Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

TRABAJO FINAL DE MÁSTER

Máster Interuniversitario en Seguridad de las TIC

Segundo semestre del curso 2014/15

Alumno: José María Martín Manjón-Cabeza

Consultor: Antonio José Segovia Henares

Resumen

El proyecto expuesto en este documento forma parte del Trabajo Final del “Máster Inter-universitario en Seguridad de las Tecnologías de la información y la Comunicación” y tiene como objeto el desarrollo de un análisis para la implantación de un Sistema de Gestión de Seguridad de la Información dentro de una organización.
Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas de administración de la información que conlleva la elaboración, mantenimiento y mejora de un esquema documental, un proceso de gestión de la seguridad y unos procedimientos que permitan gestionar todo el conjunto.
El SGSI se ha de integrar en la organización de manera que se convierta en una parte fundamental de la gestión de ésta. Un SGSI correctamente implantado permite establecer procedimientos que aseguren la Confidencialidad, Disponibilidad e Integridad de la información que se gestiona en el organización.
En el desarrollo de este trabajo se han seguido las directrices establecidas en la norma ISO 27001, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI mediante un proceso de mejora continua.
La organización sobre la que se ha realizado este trabajo es una empresa ficticia, aunque por su estructura podría asemejarse a muchas.

Summary

The project exposed in this document is part of the End-Of-Master Work of the “Inter-University Master of Security in Information Technology and Communications” and has the aim of developing an analysis to implant an Information Security Management System in an organization.
An Information Security Management System is a set of information administration policies which involves to elaborate, maintain and improve a documentation schema, a security management process and procedures to manage the whole set.
The ISMS has to be integrated in the organization to allow it become in an essential part of its management. A correctly implanted ISMS allows to establish procedures to ensure the confidentiality, availability and integrity of the information managed by the organization.
In the development of this work we have followed the guidelines set in ISO 27001, which specify the requirements for establishing, implementing, maintaining and improving an ISMS through a process of continuous improvment.
The organization on which this work has been performed is a unreal company who provides services in the area of telecommunications although it could be a real one based in its standard structure.

ÍNDICE DE CONTENIDO

1 SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL 6
1.1 Introducción 6
1.1.1 Objetivos del SGSI 6
1.1.2 Actividades asociadas a la implantación de un SGSI 7
1.2 Norma ISO/IEC 27001 8
1.2.1 Código de buenas prácticas - ISO/IEC 27002 8
1.2.2 Estructura de la norma ISO/IEC 27001 9
1.2.3 Cambios en la última revisión ISO/IEC 27001:2013 10
1.2.4 Evolución histórica 11
1.3 Enfoque y selección de empresa 11
1.3.1 Presentación 11
1.3.2 Organigrama de la empresa 12
1.3.3 Mapa de red y sistemas 13
1.3.4 Estado inicial de la seguridad 14
1.3.5 Alcance del SGSI 15
Anexo 1. Objetivos del Plan Director de Seguridad 16
Anexo 2. Análisis diferencial de la empresa 16
2 SISTEMA DE GESTIÓN DOCUMENTAL 20
2.1 Introducción 20
2.2 Política de seguridad 20
2.3 Procedimiento de auditorías internas 20
2.4 Gestión de indicadores 20
2.5 Procedimiento de revisión de la Dirección 20
2.6 Gestión de roles y responsabilidades 20
2.7 Metodología de análisis de riesgos 21
2.8 Declaración de aplicabilidad 21
Anexo 3. Esquema documental 21
3 ANÁLISIS DE RIESGOS 22
3.1 Introducción 22
3.2 Inventario de activos 22
3.3 Valoración de los activos 24

3.4 Dimensiones de seguridad 25
3.5 Tabla resumen de valoración 26
3.6 Análisis de amenazas 27
3.7 Impacto potencial 32
3.8 Nivel de riesgo aceptable y riesgo residual 33
3.9 Resultados 37
Anexo 4. Análisis de riesgos 38
4 PROPUESTAS DE PROYECTOS 39
4.1 Introducción 39
4.2 Propuestas 39
4.3 Planificación 47
4.4 Resultados 48
Anexo 5. Plan de proyectos 48
5 AUDITORÍA DE CUMPLIMIENTO 49
5.1 Introducción 49
5.2 Metodología 49
5.3 Evaluación de la madurez 49
5.4 Resultados por dominios 50
5.5 Resultados globales 70
Anexo 6. Evolución madurez controles ISO 27002-2013 72
6 CONCLUSIONES 73
6.1 Objetivos alcanzados 73
6.2 Objetivos futuros 74
Anexo 7. Presentación e informe ejecutivo. 74
7 APÉNDICES 75
7.1 Glosario 75
7.2 Bibliografía 81
7.3 Enlaces 81

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Organigrama de la organización....13
Ilustración 2. Mapa de red y sistemas....14
Ilustración 3. Análisis diferencial ISO 27002:2013....18
Ilustración 4. Análisis diferencial ISO 27001:2013....19
Ilustración 5. Evolución cumplimiento dominios ISO 27002:2013....48
Ilustración 6. Nivel de madurez - Política de seguridad....51
Ilustración 7. Nivel de madurez - Aspectos organizativos de la seguridad de la información....52
Ilustración 8. Nivel de madurez - Seguridad ligada a los recursos humanos....53
Ilustración 9. Nivel de madurez - Gestión de activos....54
Ilustración 10. Nivel de madurez - Control de acceso....55
Ilustración 11. Nivel de madurez - Cifrado....57
Ilustración 12. Nivel de madurez - Seguridad física y ambiental....58
Ilustración 13. NIvel de madurez - Seguridad en la operativa....60
Ilustración 14. Nivel de madurez - Seguridad en las telecomunicaciones....62
Ilustración 15. Nivel de madurez - Adquisición, desarrollo y mantenimiento de los sistemas de información....64
Ilustración 16. Nivel de madurez - Relaciones con los suministradores....65
Ilustración 17. Nivel de madurez - Gestión de incidentes de seguridad de la información....66
Ilustración 18. Nivel de madurez - Aspectos de seguridad de la información en la gestión de la continuidad de negocio....67
Ilustración 19. Nivel de madurez - Cumplimiento....68
Ilustración 20. Cuadro-resumen no conformidades....69
Ilustración 21. Relación-resumen de cumplimiento controles norma ISO 27002....70
Ilustración 22. Madurez CMM de los controles ISO....71
Ilustración 23. Evaluación de madurez ISO 27002:2013....71

ÍNDICE DE TABLAS

Tabla 1. Modelo CMM....17
Tabla 2. Análisis diferencial ISO 27002:2013....17
Tabla 3. Análisis diferencial ISO 27001:2013....18
Tabla 4. Inventario de activos....24
Tabla 5. Escala de valoración de activos....24
Tabla 6. Valoración dimensiones de seguridad....25
Tabla 7. Valoración de los activos....27
Tabla 8. Agrupación de amenazas en MAGERIT....29
Tabla 9. Frecuencia de ocurrencia....30
Tabla 10. Impacto de las amenzas....30
Tabla 11. Detalle del análisis de amenazas....31
Tabla 12. Detalle del análisis de impacto potencial....32
Tabla 13. Niveles de evaluación del riesgo....33
Tabla 14. Análisis del nivel de riesgo....35
Tabla 15. Tratamiento del riesgo....35
Tabla 16. Activos agrupados por tratamiento de riesgo....37

Tabla 17. Proyecto 1 40
Tabla 18. Proyecto 2 41
Tabla 19. Proyecto 3 41
Tabla 20. Proyecto 4 42
Tabla 21. Proyecto 5 42
Tabla 22. Proyecto 6 43
Tabla 23. Proyecto 7 43
Tabla 24. Proyecto 8 44
Tabla 25. Proyecto 9 44
Tabla 26. Proyecto 10 45
Tabla 27. Proyecto 11 46
Tabla 28. Proyecto 12 46
Tabla 29. Planificación de proyectos en el primer año 47
Tabla 30. Planificación de proyectos en el segundo año 47

1 SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1 Introducción

El proyecto motivo de este trabajo, como punto final del Máster de Seguridad TIC impartido por la UOC, se centra en elaborar un plan de implementación de la norma ISO/IEC 27001:2013. Este estándar de facto a escala mundial establece las directrices para implantar un Sistema de Gestión de la Seguridad de la Información (SGSI), como modelo de seguridad para cualquier organización.

Hoy en día, la información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Como punto final de esta introducción señalar que la implantación adecuada de un SGSI basado en la norma ISO/IEC 27001:2013 permite que la organización obtenga una certificación reconocida mundialmente.

1.1.1 Objetivos del SGSI

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- Garantía de la confidencialidad, disponibilidad e integridad de la información de la organización.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Concienciación entorno a la seguridad dentro de la organización.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.1.2 Actividades asociadas a la implantación de un SGSI

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.

- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

1.2 Norma ISO/IEC 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

Esta norma establece los requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados a los activos de información que la organización pretende proteger mediante la operación de sus SGSI.

1.2.1 Código de buenas prácticas - ISO/IEC 27002

Esta norma proporciona un código de buenas prácticas para la gestión de la seguridad de la información, y recoge un completo y amplio catálogo de controles y buenas prácticas en la materia. Esta no es una norma certificable y sirve de apoyo para la norma ISO 27001.

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria. La versión más reciente de la norma es la ISO/IEC 27002:2013. Las novedades sobre la ISO/IEC 27002:2013, la cual está asociada con el Anexo A de la ISO/IEC 27001:2013.

Dentro de ISO/IEC 27002 se extiende la información de los renovados anexos de ISO/IEC 27001-2013, donde básicamente se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001. En esta nueva versión de la norma se encuentran los controles que buscan mitigar el impacto o la

posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización.

Con la actualización de esta norma las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información.

1.2.2 Estructura de la norma ISO/IEC 27001

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

- Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
- Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.
- Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
- Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.
- Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
- Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
- Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
- Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

- Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.
- Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

1.2.3 Cambios en la última revisión ISO/IEC 27001:2013

A finales de 2013 se publicó la nueva versión de la norma ISO/IEC 27001. Las novedades m´s significativas se detallan en los siguientes puntos:

1. Eliminación de la referencia del enfoque de proceso de mejora continua: PDCA.
2. Reestructuración general de capítulos y subapartados. Los capítulos están alineados con el "anexo SL" publicado por ISO/IEC con el fin de que todos los estándares de sistemas de gestión tengan la misma estructura.
3. Mayor énfasis en el conocimiento del contexto de la organización y de las necesidades de las partes interesadas. Este conocimiento debe suponer el punto esencial de entrada para el establecimiento del Sistema de Gestión: definición del alcance, política, establecimiento de objetivos y análisis de riesgos. En este sentido, se alinea con la norma ISO 31000 de gestión de riesgos.
4. El proceso de análisis de riesgos se define de forma más genérica. Han sido eliminadas las referencias a la identificación de activos, amenazas y vulnerabilidades. Únicamente se hace necesario identificar riesgos (sin especificar cómo) asociados a la pérdida de confidencialidad, integridad y disponibilidad, tras analizar las potenciales consecuencias y la probabilidad para, finalmente, cuantificar el riesgo. Adicionalmente se deberá identificar al propietario del riesgo.
5. Respecto a la selección de controles de seguridad para el tratamiento del riesgo, se a decisión de las organizaciones la selección un marco de controles en caso que no se desee seguir el Anexo A/ISO 27002, aunque de cualquier modo se deberá comparar con los controles del Anexo A para comprobar que no se obvia ningún control.
6. Se otorga un mayor énfasis al liderazgo de la Dirección en el Sistema de Gestión, no sólo desde el punto de vista de un compromiso formal, como se especificaba en la anterior versión, sino con el objetivo de evitar considerar como management a la Dirección de Tecnología o Seguridad.
7. Otra novedad introducida es la redefinición de objetivos de seguridad relacionados con la seguridad de la información, como parte del Sistema de Gestión, otorgándole mayor relevancia frente a la anterior versión.
8. Mayor profundización en el área de monitorización y medición del SGSI.
9. Respecto a los requisitos documentales, se ha eliminado el listado de documentos obligatorios, aunque en el cuerpo del estándar se hace referencia a distintos requisitos documentales. Por otro lado se elimina la separación entre documentos y registros, siendo denominados simplemente "información documentada".
10. Sólo tiene en cuenta las medidas correctivas, excluyendo las medidas preventivas, que no son otra cosa que las acciones derivadas de la gestión del riesgo.
11. Los cambios en el anexo de controles de seguridad dan como resultado una estructura más lógica y actualizada a la realidad actual. Se pasa de 11 a 14 capítulos y el número total de controles se reduce de 133 a 114. Los aspectos relacionados con la criptografía se separan del capítulo de Desarrollo y Adquisición Software y se convierte en un capítulo independiente. Lo mismo ocurre con Relaciones con Proveedores que en este caso estaba

diluido entre varios capítulos. Por otro lado el capítulo de Comunicaciones y Operaciones se divide en dos diferentes.

1.2.4 Evolución histórica

La ISO 27001 ha sido resultado de la evolución de otros estándares relacionados con la seguridad de la información:

- 1901 – La British Standards Institution (BSI) es fundada por el Comité de Ingeniería de normas de Londres. Su objetivo final es la creación de normativa para la estandarización de procesos. La BSI es un organismo colaborador de la International Standard Organization (ISO).
- 1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.
- 1998 – BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
- 1999 – BS 7799-1:1999: Se revisa.
- 2000 – ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.
- 2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.
- 2005 – ISO/IEC 27001:2005 e ISO/IEC 17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.
- 2007 – ISO 17799: Se renombra y pasa a ser la ISO 27002:2005
- 2007 – ISO/IEC 27001:2007: Se publica la nueva versión.
- 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.
- 2013 – Se ha publicado la última revisión ISO/IEC 27001:2013 en la que destacan cambios significativos en su estructura, evaluación y tratamiento de los riesgos. También se ha actualizado el código de nuevas prácticas en la norma ISO/IEC 27002:2013.

1.3 Enfoque y selección de empresa

En este apartado se realizará una descripción de la empresa que se ha seleccionado para desarrollar el SGSI, indicando su actividad de negocio, su organigrama general, así como sus arquitecturas de sistemas y tecnologías de información sobre los que descansas los activos esenciales para el negocio.

1.3.1 Presentación

La compañía ficticia PateTIC es una joven empresa con vocación de ser líder en el sector de las TIC, focalizada en el comercio electrónico. Con un fuerte interés de ser una compañía innovadora en el mercado del e-commerce, para impactar y ser conocida rápidamente, toma el nombre del significado “que causa impresión” del vocablo griego de donde proviene la palabra latina “patheticus”. En este caso la intención es una idea del área de Marketing para ganar publicidad al

levantar la curiosidad en los potenciales clientes y en el sector. Por tanto se busca un sentido positivo e innovador.

Tiene un claro enfoque al desarrollo de aplicaciones de comercio electrónico y tiendas online basadas en tecnologías web aunque no descarta evolucionar hacia otras áreas de las TICs. Cuenta con una oficina y una red de colaboradores dispersos geográficamente. En total son 30 personas en plantilla, de los cuales unas 25 están ubicados en la oficina y el resto en las principales ciudades del estado.

Dentro de sus líneas de negocio cuenta con:

- Consultoría de negocio
  Estudio de la situación inicial del cliente para saber dimensionar la solución o soluciones que más le convienen y se adaptan a su negocio.
- Diseño a medida
  Proyectos llave en mano para que las expectativas del cliente se cumplan completamente. Aportando conocimiento y recomendaciones para poder ser socios tecnológicos y compañeros de viaje de la evolución del negocio del cliente.
- Marketing online
  Publicidad en buscadores, evolución del producto, campañas, marketing en Social Media, ubicación en buscadores,…
- Estudio de mercado de competencia
  Definición de procesos automatizados y dinámicos para hacer un análisis de los precios de la competencia y de sus productos para poder conocer el sector. Incluso una comparativa con productos similares de la competencia donde sólo se notificasen aquellos que han variado su precio, o por ejemplo, que son más baratos.
- Inclusión en los marketplaces más importantes
  Favorece la presencia de los productos de la tienda online o de un e-commerce en los marketplaces más importantes: Google shopping, Twenga, etc.

1.3.2 Organigrama de la empresa

La compañía está estructurada en tres áreas principales (Comercial, Técnica y Financiera) con una serie de departamentos dependientes.

Respecto al número de personas por departamentos tenemos:

- Director general (1)
- Director comercial (1), Dpto. Relaciones Públicas (3), Dpto. Marketing (2), Dpto. Ventas (3)
- Director técnico (1), Responsable de desarrollo (1), Responsable de sistemas (1), desarrolladores (5) y técnicos de sistemas (5)
- Director financiero (1), Responsables (2), Dpto Contabilidad (2), Dpto. Administración y compras (2).

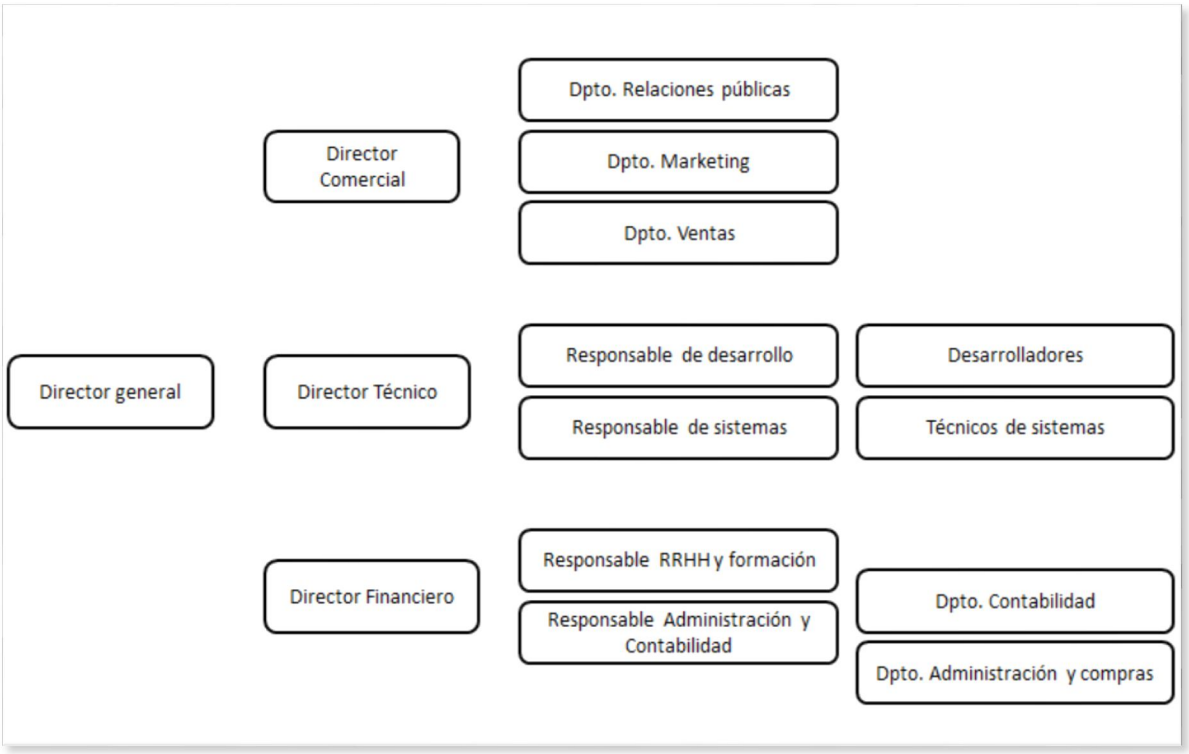

Ilustración 1. Organigrama de la organización

1.3.3 Mapa de red y sistemas

La arquitectura de red y sistemas con la que cuenta la compañía es básica para desarrollar los trabajos objeto de sus servicios y negocio. Cuenta con una conexión única a Internet por la que además acceden los usuarios/trabajadores remotos. Dispone de una DMZ para albergar su DNS y su página Web. Una red LAN distribuida en tres partes, una para los servidores, una para los usuarios y otra para el laboratorio donde se desarrollan los aplicativos y sistemas para los clientes. Además dispone de un acceso Wifi para dispositivos inalámbricos del estilo portátiles, tablets, PDAs o Smartphones.

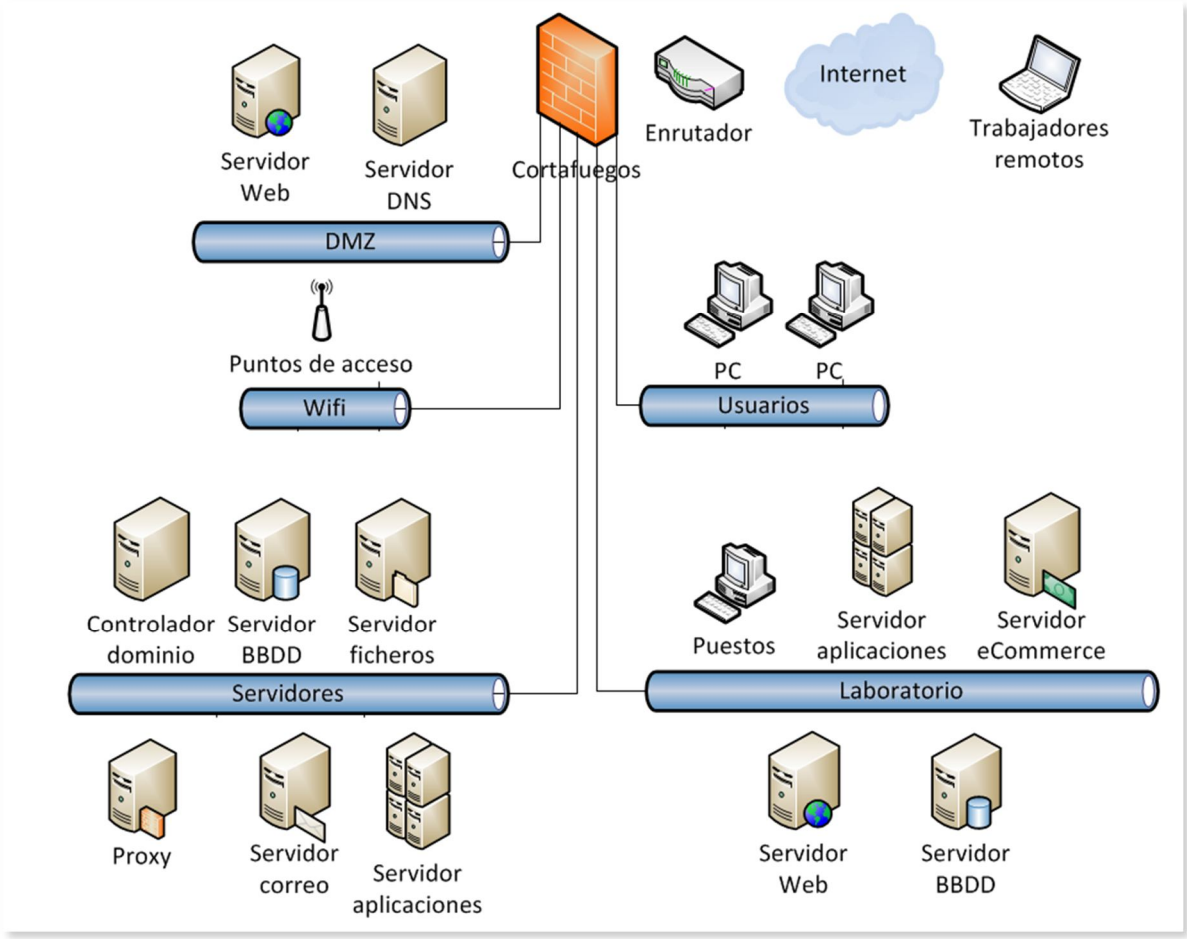

Ilustración 2. Mapa de red y sistemas

1.3.4 Estado inicial de la seguridad

La situación de seguridad en la que se encuentra la empresa es totalmente precaria. No cuenta con un departamento de seguridad ni tampoco tiene subcontratado una empresa externa que realice esta tarea. El encargado de atender las necesidades y problemas de seguridad es el responsable técnico y su grupo, que son los que administran los servidores, el cortafuegos y el resto de elementos activos/pasivos de la red.

Por otra parte, comentar que la empresa no cuenta con un inventario de activos actualizados ni detallados según su función o importancia dentro de la organización de la empresa. Por tanto, tampoco están clasificados como demanda la norma ISO 27001. Esto hace que no existan ni un análisis de riesgos ni en consecuencia un plan de continuidad de negocio.

Respecto al material comentar que los puestos de trabajo, ya sean portátiles o PCS están provistos de un sistema base compuesto por un sistema operativo, un paquete ofimático y un antivirus. Aparte, dependiendo del usuario puede albergar otro tipo de herramientas para realizar su cometido, por ejemplo las consolas de administración de servidores y servicios o los programas de desarrollo, etc.

Todo el software utilizado dispone de las licencias pertinentes. Además se dispone de tres impresoras de red para todos los trabajadores de la empresa.

Toda la compañía está en una misma planta de un edificio, por lo que cada departamento está ubicado en una sala. Además, la sala de servidores se encuentra colindante al resto de las salas de trabajo de la compañía, sin estar separada físicamente en otra sala o edificio. El acceso a esta habitación se realiza usando una llave de la que sólo tienen copia el responsable técnico y el de sistemas.

Respecto al personal tiene firmado un acuerdo de confidencialidad con la compañía para proteger la información con la que se trabaja y los productos y servicios que se desarrollan. Así como la información relativa a clientes y proveedores. Cuando una persona es dada de baja de su puesto de trabajo, se le revocan los privilegios de acceso inmediatamente.

Debido a que es una empresa de tamaño pequeño, en los accesos a la empresa no se cuenta con acreditaciones y tampoco se dispone de tarjetas para invitados de manera que estos estén identificados. Si bien hay seguridad física en la entrada con un listado de nombres y DNIs que deben presentarse para acceder al recinto.

En cuanto a los controles de acceso a la red, cada usuario tiene asignado un usuario y contraseña que le permitirá acceder a su ordenador. Para acceder a los recursos compartidos del sistema, se utiliza el usuario dado de alta en el servidor controlador de dominio, con los permisos y privilegios que haya de tener el rol que tiene en la empresa.

1.3.5 Alcance del SGSI

El alcance del SGSI englobará los sistemas de información que dan soporte a los procesos de negocio dentro del desarrollo y la consultoría de comercio electrónico, la gestión de la seguridad de los activos de la organización así como las actividades empresariales (comerciales, técnicas o financieras) que hagan uso de información sensible de la compañía o de sus clientes.

Este fundamento servirá de base para definir la versión inicial de la Declaración de Aplicabilidad, actualmente inexistente en la empresa.

Cabe destacar que se ha de aplicar la normativa aplicable en España respecto a la protección de datos y de seguridad respecto al comercio electrónico, entre otras.

Se deberán evaluar en un primer análisis y en base a la norma 27001:

- los requisitos que se están aplicando correctamente y los que no.
- los controles que se están aplicando correctamente y los que no.
- los controles y requisitos que no se estén aplicando.

Dentro de las áreas de la empresa dentro del alcance, aquellas que hacen uso de información sensible son los departamentos de ventas, marketing, RRPP, RRHH, administración y compras, contabilidad, sin obviar la que sustenta todas las TICs que es el departamento técnico.

Este alcance ha sido validado y por tanto también se ha dado la conformidad y apoyo para su desarrollo e implementación por la Dirección General de la compañía, que formará parte activa en la supervisión del cumplimiento de los logros e hitos que se vayan estableciendo por el comité de seguridad.

Anexo 1. Objetivos del Plan Director de Seguridad

El Plan Director de Seguridad se define en base a la estrategia de negocio de la organización y sus necesidades específicas, de modo que la identificación de procesos de negocio y activos que los soportan constituye un aspecto fundamental durante su desarrollo.

El motivo de la elaboración del Plan Director es el de definir un plan de acciones con el fin de cumplir con los objetivos que se establecerán en el SGSI. El ámbito del plan director abarca la totalidad de la empresa, con lo que las medidas que se establezcan se orientarán a aspectos funcionales, técnicos y organizativos.

Más en detalle, los objetivos deseados desde la Dirección General de la empresa son los siguientes:

1. Establecer la seguridad de la información como un proceso más en la empresa.
2. Convertir la seguridad de la información en la prioridad principal en la gestión diaria de los sistemas.
3. Al hilo de los objetivos anteriores descritos, establecer el marco organizativo, técnico y funcional para poder certificar a la empresa en la ISO 27001:2013
4. Certificar el SGSI para poder acceder a contratos donde los clientes solicitan disponer de tal certificación.
5. La seguridad como marca de calidad y compromiso de la compañía.

Anexo 2. Análisis diferencial de la empresa

En este apartado se lleva a cabo un análisis diferencial de la implementación de los diferentes controles de las normativas ISO 27001 e ISO 27002 en el que se encontraba la organización antes de iniciar las acciones para implementar un SGSI bajo la normativa ISO 27001:2013.

Este análisis nos permitirá establecer un punto de partida en el que poder determinar los logros y avances que materializarán a lo largo del desarrollo del proyecto.

Para llevar a cabo este análisis se ha utilizado el modelo de madurez de la capacidad (CMM) cuya escala se define de la siguiente manera.

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 1. Modelo CMM

Una vez realizado un análisis diferencial obtenemos el siguiente cuadro resumen y el posterior diagrama radial con el nivel actual de madurez de la compañía en relación a la norma ISO 27002:2013.

Análisis diferencial respecto a la ISO 27002:2013

14 DOMINIOS (114 CONTROLES)	Efectividad (%)	Apartados	Sub-apartados	Cumplimiento
5. Politicas de seguridad	0	1	2	0
6. Aspectos organizativos de la seguridad de la información	18	2	7	0
7. Seguridad ligada a los recursos humanos	17	3	6	1
8. Gestión de activos	15	3	9	1
9. Control de acceso	48	3	14	4
10. Cifrado	10	1	2	0
11. Seguridad física y ambiental	33	2	15	3
12. Seguridad en la operativa	23	7	14	4
13. Seguridad en las telecomunicaciones	14	2	7	1
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	59	3	13	5
15. Relación con los suministradores	8	2	5	0
16. Gestión de incidentes de seguridad de la información	4	1	7	0
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	0	2	4	0
18. Cumplimiento	15	2	8	1

Tabla 2. Análisis diferencial ISO 27002:2013

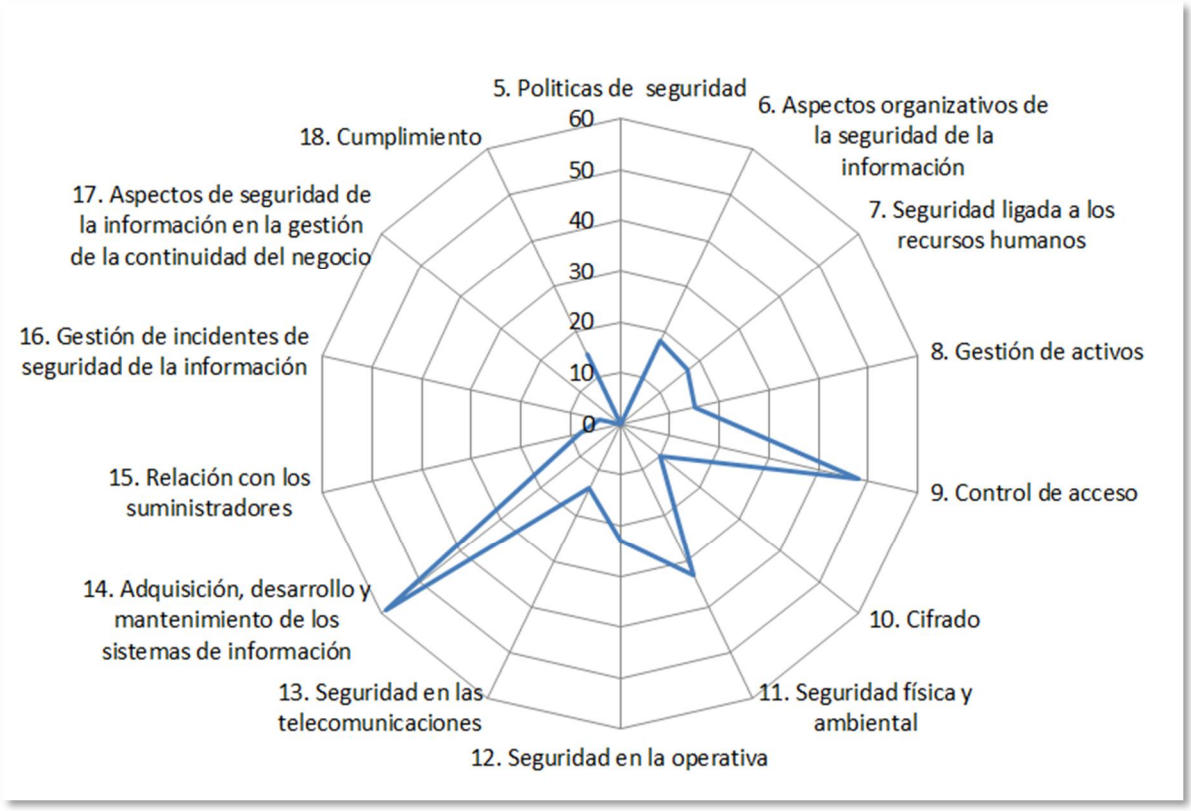

Ilustración 3. Análisis diferencial ISO 27002:2013

El análisis completo se puede ver en el fichero "Fase1. Análisis diferencial controles ISO 27002-2013)".

A continuación se muestra la tabla resumen y el diagrama radial que muestra el nivel actual de madurez de la compañía en relación a la norma ISO 27001:2013.

Análisis diferencial respecto a la ISO 27001:2013

10 APARTADOS	Efectividad (%)	Apartados	Sub-apartados	Cumplimiento
4. Contexto de la organización	20	4	0	0
5. Liderazgo	23	3	0	0
6. Planificación	16	2	3	0
7. Soporte	18	5	3	0
8. Operación	10	3	0	0
9. Evaluación del desempeño	7	3	0	0
10. Mejora	0	2	0	0

Tabla 3. Análisis diferencial ISO 27001:2013

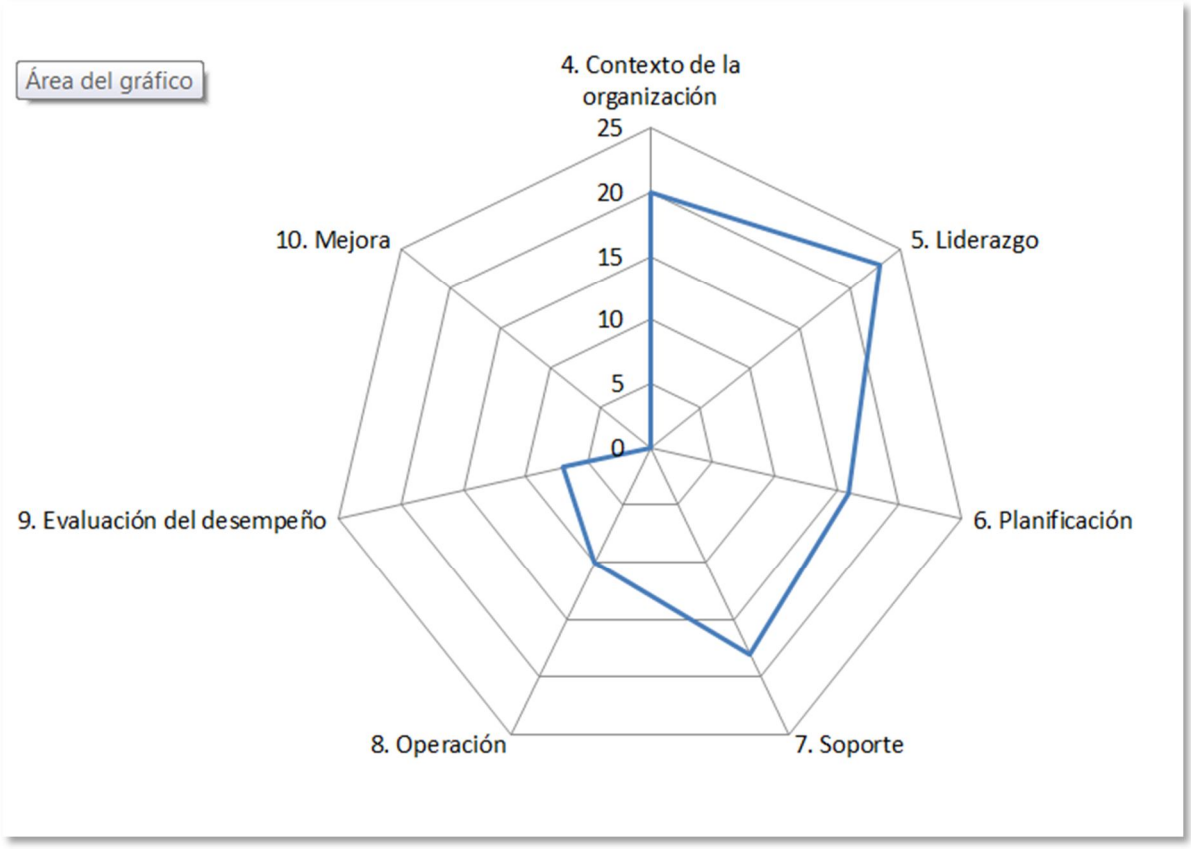

Ilustración 4. Análisis diferencial ISO 27001:2013

El análisis completo se puede ver en el fichero “Fase1. Análisis diferencial controles ISO 27001-2013)”.

2 SISTEMA DE GESTIÓN DOCUMENTAL

2.1 Introducción

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001.

2.2 Política de seguridad

Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.

2.3 Procedimiento de auditorías internas

Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

2.4 Gestión de indicadores

Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.

2.5 Procedimiento de revisión de la Dirección

La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001:2013 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones. La revisión por dirección es uno de los aspectos que contempla la normativa ISO/IEC 27001:2013 para la revisión anualmente de los aspectos más importantes que se han presentado con relación al SGSI implantados, revisando los elementos de entrada y salida de la revisión que establece la norma. De esta manera la dirección puede verificar y/o monitorear el sistema y establecer compromisos para realizar las mejoras necesarias.

2.6 Gestión de roles y responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de

Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección. Se hace necesario especificar en este documento los compromisos y responsabilidades que asume el equipo de trabajo que se estipula como comité de seguridad. En dicho comité hace parte por lo menos una persona de dirección para tener el respaldo de las directivas institucionales las decisiones que se requieran tomar.

2.7 Metodología de análisis de riesgos

Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

2.8 Declaración de aplicabilidad

Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada. Declarar la aplicabilidad de los controles es una tarea que visibiliza el alcance del SGSI, por tanto, es necesario un documento que especifique los controles de seguridad de acuerdo a la normativa que aplica a la organización en la que se implanta el SGSI. Para la declaración de aplicabilidad, ésta se puede representar a través de una tabla que especifique cada uno de los controles aplicables.

Anexo 3. Esquema documental

Los documentos que forman el conjunto del esquema se identifican y presentan de forma independiente de la siguiente manera:

- D1 SGSI PateTIC Política de seguridad de la información.pdf
- D2 SGSI PateTIC Procedimiento de auditorías internas.pdf
- D3 SGSI PateTIC Gestión de indicadores.pdf
- D4 SGSI PateTIC Procedimiento de revisión de la dirección.pdf
- D5 SGSI PateTIC Gestión de roles y responsabilidades.pdf
- D6 SGSI PateTIC Metodología de análisis de riesgos.pdf
- D7 SGSI PateTIC Declaración de aplicabilidad.pdf

3 ANÁLISIS DE RIESGOS

3.1 Introducción

El desarrollo del análisis de riesgos es una fase esencial del proceso de implementación de un SGSI. Se hace necesario, como punto de partida, la identificación de los activos de la organización. Es necesario identificarlos para saber qué se ha de proteger. Un activo es cualquier entidad que posee un valor para la empresa y que esa característica hace que necesite ser salvaguardada de posibles amenazas.

A los activos de información, se les debe efectuar un análisis y evaluación del riesgo, para posteriormente identificar los controles necesarios que tendrán que implementarse para mitigar ese riesgo.

3.2 Inventario de activos

Para comenzar el análisis de riesgos se han de identificar los activos de la organización. Para ello nos apoyaremos en la distribución que hace en su Libro II de la metodología Magerit. Se incorpora el concepto de propietario del riesgo (versus propietario del activo), quien deberá aprobar tanto el plan de tratamiento de riesgos como el riesgo residual obtenido. Estos activos serán identificados en diferentes grupos o ámbitos, tal y como se muestra en el siguiente cuadro:

Ámbito	Activo	Propietario del activo
Instalaciones (I)	(I-01) CPD	Director técnico
	(I-02) Oficina	Director general
Hardware (HW)	(HW-01) Servidor de aplicaciones (2)	Área técnica sistemas
	(HW-02) Servidor E-commerce	Área técnica sistemas
	(HW-03) Servidor Web (2)	Área técnica sistemas
	(HW-04) Servidor BBDD (2)	Área técnica sistemas
	(HW-05) Servidor DNS	Área técnica sistemas
	(HW-06) Servidor Proxy	Área técnica sistemas
	(HW-07) Controlador de dominio	Área técnica sistemas
	(HW-08) Servidor de ficheros	Área técnica sistemas
	(HW-09) Servidor de E-mail	Área técnica sistemas
	(HW-10) Comunicaciones	Área técnica sistemas
	(HW-11) Impresoras de red (3)	Área técnica sistemas
	(HW-12) PCs (15)	Área técnica sistemas
	(HW-13) Portátiles (15)	Área técnica sistemas
	(HW-14) Conmutadores	Área técnica sistemas
	(HW-15) Enrutador de Internet	Área técnica sistemas
	(HW-16) Puntos de acceso WIFI	Área técnica sistemas
	(HW-17) Cortafuegos	Área técnica sistemas
	(HW-18) Teléfonos	Área técnica sistemas

Aplicación (SW)	(SW-01) Sistemas operativos	Área técnica sistemas
	(SW-02) Desarrollos propios	Área técnica desarrollo
	(SW-03) Paquete ofimático	Área técnica desarrollo
	(SW-04) Antivirus	Área técnica sistemas
	(SW-05) Software desarrollo	Área técnica desarrollo
	(SW-06) Consolas de administración	Área técnica sistemas
	(SW-07) E-mail	Área técnica sistemas
	(SW-08) Servidores	Área técnica sistemas
Datos (D)	(D-01) Configuraciones	Responsable de sistemas
	(D-02) Código fuente	Responsable de desarrollo
	(D-03) Página Web	Responsable de desarrollo
	(D-04) Datos de e-mail	Responsable de sistemas
	(D-05) Datos de usuarios y clientes	Responsable de sistemas
	(D-06) Credenciales	Responsable de sistemas
	(D-07) Registro de actividad	Responsable de sistemas
Red (COM)	(COM-01) Internet	Área técnica sistemas
	(COM-02) Red inalámbrica	Área técnica sistemas
	(COM-03) Red cableada	Área técnica sistemas
	(COM-04) Telefonía fija	Área técnica sistemas
	(COM-05) Telefonía móvil	Área técnica sistemas
Servicios (SRV)	(SRV-01) Servicio Web	Área técnica desarrollo
	(SRV-02) Servicio E-commerce	Área técnica desarrollo
	(SRV-01) Servicio aplicaciones	Área técnica desarrollo
	(SRV-01) Servicio ficheros	Área técnica sistemas
	(SRV-05) Servicio DNS	Área técnica sistemas
	(SRV-06) Servidor Proxy	Área técnica sistemas
	(SRV-07) Servicio de acceso a dominio	Área técnica sistemas
	(SRV-08) Servicio de E-mail	Área técnica sistemas
	(SRV-09) Servicio de comunicaciones	Área técnica sistemas
Equipamiento auxiliar (EQAUX)	(EQAUX-01) Cableado	Director técnico
	(EQAUX-02) SAI	Director técnico
	(EQAUX-03) Generador eléctrico principal	Director técnico
	(EQAUX-04) Armarios	Director técnico
Personal (P)	(P-01) Director general (1)	Director general
	(P-02) Director comercial (1)	Director comercial
	(P-03) Dpto. Relaciones Públicas (3)	Dpto. Relaciones Públicas
	(P-04) Dpto. Marketing (2)	Dpto. Marketing
	(P-05) Dpto. Ventas (3)	Dpto. Ventas
	(P-06) Director técnico (1)	Director técnico
	(P-07) Responsable de desarrollo (1)	Responsable de desarrollo
	(P-08) Responsable de sistemas (1)	Responsable de sistemas
	(P-09) Desarrolladores (5)	Desarrolladores
	(P-10) Técnicos de sistemas (5)	Técnicos de sistemas

	(P-11) Director financiero (1)	Director financiero
	(P-12) Responsable RRHH y formación (1)	Responsable RRHH y formación
	(P-13) Responsable de Adm. y Contabilidad (1)	Responsable de Adm. y Contabilidad
	(P-14) Dpto Contabilidad (2)	Dpto Contabilidad
	(P-15) Dpto. Administración y compras (2)	Dpto. Administración y compras

Tabla 4. Inventario de activos

3.3 Valoración de los activos

Con la identificación de activos en relación a la seguridad de la información, hará falta valorar cada activo dentro de nuestra organización. El objetivo final del proceso es tomar un conjunto de medidas que garanticen nuestros activos.

El coste de estas medidas no ha de superar el coste del activo que se tiene que proteger, de otra forma no sería un activo rentable protegerlo, ya que sería más fácil substituirlo en caso contrario, por tanto, un punto por dónde empezar es la asignación de un valor a los activos. Para poder valorar un activo se han de tener en cuenta diferentes aspectos, como por ejemplo el coste de reposición, el valor del tiempo sin servicio, posibles penalizaciones, etc. La tabla sobre la que se procederá a realizar la valoración de activos es la siguiente:

Nivel	Valoración
Despreciable (D)	Valor de hasta 600 €
Muy bajo (MB)	Valor entre 600 y 6000 €
Bajo (B)	Valor entre 6000 y 15000 €
Medio (M)	Valor entre 15000 y 40000 €
Alto (A)	Valor entre 40000 y 100000 €
Muy alto (MA)	Valor superior a 100000 €

Tabla 5. Escala de valoración de activos

Esta tabla nos permitirá realizar la asignación de un valor a los activos en función de las categorías de la columna valoración y a su vez, tendremos un valor cuantitativo que viene representado por la columna Valor. Los valores de los activos no corresponderán a valores fijos, sino a un rango que estimará los límites del valor correspondiente.

Por otra parte, se tendrá que tener en cuenta que los activos están jerarquizados, es decir, se deberán identificar y valorar las dependencias entre activos. Se dice que un activo superior depende de otro activo inferior cuando las necesidades de seguridad del superior se muestran en las necesidades de seguridad del inferior, o dicho de otra manera, cuando la materialización de una amenaza en el activo inferior tiene consecuencias perjudiciales sobre el activo superior.

Por tanto, será requisito analizar el árbol de dependencias o jerarquía entre activos. Este apartado referente a las dependencias, quedará reflejado en la tabla de activos en la columna dependencias.

3.4 Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración de los activos, se ha de indicar cuál es el aspecto de la seguridad más crítico. Esto será de gran ayuda en el momento de pensar en posibles medidas de prevención, ya que serán enfocadas en aquellos aspectos más críticos.

Una vez identificados los activos, se ha de realizar la valoración ACIDT de los mismos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso de negocio. Esta valoración nos permitirá, a posteriori, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto. El valor que reciba el activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando el resto de activos subordinados a las necesidades de explotación y protección de la información. De esta manera, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede tener un valor diferente en cada uno de las diferentes dimensiones para la organización que deseamos analizar. Por esto, se ha de tener presente siempre que representa cada dimensión.

Las cinco dimensiones de las que se habla son:

- *Autenticidad* [A]. Hay garantía de la identidad de los usuarios o procesos que gestionarán la información.
- *Confidencialidad* [C]. Únicamente las personas autorizadas tienen acceso a la información sensible o privada.
- *Integridad* [I]. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización
- *Disponibilidad* [D]. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.
- *No repudio* [T]. Hay garantía de la autoría de una determinada acción y está asociada a quien ha producido esta acción.

Una vez detalladas las cinco dimensiones se ha de tener presente la escala en que se realizarán las valoraciones. En este caso se utilizará una escala de valoración de diez valores siguiendo el siguiente criterio:

Valor	Descripción
10	Daño muy grave a la organización
7 a 9	Daño grave a la organización
4 a 6	Daño importante a la organización
1 a 3	Daño menor a la organización
0	Daño irrelevante a la organización

Tabla 6. Valoración dimensiones de seguridad

3.5 Tabla resumen de valoración

De forma resumida, lo visto hasta ahora nos debe permitir generar una tabla donde reflejaremos tanto la valoración de activos como los aspectos críticos del mismo.

Ámbito	Activo	Dependencias	Valor	Aspectos críticos				
				A	C	I	D	T
Instalaciones (I)	(I-01) CPD		A	8	8	9	10	8
	(I-02) Oficina		MA		5	7	8	
Hardware (HW)	(HW-01) Servidor de aplicaciones (2)	(I-01)	B	8	9	7	9	8
	(HW-02) Servidor E-commerce	(I-01)	MB	8	7	8	9	8
	(HW-03) Servidor Web (2)	(I-01)	B	8	7	8	9	8
	(HW-04) Servidor BBDD (2)	(I-01)	B	8	9	8	8	7
	(HW-05) Servidor DNS	(I-01)	MB	8	7	7	7	7
	(HW-06) Servidor Proxy	(I-01)	MB	8	8	8	8	8
	(HW-07) Controlador de dominio	(I-01)	MB	8	9	9	9	8
	(HW-08) Servidor de ficheros	(I-01)	MB	8	8	8	8	7
	(HW-09) Servidor de E-mail	(I-01)	MB	8	7	7	8	7
	(HW-10) Comunicaciones	(I-01)	M	8	8	7	9	8
	(HW-11) Impresoras de red (3)	(I-02)	MB				7	
	(HW-12) PCs (15)	(I-01)(I-02)	B	8	7	9	7	9
	(HW-13) Portátiles (15)	(I-02)	B	8	8	8	7	8
	(HW-14) Conmutadores	(I-01)	M	8	7	8	7	7
	(HW-15) Enrutador de Internet	(I-01)	MB	8	7	7	7	8
	(HW-16) Puntos de acceso WIFI	(I-02)	MB	8	7	8	9	9
	(HW-17) Cortafuegos	(I-01)	A	8	7	8	7	8
	(HW-18) Teléfonos	(I-01)(I-02)	M	8	7	7	8	9
Aplicación (SW)	(SW-01) Sistemas operativos	(HW-XX)	B	8	7	7	7	6
	(SW-02) Desarrollos propios	(HW-01)(HW-02)	MB	8	6	8	8	7
	(SW-03) Paquete ofimático	(HW-12)(HW-13)	B	7	8	8	7	7
	(SW-04) Antivirus	(HW-12)(HW-13)	MB	8	7	7	6	6
	(SW-05) Software desarrollo	(HW-12)(HW-13)	MB	8	8	6	7	7
	(SW-06) Consolas de administración	(HW-12)(HW-13)	MB	7	6	7	8	6
	(SW-07) E-mail	(HW-12)(HW-13)(HW-09)	MB	7	8	6	8	6
	(SW-08) Servidores	(HW-01 a HW-09)	B	7	7	6	7	6
Datos (D)	(D-01) Configuraciones	(HW-0X)	M	7	8	8	9	7
	(D-02) Código fuente	(HW-01)(HW-02)	A	8	7	9	8	6
	(D-03) Página Web	(HW-03)	M	6	7	9	7	8
	(D-04) Datos de e-mail	(SW-07)	M	6	9	6	6	9
	(D-05) Datos de usuarios y clientes	(HW-12)(HW-13)	A	7	9	8	7	7
	(D-06) Credenciales	(HW-0X)	M	9	8	9	9	8

	(D-07) Registro de actividad	(HW-07)	B	9	8	7	6	6
Red (COM)	(COM-01) Internet	(I-01)(HW-15)	M	7	8	6	7	6
	(COM-02) Red inalámbrica	(HW-16)	M	7	7	7	7	7
	(COM-03) Red cableada	(I-01)(I-02)	A	9	9	6	7	5
	(COM-04) Telefonía fija	(HW-18)	M	8	7	7	6	8
	(COM-05) Teléfonía móvil	(HW-18)	A	7	8	7	4	9
Servicios (SRV)	(SRV-01) Servicio Web	(HW-03)(SW-08)	A	7	8	5	6	7
	(SRV-02) Servicio E-commerce	(HW-02)(SW-02)(SW-08)	A	6	5	7	6	7
	(SRV-01) Servicio aplicaciones	(HW-01)(SW-02)(SW-08)	A	5	7	5	7	8
	(SRV-01) Servicio ficheros	(HW-08)(SW-08)	M	7	7	5	8	6
	(SRV-05) Servicio DNS	(HW-05)(SW-08)	M	6	7	9	7	5
	(SRV-06) Servidor Proxy	(HW-06)(SW-08)	M	5	6	4	7	7
	(SRV-07) Servicio de acceso a dominio	(HW-07)(SW-08)	A	4	7	7	6	6
	(SRV-08) Servicio de E-mail	(HW-09)(SW-07)(SW-08)	A	7	7	5	7	4
	(SRV-09) Servicio de comunicaciones	(HW-10)(SW-08)	A	9	8	6	5	7
Equipamiento auxiliar (EQAUX)	(EQAUX-01) Cableado	(COM-03)	M				7	
	(EQAUX-02) SAI	(I-01)	B				5	
	(EQAUX-03) Generador eléctrico principal	(I-01)	B				7	
	(EQAUX-04) Armarios	(I-02)	MB				7	
Personal (P)	(P-01) Director general (1)		MA				9	
	(P-02) Director comercial (1)		A				8	
	(P-03) Dpto. Relaciones Públicas (3)		M				6	
	(P-04) Dpto. Marketing (2)		M				6	
	(P-05) Dpto. Ventas (3)		A				6	
	(P-06) Director técnico (1)		MA				8	
	(P-07) Responsable de desarrollo (1)		A				7	
	(P-08) Responsable de sistemas (1)		A				7	
	(P-09) Desarrolladores (5)		M				6	
	(P-10) Técnicos de sistemas (5)		M				6	
	(P-11) Director financiero (1)		A				8	
	(P-12) Responsable RRHH y formación (1)		A				7	
	(P-13) Responsable de Adm. y Contabilidad (1)		A				7	
	(P-14) Dpto Contabilidad (2)		M				6	
	(P-15) Dpto. Administración y compras (2)		M				6	

Tabla 7. Valoración de los activos

3.6 Análisis de amenazas

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. Se analizan qué amenazas pueden afectar a qué activos. Una vez estudiado, estimar cuán vulnerable es el activo a la materialización de la amenaza así como la frecuencia estimada de la misma.

Usamos la metodología MAGERIT (en concreto Libro 2 “Catálogo de Elementos” (Punto 5)). Las amenazas están clasificadas en los siguientes grandes bloques:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

A continuación se lista agrupadas por bloques el global de las amenazas que incluye:

Bloque 1
[N] Desastres naturales
Amenazas
[N.1] Fuego
[N.2] Daños por agua
[N.*] Otros desastres naturales

Bloque 2
[I] De origen industrial
Amenazas
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

Bloque 3
[E] Errores y fallos no intencionados
Amenazas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escapes de información
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

Bloque 4
[A] Ataques intencionados
Amenazas
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

Tabla 8. Agrupación de amenazas en MAGERIT

La información recopilada da lugar a una tabla resumen para un activo determinado. En definitiva, para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

La frecuencia o probabilidad de ocurrencia de los eventos se encuentra definida así:

Nivel	Valor	Descripción	Grado
Frecuencia muy alta (MA)	100	A diario	5<
Frecuente (F)	20	Cada mes	4
Normal (N)	1	Una vez al año	3
Poco frecuente (PF)	0,1	Cada varios años	2
Muy poco frecuente (MPF)	0,01	Casi nunca	1>

Tabla 9. Frecuencia de ocurrencia

Para el grado de impacto que la amenaza produciría si se ejecutase y por lo tanto que afectase a las dimensiones de seguridad, se utilizará una tabla con el nivel porcentual de afectación a cada dimensión:

Impacto	Valor	Grado
Muy alto	100%	5<
Alto	75%	4
Medio	50%	3
Bajo	20%	2
Muy bajo	5%	1>

Tabla 10. Impacto de las amenzas

En primer lugar se hará un análisis de las amenazas que afectan a cada activo. Con ello generaremos una tabla que cruzará las amenazas y los activos. Debido a la longitud de la tabla sólo se mostrará un detalle del análisis obtenido.

				Dimensiones de seguridad				
Bloque	**Amenaza**	**Activos**	**Frecuencia**	**A**	**C**	**I**	**D**	**T**
[N] Desastres naturales	[N.1] Fuego	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[N.2] Daños por agua	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[N.*] Otros desastres naturales	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
[I] De origen industrial	[I.1] Fuego	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[I.2] Daños por agua	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[I.*] Desastres industriales	Instalaciones (I)	0,01				100%	
		Hardware (HW)					75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[I.3] Contaminación mecánica	Hardware (HW)	0,01				50%	
		Equipamiento auxiliar (EQAUX)					50%	
	[I.4] Contaminación electromagnética	Hardware (HW)	0,01				75%	
		Equipamiento auxiliar (EQAUX)					75%	
	[I.5] Avería de origen físico o lógico	Aplicación (SW)	1				75%	
		Hardware (HW)					50%	
		Equipamiento auxiliar (EQAUX)					20%	
	[I.6] Corte del suministro eléctrico	Hardware (HW)	1				100%	
		Equipamiento auxiliar (EQAUX)					100%	
	[I.7] Condiciones inadecuadas de temperatura o humedad	Hardware (HW)	0,1				50%	
		Equipamiento auxiliar (EQAUX)					50%	
	[I.8] Fallo de servicios de comunicaciones	Red (COM)	10				75%	
	[I.9] Interrupción de otros servicios y suministros esenciales	Equipamiento auxiliar (EQAUX)	10				5%	
	[I.10] Degradación de los soportes de almacenamiento de la información	(HW-08) Servidor de ficheros	0,1				75%	
	[I.11] Emanaciones electromagnéticas	Instalaciones (I)	0,1		20%			
		Hardware (HW)			50%			
		Equipamiento auxiliar (EQAUX)			20%			

Tabla 11. Detalle del análisis de amenazas

Nota: La tabla completa del Análisis de amenazas se incluye en la hoja de cálculo anexa a esta tercera fase del proyecto.

3.7 Impacto potencial

Una vez terminado el análisis de los activos, presentado en las tablas anteriores y el análisis de las amenazas, podemos calcular el impacto potencial que pueden suponer para la empresa la materialización de estas amenazas.

En este apartado y, para el cálculo del impacto, no se tienen en cuenta contramedidas, por tanto, el resultado que obtengamos de este cálculo se podrá extraer un valor de referencia que ayudará para determinar y priorizar un plan de acción. Al aplicar las contramedidas, este valor se verá modificado.

Para realizar el cálculo del impacto potencial, se utiliza la siguiente fórmula:

Impacto Potencial = Activo x Impacto

Donde, es el valor de cada dimensión y el impacto es la degradación en cada dimensión en la que se ve afectado el activo también en caso de materializarse.

En la tabla siguiente se presentan un detalle de los resultados:

Activo	Valoración					Impacto					Impacto potencial				
	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
(I-01) CPD	8	8	9	10	8		75%	75%	100%			6	6,75	10	
(I-02) Oficina		5	7	8								3,75	5,25	8	
(HW-01) Servidor de aplicaciones (2)	8	9	7	9	8							6,75	3,5	6,75	
(HW-02) Servidor E-commerce	8	7	8	9	8							5,25	4	6,75	
(HW-03) Servidor Web (2)	8	7	8	9	8							5,25	4	6,75	
(HW-04) Servidor BBDD (2)	8	9	8	8	7							6,75	4	6	
(HW-05) Servidor DNS	8	7	7	7	7							5,25	3,5	5,25	
(HW-06) Servidor Proxy	8	8	8	8	8							6	4	6	
(HW-07) Controlador de dominio	8	9	9	9	8							6,75	4,5	6,75	
(HW-08) Servidor de ficheros	8	8	8	8	7							6	4	6	
(HW-09) Servidor de E-mail	8	7	7	8	7		75%	50%	75%			5,25	3,5	6	
(HW-10) Comunicaciones	8	8	7	9	8							6	3,5	6,75	
(HW-11) Impresoras de red (3)				7										5,25	
(HW-12) PCs (15)	8	7	9	7	9							5,25	4,5	5,25	
(HW-13) Portátiles (15)	8	8	8	7	8							6	4	5,25	
(HW-14) Conmutadores	8	7	8	7	7							5,25	4	5,25	
(HW-15) Enrutador de Internet	8	7	7	7	8							5,25	3,5	5,25	
(HW-16) Puntos de acceso WIFI	8	7	8	9	9							5,25	4	6,75	
(HW-17) Cortafuegos	8	7	8	7	8							5,25	4	5,25	
(HW-18) Teléfonos	8	7	7	8	9							5,25	3,5	6	

Tabla 12. Detalle del análisis de impacto potencial

Nota: La tabla completa del Análisis de impacto potencial se incluye en la hoja de cálculo anexa a esta tercera fase del proyecto.

3.8 Nivel de riesgo aceptable y riesgo residual

Los riesgos no pueden eliminarse por completo pese a las medidas que tomen las organizaciones. Sin embargo, de acuerdo a las estrategias comentadas en la sección anterior pueden disminuir la ocurrencia de aquellos riesgos que pueden ser más críticos a unos niveles aceptables. Este riesgo que permanece después de haber implementado las medidas se conoce como residual y la organización tomará la decisión de convivir él.

Una vez conocemos el impacto potencial causado por un activo y su impacto en el sistema, es posible obtener el riesgo integrando la frecuencia con que se puede dar un hecho concreto en nuestros sistemas. Para ello usaremos el siguiente cálculo:

*Riesgo = Impacto Potencial * Frecuencia*

Podemos afirmar que el riesgo será mayor cuanto mayor sea el impacto y mayor la frecuencia de ocurrencia.

El siguiente cuadro nos ayudará a catalogar cada activo según su probabilidad de que la amenaza ocurra y el impacto que causaría sobre él. Estos niveles de evaluación del riesgo nos indicará en qué estado actual de seguridad nos encontramos y la empresa deberá decidir hacia qué nivel se ha de orientar, es decir, el nivel de riesgo aceptable y el consiguiente riesgo residual.

Nivel de impacto						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Nivel de probabilidad de ocurrencia				

Tabla 13. Niveles de evaluación del riesgo

A continuación mostramos el cuadro de evaluación del nivel de riesgo que presenta nuestra compañía:

Activo	Frecuencia	Impacto potencial					Evaluación riesgo	Propietario del riesgo
		A	C	I	D	T		
(I-01) CPD	1		6	6,75	10		10	Director técnico
(I-02) Oficina	1		3,75	5,25	8		8	Director general
(HW-01) Servidor de aplicaciones (2)	2		6,75	3,5	6,75		13,5	Responsable de sistemas
(HW-02) Servidor E-commerce	2		5,25	4	6,75		13,5	Responsable de sistemas
(HW-03) Servidor Web (2)	2		5,25	4	6,75		13,5	Responsable de sistemas
(HW-04) Servidor BBDD (2)	2		6,75	4	6		13,5	Responsable de sistemas

(HW-05) Servidor DNS	1		5,25	3,5	5,25		5,25	Responsable de sistemas
(HW-06) Servidor Proxy	2		6	4	6		12	Responsable de sistemas
(HW-07) Controlador de dominio	2		6,75	4,5	6,75		13,5	Responsable de sistemas
(HW-08) Servidor de ficheros	2		6	4	6		12	Responsable de sistemas
(HW-09) Servidor de E-mail	2		5,25	3,5	6		12	Responsable de sistemas
(HW-10) Comunicaciones	1		6	3,5	6,75		6,75	Responsable de sistemas
(HW-11) Impresoras de red (3)	1				5,25		5,25	Responsable de sistemas
(HW-12) PCs (15)	2		5,25	4,5	5,25		10,5	Responsable de sistemas
(HW-13) Portátiles (15)	2		6	4	5,25		12	Responsable de sistemas
(HW-14) Conmutadores	1		5,25	4	5,25		5,25	Responsable de sistemas
(HW-15) Enrutador de Internet	2		5,25	3,5	5,25		10,5	Responsable de sistemas
(HW-16) Puntos de acceso WIFI	2		5,25	4	6,75		13,5	Responsable de sistemas
(HW-17) Cortafuegos	2		5,25	4	5,25		10,5	Responsable de sistemas
(HW-18) Teléfonos	1		5,25	3,5	6		6	Responsable de sistemas
(SW-01) Sistemas operativos	3	4	5,25	5,25	5,25		15,75	Responsable de sistemas
(SW-02) Desarrollos propios	3	4	4,5	6	6		18	Responsable de desarrollo
(SW-03) Paquete ofimático	3	3,5	6	6	5,25		18	Responsable de desarrollo
(SW-04) Antivirus	3	4	5,25	5,25	4,5		15,75	Responsable de sistemas
(SW-05) Software desarrollo	3	4	6	4,5	5,25		18	Responsable de desarrollo
(SW-06) Consolas de administración	3	3,5	4,5	5,25	6		18	Responsable de sistemas
(SW-07) E-mail	3	3,5	6	4,5	6		18	Responsable de sistemas
(SW-08) Servidores	3	3,5	5,25	4,5	5,25		15,75	Responsable de sistemas
(D-01) Configuraciones	2	7	8	8	9	1,4	18	Director técnico
(D-02) Código fuente	2	8	7	9	8	1,2	18	Director técnico
(D-03) Página Web	2	6	7	9	7	1,6	18	Director técnico
(D-04) Datos de e-mail	2	6	9	6	6	1,8	18	Director técnico
(D-05) Datos de usuarios y clientes	2	7	9	8	7	1,4	18	Director técnico
(D-06) Credenciales	2	9	8	9	9	1,6	18	Director técnico
(D-07) Registro de actividad	2	9	8	7	6	1,2	18	Director técnico
(COM-01) Internet	3	0,35	4	3	5,25		15,75	Director técnico
(COM-02) Red inalámbrica	3	0,35	3,5	3,5	5,25		15,75	Director técnico
(COM-03) Red cableada	2	0,45	4,5	3	5,25		10,5	Director técnico
(COM-04) Telefonía fija	1	0,4	3,5	3,5	4,5		4,5	Director técnico
(COM-05) Teléfonía móvil	1	0,35	4	3,5	3		4	Director técnico
(SRV-01) Servicio Web	3	3,5	6	2,5	3	0,35	18	Responsable de desarrollo
(SRV-02) Servicio E-commerce	3	3	3,75	3,5	3	0,35	11,25	Responsable de desarrollo
(SRV-01) Servicio aplicaciones	3	2,5	5,25	2,5	3,5	0,4	15,75	Responsable de desarrollo
(SRV-01) Servicio ficheros	3	3,5	5,25	2,5	4	0,3	15,75	Responsable de sistemas
(SRV-05) Servicio DNS	3	3	5,25	4,5	3,5	0,25	15,75	Responsable de sistemas
(SRV-06) Servidor Proxy	3	2,5	4,5	2	3,5	0,35	13,5	Responsable de sistemas
(SRV-07) Servicio de acceso a dominio	3	2	5,25	3,5	3	0,3	15,75	Responsable de sistemas
(SRV-08) Servicio de E-mail	3	3,5	5,25	2,5	3,5	0,2	15,75	Responsable de sistemas
(SRV-09) Servicio de comunicaciones	3	4,5	6	3	2,5	0,35	18	Responsable de sistemas
(EQAUX-01) Cableado	3				5,25		15,75	Director técnico

(EQAUX-02) SAI	1				3,75		3,75	Director técnico
(EQAUX-03) Generador eléctrico principal	2				5,25		10,5	Director técnico
(EQAUX-04) Armarios	3				5,25		15,75	Director técnico
(P-01) Director general (1)	2				6,75		13,5	Director general
(P-02) Director comercial (1)	2				6		12	Director comercial
(P-03) Dpto. Relaciones Públicas (3)	1				4,5		4,5	Director comercial
(P-04) Dpto. Marketing (2)	1				4,5		4,5	Director comercial
(P-05) Dpto. Ventas (3)	1				4,5		4,5	Director comercial
(P-06) Director técnico (1)	2				6		12	Director técnico
(P-07) Responsable de desarrollo (1)	2				5,25		10,5	Responsable de desarrollo
(P-08) Responsable de sistemas (1)	2				5,25		10,5	Responsable de sistemas
(P-09) Desarrolladores (5)	1				4,5		4,5	Responsable de desarrollo
(P-10) Técnicos de sistemas (5)	1				4,5		4,5	Responsable de sistemas
(P-11) Director financiero (1)	2				6		12	Director financiero
(P-12) Responsable RRHH y formación (1)	2				5,25		10,5	Director financiero
(P-13) Responsable de Adm. y Contabilidad (1)	2				5,25		10,5	Director financiero
(P-14) Dpto Contabilidad (2)	1				4,5		4,5	Responsable de Adm. y Contabilidad
(P-15) Dpto. Administración y compras (2)	1				4,5		4,5	Responsable de Adm. y Contabilidad

Tabla 14. Análisis del nivel de riesgo

Una vez definido el nivel de riesgo, la empresa ha establecido unos niveles para realizar el tratamiento del riesgo, que se resume en el siguiente cuadro.

Criterios de aceptación del riesgo	Directrices generales de tratamiento
Aceptable	No requiere tratamiento del riesgo; es decir que el riesgo se encuentra en un nivel que puede aceptarse
Moderado	Riesgo no prioritario. Requiere fortalecer controles como acción preventiva si es económicamente viable y fácil de implementar.
Alto	Requiere acciones de tratamiento del riesgo en el corto plazo, definiendo y fortaleciendo los controles.
Crítico	Acción de tratamiento del riesgo inmediata. Se debe evitar la actividad que genera el riesgo en la medida de lo posible, de lo contrario se deben implementar controles para reducir la probabilidad de ocurrencia del riesgo o su impacto, o transferir el riesgo.

Tabla 15. Tratamiento del riesgo

La empresa reconoce como riesgo aceptable todo aquel riesgo que se encuentre dentro de los niveles moderados, esto es, en color amarillo. Por tanto se deberán seleccionar los controles de la norma que nos sirvan para gestionar esos riesgos y que se sitúen sobre este umbral moderado. Todo ello se tratará en la fase siguiente del proyecto, donde se definirán los proyectos a realizar para realizar esta adecuación.

A modo de resumen, del resultado del análisis de riesgo realizado obtenemos el nivel de tratamiento de riesgo de cada activo. Se muestran a continuación agrupados por nivel de tratamiento:

Tratamiento del riesgo	Activo
Crítico	(SW-02) Desarrollos propios
	(SW-03) Paquete ofimático
	(SW-05) Software desarrollo
	(SW-06) Consolas de administración
	(SW-07) E-mail
	(D-01) Configuraciones
	(D-02) Código fuente
	(D-03) Página Web
	(D-04) Datos de e-mail
	(D-05) Datos de usuarios y clientes
	(D-06) Credenciales
	(D-07) Registro de actividad
	(SRV-01) Servicio Web
	(SRV-09) Servicio de comunicaciones

Tratamiento del riesgo	Activo
Alto	(I-01) CPD
	(HW-01) Servidor de aplicaciones (2)
	(HW-02) Servidor E-commerce
	(HW-03) Servidor Web (2)
	(HW-04) Servidor BBDD (2)
	(HW-06) Servidor Proxy
	(HW-07) Controlador de dominio
	(HW-08) Servidor de ficheros
	(HW-09) Servidor de E-mail
	(HW-12) PCs (15)
	(HW-13) Portátiles (15)
	(HW-15) Enrutador de Internet
	(HW-16) Puntos de acceso WIFI
	(HW-17) Cortafuegos
	(SW-01) Sistemas operativos
	(SW-04) Antivirus
	(SW-08) Servidores
	(COM-01) Internet
	(COM-02) Red inalámbrica
	(COM-03) Red cableada
	(SRV-02) Servicio E-commerce
	(SRV-01) Servicio aplicaciones
	(SRV-01) Servicio ficheros
	(SRV-05) Servicio DNS
	(SRV-06) Servidor Proxy
	(SRV-07) Servicio de acceso a dominio
	(SRV-08) Servicio de E-mail
	(EQAUX-01) Cableado
	(EQAUX-03) Generador eléctrico principal
	(EQAUX-04) Armarios
	(P-01) Director general (1)
	(P-02) Director comercial (1)

	(P-06) Director técnico (1)
	(P-07) Responsable de desarrollo (1)
	(P-08) Responsable de sistemas (1)
	(P-11) Director financiero (1)
	(P-12) Responsable RRHH y formación (1)
	(P-13) Responsable de Adm. y Contabilidad (1)

Tratamiento del riesgo	Activo
Moderado	(I-02) Oficina
	(HW-05) Servidor DNS
	(HW-10) Comunicaciones
	(HW-11) Impresoras de red (3)
	(HW-14) Conmutadores
	(HW-18) Teléfonos

Tratamiento del riesgo	Activo
Aceptable	(COM-04) Telefonía fija
	(COM-05) Teléfonía móvil
	(EQAUX-02) SAI
	(P-03) Dpto. Relaciones Públicas (3)
	(P-04) Dpto. Marketing (2)
	(P-05) Dpto. Ventas (3)
	(P-09) Desarrolladores (5)
	(P-10) Técnicos de sistemas (5)
	(P-14) Dpto Contabilidad (2)
	(P-15) Dpto. Administración y compras (2)

Tabla 16. Activos agrupados por tratamiento de riesgo

Una vez agrupados los activos con las distintos grados de riesgo podemos ver que tanto los datos así como algunas las aplicaciones y servicios.

En un grado de riesgo alto tenemos la mayor cantidad de activos, que cruza de forma transversal tanto a las instalaciones, como el hardware, software, servicios, comunicaciones, elementos auxiliares y personal.

Este será el foco de actuación de los proyectos que se vayan a implementar.

3.9 Resultados

Con el desarrollo del análisis de riesgos se ha conseguido obtener una visión clara y objetiva de los activos de información de la organización y su nivel de seguridad. Es ahora cuando se conocen las amenazas a las que están expuestos estos activos de información y el grado del impacto o penalización que sufriría la organización en caso de ser vulnerada alguna amenaza.

Por otra parte se define el nivel de riesgo que la dirección de la organización asume como aceptable y aquel que se mantiene una vez aplicados los controles de seguridad adecuados.

En definitiva, con todo este trabajo de análisis de riesgos se hace una foto del nivel de seguridad que tiene la empresa en relación a sus sistemas de información.

En base a este estudio y partiendo del mismo se propone en la siguiente fase un listado de proyectos y acciones a acometer para poder mejorar el estado de seguridad de la organización.

Anexo 4. Análisis de riesgos

Todo el contenido realizado en el análisis de riesgos se presenta en una hoja de cálculo con el siguiente contenido:

- Escalas (tablas de valoración sobre las que se apoya el proceso de análisis).
- Inventario de activos (incluyendo propietario del activo y del riesgo).
- Valoración de activos.
- Amenazas (agrupación de amenazas según Magerit).
- Análisis de amenazas.
- Impacto potencial.
- Evaluación del riesgo.
- Resumen.

4 PROPUESTAS DE PROYECTOS

4.1 Introducción

Una vez realizado el análisis de riesgos y obtenido las amenazas, impacto y riesgo en nuestros activos, se dispone de un conocimiento más amplio y exacto del estado de la organización en materia de seguridad. Por tanto, el objetivo principal ahora es reducir el riesgo existente en la organización, mitigando el impacto de las amenazas hasta conseguir el estado de cumplimiento de madurez óptimo de los diferentes dominios indicados en la ISO 21001:2013. En este apartado se acometerá el planteamiento de diferentes proyectos que ayudarán a conseguir este nivel óptimo que se persigue en toda organización.

El desarrollo de los proyectos se planificará para una franja temporal de 2 años; la intención es ir adaptándose a la norma para en un futuro poder llegar a certificarse. La cantidad de proyectos se ha basado en la disponibilidad de los recursos necesarios, de cualquier índole, para que el impacto sobre el negocio objetivo de la compañía sea mínimo. La empresa es pequeña, con poco personal y recursos, por lo que se ha intentado hacer algo realista dado el número de personas cualificadas que podrían dedicar tiempo a los proyectos sin desatender los proyectos de negocio de la compañía.

4.2 Propuestas

Utilizando como base el resultado del análisis de riesgos del apartado anterior, así como los análisis de los controles de la ISO 27002. Los proyectos serán aplicaciones de los controles recomendados para poder mitigar y gestionar el riesgo y establecer su nivel como mínimo en el nivel de riesgo aceptable establecido por la compañía.

Los proyectos planteados serán los resultantes de agrupar un conjunto de recomendaciones identificadas, en la fase de análisis de riesgos, para facilitar su ejecución. Se incidirá no únicamente en la mejora de la gestión de la seguridad, sino también en posibles beneficios colaterales como pueden ser la optimización de recursos, mejora de la gestión de procesos y tecnologías presentes en la organización.

Para identificar cada proyecto se detallarán los siguientes campos:

- Identificación del proyecto.
- Nombre.
- Ámbito (tecnológico, organizativo, recursos humanos, etc).
- Activos afectados.
- Descripción.
- Puntos de control (dominios y controles de la ISO 27002).
- Coste temporal (corte, medio o largo plazo).
- Coste económico.

Con este listado de puntos se establecerá de una manera clara los diferentes aspectos que tratará cada proyecto. El detalle de los dominios de la ISO 27002 está relacionado con el control detallado a forma de intentar llevar cierto control sobre los diferentes aspectos de la seguridad que se intentan mitigar.

Es importante destacar que los controles están relacionados con unos activos que se ven afectados por estos, de manera que, según el análisis de riesgos realizado en el apartado anterior, se especifica qué grupo de activos se ven favorecidos por la salvaguarda aplicada, es decir, si existe mejora por parte del proyecto en los riesgos detectados en el análisis de riesgos anterior.

Para el cálculo del coste que supondría un proyecto, se ha procedido a sumar los costes que tendría por un lado la mano de obra de los empleados que realizarán el proyecto, así como, en caso de que fuera necesario, el coste del hardware o soluciones privadas de software requeridas para llevar a cabo el proyecto.

Los empleados que realizan dichos proyectos no están a horario completo en todos los proyectos, sino que dedican tiempo de su jornada a realizar este proyecto mientras realizan las tareas propias de su trabajo.

A continuación se presentan los diferentes proyectos:

Identificación del proyecto	PR-01
Nombre	Definición de la política de seguridad
Ámbito	Documentación
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal.
Descripción	Se definirá un documento de política de la seguridad de la información que deberá aprobar la dirección, y que será publicado y distribuido a todos los miembros afectados de la organización. La política de seguridad de la información se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. La política de seguridad de la información deberá a estar a disposición de cualquier usuario sobre la que recaiga su aceptación y cumplimiento. Las fases a alto nivel serían: • Creación y mantenimiento de una política de seguridad de los sistemas de información actualizada. • Adecuación a la legislación española vigente para la gestión de datos de carácter confidencial. • Formalización de procesos y gestión de los usuarios sobre los recursos de la organización, como: o Controles de acceso adecuados al rol del usuario. o Procedimientos de seguridad claramente definido. o Roles especificados y detallados para la gestión de la información, etc. o Responsabilidades de los trabajadores. • Concienciación del usuario sobre temas de seguridad de la información. • Reducción del riesgo por desconocimiento de los controles o respuesta a incidentes. • Buenas prácticas por parte de los usuarios. • Grado de despliegue y adopción de la política en la organización.
Controles	5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información.
Coste temporal	El primer borrador que se presentará en el comité de seguridad será en el plazo de 2 meses. Las revisiones se harán por lo general cada 6 meses si no hay cambios que merezcan adelantarlas.
Coste económico	Horas del personal interno (comité de seguridad), unos 5000€.

Tabla 17. Proyecto 1

Identificación del proyecto	PR-02
Nombre	Organización de la seguridad.
Ámbito	Organizativo y recursos humanos.
Activos afectados	Personal.
Descripción	La Dirección debería prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información. Las actividades relativas a la seguridad de la información deberían ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo. Deberían mantenerse los contactos adecuados con las autoridades competentes. Deberían mantenerse los contactos adecuados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad. El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad
Controles	6.1. Organización interna.
Coste temporal	Se estiman 3 meses.
Coste económico	Horas del personal interno (comité de seguridad), unos 2000€.

Tabla 18. Proyecto 2

Identificación del proyecto	PR-03
Nombre	Contrato CPD respaldo.
Ámbito	Organizativo y recursos humanos.
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar.
Descripción	Contratar con una empresa externa una ubicación donde poder redundar los sistemas de información para poder operar en caso de desastre. Que cumpla con los requisitos de seguridad y energéticos.
Controles	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 8. Gestión de activos. 11.1. Areas seguras. 11.2. Seguridad de los equipos. 15.1. Seguridad de la información en las relaciones con suministradores. 15.2. Gestión de la prestación del servicio por suministradores.
Coste temporal	Se estiman 1 mes de búsqueda de opciones.
Coste económico	Unos 3000€ mensuales de alquiler. Unos 500 € de coste del departamento financiero.

Tabla 19. Proyecto 3

Identificación del proyecto	PR-04
Nombre	Seguridad dispositivos para movilidad y trabajo
Ámbito	Organizativo y recursos humanos.
Activos afectados	Personal y Hardware.
Descripción	Implantación de una política formal y adopción de las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles. Redacción e implantación de una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes
Controles	6.2.1. Política de uso de dispositivos de movilidad. 6.2.2. Teletrabajo.
Coste temporal	Se estiman 1 mes.
Coste económico	Horas del personal interno (comité de seguridad), unos 1000€.

Tabla 20. Proyecto 4

Identificación del proyecto	PR-05
Nombre	Actualización de procedimiento de contratación.
Ámbito	Recursos humanos.
Activos afectados	Personal.
Descripción	La intención del proyecto es la actualización del procedimiento de contratación de personal o servicios por la compañía. La comprobación de los antecedentes de todos los candidatos a un puesto de trabajo, de los contratistas o de los terceros, se debería llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos considerados. Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deberían aceptar y firmar los términos y condiciones de su contrato de trabajo, que debería establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información. La Dirección debería exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización. Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad
Controles	7.1. Antes de la contratación. 7.2. Durante la contratación. 15.1. Seguridad de la información en las relaciones con suministradores. 15.2. Gestión de la prestación del servicio por suministradores.
Coste temporal	Se estiman 2 meses.
Coste económico	Responsable de RRHH y responsable de SI, unos 2000€.

Tabla 21. Proyecto 5

Identificación del proyecto	PR-06
Nombre	Documento del plan de continuidad de negocio.
Ámbito	Documentación.
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal..
Descripción	Es necesario la creación y formalización de un documento que garantice la continuidad de negocio, juntamente con el seguimiento del mismo apoyado de pruebas periódicas por parte de las partes que lo integran. Este plan de continuidad de negocio surge a partir del análisis de riesgos y por parte del comité de seguridad para gestionar la situación en caso de que se materialicen las amenazas sobre los activos de la organización y, mas en concreto, en aquellos activos que son más importantes para la continuidad del negocio. El plan sufrirá un seguimiento continuo por parte de las partes implicadas para evolucionar y poner en práctica el plan para afrontar de manera óptima las posibles amenazas que puedan surgir.
Controles	17.1 Aspectos de la gestión de continuidad de negocio
Coste temporal	Se estiman 6 meses.
Coste económico	Dirección y responsables de area. Unos 5000 €.

Tabla 22. Proyecto 6

Identificación del proyecto	PR-07
Nombre	Auditorías externas de seguridad.
Ámbito	Procedimiento.
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal.
Descripción	La organización ha de realizar auditorías de seguridad técnicas de forma periódica en sus sistemas para comprobar el estado en que se encuentran sus servicios. Estas auditorías deberían reflejar lo vulnerables que son sus servicios de cara a atacantes externos que intenten aprovechar los agujeros de seguridad para comprometer la confidencialidad, integridad o disponibilidad de los datos. Estas auditorías de seguridad técnicas deberían correr a cargo de una entidad externa a la organización, de manera que no disponga de información adicional sobre ella y de esta forma la auditoría se pueda ajustar más a la realidad.
Controles	18.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
Coste temporal	Se estiman 1 mes.
Coste económico	Personal externo y responsable de seguridad. Unos 4000 €.

Tabla 23. Proyecto 7

Identificación del proyecto	PR-08
Nombre	Identificación de activos e información
Ámbito	Documentación.
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal.
Descripción	Será necesario disponer de un listado de los activos de que dispone la organización, organizados según funcionalidad y ámbito al que corresponden. Junto con el listado, debería constar una descripción del activo, la función que desempeña, el ámbito al que hace referencia y el propietario, el cual será el responsable de su mantenimiento o responsable en caso de incidencia de actuar como esté definido en el documento de seguridad. Esta lista de activos deberá someterse a revisión de forma periódica para incorporar los nuevos activos que se añaden al sistema o bien para actualizarlos en caso de que alguno deje de dar soporte. La información será clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización. Se desarrollará e implantará un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización. Se desarrollará e implantará un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
Controles	8.1 Responsabilidad sobre los activos. 8.2. Clasificación de la información.
Coste temporal	Se estiman 1.5 meses.
Coste económico	Responsables de area. Unos 2000 €.

Tabla 24. Proyecto 8

Identificación del proyecto	PR-09
Nombre	Procedimiento de cumplimiento de normas y requisitos legales
Ámbito	Procedimiento.
Activos afectados	Personal.
Descripción	Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software propietario. Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales. Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes. Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes.
Controles	18.1.2. Derechos de propiedad intelectual. 18.1.3. Protección de los registros de la organización. 18.1.4. Protección de datos y privacidad de la información de carácter personal. 18.1.5. Regulación de los controles criptográficos.
Coste temporal	Se estiman 3 meses.
Coste económico	Responsables de área y dirección. Unos 3000 €.

Tabla 25. Proyecto 9

Identificación del proyecto	PR-10
Nombre	Instalación de un sistema SIEM. Procedimiento gestión de eventos de seguridad.
Ámbito	Tecnológico y procedimental.
Activos afectados	Aplicaciones, datos y servicios.
Descripción	Se realizará la instalación de un sistema SIEM que permita recoger y correlar los logs de los diferentes sistemas. Con ello se definirá una serie de reglas en base a los requerimientos de la empresa para poder gestionar la seguridad. Se definirá un procedimiento de gestión de los eventos de seguridad. Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. Los eventos de seguridad de la información se deberían notificar a través de los canales adecuados de gestión lo antes posible. Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deberían estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios. Los eventos de seguridad de la información deben ser evaluados y que se deben decidir si han de ser clasificados como incidentes de seguridad de la información. Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados. Deberían existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información. Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deberían recopilarse las evidencias, y conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.
Controles	16.1. Gestión de incidentes de seguridad de la información y mejoras.
Coste temporal	Se estiman 3 meses.
Coste económico	Empresa externa y responsable técnico. Unos 12000€

Tabla 26. Proyecto 10

Identificación del proyecto	PR-11
Nombre	Procedimiento de programación segura y pruebas del software
Ámbito	Procedimiento.
Activos afectados	Servicios, aplicaciones y datos.
Descripción	Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización. Los cambios en los sistemas dentro del ciclo de vida de desarrollo deben ser controlados por el uso de procedimientos formales de control de cambio. Cuando se cambian las plataformas que operan, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad. Las modificaciones a los paquetes de software deben ser desalentados, otros, las modificaciones necesarias y todos los cambios deben ser estrictamente controlados. Principios para sistemas seguros de ingeniería deben establecerse, documentarse, mantenerse y aplicarse a cualquier esfuerzo de implementación de sistemas de información. Programas de pruebas de aceptación y criterios relacionados deben establecerse para los nuevos sistemas de información, actualizaciones y nuevas versiones. Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados. Se define un nuevo entorno de pruebas del software para poder controlar los posibles errores y defectos que tenga el software antes de ponerse en producción. Al realizar las pruebas en un entorno especializado es posible identificar y corregir desviaciones antes de que el software se encuentre en producción, a la vez que se mitiga el impacto que estos errores puedan tener sobre los activos y recursos de la organización. Este procedimiento de pruebas debería también especificar qué usuarios tienen acceso para poder probar el software en busca de vulnerabilidades en el código. Así mismo, también se deberían especificar revisiones de estos controles para comprobar que las autorizaciones van en la misma línea de evolución que la organización.
Controles	14.2. Tratamiento correcto de las aplicaciones. 14.3. Datos de prueba.
Coste temporal	Se estiman 2 meses.
Coste económico	Personal y responsable de desarrollo. Unos 4500€

Tabla 27. Proyecto 11

Identificación del proyecto	PR-12
Nombre	Instalación de un IDS
Ámbito	Tecnológico.
Activos afectados	Instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal.
Descripción	Las principales actividades de negocio de la organización se basan en aplicaciones web, es decir, servicios orientados a usuarios externos. Es por este motivo que es necesario disponer de dispositivos que sean capaces de detectar y mitigar posibles intrusiones en el sistema antes de que causen alteración en los datos u obtengan información confidencial. Es importante analizar la actividad que se genera en la red de forma periódica para comprobar que no ha habido intrusiones no autorizadas y que dicha actividad en la red queda registrada ,para que en caso de incidente, se tengan las suficientes muestras para comprender qué fue lo sucedido y poder solucionarlo o prevenirlo en acciones futuras.
Controles	13.1 Gestión de la seguridad en las redes.
Coste temporal	Se estiman 1 mes.
Coste económico	Responsable técnico y personal externo. Unos 5000 €.

Tabla 28. Proyecto 12

4.3 Planificación

A fin de poder ir evolucionando en la adecuación de la gestión de la seguridad de la información a la norma ISO 27001:2013 se irán realizando los diferentes proyectos planteados. Si bien su ejecución no terminará por abordar y cumplir todos los apartados de la norma, si es la intención abarcar la mayor parte de apartados posibles para ir progresivamente adecuándose a la misma. Debido a los recursos necesarios para poder acometer el desarrollo e implementación de los distintos proyectos, se planificarán para ir realizándose durante dos años, si bien en caso de liberación de recursos podrían agilizarse algunos e inclusive proponer, desarrollar y evolucionar otros.

A continuación se presenta dos diagramas con la disposición temporal de proyectos en el primer año y en el segundo año:

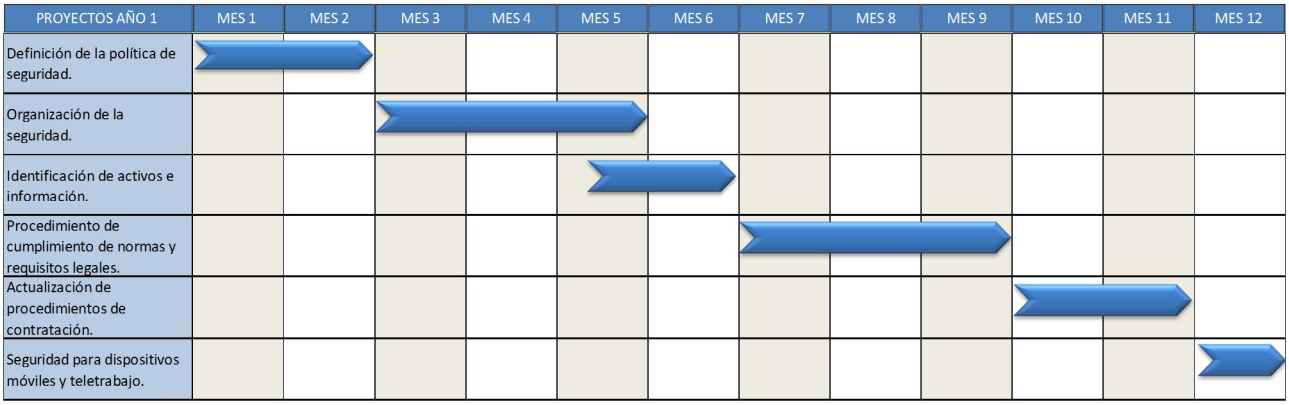

Tabla 29. Planificación de proyectos en el primer año

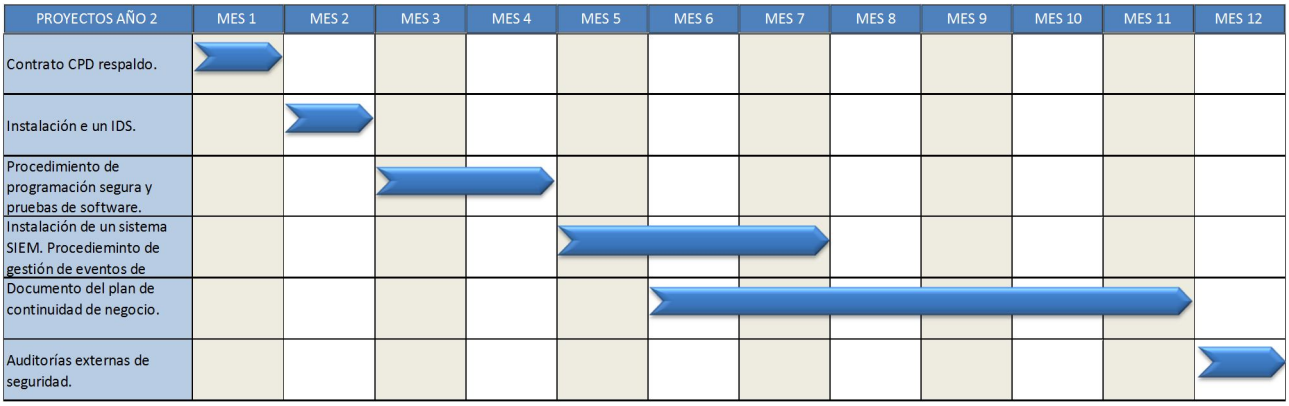

Tabla 30. Planificación de proyectos en el segundo año

4.4 Resultados

La propuesta de proyectos está alineada con un análisis del impacto sobre la seguridad. Esto comporta, que su ejecución nos debe indicar cómo evoluciona el riesgo y el impacto de materialización, así como el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002. El objetivo debe ser ir evolucionando hacia un nivel de madurez optimizado. Deberá indicarse de forma gráfica en un diagrama de radar la evolución de los diferentes dominios y su cumplimiento antes y después de la realización de los diferentes proyectos.

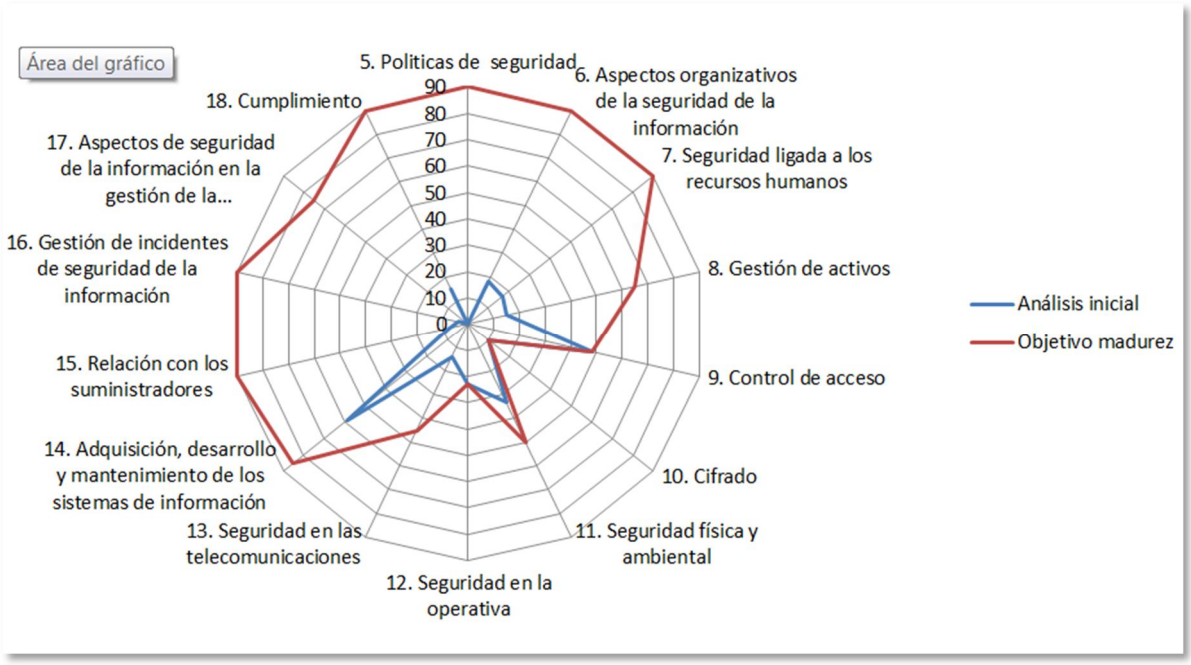

Ilustración 5. Evolución cumplimiento dominios ISO 27002:2013

Anexo 5. Plan de proyectos

Todo el contenido realizado en el plan de proyectos se presenta en una hoja de cálculo adjunta en la carpeta de anexos de la fase 4.

5 AUDITORÍA DE CUMPLIMIENTO

5.1 Introducción

Una vez realizado el análisis de activos de información de la empresa, sus amenazas y sus riesgos asociados, se plantearon y planificaron una serie de proyectos a implementar en el plazo de 2 años, que sirviesen para ir evolucionando en las distintas áreas que propone la norma ISO 27002.

La auditoría de cumplimiento analiza la evolución y estado de la gestión de la seguridad de la información en la organización. En este caso desde el nivel inicial al nivel de madurez una vez implementados los proyectos que en obligan a una evolución y revisión continua que irán optimizando el nivel de madurez en el tiempo.

Cabe destacar la importancia de estas auditorías como herramienta de análisis y revisión de la gestión de la seguridad de la información, como modo de obtener conocimiento del estado real y por lo tanto de las posibles acciones a implantar o mejorar.

5.2 Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles ISO/IEC 27002:2013 o de cualquier otro catálogo. Estos son en general:

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

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

5.3 Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los 14 dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

De forma resumida, los dominios que deben analizarse son:

- Políticas de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Cifrado.

- Seguridad física y ambiental.
- Seguridad en la operativa.
- Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relación con los suministradores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento.

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los 14 dominios. Esta estimación la realizaremos según la tabla del Modelo de Madurez de la Capacidad (CMM) que fue de la misma que se hizo uso cuando se realizó el estudio del Gap de la empresa sobre la norma.

Nota: Ver Tabla 1 del modelo CMM en el apartado 1 anexo 2 de este trabajo.

5.4 Resultados por dominios

En este apartado se presenta el estudio del nivel de madurez por cada dominio. Por tanto, se podrá apreciar el estudio gráfico de la evolución de la madurez de los 14 dominios y 114 controles de la norma ISO 27002:2013.

En una auditoría interna se lleva a cabo una revisión del cumplimiento normativo de la organización, donde se pueden identificar los diferentes tipos de desviaciones:

- *No conformidad Mayor*: Incumple un apartado completo de la norma.
- *No conformidad Menor*: Incumple un punto de un apartado.
- *Observación*: No incumple nada, es sólo una recomendación, aunque si no se trata, en la siguiente auditoría se puede convertir en *No conformidad*.

En base a estos principios se realizará el análisis de adecuación a la norma de los diferentes controles que conforman los distintos dominios que establece la norma:

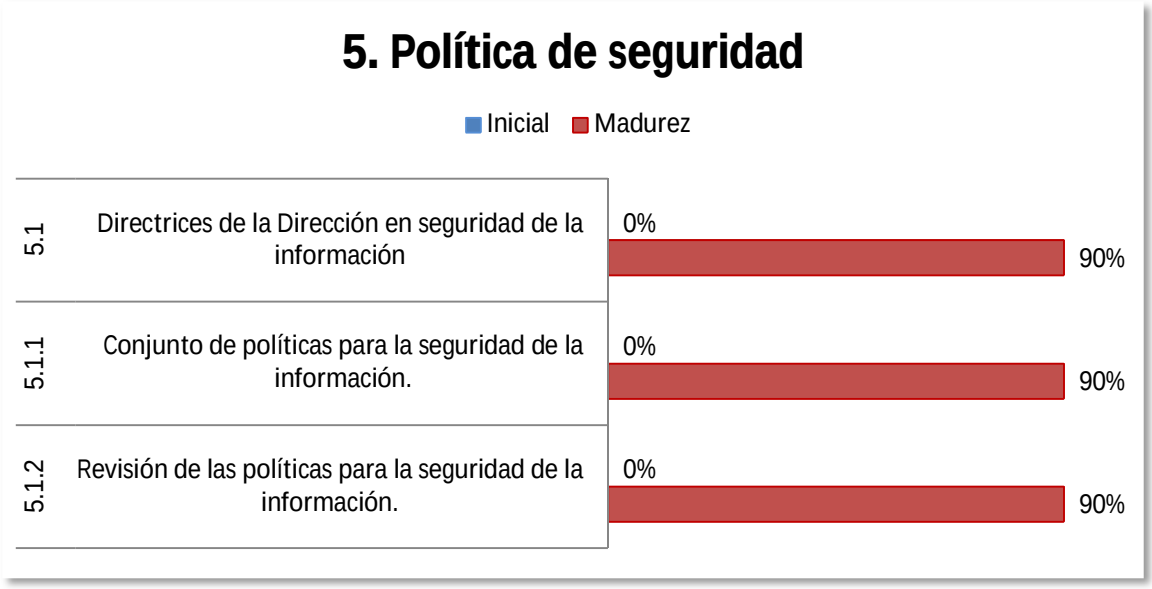

Ilustración 6. Nivel de madurez - Política de seguridad

El dominio de *Política de seguridad* ha tenido una evolución de madurez óptima, por lo tanto ha alcanzo un nivel acorde a la norma. La empresa cuanta ahora con un documento de *Política de Seguridad de la Información* al alcance de los afectados y tiene un plan de revisión de la misma.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

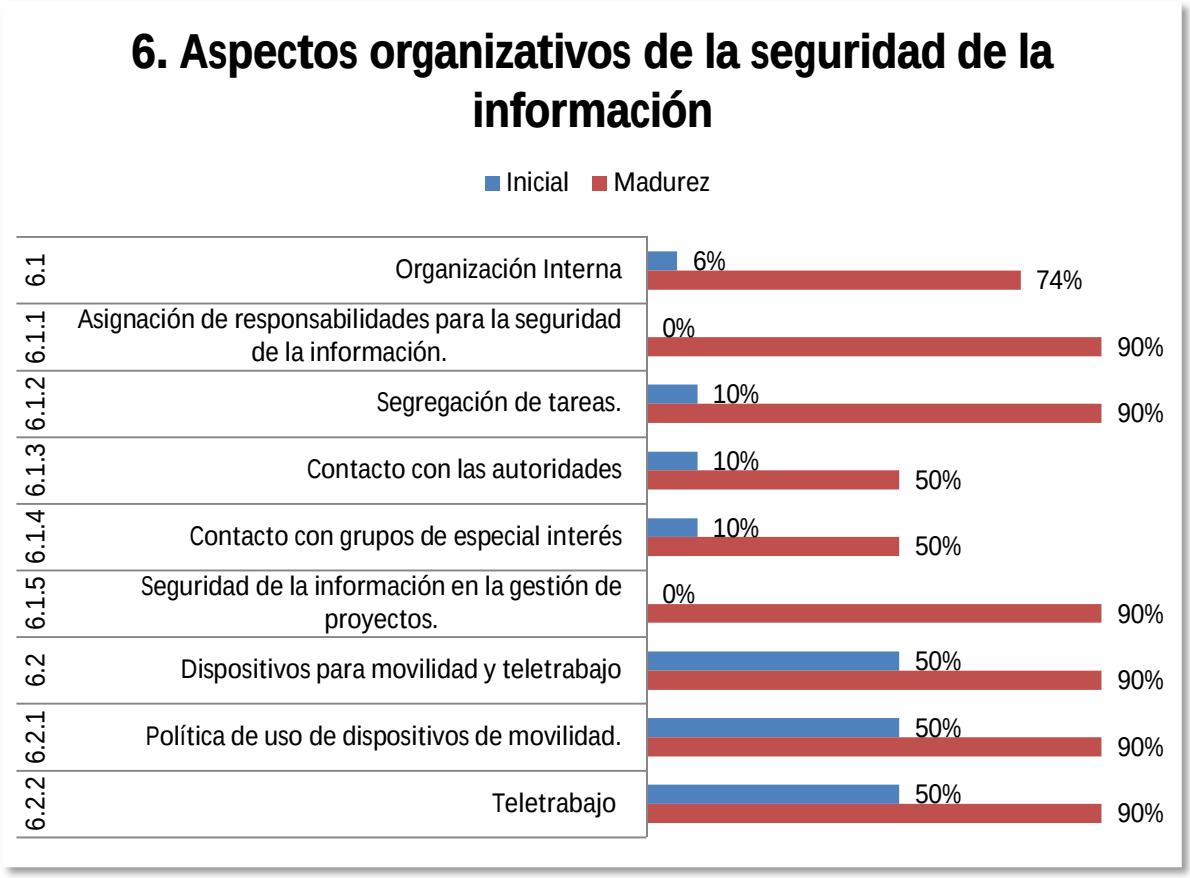

Ilustración 7. Nivel de madurez - Aspectos organizativos de la seguridad de la información

La auditoría del dominio *Aspectos organizativos de la seguridad de la información* presenta dos no conformidades menores focalizadas en la apartado 6.1 referido a la *Organización interna*. Se deberían mejorar aspectos relativos a:

- Control 6.1.3 *Contacto con las autoridades*. Deberían mantenerse los contactos adecuados con las autoridades competentes.
- Control 6.1.4 *Contactos con grupos de especial interés*. Deberían mantenerse los contactos adecuados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 6.1.1, 6.1.2 y 6.1.5.

El apartado 6.2 *Dispositivos para movilidad y trabajo* se adecúa a lo requerido en la norma, tiene un nivel correcto de madurez.

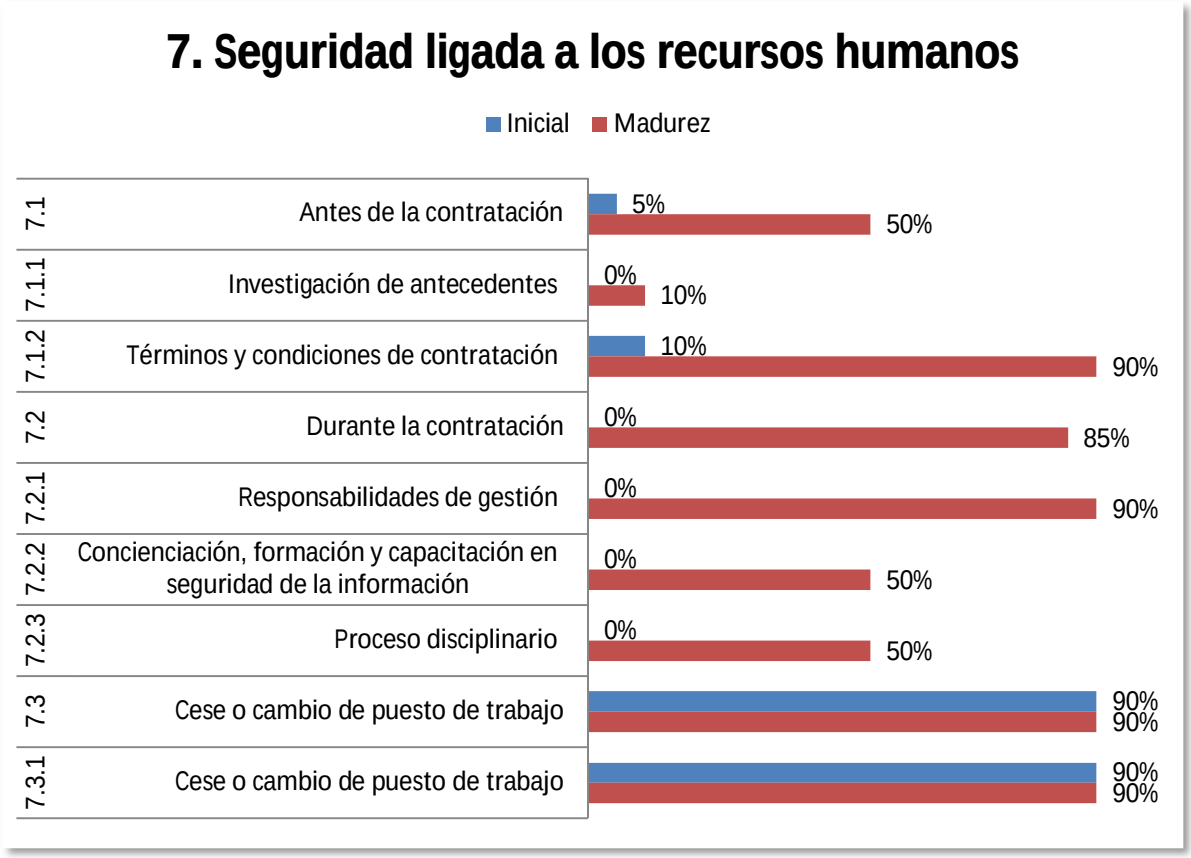

Ilustración 8. Nivel de madurez - Seguridad ligada a los recursos humanos

La auditoría del dominio *Seguridad ligada a los recursos humanos* presenta tres no conformidades menores focalizadas en:

En el apartado 7.1 *Antes de la contratación* se deberían mejorar aspectos relativos a:

- Control 7.1.1 *Investigación de antecedentes*. La comprobación de los antecedentes de todos los candidatos a un puesto de trabajo, de los contratistas o de los terceros, se debería llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos considerados.

En el apartado 7.2 *Durante la contratación* se deberían mejorar aspectos relativos a:

- Control 7.2.2 *Concienciación, formación y capacitación en seguridad de la información*. Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.
- Control 7.2.3 *Proceso disciplinario*. Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 7.1.2 y 7.2.1. El apartado 7.3 *Cese o cambio de puesto de trabajo* se adecúa a lo requerido en la norma, tiene un nivel correcto de madurez.

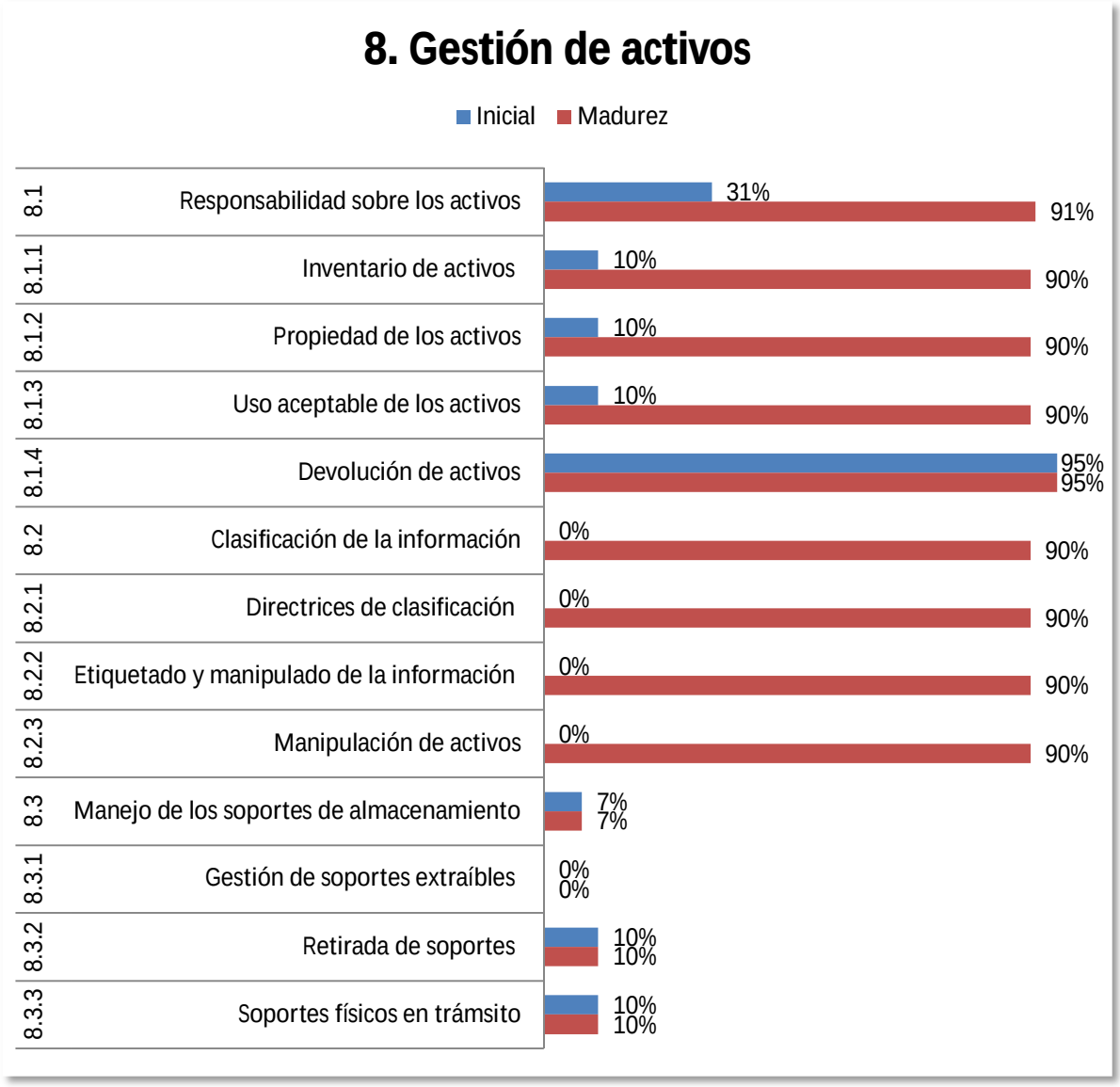

Ilustración 9. Nivel de madurez - Gestión de activos

La auditoría del dominio *Gestión de activos* presenta una no conformidad mayor en la apartado 8.3 referido a *Manejo de soportes de almacenamiento.* Se deberían mejorar aspectos relativos a:

- Control 8.3.1 *Gestión de soportes extraíbles.* Se deberían establecer procedimientos para la gestión de los soportes extraíbles.
- Control 8.3.2 *Retirada de soportes.* Los soportes deberían ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.
- Control 8.3.3 *Soportes físicos en tránsito.* Los soportes físicos en tránsito deberán ser controlados de forma segura para evitar su manipulación o daño.

Los apartados 8.1 *Responsabilidad sobre los activos* y 8.2 *Clasificación de la información* se adecúan a lo requerido en la norma, tiene un nivel correcto de madurez.

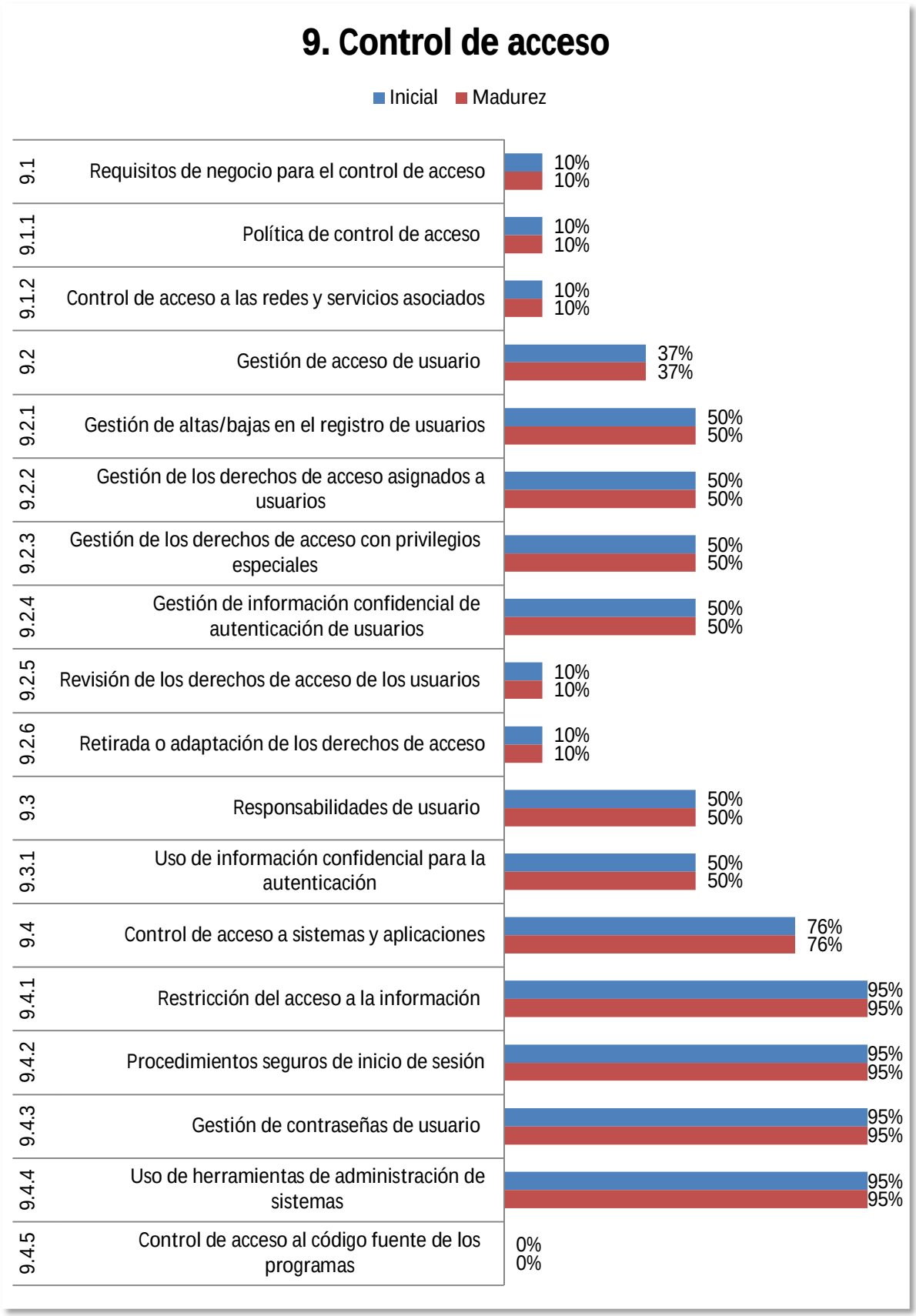

Ilustración 10. Nivel de madurez - Control de acceso

La auditoría del dominio *Control de acceso* presenta tres no conformidades mayores y una no conformidad menor que se exponen de la siguiente manera:

En el apartado 9.1 *Requisitos de negocio para el control de acceso* se deberían mejorar aspectos relativos a:

- Control 9.1.1 *Política de control de acceso*. Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.
- Control 9.1.2 *Control de acceso a las redes y servicios asociados.* Se debería establecer métodos de control de acceso a las redes y a los servicios que se soportan sobre ella.

En el apartado 9.2 *Gestión de acceso de usuario* se deberían mejorar aspectos relativos a:

- Control 9.2.1 *Gestión de altas/bajas en el registro de usuarios.* Debería establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
- Control 9.2.2 *Gestión de los derechos de acceso asignados a usuarios.* Debería establecerse un procedimiento formal de registro y de anulación de derechos de acceso asignados a usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
- Control 9.2.3 *Gestión de los derechos de acceso con privilegios especiales*. La asignación y el uso de privilegios deberían estar restringidos y controlados.
- Control 9.2.4 *Gestión de información confidencial de autenticación de usuarios.* La asignación de contraseñas debería ser controlada a través de un proceso de gestión formal.
- Control 9.2.5 *Revisión de los derechos de acceso de los usuarios.* La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.
- Control 9.2.6 *Retirada o adaptación de los derechos de acceso*. La Dirección debería retirar o adaptar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.

En el apartado 9.3 *Responsabilidades de usuario* se deberían mejorar aspectos relativos a:

- Control 9.3.1 *Uso de información confidencial para la autenticación.* Se debería requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas.

En el apartado 9.4 *Gestión de acceso de usuario* se deberían mejorar aspectos relativos:

- Control 9.4.5 *Control de acceso al código fuente de los programas.* Se debería restringir el acceso al código fuente de los programas.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 9.4.1, 9.4.2, 9.4.3 y 9.4.4.

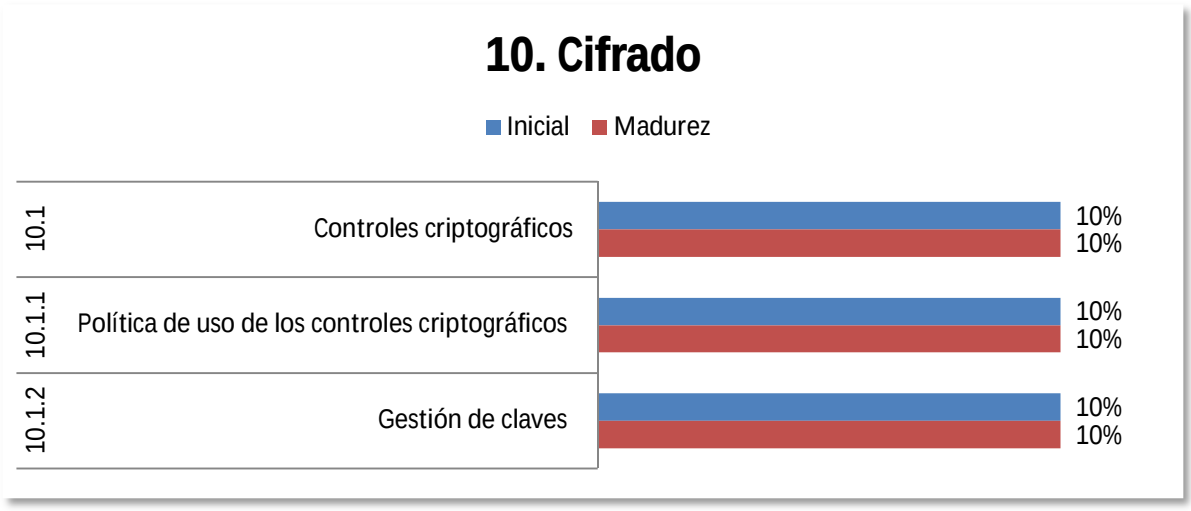

Ilustración 11. Nivel de madurez - Cifrado

La auditoría del dominio *Cifrado* presenta una no conformidad mayor debido a que no cumple ningún apartado del dominio.

En el apartado 10.1 *Controles criptográficos* se deberían mejorar aspectos relativos a:

- Control 10.1.1 *Política de uso de los controles criptográficos.* Se debería formular e implantar una política para el uso de los controles criptográficos para proteger la información.
- Control 10.1.2 *Gestión de claves.* Debería implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.

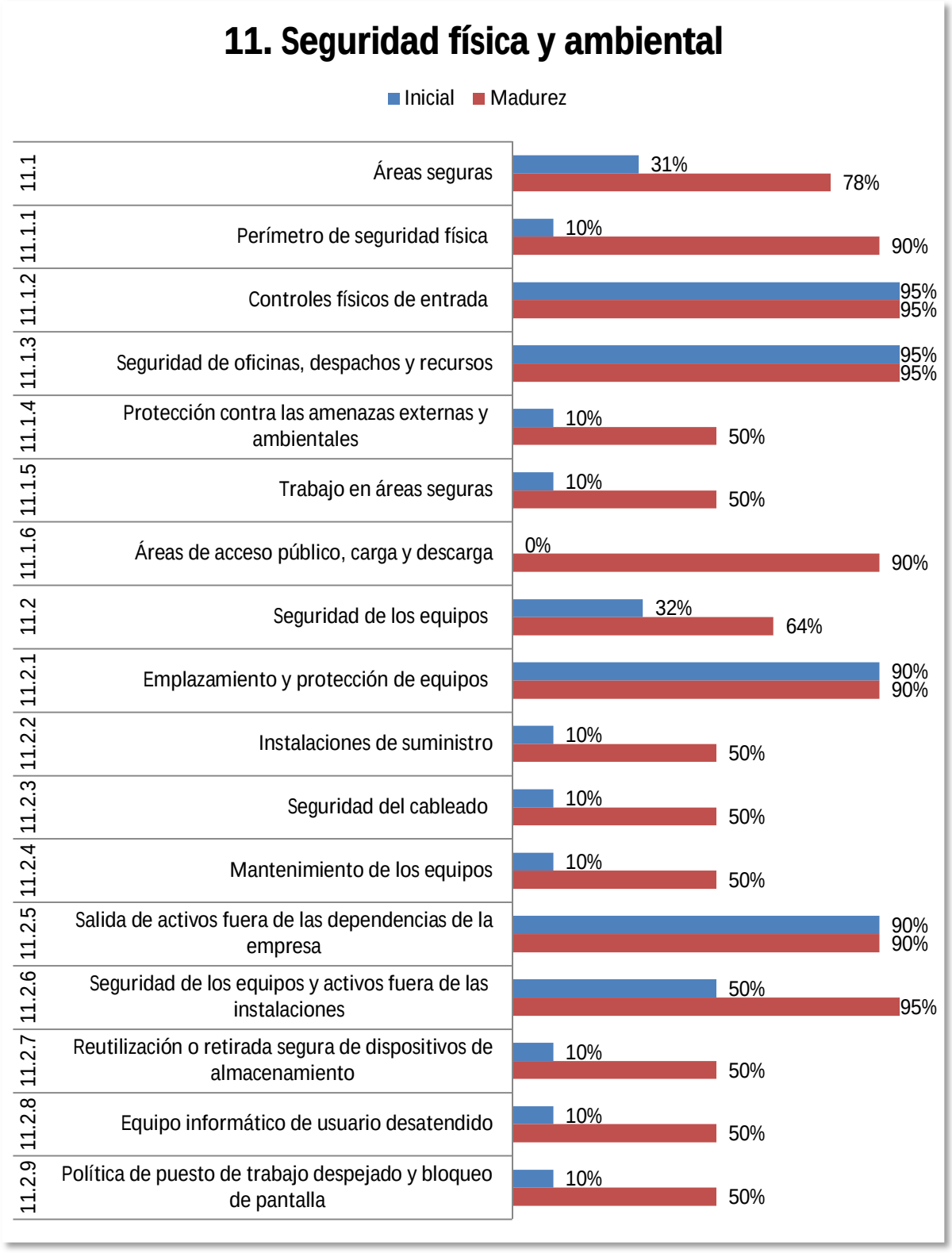

Ilustración 12. Nivel de madurez - Seguridad física y ambiental

La auditoría del dominio *Seguridad física y ambiental* presenta ocho no conformidades menores que se muestran a continuación:

En el apartado 11.1 *Áreas seguras* se deberían mejorar aspectos relativos a:

- Control 11.1.4 *Protección contra las amenazas externas y ambientales.* Se debería diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.
- Control 11.1.5 *Trabajo en áreas seguras.* Se deberían diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 11.1.1, 11.1.2, 11.1.3 y 11.1.6.

En el apartado 11.2 *Gestión de acceso de usuario* se deberían mejorar aspectos relativos a:

- Control 11.2.2 *Instalaciones de suministro.* Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.
- Control 11.2.3 *Seguridad del cableado.* El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debería estar protegido frente a interceptaciones o daños.
- Control 11.2.4 *Mantenimiento de los equipos.* Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.
- Control 11.2.7 *Reutilización o retirada segura de dispositivos de almacenamiento.* Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han borrado o sobrescrito de manera segura, antes de su retirada.
- Control 11.2.8 *Equipo informático de usuario desatendido.* Los usuarios deberían asegurarse de que el equipo desatendido tiene la protección adecuada.
- Control 11.2.9 *Política de puesto de trabajo despejado y bloqueo de pantalla.* Debería adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de tratamiento de la información.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 11.1.1, 11.1.5 y 11.2.6.

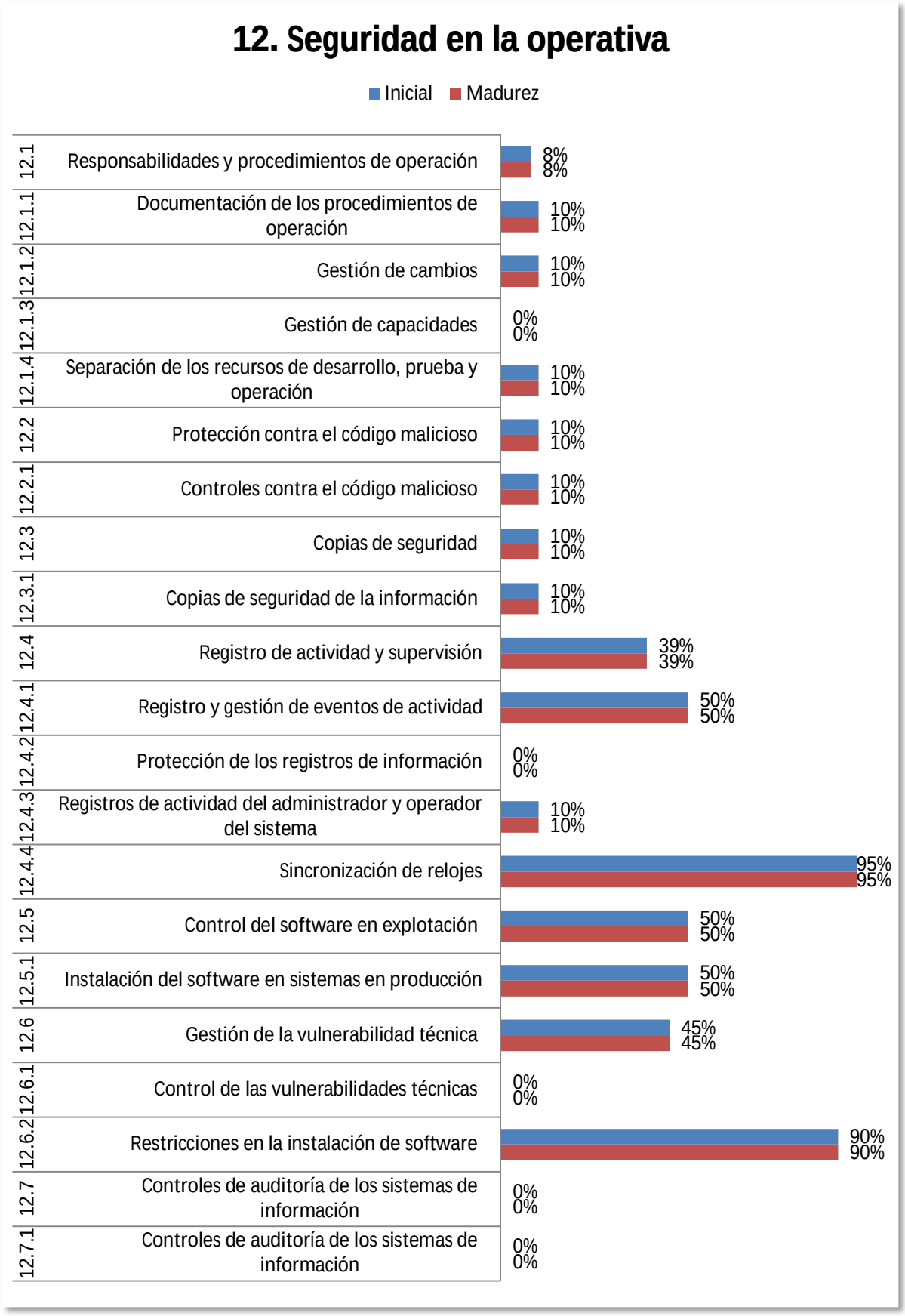

Ilustración 13. NIvel de madurez - Seguridad en la operativa

La auditoría del dominio *Seguridad en la operativa* presenta cinco no conformidades mayores y cuatro no conformidades menores de la siguiente manera:

En el apartado 12.1 *Responsabilidades y procedimientos de operación* se deberían mejorar aspectos relativos a:

- Control 12.1.1 *Documentación de los procedimientos de operación.* Deberían documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
- Control 12.1.2 *Gestión de cambios.* Deberían controlarse los cambios en los recursos y en los sistemas de tratamiento de la información.
- Control 12.1.3 *Gestión de capacidades.* La utilización de los recursos se debería supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.
- Control 12.1.4 *Separación de los recursos de desarrollo, prueba y operación.* Deberían separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema en producción.

En el apartado 12.2 *Protección contra el código malicioso* se deberían mejorar aspectos relativos a:

- Control 12.2.1 *Controles contra el código malicioso.* Se deberían implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deberían implantar procedimientos adecuados de concienciación del usuario.

En el apartado 12.3 *Copias de seguridad* se deberían mejorar aspectos relativos a:

- Control 12.3.1 *Copias de seguridad de la información.* Se deberían realizar copias de seguridad de la información y del software, y se deberían probar periódicamente conforme a la política de copias de seguridad acordada.

En el apartado 12.4 *Registro de actividad y supervisión* se deberían mejorar aspectos relativos a:

- Control 12.4.1 *Registro y gestión de eventos de actividad.* Se deberían generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberían mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.
- Control 12.4.2 *Protección de los registros de información.* Los dispositivos de registro y la información de los registros deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.
- Control 12.4.3 *Registros de actividad del administrador y operador del sistema.* Se deberían registrar las actividades del administrador y del operador del sistema.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 12.4.4.

En el apartado 12.5 *Control del software en explotación* se deberían mejorar aspectos relativos a:

- Control 12.5.1 *Instalación del software en sistemas en producción.* Deberían aplicarse procedimientos para controlar la instalación del software en los sistemas operativos.

En el apartado 12.6 *Gestión de la vulnerabilidad técnica* se deberían mejorar aspectos relativos a:

- Control 12.6.1 *Control de las vulnerabilidades técnicas.* Se debería obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: el punto 12.6.2.

En el apartado 12.7 *Controles de auditoría de los sistemas de información* se deberían mejorar aspectos relativos a:

- Control 12.7.1 *Controles de auditoría de los sistemas de información.* Se debería obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

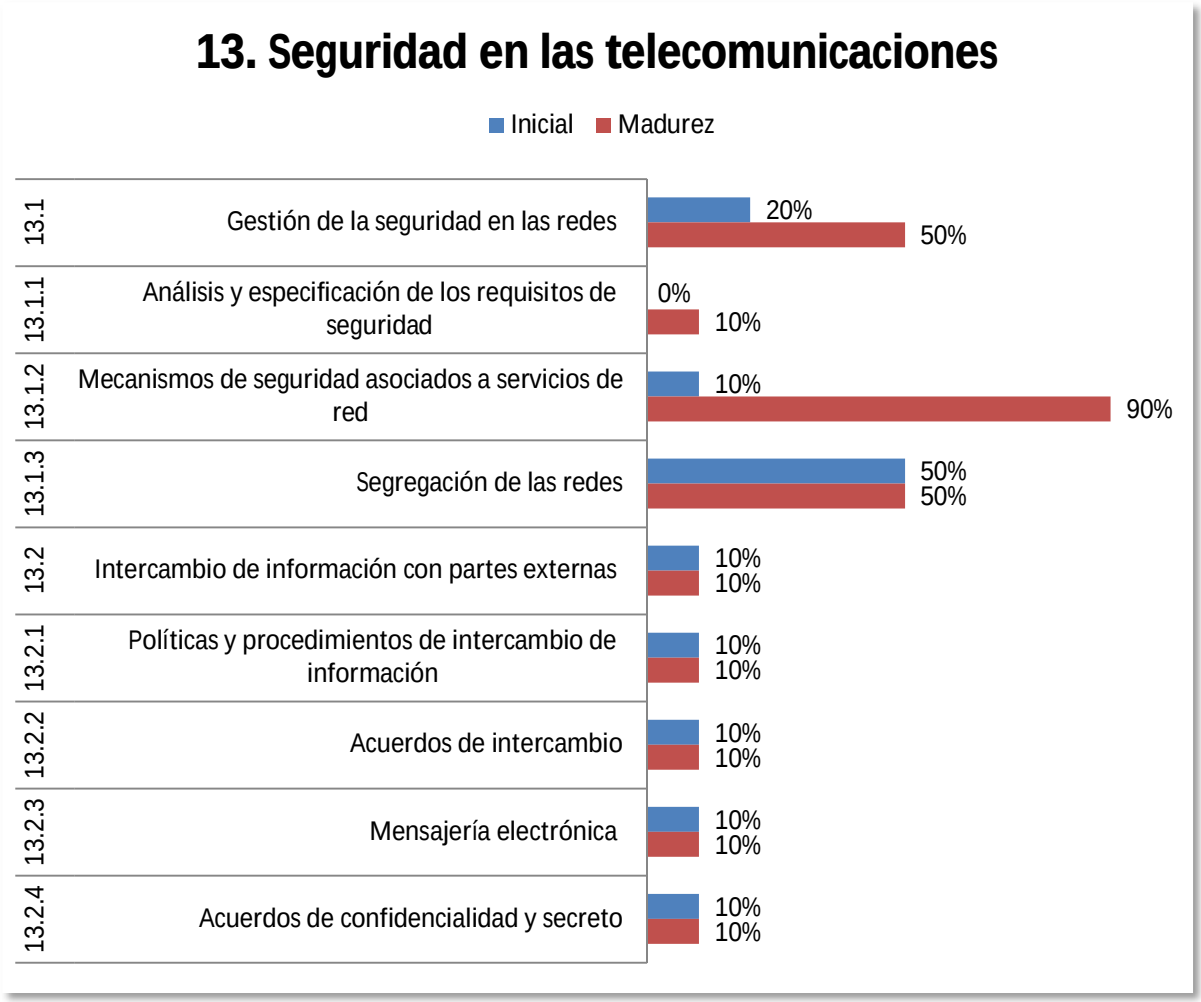

Ilustración 14. Nivel de madurez - Seguridad en las telecomunicaciones

La auditoría del dominio *Seguridad en las telecomunicaciones* presenta una no conformidad mayor y dos no conformidades menores debido a que no cumple algún apartado del dominio aunque sí lo hace en algunos de sus controles:

En el apartado 13.1 *Gestión de la seguridad en las redes* se deberían mejorar aspectos relativos a:

- Control 13.1.1 *Análisis y especificación de los requisitos de seguridad*. En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deberían especificar los requisitos de los controles de seguridad.
- Control 13.1.3 *Segregación de las redes*. Los grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: el punto 13.1.2.

En el apartado 13.2 *Intercambio de información con partes externas* se deberían mejorar aspectos relativos a:

- Control 13.2.1 *Políticas y procedimientos de intercambio de información*. Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
- Control 13.2.2 *Acuerdos de intercambio*. Deberían establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros.
- Control 13.2.3 *Mensajería electrónica*. La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.
- Control 13.2.4 *Acuerdos de confidencialidad y secreto*. Deberían formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales.

Ilustración 15. Nivel de madurez - Adquisición, desarrollo y mantenimiento de los sistemas de información

La auditoría del dominio *Adquisición, desarrollo y mantenimiento de los sistemas de información* presenta dos no conformidades menores focalizadas en:

En el apartado 14.1 *Requisitos de seguridad de los sistemas de información* se deberían mejorar aspectos relativos a:

- Control 14.1.1 *Análisis y especificación de los requisitos de seguridad*. Los requisitos relacionados con la seguridad de la información deben ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 14.1.2 y 14.1.3.

En el apartado 14.2 *Tratamiento correcto de las aplicaciones* se deberían mejorar aspectos relativos a:

- Control 14.2.1 *Política de desarrollo seguro de software*. Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización..

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8 y 14.2.9.

El apartado 14.3 *Datos de prueba* se adecúa a lo requerido en la norma, tiene un nivel correcto de madurez.

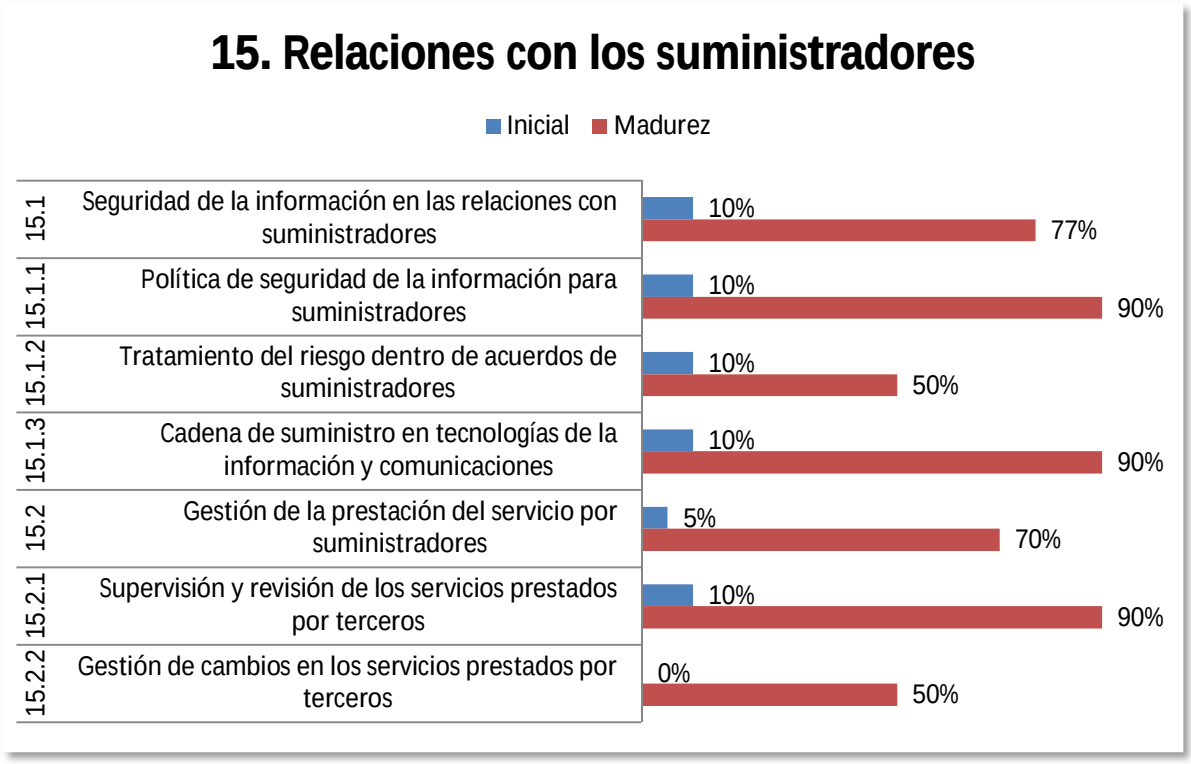

Ilustración 16. Nivel de madurez - Relaciones con los suministradores

La auditoría del dominio *Relaciones con los suministradores* presenta dos no conformidades menores debido a que no cumple algunos de sus controles:

En el apartado 15.1 *Seguridad de la información en las relaciones con suministradores* se deberían mejorar aspectos relativos a:

- Control 15.1.2 *Tratamiento del riesgo dentro de acuerdos de suministradores.* Deberían tratarse todos los requisitos de seguridad identificados, antes de otorgar acceso a los clientes a los activos o a la información de la organización.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 15.1.1 y 15.1.3.

En el apartado 15.2 *Gestión de la prestación del servicio por suministradores* se deberían mejorar aspectos relativos a:

- Control 15.2.2 *Gestión de cambios en los servicios prestados por terceros.* Se deberían gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la re-evaluación de los riesgos.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: el punto 15.2.1.

Ilustración 17. Nivel de madurez - Gestión de incidentes de seguridad de la información

El dominio de *Gestión de incidentes de seguridad de la información* ha tenido una evolución de madurez óptima, por lo tanto ha alcanzo un nivel acorde a la norma. Se han implementado convenientemente los 7 controles que establece el apartado *Gestión de incidentes de seguridad de la información y mejoras.*

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

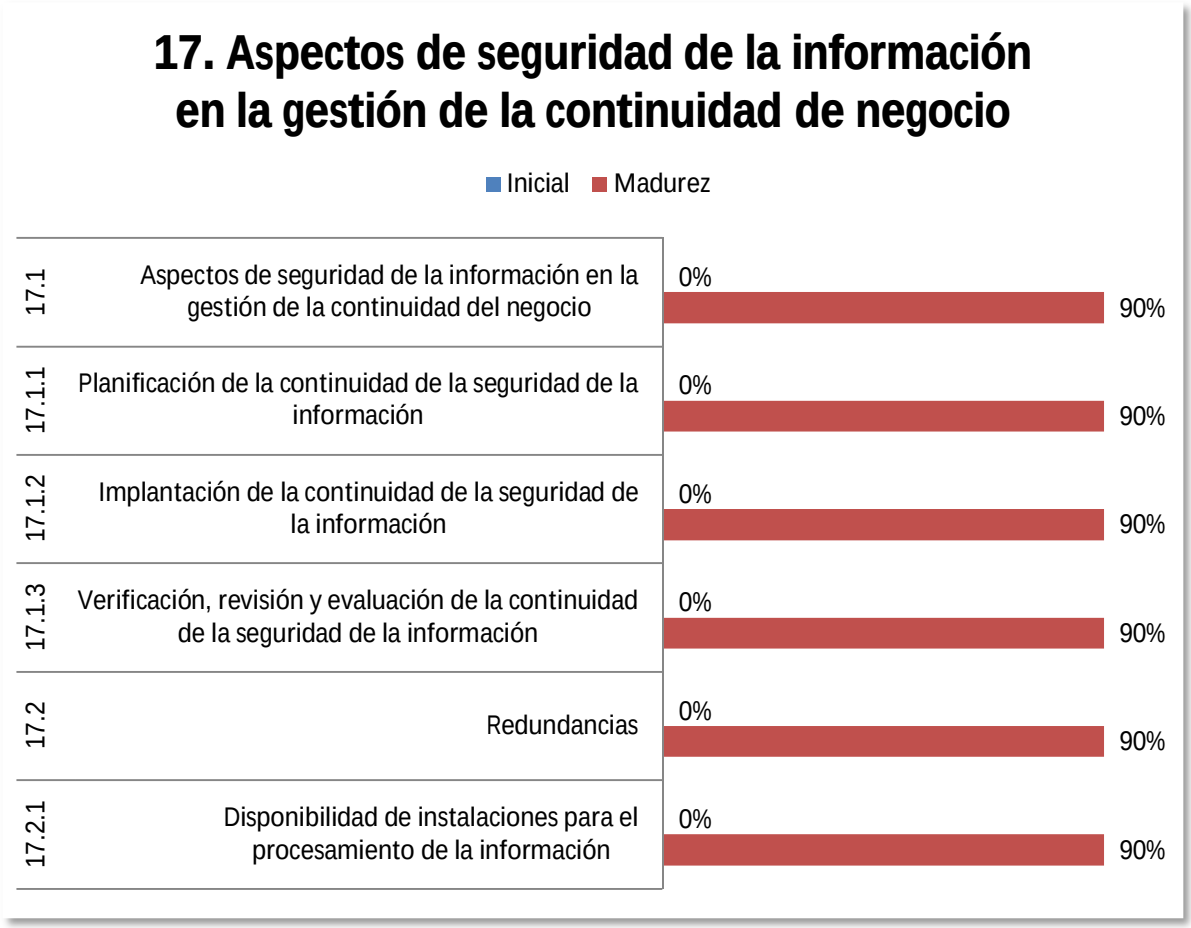

Ilustración 18. Nivel de madurez - Aspectos de seguridad de la información en la gestión de la continuidad de negocio

El dominio de *Aspectos de seguridad de la información en la gestión de la continuidad de negocio* ha tenido una evolución de madurez óptima, por lo tanto ha alcanzo un nivel acorde a la norma. Se han implementado convenientemente todos controles que establece el apartado *Aspectos de seguridad de la información en la gestión de la continuidad del negocio* y *Redundancias.*

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

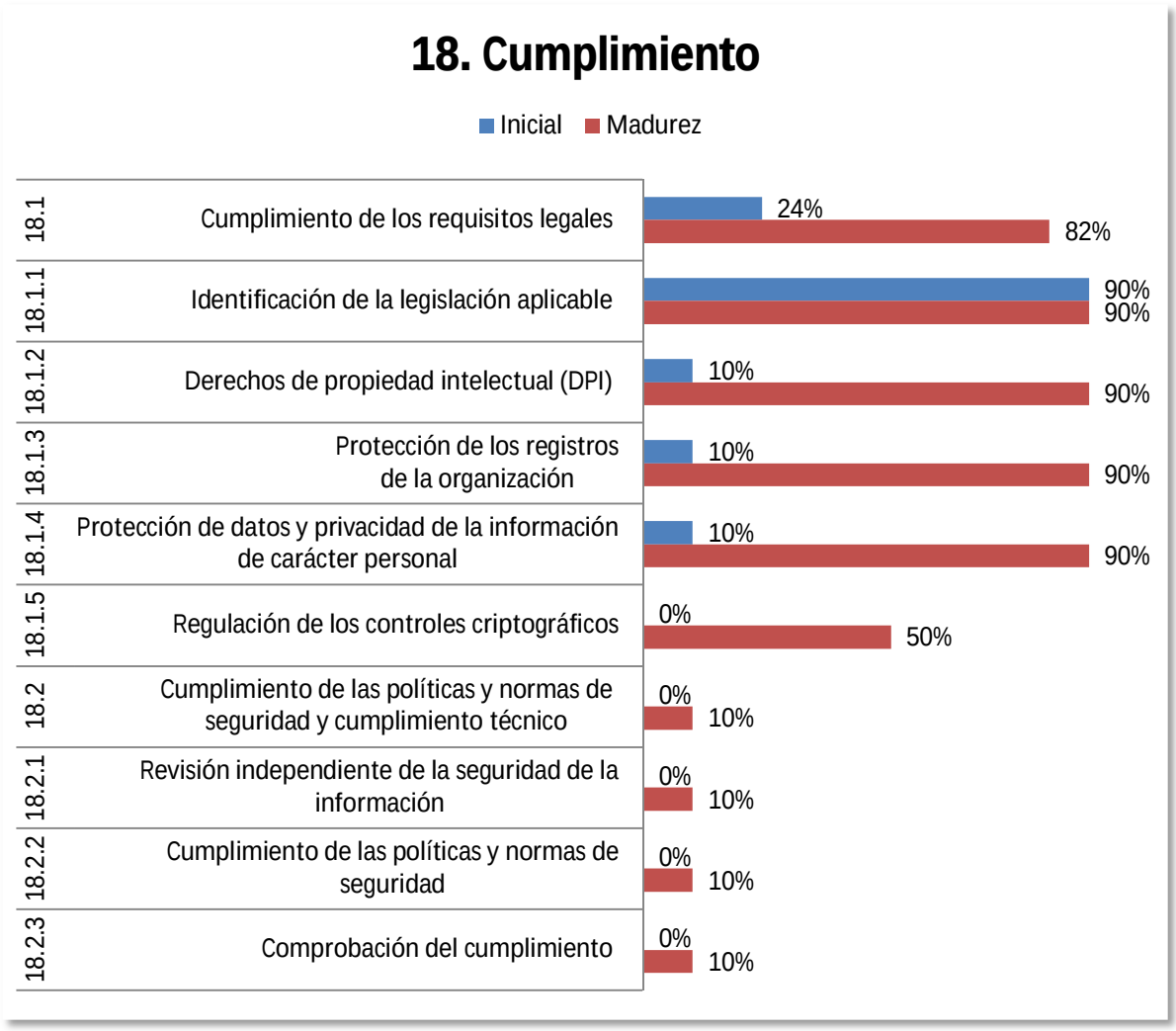

Ilustración 19. Nivel de madurez - Cumplimiento

La auditoría del dominio *Cumplimiento* presenta una no conformidad mayor y una no conformidad menor debido a:

En el apartado 18.1 *Cumplimiento de los requisitos legales* se deberían mejorar aspectos relativos a:

- Control 18.1.5 *Regulación de los controles criptográficos*. Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y reglamentaciones pertinentes.

Como observaciones comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo: los puntos 18.1.1, 18.1.2, 18.1.3 y 18.1.4.

En el apartado 18.2 *Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico* se deberían mejorar aspectos relativos a:

- Control 18.2.1 *Revisión independiente de la seguridad de la información*. Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas en producción deberían ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos del negocio.
- Control 18.2.2 *Cumplimiento de las políticas y normas de seguridad*. Los directores deberían asegurarse de que todos los procedimientos de seguridad dentro de su área de

responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.

- Control 18.2.3 *Comprobación del cumplimiento*. Debería comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación para la implantación.

Como resumen final del análisis de la auditoría de cumplimiento se presenta de modo gráfico el cómputo general de no conformidades mayores, menores y observaciones por dominio:

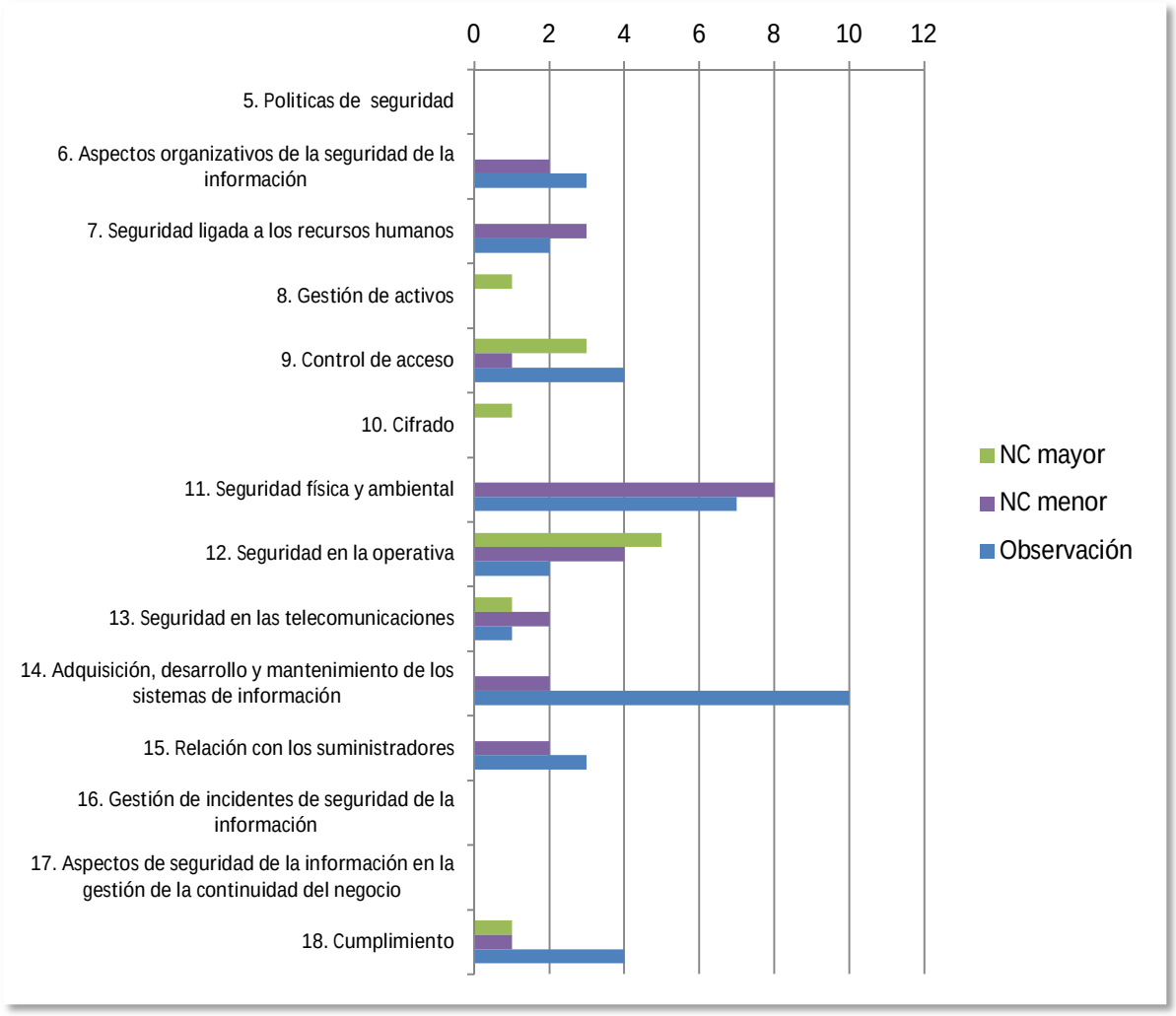

Ilustración 20. Cuadro-resumen no conformidades

Igualmente se presenta de forma gráfica la relación entre el número total de controles por dominio y el número de que han cumplido con el requerimiento de la norma:

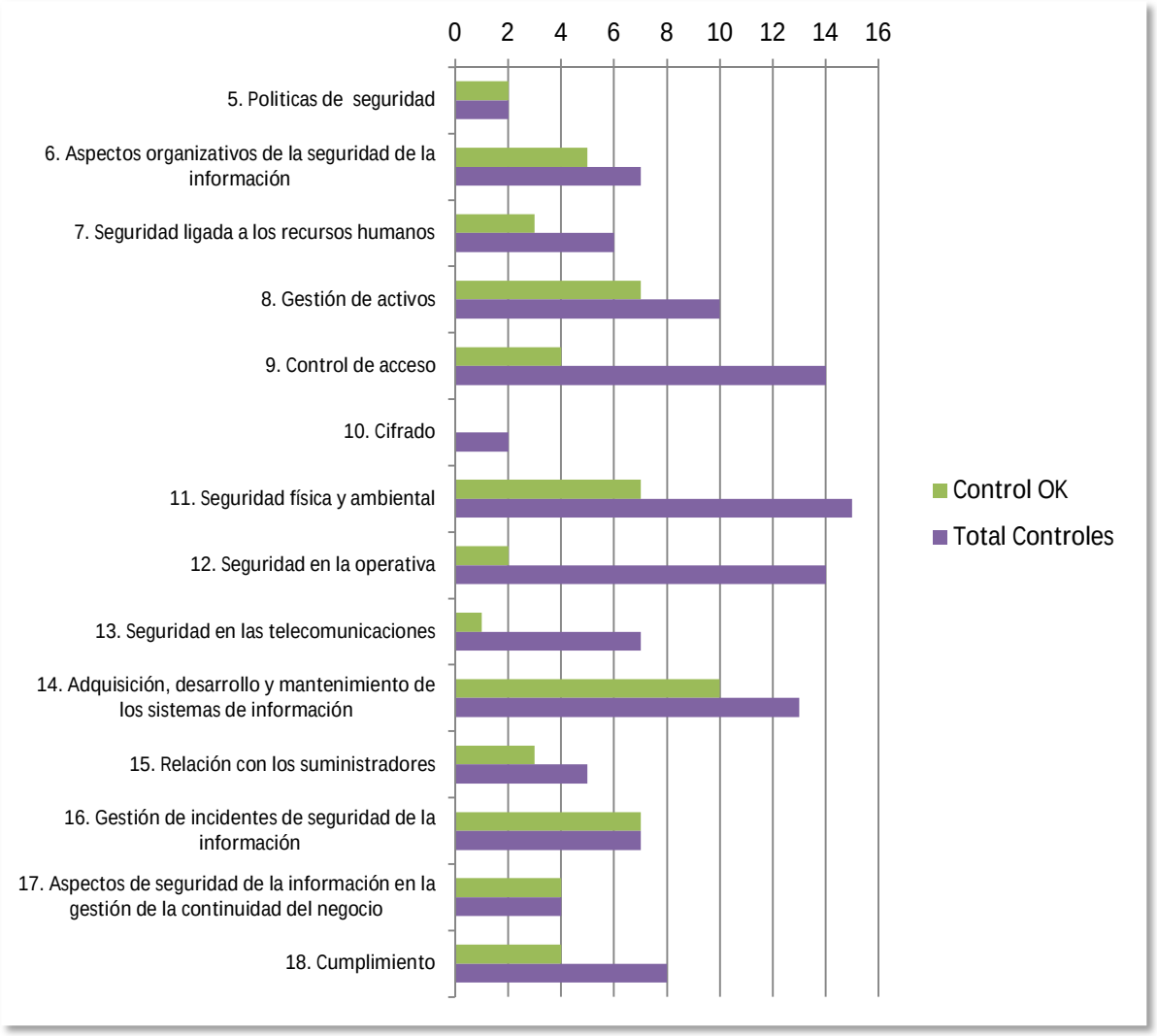

Ilustración 21. Relación-resumen de cumplimiento controles norma ISO 27002

5.5 Resultados globales

De una forma más sintetizada se presenta un diagrama donde se puede apreciar el grado porcentual de madurez en base a los 114 controles de la norma ISO 27002 y de los niveles de madurez basados en CMM. De esta forma podemos, de una manera rápida y global, evaluar el estado de la seguridad en su conjunto.

En líneas generales podemos ver que el plan de proyectos aplicado ha elevado a un nivel bastante aceptable en grado de seguridad, aunque aun ha de evolucionar hasta llegar a los niveles óptimos.

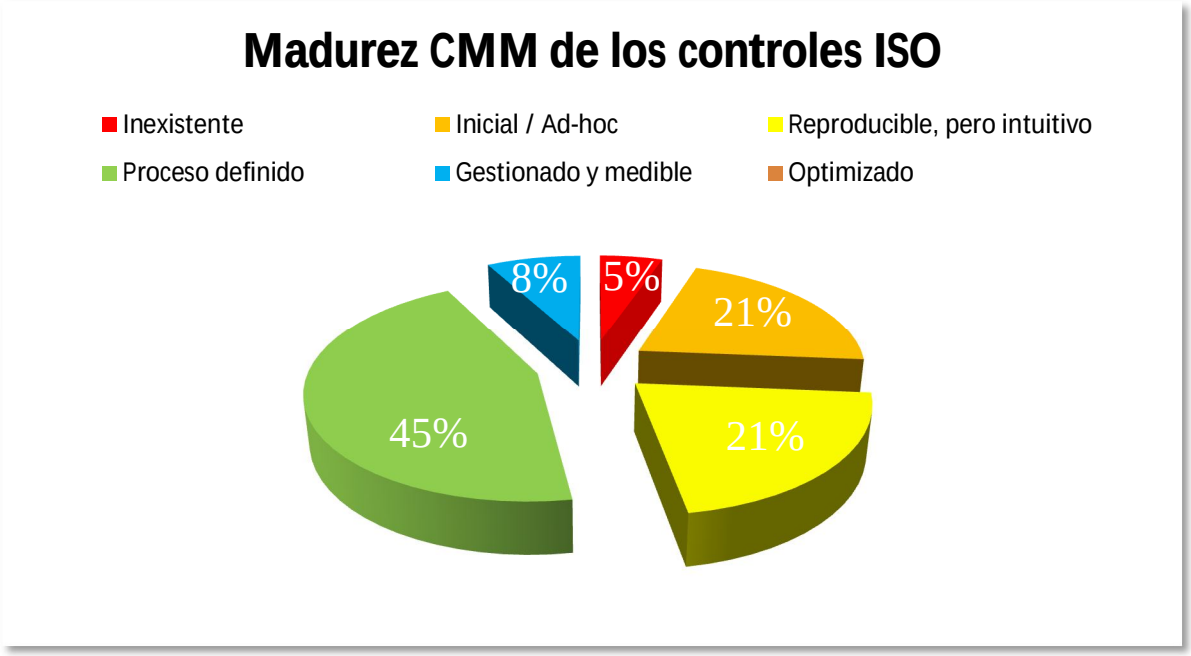

Ilustración 22. Madurez CMM de los controles ISO

En cuanto al grado de madurez basado en los 14 dominios del código de buenas prácticas que facilita la norma ISO/IEC 27002:2013 tenemos los siguientes resultados:

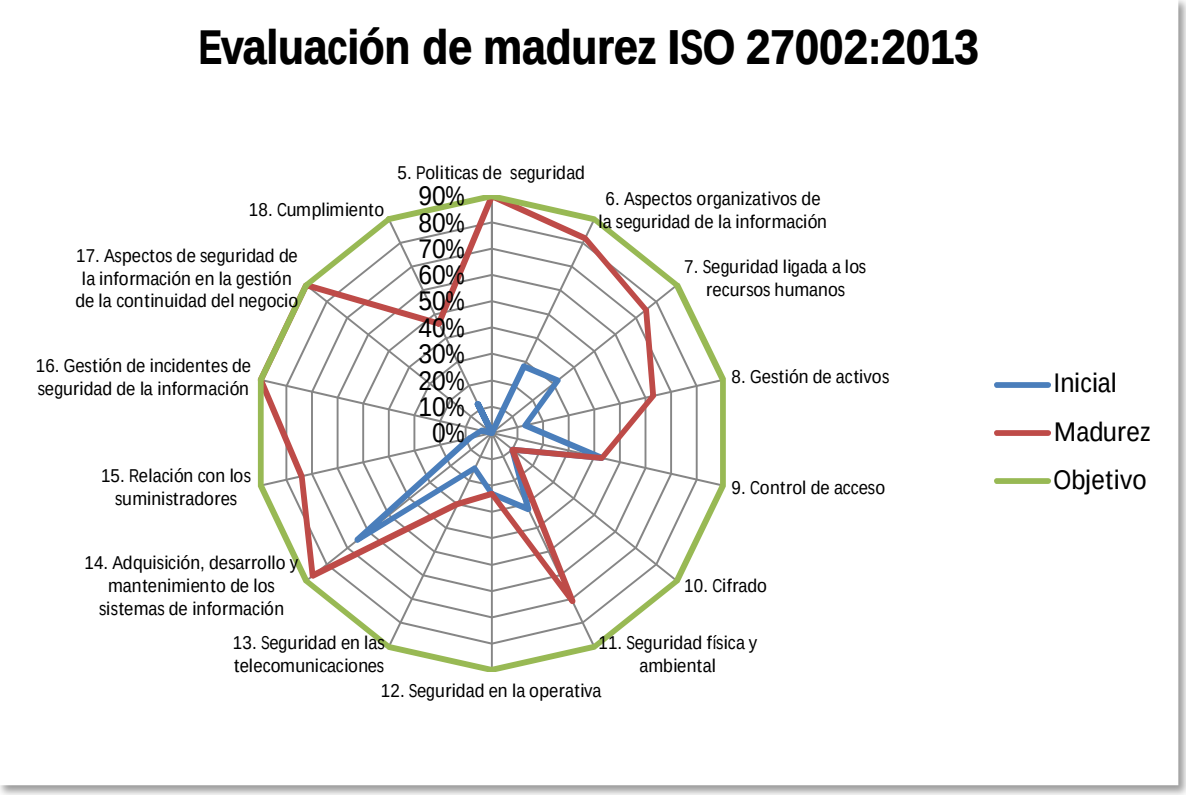

Ilustración 23. Evaluación de madurez ISO 27002:2013

Anexo 6. Evolución madurez controles ISO 27002-2013

En la carpeta de anexos que hace referencia a este apartado se encuentra una hoja de cálculo con todas las tablas de cálculo, evaluación e los controles en el nivel anterior uy posterior a la ejecución del plan de proyectos, además de distintas gráficas específicas de cada dominio y generales.

6 CONCLUSIONES

La realización de este trabajo ha servido para tomar conciencia de la importancia que tiene la gestión de los sistemas de información en la actualidad. Las organizaciones y las empresas pueden utilizar esta norma ISO 27001:2013 como base para desarrollar un análisis profundo de su estado en materia de gestión de la seguridad y evolucionar en consecuencia.

ISO 27001 conforma un marco de trabajo para definir un SGSI, centrándose en la visión de la gestión de la seguridad como algo continuo en el tiempo. Es imprescindible analizar y gestionar los riesgos a los que se expone una organización en relación a sus diferentes procesos. Al tiempo que hemos identificado los riesgos, es importante establecer la estrategia a tomar para cada uno de ellos, ya sea traspasar el riesgo a terceros, por ejemplo mediante pólizas de seguros; evitar el riesgo, abandonando la actividad que lo genera cuando el riesgo exceda a los beneficios que aporta; asumir el riesgo, cuando el establecimiento de las medidas supere el coste que pueda suponer la materialización del mismo; gestionar el riesgo, mediante medidas que mitiguen el riesgo, reduciendo la probabilidad de que se materialicen las consecuencias que de éste puedan resultar.

6.1 Objetivos alcanzados

El desarrollo e implementación de este Plan Director de Seguridad de la Información ha mejorado notablemente el nivel que existía en la empresa en materia de seguridad.

Ahora se cuenta con un análisis real de la empresa, en base a la norma ISO 27001:2013, sobre el que ir trabajando y mejorando de manera continuada.

Se ha definido el alcance del SGSI respecto a la compañía para definir aquellos procesos organizativos y funcionales a los que debe afectar el sistema de gestión por ser contenedores activos de información que requieren ser protegidos.

Se ha establecido una metodología de gestión de la seguridad clara y estructurada. Se han generado los diferentes documentos o procedimientos que establece la norma:

- Política de seguridad
- Procedimiento de auditorías internas
- Gestión de indicadores
- Procedimiento de revisión de la dirección
- Gestión de roles y responsabilidades
- Metodología de análisis de riesgos
- Declaración de aplicabilidad

Se ha hecho un inventario de activos actualizado y se ha analizado y detallado este inventario. Se ha identificado a los propietarios de cada activo, su valoración cuantitativa y también criticidad por activo en referencia a las cinco dimensiones de seguridad.

Se ha hecho un estudio, en base a la metodología Magerit, de las amenazas a las que están expuestos dichos activos. Igualmente se ha hecho un estudio de su impacto potencial de esas amenazas en los activos. Se ha identificado al propietario del riesgo.

Con estos datos y ayudado del código de buenas prácticas que establece la norma ISO 27002:2013 se ha realizado un plan de acción con un listado de proyectos cuya ejecución mejorarían el nivel de seguridad de esos activos hasta un nivel aceptado por la dirección de la compañía, el llamado riesgo residual.

El plan de auditorías internas de cumplimiento nos servirá para obtener una fotografía del estado nivel de evolución del SGSI en la compañía, como medio para poder lograr a medio plazo una adecuación total y tener la opción de optar a la certificación en la norma ISO 27001:2013.

Aunque hay muchos aspectos que cubrir y otros que mejorar, se ha podido comprobar desde que se comenzó el trabajo hasta este punto final que ha habido una evolución y una madurez notable en la compañía respecto a la gestión de la seguridad de la información, lo que vaticina que si sigue en esta línea vaya a lograr cumplir completamente con los requerimientos de la norma ISO 27001.

6.2 Objetivos futuros

Se debe seguir trabajando en mantener en nivel de madurez en aquellos dominios que ya cumplen con los requisitos de la norma.

Se debe realizar un plan de acción con un conjunto de proyectos que sirvan para ir madurando aquellos dominios que están todavía en unos niveles de incumplimiento respecto a la norma. Si bien es cierto que al ser una empresa pequeña, no es posible dedicar recursos físicos y económicos suficientes para poder alcanzar los objetivos a corto plazo. El proceso irá evolucionando en el tiempo hasta al proceso de evolución continua que mantenga el nivel adecuado de madurez se le vayan agregando el resto de apartados y dominios que establece la norma.

Se deberá incidir de manera intensa en llevar a cabo el cumplimiento de los controles asociados a los dominios cuyo grado de madurez es aún muy bajo e insistir y potenciar aquellos controles que dotarían de un nivel óptimo a aquellos dominios de la norma que están en una fase mejorada de madurez.

Para concluir, comentar por su gran importancia hacer que la gestión de la seguridad sea un elemento transversal en la compañía y todos los recursos humanos de la misma se hagan valedores de ella en su día a día.

Anexo 7. Presentación e informe ejecutivo.

Este documento *Memoria del proyecto* engloba la parte fundamental del trabajo realizado, contemplando todas las fases realizadas del mismo: su definición, análisis y estudio. De él se ha nutrido y ha nutrido al resto de documentos y hojas de cálculo que conforman los distintos anexos.

En esta última fase, dentro de la carpeta Anexos fase 6 se incluye dos entregas:

1. *Informe ejecutivo* que incluye una breve descripción de la motivación, enfoque y principales conclusiones extraídas del proyecto.
2. *3 Presentaciones* que muestran la descripción de la compañía, la importancia del SGSI y la motivación para acometer un plan director de seguridad de la información. También se expondrá el estado de salud de la seguridad en relación al cumplimiento y grado de madurez de los controles que establece la norma. De este análisis surgirán los distintos proyectos a acometer dentro de un plan de acción a realizar en un periodo de tiempo determinado. Finalmente se presentarán los resultados obtenidos tras desarrollar e implementar los proyectos. Con ello obtendremos el nivel de adecuación a la norma y los puntos pendientes a resolver para adecuarse completamente, estableciendo los objetivos alcanzados y aquellas tareas que quedan pendientes de realizar.

7 APÉNDICES

7.1 Glosario

-A-

Acción correctiva (Inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva (Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo (Inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.

Activo (Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance (Inglés: Scope). Ámbito de la organización que queda sometido al SGSI.

Amenaza (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos (Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo (Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo (Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditor (Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditor de primera parte (Inglés: First party auditor). Auditor interno que audita la organización en nombre de ella misma.

Auditor de segunda parte (Inglés: Second party auditor). Auditor que audita una organización en nombre de otra. Por ejemplo, cuando una empresa audita a su proveedor de outsourcing, o cuando una administración pública ordena una auditoría de una empresa.

Auditor de tercera parte (Inglés: Third party auditor). Auditor que audita una organización en nombre de una tercera parte independiente que emite un certificado de cumplimiento.

Auditor jefe (Inglés: Lead auditor). Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría acordado.

Auditoría (Inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación (Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad (Inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.

-B-

BS 7799 Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de éstos últimos.

BSI British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de AENOR en España.

-C-

CID (Inglés: CIA). Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

Checklist Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

CobiT Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección (Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

Confidencialidad (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control correctivo (Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo (Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio (Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Control preventivo (Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Corrección (Inglés: Correction). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

-D-

Declaración de aplicabilidad (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Desastre (Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz (Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

-E-

ENAC Entidad Nacional de Acreditación. Es el organismo español de acreditación, auspiciado por la Administración, que acredita organismos que realizan actividades de evaluación de la conformidad, sea cual sea el sector en que desarrollen su actividad. Además de laboratorios, entidades de inspección, etc., también acredita a las entidades de certificación, que son las que a su vez certificarán a las empresas en las diversas normas.

Entidad de acreditación (Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

Entidad de certificación (Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Entidad de normalización (Inglés: Standards body). Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

Estimación de riesgos (Inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Evaluación de riesgos (Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

Evidencia objetiva (Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos

relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

-F-

Fase 1 de auditoría (Inglés: Stage 1 Audit). Etapa de la auditoría de primera certificación en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.

Fase 2 de auditoría (Inglés: Stage 2 Audit). Etapa de la auditoría de primera certificación en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo eficaz.

-G-

Gestión de claves (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos (Inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

-H-

Humphreys, Ted Experto en seguridad de la información y gestión del riesgo, considerado "padre" de las normas BS 7799 e ISO 17799 y, por tanto, de ISO 27001 e ISO 27002.

-I-

Identificación de riesgos (Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

IEC International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Impacto (Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Incidente de seguridad de la información (Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad (Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos (Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799 Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

ISO 19011 "Guidelines for auditing management systems". Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.

ISO/IEC 27001 Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002 Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ISO 9001 Norma que establece los requisitos para un sistema de gestión de la calidad.ISSAInformation Systems Security Association.

ITIL IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

-N-

NIST (ex NBS) Instituto Nacional de Normas y Tecnología, con sede en Washington, D.C.

No conformidad (Inglés: Nonconformity). Incumplimiento de un requisito.

No repudio Según [CCN-STIC-405:2006]: El no repudio es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

-O-

Objetivo (Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

-P-

Parte interesada (Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PDCA Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de continuidad del negocio (Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado (Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso (Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del riesgo (Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

-R-

Recursos de tratamiento de información (Inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo (Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual (Inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo.

-S-

Sarbanes-Oxley Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

SC27 Subcomité 27 del JTC1 (Joint Technical Committee) de ISO e IEC. Se encarga del desarrollo de los estándares relacionados con técnicas de seguridad de la información..

Segregación de tareas (Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información (Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles (Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI (Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información (Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

SoA Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

-T-

Tratamiento de riesgos (Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad (Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

-V-

Vulnerabilidad (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7.2 Bibliografía

- **Norma ISO/IEC 27001:2013**
- **Norma ISO/IEC 27002:2013**
- **MAGERIT – versión 3.0**: Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones
  - Libro I – Método.
  - Libro II - Catálogo de Elementos.
  - Libro III - Guía de Técnicas.
- **Sistema de gestión de la seguridad de la información** (Silvia Garre Guí y Daniel Cruz Allende) – Material docente de la UOC.

7.3 Enlaces

- **Nueva ISO 27001:2013**

https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/nueva_version_iso27001

- **Portal sobre SGSI**

http://www.pmg-ssi.com/category/iso-270012013/

- **Portal sobre ISO 27001**

http://www.iso27001standard.com/

- **ISO 27001. Origen e historia**

http://www.pmg-ssi.com/2013/12/iso27001-origen/

- **Artículo sobre ISO 27002:2013**

http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

- **Evolución histórica de la norma ISO/IEC 27001**

http://www.it360.es/infografia-iso27001-historia-familia-normas-ISO-27000.php

- **British Estándar Institution**

http://es.wikipedia.org/wiki/British_Standards_Institution

- **Glosario de términos**

http://www.iso27000.es/glosario.html

- **Ejemplo de análisis y evaluación de riesgos**

http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf