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.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Sistemas de gestión de la seguridad de la información.*
Nombre del autor:	*Francisco Antonio Lievano Cos.*
Nombre del consultor:	*Arsenio Tortajada Gallego.*
Fecha de entrega:	*06/2016.*
Idioma del trabajo:	*Castellano.*
Área del Trabajo Final:	*Gestión de la seguridad.*
Titulación:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resumen del Trabajo:

El presente Trabajo de Fin de Máster recopila todos los conocimientos adquiridos a lo largo del máster, poniendo en práctica dichos conocimientos sobre un caso real, en el que es necesario aplicar técnicas y metodologías aprendidas para solventar una necesidad real y gestionar de la mejor forma la seguridad de la información de una empresa determinada.

Abstract:

This Project collects all the knowledge acquired during the master, implementing such knowledge on a real case, in which it is necessary to apply techniques and methodologies learned to solve a real need and manage the best way the information security of a particular company.

Palabras clave:

Seguridad, Sistemas, Análisis, Normativa, Información, ISO, Gestión.

Índice

1. Introducción – Situación actual

1.1 Contexto y justificación

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.

1.2 Objetivos del Trabajo

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.

1.3 Descripción de la organización

La organización que se utilizará para el estudio y análisis en base a sistemas de gestión de la seguridad se dedica al desarrollo de software de simulación y de modelado 3D. Esta empresa únicamente se dedica al desarrollo de productos y a la comercialización del mismo.

La empresa elegida para el estudio tiene una dimensión de entre 60 y 70 empleados ubicados en una misma oficina, donde trabajan juntos departamentos de desarrollo, de sistemas, de administración, de marketing y comunicación, disponiendo de una sala de servidores en el mismo edificio.

La empresa se encuentra ubicada en Madrid y tiene colaboradores (freelance) que trabajan desde Barcelona (una persona), Canarias (una persona) y China (una persona). La oficina central de Madrid ocupa físicamente un edificio de tres alturas: la planta baja está ocupada por las áreas de servicios, como Sistemas e IT, Marketing, Administración y Dirección, además de tener el office o cocina. La primera planta está ocupada por todas las áreas de desarrollo de software y la tercera se utiliza como sala de conferencias. El sótano se utiliza como garaje y tiene un habitáculo acondicionado que funciona como CPD o centro de datos. En él se ubican todos los servidores y elementos de red (como routers y firewall), disponiendo de dos sistemas de aire acondicionado y una SAI.

Todas las zonas de la oficina están protegidas mediante un sistema de control de acceso utilizando tarjetas de proximidad. Cada persona dispone de unos accesos distintos, dependiendo de su función dentro de la empresa. El único habitáculo no controlado mediante tarjetas de proximidad es el CPD, que requiere de llave física para acceder. Únicamente disponen de llave el CEO de la empresa y el responsable de Sistemas e IT.

A continuación, se muestra el diagrama de la red de la empresa objeto de este estudio:

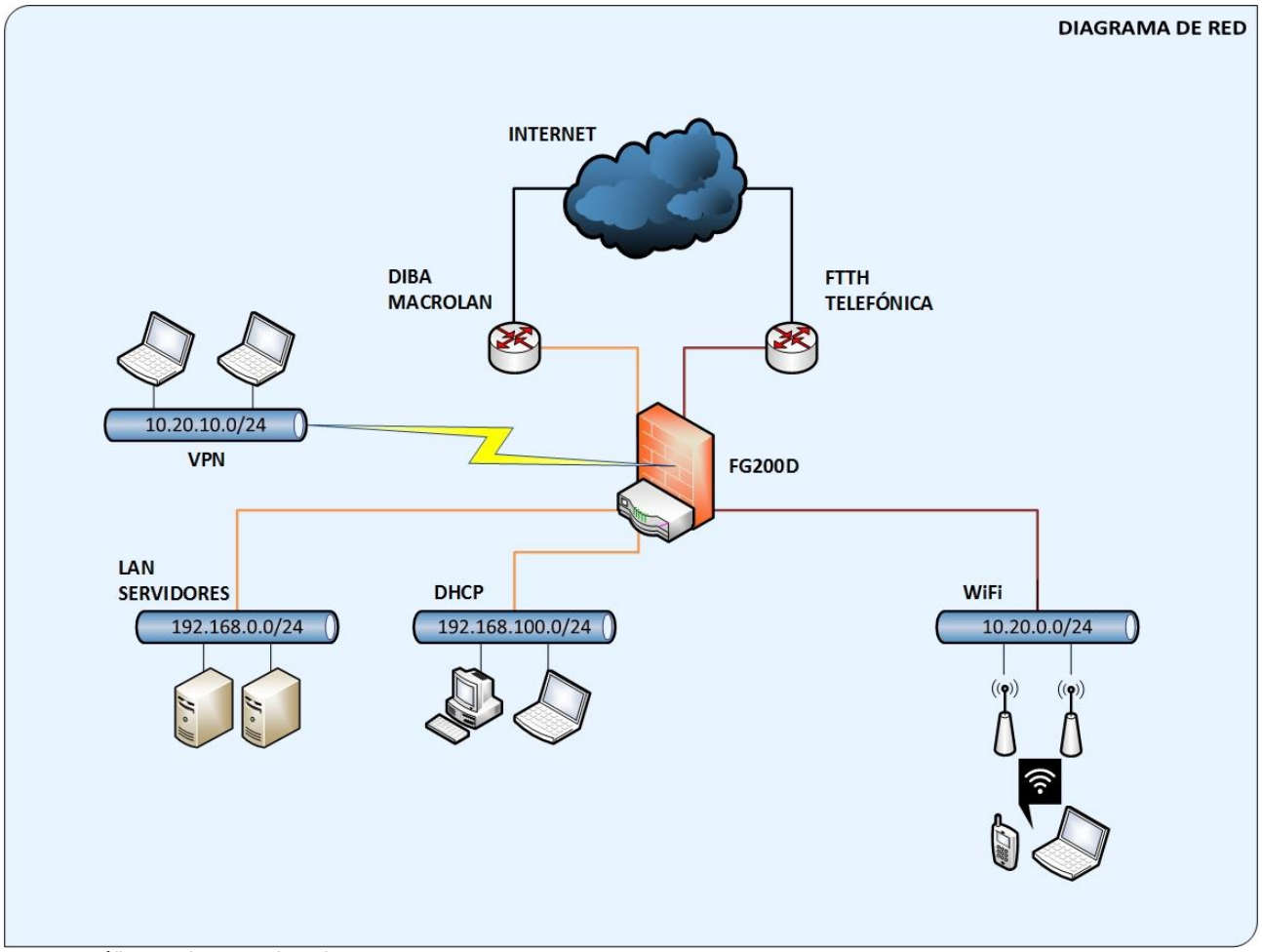

Gráfico 1: Diagrama de red.

En cuanto a aplicaciones utilizadas dentro de la empresa cabe destacar:

- Correo electrónico: Postfix alojado en un proveedor externo. La compañía únicamente tiene gestión de alto nivel (gestión de cuentas, redirecciones, listas) y no tiene acceso administrador al Sistema Operativo del servidor que presta servicio.

- Repositorio de código: dependiendo del proyecto, se utiliza GIT, SVN o Mercurial. Dichos motores están instalados en un mismo servidor repositorio de código.

- Intercambio de ficheros: servidor Fedora con Samba instalado para compartición de ficheros. Se gestiona mediante usuarios y cuentas locales.

- GLPI: aplicación para el reporte y gestión de inventario de Sistemas e IT, incidencias, peticiones de servicio y problemas, además de servir como herramienta de planificación de proyectos para dicho departamento.

- Jira: aplicación para la gestión de proyectos de desarrollo de software de las diversas unidades de negocio de la compañía.

- Freshdesk: herramienta de gestión de incidencias y comunicación con usuarios clientes o potenciales clientes. En esta herramienta se crean casos a partir de comunicaciones de usuarios (mediante webs o foros).

1.4 Alcance del Plan Director de Seguridad

Como se ha comentado con anterioridad, el Plan Director de Seguridad en sí mismo no tiene interés, ha de ir alineado con un objetivo estratégico que es el que va a delimitar el alcance del Plan Director de Seguridad.

En nuestro caso concreto, el alcance del Plan Director de Seguridad se va a enmarcar dentro del objetivo de "mejorar la seguridad de los sistemas utilizados por empleados y clientes".

Se trata de un objetivo amplio que requiere la revisión de todos los sistemas de la empresa y determinar qué puntos débiles existen en cada uno de ellos y realizar propuestas de mejora puntuales y continuas.

1.5 Análisis de cumplimiento inicial

A continuación, se realiza el análisis inicial de todos los objetivos de control y controles estipulados por la normativa ISO 27002:

CONTROL	NIVEL DE CUMPLIMIENTO (%)
5 POLÍTICAS DE SEGURIDAD.	40
5.1 Directrices de la Dirección en seguridad de la información.	40
5.1.1 Conjunto de políticas para la seguridad de la información.	50
5.1.2 Revisión de las políticas para la seguridad de la información.	30
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	55

6.1 Organización interna.	60
6.1.1 Asignación de responsabilidades para la seguridad de la información.	50
6.1.2 Segregación de tareas.	75
6.1.3 Contacto con las autoridades.	80
6.1.4 Contacto con grupos de interés especial.	75
6.1.5 Seguridad de la información en la gestión de proyectos.	20
6.2 Dispositivos para movilidad y teletrabajo	50
6.2.1 Política de uso de dispositivos para movilidad.	50
6.2.2 Teletrabajo.	50
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	63,3
7.1 Antes de la contratación.	65
7.1.1 Investigación de antecedentes.	50
7.1.2 Términos y condiciones de contratación.	80
7.2 Durante la contratación.	75
7.2.1 Responsabilidades de gestión.	80
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	70
7.2.3 Proceso disciplinario.	75
7.3 Cese o cambio de puesto de trabajo.	50
7.3.1 Cese o cambio de puesto de trabajo.	50
8. GESTIÓN DE ACTIVOS.	68,6
8.1 Responsabilidad sobre los activos.	82,5
8.1.1 Inventario de activos.	80
8.1.2 Propiedad de los activos.	90
8.1.3 Uso aceptable de los activos.	80
8.1.4 Devolución de activos.	80
8.2 Clasificación de la información.	83,3
8.2.1 Directrices de clasificación.	80
8.2.2 Etiquetado y manipulado de la información.	90
8.2.3 Manipulación de activos.	80
8.3 Manejo de los soportes de almacenamiento.	40
8.3.1 Gestión de soportes extraíbles.	40
8.3.2 Eliminación de soportes.	40
8.3.3 Soportes físicos en tránsito.	40
9. CONTROL DE ACCESOS.	70,2
9.1 Requisitos de negocio para el control de accesos.	70
9.1.1 Política de control de accesos.	90

9.1.2 Control de acceso a las redes y servicios asociados.	50
9.2 Gestión de acceso de usuario.	70,8
9.2.1 Gestión de altas/bajas en el registro de usuarios.	75
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	80
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	80
9.2.4 Gestión de información confidencial de autenticación de usuarios.	50
9.2.5 Revisión de los derechos de acceso de los usuarios.	70
9.2.6 Retirada o adaptación de los derechos de acceso.	70
9.3 Responsabilidades del usuario.	70
9.3.1 Uso de información confidencial para la autenticación.	70
9.4 Control de acceso a sistemas y aplicaciones.	70
9.4.1 Restricción del acceso a la información.	80
9.4.2 Procedimientos seguros de inicio de sesión.	60
9.4.3 Gestión de contraseñas de usuario.	60
9.4.4 Uso de herramientas de administración de sistemas.	80
9.4.5 Control de acceso al código fuente de los programas.	70
10. CIFRADO.	60
10.1 Controles criptográficos.	60
10.1.1 Política de uso de los controles criptográficos.	50
10.1.2 Gestión de claves.	70
11. SEGURIDAD FÍSICA Y AMBIENTAL.	74,7
11.1 Áreas seguras.	85
11.1.1 Perímetro de seguridad física.	90
11.1.2 Controles físicos de entrada.	90
11.1.3 Seguridad de oficinas, despachos y recursos.	70
11.1.4 Protección contra las amenazas externas y ambientales.	80
11.1.5 El trabajo en áreas seguras.	90
11.1.6 Áreas de acceso público, carga y descarga.	90
11.2 Seguridad de los equipos.	64,4
11.2.1 Emplazamiento y protección de equipos.	60
11.2.2 Instalaciones de suministro.	80
11.2.3 Seguridad del cableado.	80

11.2.4 Mantenimiento de los equipos.	70
11.2.5 Salida de activos fuera de las dependencias de la empresa.	60
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	60
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	50
11.2.8 Equipo informático de usuario desatendido.	60
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	60
12. SEGURIDAD EN LA OPERATIVA.	56,4
12.1 Responsabilidades y procedimientos de operación	60
12.1.1 Documentación de procedimientos de operación.	70
12.1.2 Gestión de cambios.	50
12.1.3 Gestión de capacidades.	70
12.1.4 Separación de entornos de desarrollo, prueba y producción.	50
12.2 Protección contra código malicioso.	70
12.2.1 Controles contra el código malicioso.	70
12.3 Copias de seguridad.	80
12.3.1 Copias de seguridad de la información.	80
12.4 Registro de actividad y supervisión.	65
12.4.1 Registro y gestión de eventos de actividad.	70
12.4.2 Protección de los registros de información	70
12.4.3 Registros de actividad del administrador y operador del sistema.	80
12.4.4 Sincronización de relojes.	40
12.5 Control del software en explotación.	50
12.5.1 Instalación del software en sistemas en producción.	50
12.6 Gestión de la vulnerabilidad técnica.	40
12.6.1 Gestión de las vulnerabilidades técnicas.	40
12.6.2 Restricciones en la instalación de software.	40
12.7 Consideraciones de las auditorías de los sistemas de información.	30
12.7.1 Controles de auditoría de los sistemas de información.	30
13. SEGURIDAD EN LAS TELECOMUNICACIONES	55,8
13.1 Gestión de la seguridad en las redes.	46,6
13.1.1 Controles de red.	40
13.1.2 Mecanismos de seguridad asociados a servicios	60

en red.	
13.1.3 Segregación de redes.	40
13.2 Intercambio de información con partes externas.	65
13.2.1 Políticas y procedimientos de intercambio de información.	50
13.2.2 Acuerdos de intercambio.	50
13.2.3 Mensajería electrónica.	70
13.2.4 Acuerdos de confidencialidad y secreto.	90
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	65,1
14.1 Requisitos de seguridad de los sistemas de información	73,3
14.1.1 Análisis y especificación de los requisitos de seguridad.	60
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	80
14.1.3 Protección de las transacciones por redes telemáticas.	80
14.2 Seguridad en los procesos de desarrollo y soporte.	62,2
14.2.1 Política de desarrollo seguro de software.	70
14.2.2 Procedimientos de control de cambios en los sistemas.	60
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	80
14.2.4 Restricciones a los cambios en los paquetes de software.	40
14.2.5 Uso de principios de ingeniería en protección de sistemas.	50
14.2.6 Seguridad en entornos de desarrollo.	60
14.2.7 Externalización del desarrollo de software.	50
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	70
14.2.9 Pruebas de aceptación.	80
14.3 Datos de prueba.	60
14.3.1 Protección de los datos utilizados en pruebas.	60
15. RELACIONES CON SUMINISTRADORES.	60
15.1 Seguridad de la información en las relaciones con suministradores.	70
15.1.1 Política de seguridad de la información para suministradores.	70
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	70
15.1.3 Cadena de suministro en tecnologías de la	70

información y comunicaciones.	
15.2 Gestión de la prestación del servicio por suministradores.	50
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	50
15.2.2 Gestión de cambios en los servicios prestados por terceros.	50
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	62,8
16.1 Gestión de incidentes de seguridad de la información y mejoras.	62,8
16.1.1 Responsabilidades y procedimientos.	60
16.1.2 Notificación de los eventos de seguridad de la información.	60
16.1.3 Notificación de puntos débiles de la seguridad.	70
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	70
16.1.5 Respuesta a los incidentes de seguridad.	70
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	60
16.1.7 Recopilación de evidencias.	50
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	65
17.1 Continuidad de la seguridad de la información.	60
17.1.1 Planificación de la continuidad de la seguridad de la información.	60
17.1.2 Implantación de la continuidad de la seguridad de la información.	60
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	60
17.2 Redundancias.	70
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	70
18. CUMPLIMIENTO.	71
18.1 Cumplimiento de los requisitos legales y contractuales.	72
18.1.1 Identificación de la legislación aplicable.	80
18.1.2 Derechos de propiedad intelectual (DPI).	80
18.1.3 Protección de los registros de la organización.	80
18.1.4 Protección de datos y privacidad de la información personal.	70
18.1.5 Regulación de los controles criptográficos.	50
18.2 Revisiones de la seguridad de la información.	70

18.2.1 Revisión independiente de la seguridad de la información.	70
18.2.2 Cumplimiento de las políticas y normas de seguridad.	70
18.2.3 Comprobación del cumplimiento.	70

Se puede comprobar que en la mayoría de dominios no se obtiene una valoración superior a 75%. Esto quiere decir que, 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.

2. Sistema de gestión documental

A continuación, se detalla el esquema documental que va vinculado a la presente memoria. Los documentos a continuación descritos vienen definidos por la norma ISO/IEC 27001 como necesarios para certificar el sistema, entre otros no incluidos en el presente TFM.

2.1 Política de Seguridad

La Política de Seguridad es establecida por la Dirección de la empresa y tiene en consideración que:

- Ha de adecuarse a la estrategia de la empresa.
- Ha de reflejar los objetivos de seguridad de la Información y un marco o framework para ella.
- Ha de reflejar un compromiso y deber por parte de la audiencia de la política.
- Ha de estar disponible y constantemente comunicada a las personas que afecte.

La Política de Seguridad de la empresa reconoce como activo estratégico y fundamental la información, por lo que debe ser utilizada y mantenida con las medidas de protección que, como activo de gran importancia, merece. Es necesario tener en cuenta que la información generado por la empresa es el primer activo de la misma y tiene una importancia vital en la consecución de los objetivos de la misma.

La empresa, en este sentido, declara lo siguiente:

- Se ha de mantener los principios fundamentales de confidencialidad, integridad y disponibilidad de la información.

- Se ha de identificar y reconocer todos los requisitos de protección de la información, así como requisitos legales que apliquen a la misma.

- Se ha de implementar y utilizar el modelo de Gestión de la Seguridad de la Información de forma continua en el tiempo.

- Se ha de mantener una comunicación constante con las personas y equipos que afecte la Política de Seguridad.

- Se ha de establecer roles y responsabilidades frente a la protección de los datos e información de la empresa.

En el documento adjunto "**SGSI - Política de Seguridad v1-1.pdf**", se hace referencia de forma más extensa y minuciosa a la Política de Seguridad de la empresa objeto de estudio de este TFM.

2.2 Procedimiento de Auditorías Internas

Dentro de la empresa es imprescindible implementar un proceso de auditorías internas para realizar un correcto mantenimiento continuado y evolutivo del Sistema de Gestión de la Seguridad de la Información. Mediante estas auditorías internas se realiza una mejora del sistema a partir de la implementación inicial.

A continuación, se describe el proceso de auditorías internas, una planificación de las mismas, el perfil del encargado de dicha responsabilidad (auditor interno), así como un modelo de informe de auditorías internas.

2.2.1. Perfil del auditor interno

El auditor interno es la persona encargada de realizar periódicamente la auditoría interna en la empresa. Es su responsabilidad la coordinación entre todas las partes implicadas, realizar un correcto registro de todos los elementos auditables y en resumen planificar, preparar y realizar las auditorías internas.

Las funciones específicas del auditor interno son:

- 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.

El auditor interno debería poseer título universitario en el área de la Ingeniería Informática o de Telecomunicaciones, deberá haber realizado el curso de auditor interno ISO 27001 y experiencia en la ejecución de auditorías de Sistemas de Gestión de la Seguridad de la Información.

2.2.2. Programa anual de auditorías

Se planifica la realización de auditorías parciales (por control previsto en la normativa ISO 27002), realizando la auditoría de todos los puntos a auditar a lo largo de un año.

La planificación inicial de auditorías de seguridad es la siguiente:

	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**	

2.2.3. Modelo de informe de auditoría

El siguiente modelo de informe servirá de guía para registrar cada una de las auditorías internas de seguridad que se realicen en la empresa:

INFORME DE AUDITORÍA INTERNA <EMPRESA>	**CÓDIGO**
	VERSIÓN

1. DATOS DE LA AUDITORÍA INTERNA	
Auditoría Nº	
Norma de referencia	
Período de la auditoría	
Lugar de la auditoría	
Equipo auditor	

2. ALCANCE DE LA AUDITORÍA INTERNA

3. OBJETIVOS DE LA AUDITORÍA INTERNA

4. DEFINICIONES
4.1. No conformidad: incumplimiento de un requisito, política o documento, cuya repetición pone en riesgo la efectividad del SGSI. **4.2. Observación:** es un fallo aislado en el contenido o implementación de los documentos o cualquier incumplimiento parcial en un requisito. **4.3. Oportunidad de mejora:** acción recomendada que al ser implementada implica una mejora del SGSI.

5. FORTALEZAS Y DEBILIDADES	
<u>Fortalezas:</u> 1. 2. 3. 4. 5.	<u>Debilidades:</u> 1. 2. 3. 4. 5.

6. RESULTADOS DE LA AUDITORÍA INTERNA			
Se encontraron ___ no conformidades, resumidas a continuación:			
ÁREA	DESCRIPCIÓN	RESPONSABLE	AUDITOR
Se detectaron las siguientes oportunidades de mejora:			

7. CONCLUSIONES DE LA AUDITORÍA INTERNA
1. 2. 3. 4. 5.

2.3 Gestión de Indicadores

La validación del correcto cumplimiento de la implementación del Sistema de Gestión de la Seguridad de la Información se realiza evaluando o midiendo distintos criterios. El proceso de evaluación de procesos y medición de criterios tiene como fin la mejora del SGSI y constatar su correcto funcionamiento dentro de la empresa.

Crear un sistema que mida mediante indicadores cada control especificado en la ISO sería poco práctico, por lo que se crean indicadores que son de gran utilidad y que aglutinan varios controles a su vez, para de esta forma crear un análisis que sea lo más realista y funcional posible.

Los indicadores que se van a gestionar son los siguientes:

1. Control de repositorio de código.
2. Control de webs (marketing y venta online).
3. Control de soporte y satisfacción de clientes.
4. Control de contabilidad.
5. Control de equipos informáticos.
6. Control de cumplimiento de normativa.
7. Control de cumplimiento y seguimiento de resultados de auditorías del SGSI.

A continuación, se detalla en qué consiste cada uno de ellos:

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

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

2.4 Procedimiento de Revisión por la Dirección

Como se ha comentado con anterioridad, debido al carácter prioritario y vital de la Información dentro de la empresa, la Dirección de la misma toma parte activa en la revisión del cumplimiento de los aspectos de seguridad relativa a la Información, por lo que la normativa ISO 27001 establece que:

- Se debe realizar una revisión en intervalos planificados para asegurar la adecuación continua del SGSI.

- Se debe incluir consideraciones relativas a:

    - Estado de acciones basadas en revisiones anteriores, en caso de existir.

    - Cambios en el contexto de la empresa que afecten al SGSI, como el cambio de estrategia de la organización.

    - Retroalimentación relativa al desempeño de la Seguridad de la Información, como no conformidades, acciones correctivas, resultados de auditorías y cumplimiento de objetivos de seguridad).

- Comentarios de las partes implicadas que consten entre cada revisión de la Dirección.

- Resultados de valoración de riesgo.

- Oportunidades de mejora referentes al SGSI.

- Se ha de conservar la información documentada de forma detallada como evidencia de revisión.

- Como salidas de la revisión de Dirección se consideran las decisiones relacionadas con oportunidades de mejora y necesidades de cambio estratégicas.

La revisión del SGSI por la Dirección de la empresa la realiza la Presidencia como responsable de la administración del sistema de gestión, verificando entre otros 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.

- Cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.

- Resultados de la gestión de riesgos corporativos, incluyendo vulnerabilidades o amenazas.

2.4.1. Programa de revisiones

Se planifica la realización de revisiones de forma anual o de forma extraordinaria cuando la Presidencia de la empresa así lo considere oportuno.

Se ha de tener en cuenta por parte de la Dirección que la planificación inicial de auditorías de seguridad es la siguiente:

	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**	

2.4.2. Modelo de informe de revisión por la Dirección

El siguiente modelo de informe servirá de guía para registrar cada una de las revisiones por la Dirección de la seguridad que se realicen en la empresa:

INFORME DE REVISIÓN POR LA DIRECCIÓN <EMPRESA>	**CÓDIGO**
	VERSIÓN

1. DATOS DE LA REVISIÓN	
Revisión Nº	
Norma de referencia	
Período de la revisión	
Lugar de la auditoría	
Comité revisor	

2. ALCANCE DE LA REVISIÓN

3. OBJETIVOS DE LA REVISIÓN

4. RESULTADOS DE LA REVISIÓN			
ÁREA	DESCRIPCIÓN	RESPONSABLE	AUDITOR
Comentarios:			

5. CONCLUSIONES DE LA REVISIÓN
1. 2. 3. 4. 5.

2.5 Gestión de Roles y Responsabilidades

En la norma ISO 27001 se establece que los roles, responsabilidades y autoridades en la organización han de cumplir los siguientes requerimientos:

- La Dirección ha de asegurar la comunicación y asignación de roles dentro de la organización.
- La Dirección debe asignar responsabilidades y autoridad para asegurar la conformidad del SGSI con la normativa ISO 27001.
- La Dirección ha de asignar responsabilidad y autoridad para tener una fuente que reporte sobre el desempeño del SGSI.

2.5.1. Definición de roles y responsabilidades

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:

Gráfico 2: Organización SGSI dentro de la empresa.

Existe un nivel de responsabilidades, agrupados de la siguiente forma:

- **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.

- **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.

2.6 Metodología de Análisis de Riesgos

El análisis de riesgos, como pueden ser la pérdida de confidencialidad, integridad o disponibilidad de los activos de la empresa ha de seguir una metodología que define los criterios que influyen en el riesgo global, escalas de impacto, criterios de aceptación de riesgo y tipos de impacto, entre otros elementos a analizar.

2.6.1. Proceso de análisis de riesgos

El primer paso es definir la metodología que utilizará la empresa para valorar o calcular los riesgos. Se ha de ser coherente con la estrategia de la empresa.

- **Escala de valoración de activos:** se toma como máximo el valor máximo de un activo dentro de la empresa y se crea la siguiente escala a partir de ella:

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

- **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

- **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, que son:

  - **Autenticidad (A):** garantías de identidad de los usuarios.
  - **Confidencialidad (C):** accesos a información sensible.
  - **Integridad (I):** garantía de que los métodos de acceso a la información son completos.
  - **Disponibilidad (D):** garantía de disponibilidad máxima de la información.
  - **Trazabilidad (T):** garantía de revisión de acciones sobre la información.

La escala de valoración es:

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		
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

2.7 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.

A continuación, se muestra la matriz de aplicabilidad por dominio y control:

ID	Dominio / Control	Aplicabilidad	Registro de implementación
5	POLÍTICAS DE SEGURIDAD		
5.1.1	Documento de la política de seguridad de la información.	Aplica	Ya visado por la Dirección, comunicado a los empleados pero no firmado por los empleados.
5.1.2	Revisión de las políticas de seguridad de la información.	Aplica	Existe plantilla de registro de revisión periódica. A utilizar en siguiente
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1.1	Asignación de responsabilidades para la seguridad de la información.	Aplica	Equipos de trabajo formados.
6.1.2	Segregación de tareas.	Aplica	Tareas asignadas a equipos de trabajo según responsabilidades asignadas.
6.1.3	Contacto con las autoridades.	Aplica	Claúsulas contractuales, modelos de contratos con las claúsulas de confidencialidad.
6.1.4	Contacto con grupos de interés especial.	Aplica	Claúsulas contractuales, modelos de contratos con las claúsulas de confidencialidad.
6.1.5	Seguridad de la información en la gestión de proyectos.	Aplica	Documento con recomendaciones a la hora de gestionar proyectos.
6.2.1	Política de uso de dispositivos para movilidad.	Aplica	Documento con recomendaciones y "guidelines" para el uso de dispositivos.
6.2.2	Teletrabajo.	Aplica	Documento con recomendaciones y "guidelines" para el uso de dispositivos.
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
7.1.1	Investigación de antecedentes.	Aplica	Proceso de revisión de antecedentes dentro de la compañía y en redes
7.1.2	Términos y condiciones de contratación.	Aplica	Inlcusión de elementos de seguridad sobre los procesos de selección de personal
7.2.1	Responsabilidades de gestión.	Aplica	Responsabilidades asignadas al equipo de RRHH.
7.2.2	Concienciación, educación y capacitación en seguridad de la información.	Aplica	Plan de formación y capacitación contínua (Intranet y sesiones presenciales).
7.2.3	Proceso disciplinario.	Aplica	Existe proceso de apertura y seguimiento de procesos disciplinarios.
7.3.1	Cese o cambio de puesto de trabajo.	Aplica	Existe proceso de cese o cambio de puesto de trabajo.
8	GESTIÓN DE ACTICVOS		
8.1.1	Inventario de activos.	Aplica	Existe inventario en herramienta de gestión GLPI.
8.1.2	Propiedad de los activos.	Aplica	Propiedad reflejada en inventario de activos.
8.1.3	Uso aceptable de los activos.	Aplica	Política de uso aceptable de activos pendiente de firma por parte de los empleados.
8.1.4	Devolución de activos.	Aplica	Incluido en procedimiento existente de uso de activos.
8.2.1	Directrices de clasificación.	Aplica	Incluido en procedimiento existente de uso de activos.
8.2.2	Etiquetado y manipulado de la información.	Aplica	Incluido en procedimiento existente de uso de activos.
8.2.3	Manipulación de activos.	Aplica	Incluido en procedimiento existente de uso de activos.
8.3.1	Gestión de soportes extraíbles.	Aplica	Incluido en procedimiento existente de uso de activos.
8.3.2	Eliminación de soportes.	Aplica	Incluido en procedimiento existente de uso de activos.
8.3.3	Soportes físicos en tránsito.	Aplica	Incluido en procedimiento existente de uso de activos.
9	CONTROL DE ACCESOS		
9.1.1	Política de control de accesos.	Aplica	Ya visado por la Dirección, comunicado a los empleados pero no firmado por los empleados.
9.1.2	Control de acceso a las redes y servicios asociados.	Aplica	Existe procedimiento implementado por departamento de Sistemas y TI
9.2.1	Gestión de altas/bajas en el registro de usuarios.	Aplica	Existe procedimiento implementado por departamento de Sistemas y TI
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Aplica	Inventario de accesos mantenido por departamento de Sistemas y TI
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	Aplica	Inventario de accesos mantenido por departamento de Sistemas y TI (SITIC).
9.2.4	Gestión de información confidencial de autenticación de usuarios.	Aplica	Inventario de accesos mantenido por departamento de Sistemas y TI (SITIC).
9.2.5	Revisión de los derechos de acceso de los usuarios.	Aplica	Procedimiento de revisión periódica de accesos pendiente de implementar.
9.2.6	Retirada o adaptación de los derechos de acceso.	Aplica	Procedimiento de revisión periódica de accesos pendiente de implementar.
9.3.1	Uso de información confidencial para la autenticación.	Aplica	Procedimientos para el control de accesos implementado.
9.4.1	Restricción del acceso a la información.	Aplica	Procedimientos para el control de accesos implementado.
9.4.2	Procedimientos seguros de inicio de sesión.	Aplica	Pendiente de integrar en aplicaciones sistema que permita inicio seguro de sesión único.
9.4.3	Gestión de contraseñas de usuario.	Aplica	Procedimiento de autogestión de contraseñas implementado y comunicado.
9.4.4	Uso de herramientas de administración de sistemas.	Aplica	Herramientas implementadas y en uso por SITIC.
9.4.5	Control de acceso al código fuente de los programas.	Aplica	Inventario de accesos mantenido por departamento de Sistemas y TI
10	CIFRADO		
10.1.1	Política de uso de los controles criptográficos.	Aplica	Procedimiento implantado por departamento de Sistemas y TI (SITIC).
10.1.2	Gestión de claves.	Aplica	Inventario de accesos mantenido por departamento de Sistemas y TI

11	**SEGURIDAD FÍSICA Y AMBIENTAL**		
11.1.1	Perímetro de seguridad física.	Aplica	Medidas físicas de seguridad en perímero de la empresa implementados.
11.1.2	Controles físicos de entrada.	Aplica	Medidas de control de acceso físico implementadas.
11.1.3	Seguridad de oficinas, despachos y recursos.	Aplica	Medidas de control de acceso físico implementadas.
11.1.4	Protección contra las amenazas externas y ambientales.	Aplica	Medidas de control de acceso físico implementadas.
11.1.5	El trabajo en áreas seguras.	Aplica	Auditorías de cumplimiento de normativa de seguridad en el puesto de trabajo realizadas por empresa externa.
11.1.6	Áreas de acceso público, carga y descarga.	Aplica	Áreas delimitadas.
11.2.1	Emplazamiento y protección de equipos.	Aplica	Ubicación y seguridad física de equipos reglamentadas.
11.2.2	Instalaciones de suministro.	Aplica	Suministro instalado e inventariado.
11.2.3	Seguridad del cableado.	Aplica	Cableado implementado de forma ordenada y segura.
11.2.4	Mantenimiento de los equipos.	Aplica	Equipos revisados de forma periódica según procedimiento.
11.2.5	Salida de activos fuera de las dependencias de la empresa.	Aplica	No se permite, según la política de uso aceptable.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Aplica	Política de uso aceptable de activos pendiente de firma por parte de los empleados.
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Aplica	Política de uso aceptable de activos pendiente de firma por parte de los empleados.
11.2.8	Equipo informático de usuario desatendido.	Aplica	Política de uso aceptable de activos pendiente de firma por parte de los empleados.
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	Aplica	Política de uso aceptable de activos pendiente de firma por parte de los empleados.
12	**SEGURIDAD EN LA OPERATIVA**		
12.1.1	Documentación de los procedimientos de operación.	Aplica	Documentos y manuales de operación existentes.
12.1.2	Gestión de cambios.	Aplica	Documentos y procedimientos para la gestión del cambio.
12.1.3	Gestión de capacidades.	Aplica	Documento con la inclusión de las responsabilidades, funciones o en los cargos o en los procesos implementados.
12.1.4	Separación de las instalaciones de desarrollo, prueba y producción.	Aplica	Documento de arquitecturade red y entornos mantenido por SITIC.
12.2.1	Controles contra el código malicioso.	Aplica	Procesos de ejecución de software de análisis.
12.3.1	Copias de seguridad de la información.	Aplica	Procedimientos de realización de copias de seguridad existente.
12.4.1	Registro y gestión de eventos de actividad.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.4.2	Protección de los registros de información.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.4.3	Registros de actividad del administrador y operador del sistema.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.4.4	Sincronización de relojes.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.5.1	Instalación del software en sistemas en producción.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.6.1	Gestión de las vulnerabilidades técnicas.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.6.2	Restricciones en la instalación de software.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
12.7.1	Controles de auditoría de los sistemas de información.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**		
13.1.1	Controles de red.	Aplica	Documento de uso aceptable de recursos existente.
13.1.2	Mecanismos de seguridad asociados a servicios en red.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
13.1.3	Segregación de redes.	Aplica	Documento de procedimientos de uso de entornos mantenido por SITIC.
13.2.1	Políticas y procedimientos de intercambio de información.	Aplica	Documento de uso aceptable de recursos existente.
13.2.2	Acuerdos de intercambio.	Aplica	Documento de uso aceptable de recursos existente.
13.2.3	Mensajería electrónica.	Aplica	Documento de uso aceptable de recursos existente.
13.2.4	Acuerdos de confidencialidad y secreto.	Aplica	Contratos suscritos por diversos proveedores y contratantes. Documento de uso aceptable de recursos existente.
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**		
14.1.1	Análisis y especificación de los requisitos de seguridad.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.1.3	Protección de las transacciones por redes telemáticas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.1	Política de desarrollo seguro de software.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.2	Procedimientos de control de cambios en los sistemas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.4	Restricciones a los cambios en los paquetes de software.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.5	Uso de principios de ingeniería en protección de sistemas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.6	Seguridad en entornos de desarrollo.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.7	Externalización del desarrollo de software.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).

14.2.9	Pruebas de aceptación.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
14.3.1	Protección de los datos utilizados en pruebas.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
15	**RELACIONES CON SUMINISTRADORES**		
15.1.1	Política de seguridad de la información para suministradores.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Aplica	Procedimiento de especificaciones de seguridad implantado por departamento de Sistemas y TI (SITIC).
15.2.2	Gestión de cambios en los servicios prestados por terceros.	Aplica	Responsabilidades asignadas y procedimiento de seguridad implementado.
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**		
16.1.1	Responsabilidades y procedimientos.	Aplica	Responsabilidades asignadas a los distintos grupos creados.
16.1.2	Notificación de los eventos de seguridad de la información.	Aplica	Procedimiento de notificación de eventos de seguridad a SITIC y a Dirección por implantar.
16.1.3	Notificación de puntos débiles de la seguridad.	Aplica	Resultado de la auditoría de seguridad interna.
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Aplica	Resultado de la auditoría de seguridad interna.
16.1.5	Respuesta a los incidentes de seguridad.	Aplica	Pendiente de realizar auditoría de seguridad interna.
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Aplica	Resultado de la auditoría de seguridad interna.
16.1.7	Recopilación de evidencias.	Aplica	Procedimientos para la identificación, recolección, embalaje y tratamiento de la evidencias.
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**		
17.1.1	Planificación de la continuidad de la seguridad de la información.	Aplica	Procedimiento de continuidad pendiente de implementación.
17.1.2	Implantación de la continuidad de la seguridad de la información.	Aplica	Sistemas preparados para asegurar la continuidad pero documento pendiente de implementación.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Aplica	Sistemas preparados para asegurar la continuidad pero documento pendiente de implementación.
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Aplica	Sistemas preparados para asegurar la continuidad pero documento pendiente de implementación.
18	**CUMPLIMIENTO**		
18.1.1	Identificación de la legislación aplicable.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.1.2	Derechos de propiedad intelectual (DPI).	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.1.3	Protección de los registros de la organización.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.1.4	Protección de los datos y privacidad de la información personal.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.1.5	Regulación de los controles criptográficos.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.2.1	Revisión independiente de la seguridad de la información.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.2.2	Cumplimiento de las políticas y normas de seguridad.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.
18.2.3	Comprobación del cumplimiento.	Aplica	Documento con normativa vigente aplicable y procedimientos de verificación de cumplimiento.

3. Análisis de riesgos

Antes de realizar una propuesta de proyectos a implementar en la empresa para mitigar ciertas amenazas o riesgos, primero es necesario evaluar, dentro del marco del SGSI, los activos de la empresa y valorando los distintos riesgos y amenazas que los afectan.

A continuación, se detalla el análisis de los activos de la empresa, los riesgos asociados y el impacto potencial sobre los activos, a partir de la metodología definida en el punto "**2.6. Metodología de Análisis de Riesgos**".

3.1. Identificación de activos

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.

En el caso de la empresa objeto de estudio, tenemos los siguientes activos:

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

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

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

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

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

3.2. Valoración de Activos

Aplicando las escalas anteriores a los activos de la empresa, tenemos:

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

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

3.3. Análisis de amenazas y vulnerabilidades

Existe diversidad de amenazas que pueden poner en riesgo el objetivo del SGSI en la empresa. Estas amenazas pueden ser clasificadas según su origen:

- Natural / desastres naturales.
- Industrial.
- Fallos no intencionados / errores.
- Ataques intencionados.

Para completar la metodología de análisis de riesgos antes de ser aplicada para el caso concreto de la empresa objeto de estudio, tenemos la siguiente tabla, que refleja las amenazas potenciales clasificadas por su 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

Cruzando esta información junto con las frecuencias indicadas en el documento de metodología de análisis y las dimensiones de seguridad, obtenemos el análisis del impacto que tiene cada incidencia sobre los activos de la empresa:

Valoración de activos								
Nombre	Amenaza	Frecuencia	Impacto					
			A	C	I	D	T	
Redes de comunicación								
Cableado de datos para puestos de trabajo	A-NAT3	F-5				100%		
Cableado de datos para puestos de trabajo	A-NOINT2	F-5				100%		
Cableado de datos para servidores	A-NAT3	F-5				100%		
Cableado de datos para servidores	A-NOINT2	F-5				100%		
Cableado de datos entre dispositivos de red	A-NAT3	F-5				100%		
Cableado de datos entre dispositivos de red	A-NOINT2	F-5				100%		
Switch	A-NAT3	F-5				100%		
Switch	A-NOINT2	F-5				100%		
Switch	A-INT3	F-5	80%	100%	80%	80%	80%	
Access Points	A-NAT3	F-5				100%		
Access Points	A-NOINT2	F-5				100%		
Access Points	A-INT3	F-5	80%	100%	80%	80%	80%	
Firewalls	A-NAT3	F-5				100%		
Firewalls	A-NOINT2	F-5				100%		
Firewalls	A-INT3	F-5	80%	100%	80%	80%	80%	
Routers	A-NAT3	F-5				100%		
Routers	A-NOINT2	F-5				100%		
Routers	A-INT3	F-5	80%	80%	80%	100%	80%	
Hardware (PCs, servidores, consumo)								
PCs	A-NAT1	F-5				100%		
PCs	A-NAT2	F-4				75%		
PCs	A-NAT3	F-5				100%		
PCs	A-NOINT2	F-4				100%		
PCs	A-INT1	F-5				50%		
PCs	A-INT3	F-5		80%	50%		80%	
Portátiles	A-NAT1	F-5				100%		
Portátiles	A-NAT2	F-4				75%		
Portátiles	A-NAT3	F-5				100%		
Portátiles	A-NOINT2	F-4				100%		
Portátiles	A-INT1	F-5				50%		
Portátiles	A-INT2	F-5		100%		100%	100%	
Portátiles	A-INT3	F-5		80%	50%		80%	
Impresoras	A-NAT1	F-5				100%		
Impresoras	A-NAT2	F-4				75%		
Impresoras	A-NAT3	F-5				100%		
Teléfonos	A-NAT3	F-5				100%		
Teléfonos	A-NOINT2	F-5				100%		
Lectores de tarjetas de proximidad	A-NAT3	F-5				100%		
Lectores de tarjetas de proximidad	A-NOINT2	F-5				100%		
Servidores	A-NAT1	F-5				100%		
Servidores	A-NAT2	F-4				75%		
Servidores	A-NAT3	F-5				100%		
Servidores	A-NOINT2	F-4				100%		
Servidores	A-INT1	F-5	50%	100%	75%	50%	50%	
Servidores	A-INT3	F-5	50%	80%	50%	80%	100%	
Ratones (stock)	A-NAT3	F-5				100%		
Ratones (stock)	A-INT2	F-5				100%		
Teclados (stock)	A-NAT3	F-5				100%		

Teclados (stock)	A-INT2	F-5				100%	
Pantallas (stock)	A-NAT3	F-5				100%	
Pantallas (stock)	A-INT2	F-5				100%	
Software							
Ofimática	A-INT2	F-5				100%	
Aplicaciones de desarrollo	A-INT2	F-5				100%	
Aplicaciones de administración	A-INT2	F-5				100%	
Motores de bases de datos	A-INT2	F-5				100%	
Aplicaciones							
Webs	A-NOINT2	F-4	50%	50%	75%	100%	50%
Webs	A-INT1	F-4	75%	75%	80%	100%	100%
Webs	A-INT3	F-5	80%	100%	100%	80%	100%
Servidor de licencias	A-NOINT2	F-4	50%	50%	75%	100%	50%
Servidor de licencias	A-INT1	F-4	75%	75%	80%	100%	100%
Servidor de licencias	A-INT3	F-5	80%	100%	100%	80%	100%
Datos							
Repositorio de código	A-NOINT2	F-4				100%	
Repositorio de código	A-INT1	F-5	50%	100%	75%	50%	50%
Repositorio de código	A-INT3	F-5	50%	80%	50%	80%	100%
Base de datos de clientes	A-NOINT2	F-4				100%	
Base de datos de clientes	A-INT1	F-5	50%	100%	75%	50%	50%
Base de datos de clientes	A-INT3	F-5	50%	80%	50%	80%	100%
Base de datos de proveedores	A-NOINT2	F-4				100%	
Base de datos de proveedores	A-INT1	F-5	50%	100%	75%	50%	50%
Base de datos de proveedores	A-INT3	F-5	50%	80%	50%	80%	100%
Base de datos de recursos humanos	A-NOINT2	F-4				100%	
Base de datos de recursos humanos	A-INT1	F-5	50%	100%	75%	50%	50%
Base de datos de recursos humanos	A-INT3	F-5	50%	80%	50%	80%	100%
Personal							
Empleados	A-IND1	F-3				50%	
Empleados	A-IND2	F-3				50%	
Empleados	A-NOINT1	F-5				50%	
Socios directivos	A-IND1	F-3				50%	
Socios directivos	A-IND2	F-3				50%	
Socios directivos	A-NOINT1	F-5				50%	
Intangibles							
Satisfacción de clientes	A-NOINT2	F-5				50%	
Imagen corporativa de la empresa	A-NOINT2	F-5				50%	

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
Datos	
Repositorio de código	Muy alta
Base de datos de clientes	Muy alta
Base de datos de proveedores	Muy alta
Base de datos de recursos humanos	Muy alta
Personal	
Empleados	Muy alta
Socios directivos	Muy alta
Intangibles	
Satisfacción de clientes	Muy alta
Imagen corporativa de la empresa	Muy alta

El cálculo del riesgo intrínseco, teniendo en cuenta los activos de la empresa, las vulnerabilidades detectadas y el impacto que tendría su materialización, se realiza mediante la siguiente fórmula:

```
Riesgo_Intrínseco = Valor_activo x Vulnerabilidad x Impacto
```

De esta forma tenemos el riesgo intrínseco. Para obtener el riesgo efectivo, aplicando atenuantes que hacen más realista el cálculo, se emplea la fórmula siguiente:

```
Riesgo_Efectivo = Riesgo_Intrínseco x
%_disminución_vulnerabilidad x %_disminución_impacto
```

4. Propuestas de proyectos

Una vez se ha realizado un análisis sobre el impacto de diversas amenazas sobre los activos de la empresa y se ha estudiado la madurez de la seguridad, a nivel informático de la empresa, se plantea la realización de algunos proyectos que ayuden a mejorar la seguridad de la organización.

La elección de los proyectos descritos a continuación surge a partir del análisis de riesgos realizado anteriormente, priorizando la implementación de los que aporten mejoras en la seguridad en el menor plazo posible y analizando el impacto económico que tendría su ejecución.

En cada proyecto propuesto se realizará un análisis de cómo afectaría la madurez de la seguridad de la organización, teniendo siempre en cuenta que estas mejoras forman parte de un plan de mejora continua dentro de la empresa, objetivo principal del SGSI objeto de estudio del presente documento.

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.

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.

Descripción: Como primera fase del plan desarrollado tras el análisis del SGSI, es necesario acordar, a nivel de Dirección de la organización, la política que gobierna la seguridad de la información de la misma, asignando responsabilidades, definiendo procesos y adecuando todo lo relacionado con la seguridad para el correcto cumplimiento de la normativa referente a 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).

Duración: Ha de empezar justo después de finalizar el análisis inicial del estado de madurez de la seguridad, redactando y aprobando documentos que forman parte de la política para solventar o mitigar problemas graves. Se planea finalizar en 4 meses después de la aprobación de la primera versión de la política de seguridad.

Costes: Porcentaje equivalente al 10% del sueldo (por 4 meses) de los integrantes de Dirección (2 personas) más el porcentaje equivalente del 60% del sueldo del responsable de sistemas y TI (por 4 meses). Aproximadamente 7.500€ en total.

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.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

ID DOMINIO	ORIGINAL	PROJ001
5	40	80
6	50	80
7	63,3	63,3
8	68,6	80
9	70,2	70,2
10	60	60
11	74,7	74,7
12	56,4	70
13	55,8	55,8
14	65,1	65,1
15	60	60
16	62,8	62,8
17	65	65
18	71	71

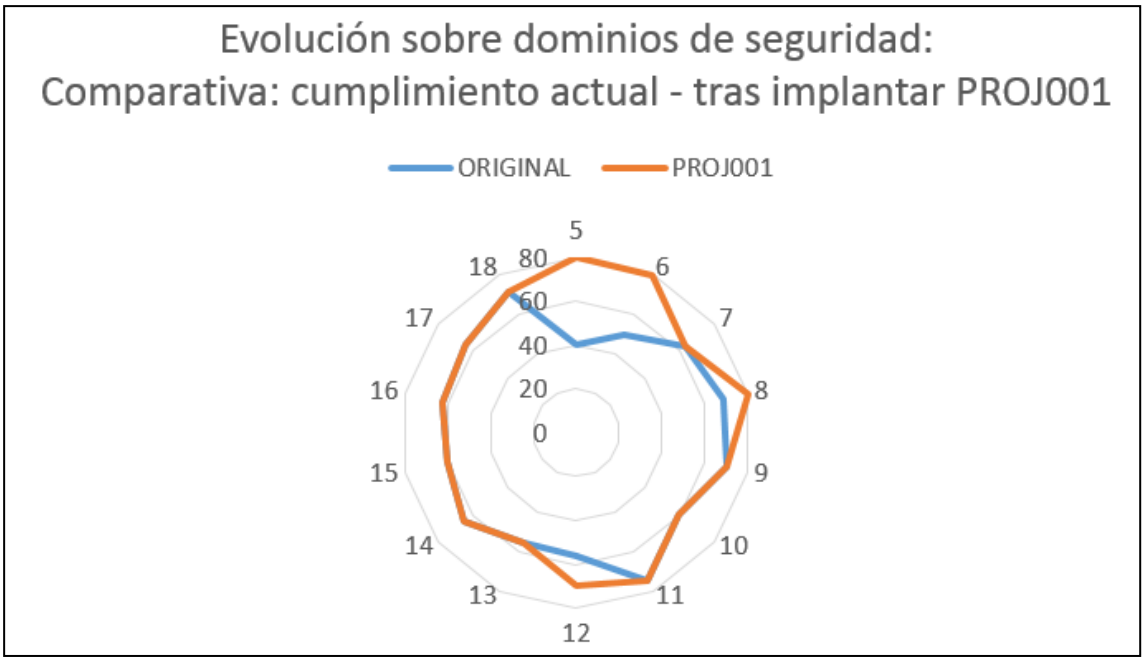

Gráfico 3: Comparativa: cumplimiento actual – tras implantar PROJ001.

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).

Descripción: Además de la implantación de la política de seguridad, uno de los puntos más críticos para la organización es asegurar la continuidad de negocio y evitar pérdidas de datos. Como se ha comentado, la organización genera código que es esencial para su actividad, por lo que es necesario asegurarlo.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Ha de empezar justo después de finalizar el análisis inicial del estado de madurez de la seguridad, redactando y aprobando documentos que forman parte de la política para solventar o mitigar problemas graves. Se planea finalizar en 4 meses después de la aprobación de la primera versión de la política de seguridad.

Costes:

- NAS de almacenamiento con 4TB: 700€
- Servidor para alojar software de backup y recuperación: 1200€
- Dedicación del 50% del sueldo de un técnico de sistemas durante 1 mes. Aproximadamente 800€.

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.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

ID DOMINIO	ORIGINAL	PROJ002
5	40	40
6	50	50
7	63,3	63,3
8	68,6	68,6
9	70,2	70,2
10	60	60
11	74,7	74,7
12	56,4	56,4
13	55,8	55,8
14	65,1	65,1
15	60	60
16	62,8	62,8
17	65	90
18	71	85

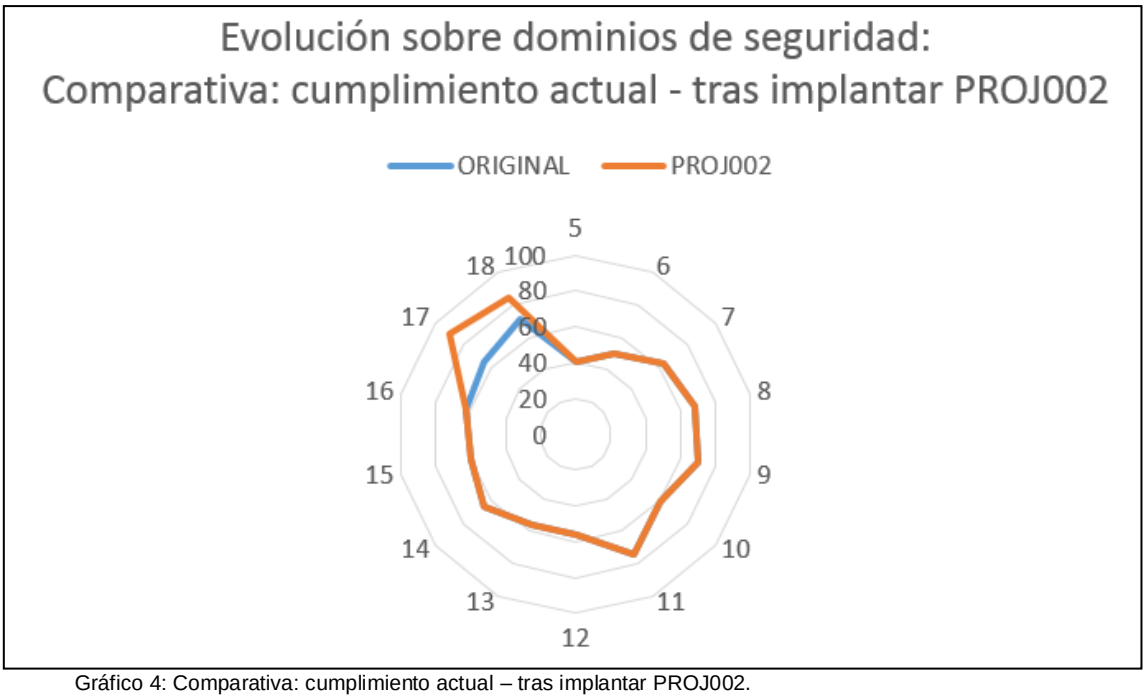

Gráfico 4: Comparativa: cumplimiento actual – tras implantar PROJ002.

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.

Descripción: Se plantea realizar un cambio de router/firewall por uno con mejores prestaciones para asegurar el correcto servicio a los empleados de la empresa. El cambio requiere quitar el dispositivo Huawei e instalar uno con capacidad de doble WAN, gestión de políticas de firewall, creación de túneles VPN y gestión de puntos de acceso Wifi.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Ha de empezar justo después de finalizar la implantación del sistema de seguridad, aunque la solicitud y análisis de propuestas económicas puede empezar mientras se realiza la implantación de dicho sistema. Se planifica para que la implantación dure 5 meses.

Costes:

- Dispositivo de seguridad nuevo: 7.000€
- Porcentaje equivalente al 10% del sueldo del responsable de sistemas y TI (por 5 meses) y el 20% del tiempo de un técnico de sistemas durante 5 meses. Aproximadamente 3.000€.

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.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

ID DOMINIO	ORIGINAL	PROJ003
5	40	40
6	50	80
7	63,3	75
8	68,6	68,6
9	70,2	85
10	60	90
11	74,7	80
12	56,4	75
13	55,8	85
14	65,1	75
15	60	60
16	62,8	75
17	65	70
18	71	71

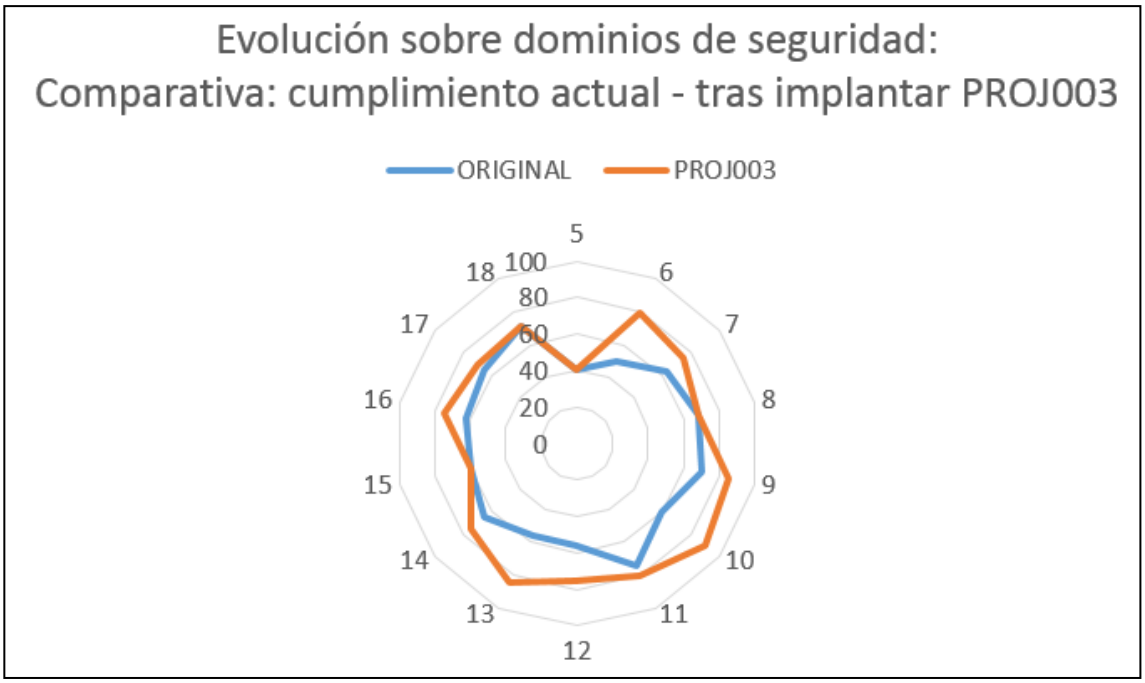

Gráfico 5: Comparativa: cumplimiento actual – tras implantar PROJ003.

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.

Descripción: Se plantea la migración del servicio de correo electrónico, actualmente alojado en servidores físicos desactualizados y sin mantenimiento, a un servicio en la nube, como puede ser Google Apps for Work o Microsoft Office365.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: Debe empezar durante la fase de migración de dispositivos de seguridad de la red. Se plantea que la fase piloto dure 1 mes y la migración 1 mes adicional. En total, 2 meses.

Costes:

- Servicio: 75 cuentas de correo por 4€, que son 300€ al mes.
- Implantación: el 10% del sueldo del responsable de sistemas por 1 mes más el 40% del sueldo de un técnico de sistemas por 2 meses. Aproximadamente 1800€

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.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

ID DOMINIO	ORIGINAL	PROJ004
5	40	40
6	50	75
7	63,3	63,3
8	68,6	68,6
9	70,2	80
10	60	80
11	74,7	74,7
12	56,4	80
13	55,8	75
14	65,1	70
15	60	60
16	62,8	62,8
17	65	75
18	71	80

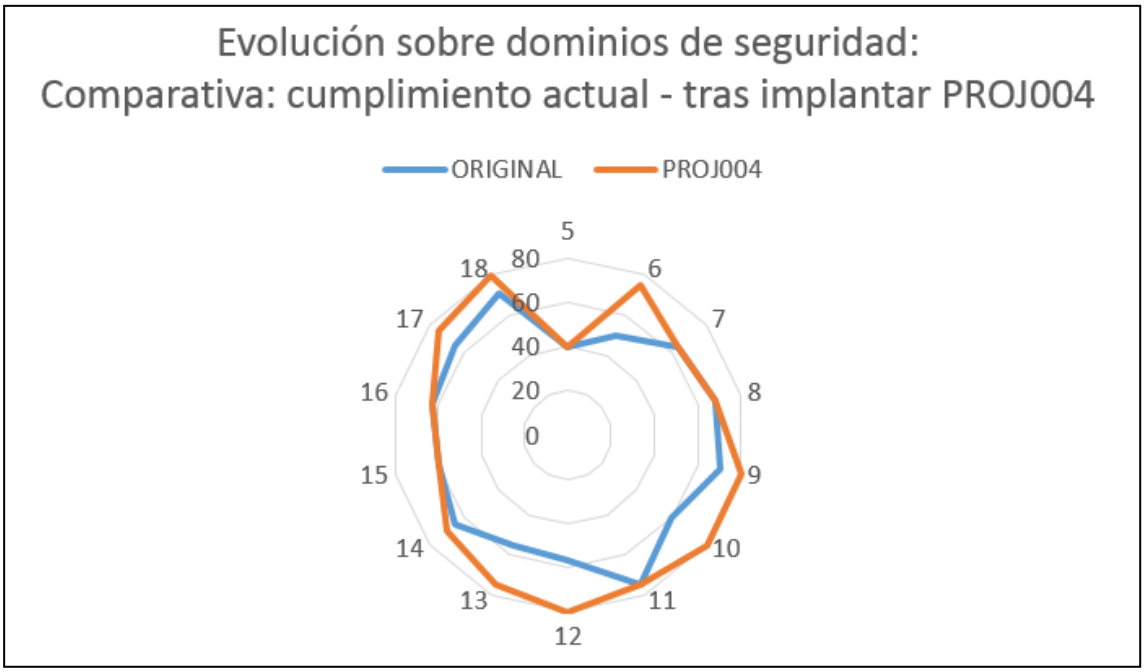

Gráfico 6: Comparativa: cumplimiento actual – tras implantar PROJ004.

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.

Descripción: Es necesario implementar un sistema que permita hacer un tratamiento correcto de las incidencias y peticiones de servicio que los empleados de la empresa generan al departamento de Sistemas y TI.

Responsable: Responsable de sistemas y tecnologías de la información.

Duración: La duración estimada es de 1 mes, ya que no requiere de grandes cambios en la infraestructura informática.

Costes:

- El software planteado es OpenSource, por lo que únicamente hay coste de servidor. Aproximadamente 100€ (al ser virtual).
- Porcentaje equivalente al 20% del sueldo (por 1 mese) del responsable de sistemas y TI y el 50% del sueldo de un mes de un técnico de sistemas. Aproximadamente 1000€.

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.

Impacto sobre los dominios de la seguridad: A continuación, se muestra tanto la tabla como el gráfico de radar comparativo entre el nivel de cumplimiento de los dominios de la norma ISO afectados por la implantación del proyecto propuesto respecto al cumplimiento sin la aplicación del mismo. De esta forma se puede ver de forma sencilla el grado de mejora que implicaría la realización de este proyecto:

ID DOMINIO	ORIGINAL	PROJ005
5	40	80
6	50	80
7	63,3	63,3
8	68,6	80
9	70,2	70,2
10	60	60
11	74,7	74,7
12	56,4	70
13	55,8	55,8
14	65,1	65,1
15	60	60
16	62,8	62,8
17	65	65
18	71	71

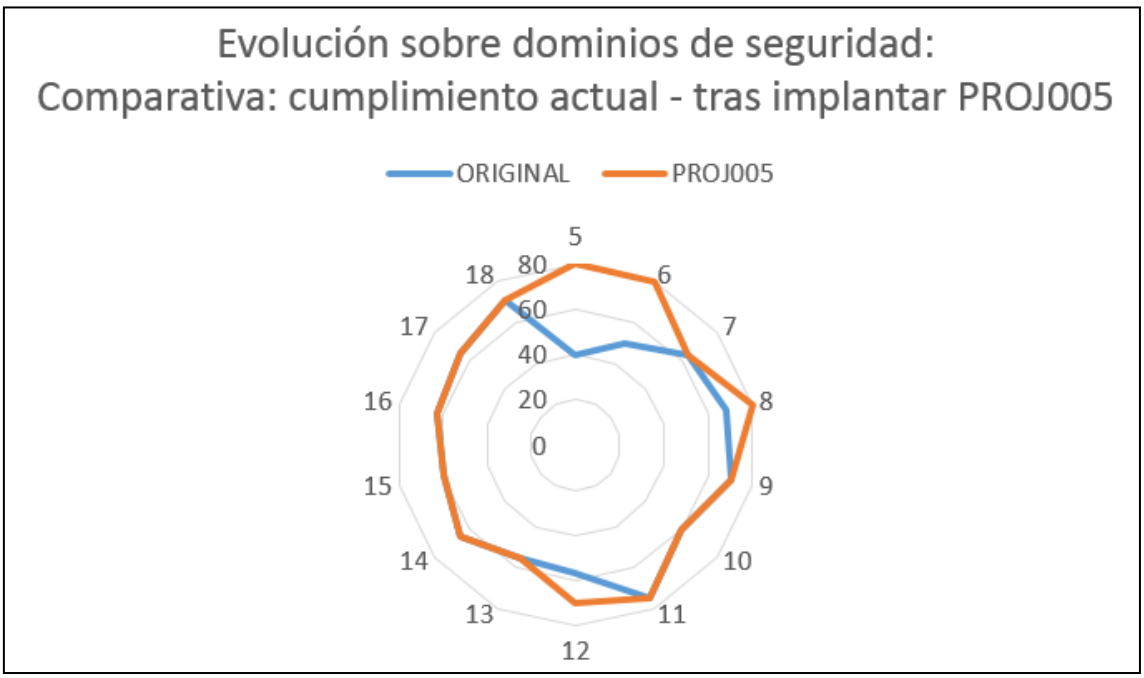

Gráfico 7: Comparativa: cumplimiento actual – tras implantar PROJ005.

En cuanto a la planificación temporal en la ejecución de los proyectos, tenemos lo siguiente:

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

Todos los proyectos planteados tienen un impacto positivo sobre todos los dominios de la seguridad. Comparando la situación encontrada al inicio del presente estudio y la situación una vez se implanten todos los proyectos propuestos, obtenemos la siguiente tabla de madurez, en porcentajes:

ID DOMINIO	ORIGINAL	FINAL
5	40	80
6	50	85
7	63,3	75
8	68,6	90
9	70,2	85
10	60	90
11	74,7	80
12	56,4	80
13	55,8	85
14	65,1	85
15	60	80
16	62,8	95
17	65	90
18	71	85

Representando esta información en un gráfico de radar, se hace más evidente las mejoras sobre los dominios de la seguridad que implicaría la ejecución de los proyectos propuestos:

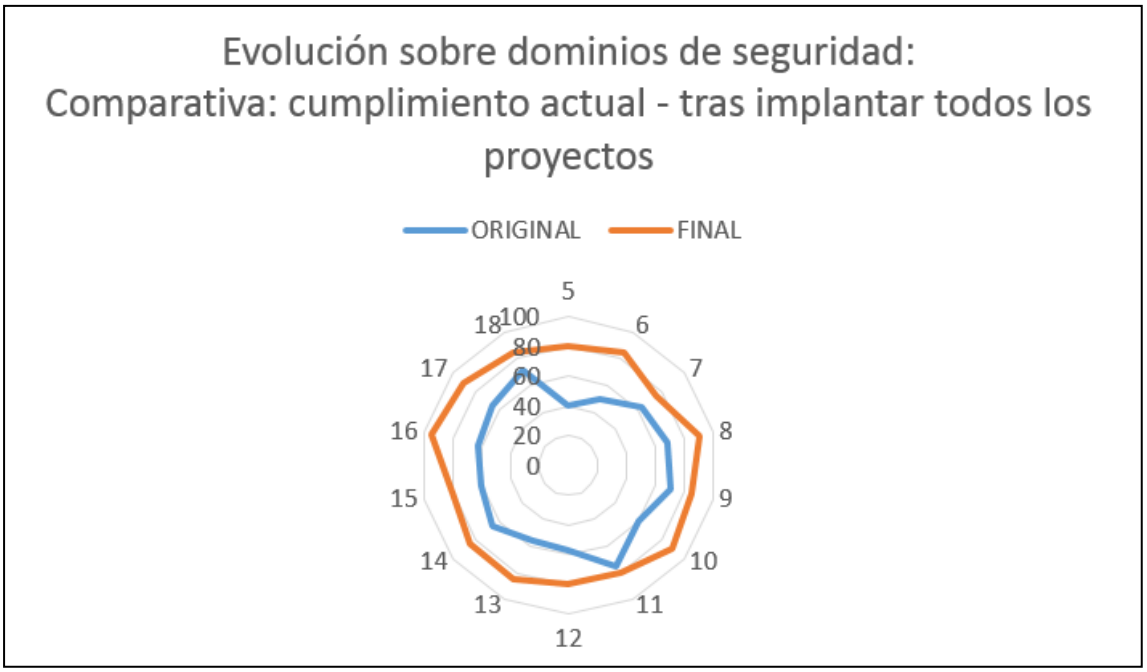

Gráfico 8: Comparativa: cumplimiento actual – tras implantar todos los proyectos.

5. Auditoría de Cumplimiento de la ISO/IEC 27002:2013

Esta fase del estudio se realizará una evaluación de las amenazas y la madurez del estado de la seguridad una vez se ha realizado la implantación de todos los proyectos propuestos en el apartado anterior.

Para medir de alguna forma el nivel de madurez de la seguridad, se realizará un análisis de los controles o medidas preventivas sobre buenas prácticas que estipula la normativa ISO/IEC 27002:2013, con 113 controles, 14 áreas y 35 objetivos de control. Por otra parte, hay otras medidas o puntos a tener en cuenta para mejorar la seguridad dentro de la organización, como:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware, comunicaciones).
- Seguridad física.

La estimación 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.

Se tendrá en cuenta los valores obtenidos en cada apartado para determinar de forma orientativa la madurez inicial de cada control y dominio de la seguridad con respecto a los valores CMM representados en la tabla anterior. Esta clasificación inicial de los controles contempla varios estados:

- Planificado.
- Iniciado.
- Implantado – sin documentar.
- Implantado – sin auditar.
- Auditado.

Los estados representan el grado de madurez, empezando por el menos maduro y finalizando por el que mayor grado de madurez presenta al inicio de este estudio.

A continuación, se muestra la valoración de madurez inicial y CMM tras la implantación de los proyectos propuestos:

ID	Dominio / Control	Aplicabilidad	Madurez inicial	Madurez CMM (%)
5	POLÍTICAS DE SEGURIDAD			80
5.1.1	Documento de la política de seguridad de la información.	Aplica	Implantado - sin documentar	85
5.1.2	Revisión de las políticas de seguridad de la información.	Aplica	Planificado	75
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			85
6.1.1	Asignación de responsabilidades para la seguridad de la información.	Aplica	Implantado - sin documentar	80
6.1.2	Segregación de tareas.	Aplica	Implantado - sin documentar	85
6.1.3	Contacto con las autoridades.	Aplica	Implantado - sin documentar	85
6.1.4	Contacto con grupos de interés especial.	Aplica	Implantado - sin documentar	80
6.1.5	Seguridad de la información en la gestión de proyectos.	Aplica	Implantado - sin documentar	90
6.2.1	Política de uso de dispositivos para movilidad.	Aplica	Implantado - sin documentar	85
6.2.2	Teletrabajo.	Aplica	Implantado - sin documentar	90
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			75
7.1.1	Investigación de antecedentes.	Aplica	Implantado - sin documentar	80
7.1.2	Términos y condiciones de contratación.	Aplica	Implantado - sin documentar	70
7.2.1	Responsabilidades de gestión.	Aplica	Implantado - sin documentar	75
7.2.2	Concienciación, educación y capacitación en seguridad de la información.	Aplica	Implantado - sin documentar	70
7.2.3	Proceso disciplinario.	Aplica	Implantado - sin auditar	85
7.3.1	Cese o cambio de puesto de trabajo.	Aplica	Implantado - sin auditar	85
8	GESTIÓN DE ACTICVOS			90
8.1.1	Inventario de activos.	Aplica	Implantado - sin documentar	85
8.1.2	Propiedad de los activos.	Aplica	Implantado - sin documentar	90
8.1.3	Uso aceptable de los activos.	Aplica	Implantado - sin documentar	90
8.1.4	Devolución de activos.	Aplica	Implantado - sin documentar	90
8.2.1	Directrices de clasificación.	Aplica	Implantado - sin documentar	90
8.2.2	Etiquetado y manipulado de la información.	Aplica	Implantado - sin documentar	90
8.2.3	Manipulación de activos.	Aplica	Implantado - sin documentar	90
8.3.1	Gestión de soportes extraíbles.	Aplica	Implantado - sin documentar	90
8.3.2	Eliminación de soportes.	Aplica	Implantado - sin documentar	95
8.3.3	Soportes físicos en tránsito.	Aplica	Implantado - sin documentar	90
9	CONTROL DE ACCESOS			85
9.1.1	Política de control de accesos.	Aplica	Implantado - sin auditar	95
9.1.2	Control de acceso a las redes y servicios asociados.	Aplica	Implantado - sin auditar	90
9.2.1	Gestión de altas/bajas en el registro de usuarios.	Aplica	Implantado - sin auditar	90
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Aplica	Implantado - sin auditar	90
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	Aplica	Implantado - sin auditar	90
9.2.4	Gestión de información confidencial de autenticación de usuarios.	Aplica	Implantado - sin auditar	90
9.2.5	Revisión de los derechos de acceso de los usuarios.	Aplica	Planificado	80
9.2.6	Retirada o adaptación de los derechos de acceso.	Aplica	Planificado	80
9.3.1	Uso de información confidencial para la autenticación.	Aplica	Implantado - sin auditar	85
9.4.1	Restricción del acceso a la información.	Aplica	Implantado - sin auditar	85
9.4.2	Procedimientos seguros de inicio de sesión.	Aplica	Iniciado	80
9.4.3	Gestión de contraseñas de usuario.	Aplica	Iniciado	80
9.4.4	Uso de herramientas de administración de sistemas.	Aplica	Iniciado	80
9.4.5	Control de acceso al código fuente de los programas.	Aplica	Iniciado	80
10	CIFRADO			90
10.1.1	Política de uso de los controles criptográficos.	Aplica	Iniciado	90
10.1.2	Gestión de claves.	Aplica	Iniciado	90
11	SEGURIDAD FÍSICA Y AMBIENTAL			80
11.1.1	Perímetro de seguridad física.	Aplica	Implantado - sin documentar	80
11.1.2	Controles físicos de entrada.	Aplica	Implantado - sin documentar	80
11.1.3	Seguridad de oficinas, despachos y recursos.	Aplica	Implantado - sin documentar	80
11.1.4	Protección contra las amenazas externas y ambientales.	Aplica	Implantado - sin documentar	80
11.1.5	El trabajo en áreas seguras.	Aplica	Implantado - sin documentar	75
11.1.6	Áreas de acceso público, carga y descarga.	Aplica	Implantado - sin auditar	90
11.2.1	Emplazamiento y protección de equipos.	Aplica	Implantado - sin auditar	80
11.2.2	Instalaciones de suministro.	Aplica	Implantado - sin auditar	80
11.2.3	Seguridad del cableado.	Aplica	Implantado - sin auditar	80
11.2.4	Mantenimiento de los equipos.	Aplica	Implantado - sin auditar	80
11.2.5	Salida de activos fuera de las dependencias de la empresa.	Aplica	Implantado - sin auditar	80
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Aplica	Implantado - sin auditar	80
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Aplica	Implantado - sin auditar	80
11.2.8	Equipo informático de usuario desatendido.	Aplica	Implantado - sin auditar	80
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	Aplica	Implantado - sin auditar	80
12	SEGURIDAD EN LA OPERATIVA			80
12.1.1	Documentación de los procedimientos de operación.	Aplica	Planificado	70
12.1.2	Gestión de cambios.	Aplica	Planificado	70
12.1.3	Gestión de capacidades.	Aplica	Planificado	70
12.1.4	Separación de las instalaciones de desarrollo, prueba y producción.	Aplica	Iniciado	80
12.2.1	Controles contra el código malicioso.	Aplica	Implantado - sin auditar	90
12.3.1	Copias de seguridad de la información.	Aplica	Planificado	80
12.4.1	Registro y gestión de eventos de actividad.	Aplica	Planificado	80
12.4.2	Protección de los registros de información.	Aplica	Planificado	80

12.4.3	Registros de actividad del administrador y operador del sistema.	Aplica	Planificado	80
12.4.4	Sincronización de relojes.	Aplica	Planificado	80
12.5.1	Instalación del software en sistemas en producción.	Aplica	Planificado	80
12.6.1	Gestión de las vulnerabilidades técnicas.	Aplica	Planificado	80
12.6.2	Restricciones en la instalación de software.	Aplica	Planificado	80
12.7.1	Controles de auditoría de los sistemas de información.	Aplica	Planificado	80
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**			**85**
13.1.1	Controles de red.	Aplica	Planificado	80
13.1.2	Mecanismos de seguridad asociados a servicios en red.	Aplica	Planificado	80
13.1.3	Segregación de redes.	Aplica	Planificado	80
13.2.1	Políticas y procedimientos de intercambio de información.	Aplica	Planificado	80
13.2.2	Acuerdos de intercambio.	Aplica	Planificado	80
13.2.3	Mensajería electrónica.	Aplica	Implantado - sin auditar	95
13.2.4	Acuerdos de confidencialidad y secreto.	Aplica	Implantado - sin auditar	95
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**			**85**
14.1.1	Análisis y especificación de los requisitos de seguridad.	Aplica	Planificado	75
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Aplica	Planificado	75
14.1.3	Protección de las transacciones por redes telemáticas.	Aplica	Implantado - sin documentar	90
14.2.1	Política de desarrollo seguro de software.	Aplica	Implantado - sin documentar	90
14.2.2	Procedimientos de control de cambios en los sistemas.	Aplica	Planificado	80
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Aplica	Planificado	80
14.2.4	Restricciones a los cambios en los paquetes de software.	Aplica	Planificado	80
14.2.5	Uso de principios de ingeniería en protección de sistemas.	Aplica	Planificado	80
14.2.6	Seguridad en entornos de desarrollo.	Aplica	Planificado	80
14.2.7	Externalización del desarrollo de software.	Aplica	Planificado	80
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Aplica	Implantado - sin documentar	90
14.2.9	Pruebas de aceptación.	Aplica	Implantado - sin documentar	90
14.3.1	Protección de los datos utilizados en pruebas.	Aplica	Implantado - sin documentar	90
15	**RELACIONES CON SUMINISTRADORES**			**80**
15.1.1	Política de seguridad de la información para suministradores.	Aplica	Iniciado	80
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Aplica	Iniciado	80
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Aplica	Iniciado	80
15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Aplica	Planificado	80
15.2.2	Gestión de cambios en los servicios prestados por terceros.	Aplica	Planificado	80
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**			**95**
16.1.1	Responsabilidades y procedimientos.	Aplica	Iniciado	95
16.1.2	Notificación de los eventos de seguridad de la información.	Aplica	Planificado	90
16.1.3	Notificación de puntos débiles de la seguridad.	Aplica	Planificado	90
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Aplica	Planificado	95
16.1.5	Respuesta a los incidentes de seguridad.	Aplica	Iniciado	95
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Aplica	Planificado	95
16.1.7	Recopilación de evidencias.	Aplica	Planificado	95
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**			**90**
17.1.1	Planificación de la continuidad de la seguridad de la información.	Aplica	Iniciado	90
17.1.2	Implantación de la continuidad de la seguridad de la información.	Aplica	Iniciado	90
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Aplica	Iniciado	90
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Aplica	Iniciado	90
18	**CUMPLIMIENTO**			**85**
18.1.1	Identificación de la legislación aplicable.	Aplica	Implantado - sin auditar	90
18.1.2	Derechos de propiedad intelectual (DPI).	Aplica	Imppropiedadntado - sin auditar	80
18.1.3	Protección de los registros de la organización.	Aplica	Implantado - sin documentar	80
18.1.4	Protección de los datos y privacidad de la información personal.	Aplica	Implantado - sin documentar	90
18.1.5	Regulación de los controles criptográficos.	Aplica	Implosntado - sin auditar	90
18.2.1	Revisión independiente de la seguridad de la información.	Aplica	Implantado - sin documentar	90
18.2.2	Cumplimiento de las políticas y normas de seguridad.	Aplica	Implantado - sin documentar	90
18.2.3	Comprobación del cumplimiento.	Aplica	Implantado - sin documentar	80

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:

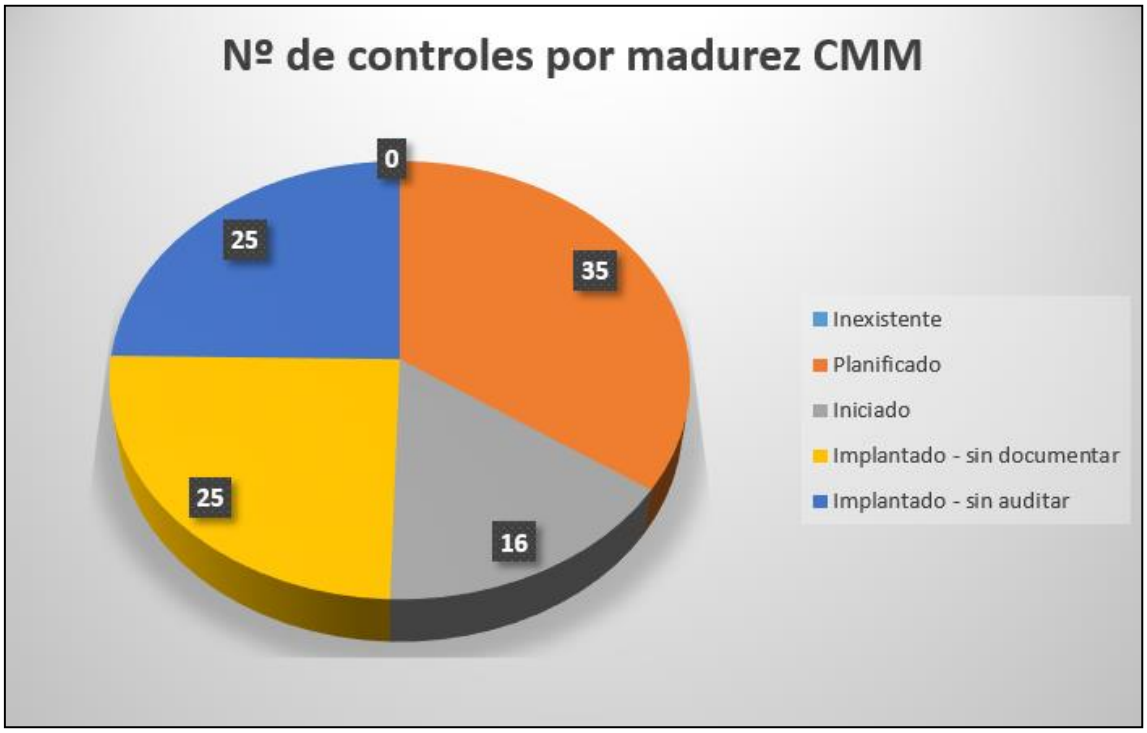

Gráfico 9: Número de controles por madurez CMM.

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%:

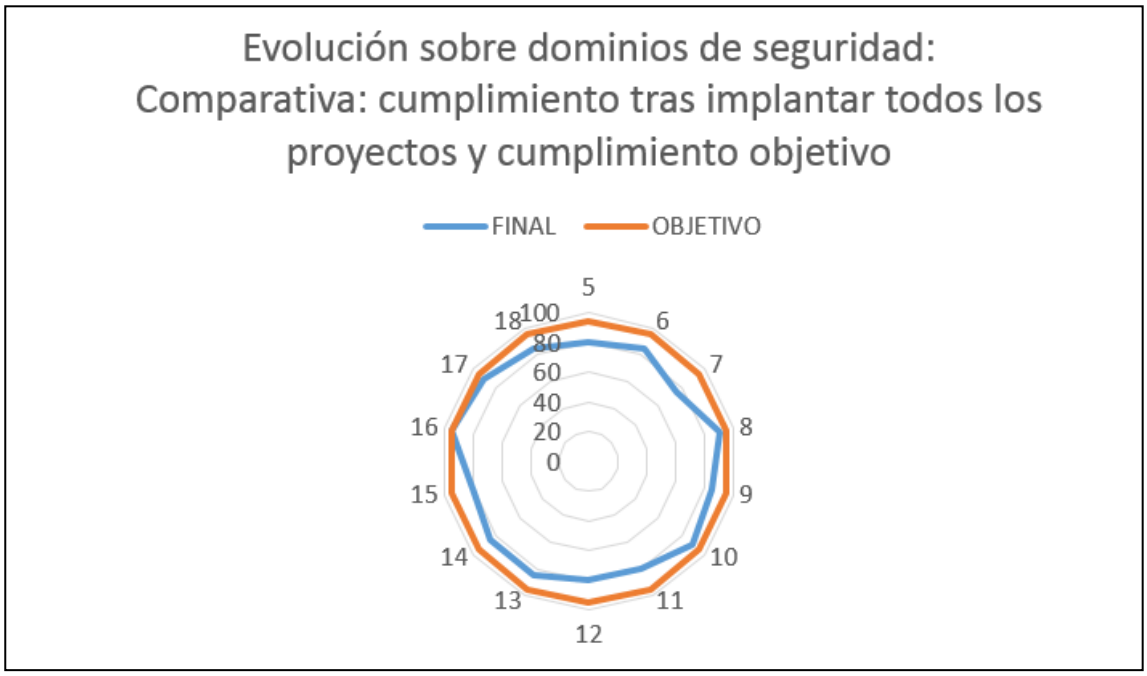

Gráfico 10: Comparativa: cumplimiento tras implantar todos los proyectos y cumplimiento objetivo.

5.1 Informe de auditoría

A continuación, se presenta el informe de auditoría resultante de la auditoría realizada en este punto:

INFORME DE AUDITORÍA INTERNA EMPRESA DESARROLLADORES DE SOFTWARE	**CÓDIGO 20160606**
	VERSIÓN 001

1. DATOS DE LA AUDITORÍA INTERNA	
Auditoría Nº	001
Norma de referencia	ISO/IEC 27002:2013
Período de la auditoría	Junio 2016
Lugar de la auditoría	Oficinas centrales de la empresa
Equipo auditor	Equipo auditor interno

2. ALCANCE DE LA AUDITORÍA INTERNA
Revisión de todos los dominios y controles de seguridad abarcados en la normativa ISO/IEC 27002:2013

3. OBJETIVOS DE LA AUDITORÍA INTERNA
Determinar el nivel de cumplimiento de la normativa por parte de la empresa y detectar no conformidades en la misma.

4. DEFINICIONES
4.1. No conformidad: incumplimiento de un requisito, política o documento, cuya repetición pone en riesgo la efectividad del SGSI. **4.2. Observación:** es un fallo aislado en el contenido o implementación de los documentos o cualquier incumplimiento parcial en un requisito. **4.3. Oportunidad de mejora:** acción recomendada que al ser implementada implica una mejora del SGSI.

5. FORTALEZAS Y DEBILIDADES	
Fortalezas: 1. Se han realizado todos los proyectos propuestos por la organización. 2. SGSI alineado con la dirección y estrategia de la empresa. 3. Dirección comprometida con el SGSI.	Debilidades: 1. La operativa de la empresa no está clara en algunos aspectos, por ejemplo, en la gestión de los Recursos Humanos.

6. RESULTADOS DE LA AUDITORÍA INTERNA			
Se encontraron 0 no conformidades, resumidas a continuación:			
ÁREA	DESCRIPCIÓN	RESPONSABLE	AUDITOR
Se detectaron las siguientes oportunidades de mejora:			
Sistemas de gestión de los Recursos Humanos y en la operativa de la empresa.			

7. CONCLUSIONES DE LA AUDITORÍA INTERNA
1. Inexistencia de no conformidades. 2. Proyectos de mejora abarcados en su totalidad. 3. Oportunidades de mejora puntuales.

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.

7. Listado de gráficos

8. Anexos

- Política de Seguridad: “SGSI - Política de Seguridad v1-1.pdf”.

9. Bibliografía

- Webs:

  http://www.iso27000.es/download/ControlesISO27002-2013.pdf

  https://es.wikipedia.org/wiki/ISO/IEC_27002

  http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf