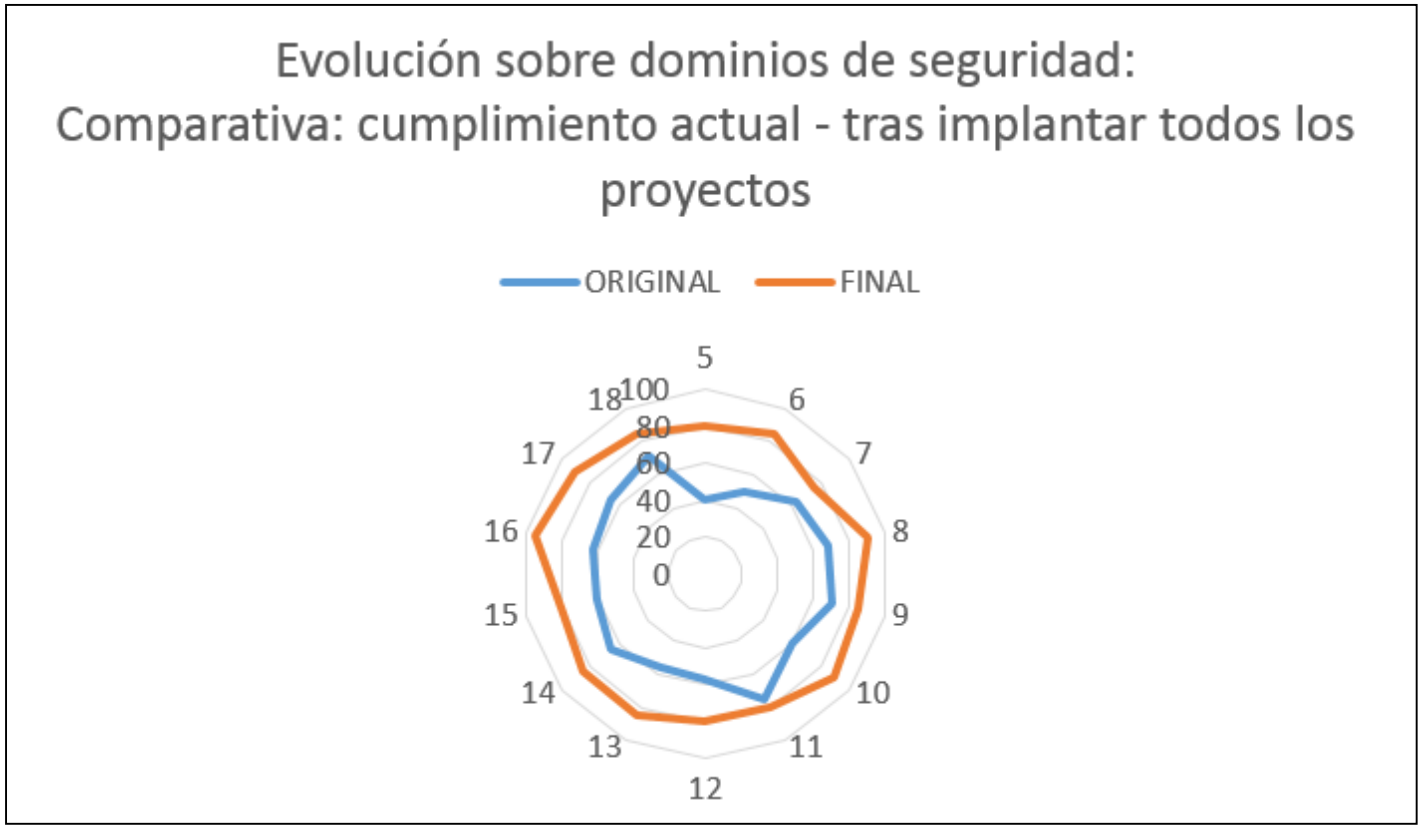
4. Propuestas de proyectos (11/12)

- Planificación inicial para la realización de los proyectos propuestos:

PLANIFICACIÓN DE IMPLANTACIÓN DE PROYECTOS												
PROYECTO	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
001												
002												
003												
004												
005												

Autor: Francisco Antonio Lievano Cos.

4. Propuestas de proyectos (12/12)



Autor: Francisco Antonio Lievano Cos.

5. Auditoría de cumplimiento (1/5)

La estimación del estado de cumplimiento de cada dominio y control estipulado en la norma se basa en el CMM (Modelo de Madurez de la Capacidad), según la definición de la siguiente escala:

CMM	EFECTIVIDAD	SIGNIFICADO	DESCRIPCIÓN
L0	0%	Inexistente	Carencia completa de procesos que reconocemos.
L1	10%	Inicial	El éxito de los procesos se basa mayoritariamente en el esfuerzo del personal. Los procesos son inexistentes o enfocados a áreas muy concretas. No existen plantillas.
L2	50%	Reproducible, no intuitivo	Los procesos similares se realizan de forma similar por distintas personas con la mismsa tarea. Se normalizan las buenas prácticas en base a la experiencia y el método.
L3	90%	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados y documentados.
L4	95%	Gestionado, medible	La evolución de los procesos se puede seguir con indicadores numéricos y estadísticas. Se dispone de la tecnología necesaria para automatizar el flujo de trabajo.
L5	100%	Optimizado	Los procesos están en constante mejora. Se determinan las desviaciones en base a criterios cuantitativos.

Autor: Francisco Antonio Lievano Cos.

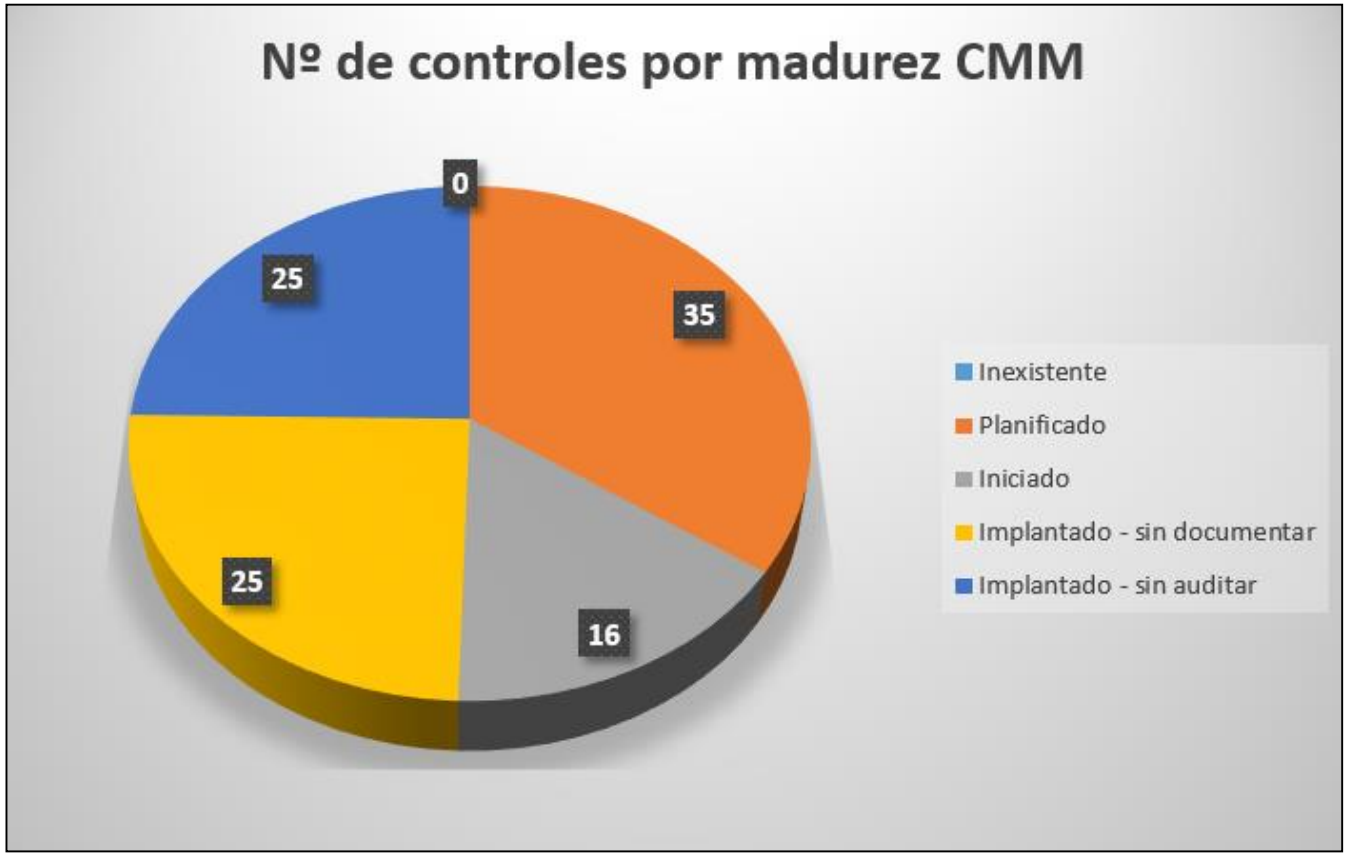
5. Auditoría de cumplimiento (2/5)

Como resultado, tenemos la siguiente cantidad de controles por tipo de madurez inicial:

Madurez inicial	Nº de controles
Inexistente	0
Planificado	35
Iniciado	16
Implantado - sin documentar	25
Implantado - sin auditar	25

Representando de forma gráfica la madurez CMM de todos los controles ISO anteriores, tenemos:

5. Auditoría de cumplimiento (3/5)



Autor: Francisco Antonio Lievano Cos.

5. Auditoría de cumplimiento (4/5)

En cuanto a las no conformidades, se clasificarían de acuerdo con el Modelo de Madurez de la Capacidad (CMM) de la siguiente forma:

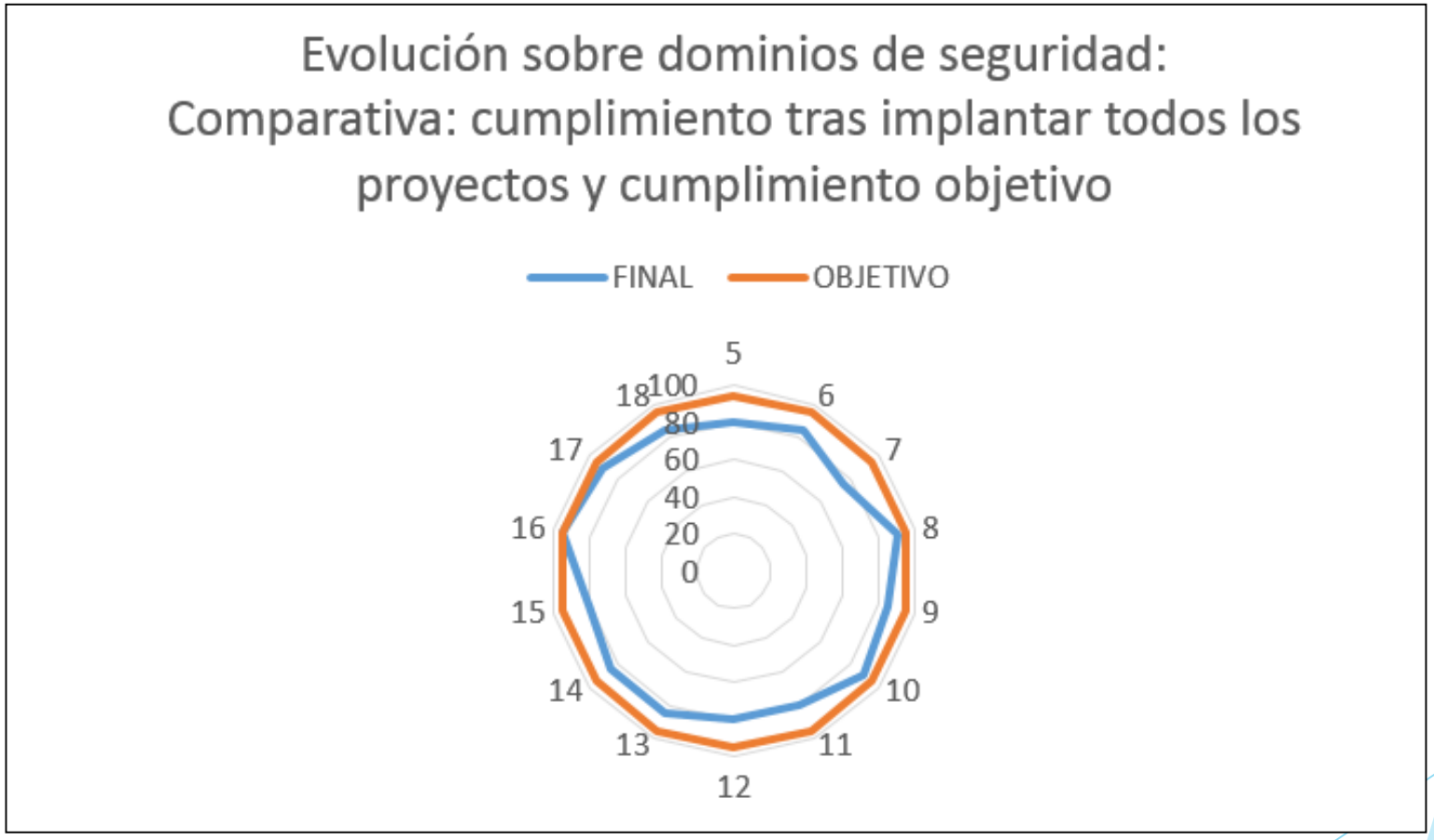
- No conformidades mayores: CMM 0 y 1.
- No conformidades menores: CMM 2 y 3.
- Observaciones: CMM 4 y 5.

En el caso particular del caso en estudio, vemos que no hay no conformidades ni observaciones, ya que todos los controles, una vez implantados todos los proyectos planteados, tienen una madurez superior a 6.

Para finalizar, se muestra un gráfico de radar donde se refleja la distancia que hay entre la madurez por dominio de la seguridad respecto del objetivo de madurez de la compañía, que se establece en 95%:

Autor: Francisco Antonio Lievano Cos.

5. Auditoría de cumplimiento (5/5)



Autor: Francisco Antonio Lievano Cos.

6. Conclusiones

Como resultado del presente trabajo, se puede constatar que la implantación del SGSI reveló importantes carencias en cuanto a medidas de seguridad, políticas y medidas técnicas dentro de la empresa para proteger la información y las tecnologías de la misma.

Tras implementar diversos proyectos enfocados en mitigar esta situación y mejorar la seguridad, se constata que mejoran de forma sustancial las conclusiones del análisis de cada dominio y control de seguridad planteado por la normativa.

Es importante tener en consideración que la implantación de este SGSI, dentro de cualquier organización, no debe quedarse en el análisis inicial e implementación de proyectos puntuales para subsanar una situación puntual de riesgo, sino que es necesario y conveniente mantener una disciplina interna enfocada en hacer un seguimiento riguroso al análisis continuo y la constante mejora de la seguridad a lo largo del tiempo.

Fin.

Estudiante: Francisco Antonio Lievano Cos.
Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC).
Consultor: Arsenio Tortajada Gallego.
Centro: Universitat Oberta de Catalunya.
Entrega: Junio de 2016.