Máster Universitario en Ciberseguridad y Privacidad (MUCIP)

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

Nombre Estudiante: ***Natividad García Lacárcel***
Programa: ***Máster Universitario en Ciberseguridad y Privacidad (MUCIP)***
Área: ***Sistemas de Gestión de la Seguridad de la Información***

Consultor: ***Antonio José Segovia***
Profesor responsable de la asignatura: ***Carles Garrigues Olivella***
Centro: ***Universitat Oberta de Catalunya***

Fecha entrega: ***Junio de 2021***

Universitat Oberta de Catalunya

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Natividad García Lacárcel*
Nombre del consultor/a:	*Nombre y dos apellidos*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega:	Junio/2021
Titulación:	Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*SGSI, Seguridad de la Información, ISO/IEC 27001*

Resumen del Trabajo

La información es uno de los principales activos que actualmente tienen las organizaciones. Por este motivo debe estar debidamente protegida y preservarse su confidencialidad, integridad y disponibilidad. Así como salvaguardar los sistemas y aplicaciones que la tratan.

La norma ISO/IEC 27001:2013 es una herramienta, que mediante su aplicación pretende conseguir que la organización alcance un nivel adecuado de seguridad de la información. Ofrece una visión inicial del estado de la organización, sus deficiencias y las medidas necesarias para corregir dichos problemas y la situación final después de la aplicación de los proyectos emprendidos. Sienta las bases del proceso de mejora continua y plantea las acciones necesarias para minimizar el impacto de los riesgos potenciales.

El presente proyecto incluye todas las fases de implantación de un SGSI, incluyendo las tareas, documentos, procedimientos y medias organizativas necesarias para cumplir con lo establecido por la norma.

- Contextualización y situación actual de la organización.
- Objetivos del SGSI.
- Análisis de riesgos. Identificación y valoración de los activos. Identificación de amenazas, evaluación y clasificación.
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013
- Proyectos a implantar para adecuar la gestión de la seguridad.
- Esquema documental del SGSI.

Abstract:

Information is one of the main assets that organizations currently have. For this

reason, it must be duly protected, and its confidentiality, integrity and availability must be preserved. As well as safeguarding the systems and applications that deal with it.

The ISO/IEC 27001: 2013 standard is a tool, which through its application aims to ensure that the organization reaches an adequate level of information security. It offers an initial vision of the state of the organization, its deficiencies and the necessary measures to correct these problems and the final situation after the implementation of the projects undertaken. It lays the foundations for the continuous improvement process and proposes the necessary actions to minimize the impact of potential risks.

This project includes all the phases of implementation of an ISMS, including the tasks, documents, procedures and organizational means necessary to comply with the provisions of the standard.

- Contextualization and current situation of the organization.
- Objectives of the ISMS.
- Risk analysis. Identification and valuation of assets. Threat identification, evaluation and classification.
- Evaluation of the level of compliance with ISO/IEC 27002: 2013
- Projects to be implemented to adapt security management.
- Documentary scheme of the SGSI.

Índice

Listado de Ilustraciones

Listado de Tablas

INTRODUCCIÓN

1.1 CONTEXTO Y JUSTIFICACIÓN DEL TRABAJO

El objeto del presente proyecto es desarrollar el Plan de Implementación de la ISO/IEC 27001:2013 en una empresa. La implementación de dicho Plan conlleva revisar y evaluar todas las áreas de la organización, los controles y procesos, con el fin de conocer el estado de la empresa en materia de seguridad y establecer las líneas de actuación para mejorarla. El modelo PDCA (Plan-Do-Check-Act) procurará la mejora continua de la calidad.

Actualmente, todas las acciones en seguridad de la información que se efectúan en la empresa se realizan sin formar parte de un proceso planificado, no están claramente identificadas, ni documentadas. Tampoco se conocen las responsabilidades. El proyecto pretende corregir todas estas carencias y alinear los objetivos y principios de seguridad a la normativa Internacional.
El personal de la empresa será clave para implementar los sistemas de gestión y evitar su fracaso. Para lograrlo todo el personal, sin importar el área a la que pertenezcan, deberá concienciarse y formarse sobre la seguridad de la información.

1.2 OBJETIVOS DEL TRABAJO

Objetivo General:

Planificar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) para la empresa, enfocado al tratamiento de la información por parte de las diferentes áreas, administración, informática, seguridad física, etc.

Objetivos específicos

- Alinear los procesos de la organización para cumplir con los requisitos de la norma ISO 27001:2013.
- Identificar los procesos que permitan realizar los controles y gestionar el SGSI.
- Elaborar documentación que facilite la gestión de la seguridad.
- Involucrar a la alta dirección en el desarrollo y toma de decisiones del SGSI.
- Crear un plan de concienciación y capacitación para el personal de la organización, incluyendo directivos, personal administrativo, técnicos, etc para conseguir un mejor manejo de los activos de la información.
- Generar un plan de continuidad de negocio, así como disminuir el número de incidentes de seguridad.

1.3 ENFOQUE Y MÉTODO SEGUIDO

La ISO 27001 no prescribe una determinada metodología porque cada organización tiene sus propios requisitos y preferencias. Pero la norma sí solicita que se documente todo el proceso de evaluación de riesgo. Para asegurar que todos en la organización estén sincronizados bajo los mismos criterios en lo relacionado con la medición y evaluación de riesgos.
La metodología debe contener los siguientes puntos:

- Identificar los riesgos en la organización.
- Definir quién es el propietario del riesgo.

- Evaluar el nivel de impacto y la probabilidad.
- Calcular el nivel de riesgos.
- Definir qué riesgos son aceptables y cuáles no.

La ISO 27001:2013 es la norma principal de la serie ISO 27000 y contiene los requisitos del SGSI. Se utiliza como base para los sistemas de información y la ISO 27002:2013 como código de buenas prácticas.
A nivel metodológico, se realizará una aproximación por fases al proyecto. La propuesta es ir cubriendo los diferentes apartados de forma que pueda realizarse el proyecto en el tiempo planteado. Seguidamente se planteará un calendario de la asignatura adaptado a las fases del proyecto.

1.4 PLANIFICACIÓN DEL TRABAJO

La planificación del proyecto se ha elaborado en base a las fechas de entrega de las diferentes PEC. En el siguiente diagrama de Gantt se describen los hitos de cada PEC y la planificación de cada tarea.

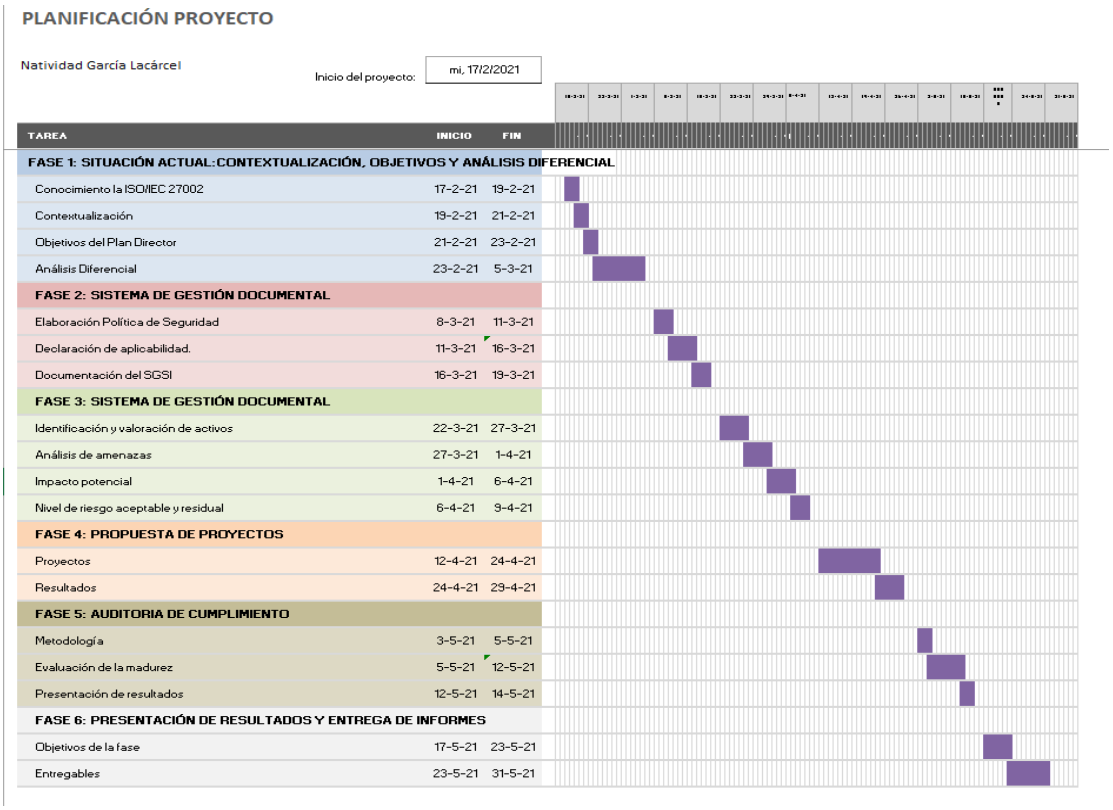


Ilustración 1.Planificación proyecto

1.5. BREVE SUMARIO DE PRODUCTOS OBTENIDOS

Como entregables del proyecto, se presentarán los productos que se especifican a continuación:

- Resumen ejecutivo
- Memoria de Proyecto. Figurarán como anexos:
  Objetivos del Plan Director e Informe Análisis Diferencial
  Resultados del análisis de riesgos
  Nivel de cumplimiento de la ISO basado en el análisis de los 114 controles planteados por la norma.

Proyectos planteados a la dirección, detallando el coste económico de los mismos, su planificación temporal y su impacto sobre el cumplimiento normativo de la ISO/IEC 27002:2013 en los diferentes dominios.
Esquema documental indicado en el apartado 2.2

- Presentación

1.6 BREVE DESCRIPCIÓN DE LOS OTROS CAPÍTULOS DE LA MEMORIA

Seguidamente se describe el contenido de cada fase del proyecto que coincide con los capítulos que aparecen a continuación en la memora.

Fase 1: Situación actual: Contextualización y análisis diferencial

Introducción: Incluirá el planteamiento del proyecto que siente las bases del Plan de Director de Seguridad para la empresa.
Conociendo la ISO/IEC 27002: Conocer y documentarse sobre la ISO/IEC 27002. Documentarse sobre la metodología de Análisis de Riesgos MAGERIT que servirá de ayuda en las siguientes fases del proyecto.
Contextualización: Escoger y describir el entorno de actividad, tamaño, estado inicial de seguridad y los datos relevantes de la empresa de estudio. Concretar el alcance sobre los sistemas de información que dan soporte a sus procesos de negocio.
Objetivo: Especificar los objetivos del Plan Director de Seguridad.
Análisis diferencial: Elaboración de un análisis diferencial de las medidas de seguridad y la normativa que tiene la organización en relación, a la seguridad de la información. Análisis con respecto a la norma ISO/IEC 27001 e ISO/IEC 27002.
Resultados: Descripción de los resultados sobre el estado de la organización.

Fase 2: Sistema de gestión documental

Introducción: Al sistema documental establecido sobre el Sistema de Gestión de Seguridad de la Información establecidos por la norma ISO/IEC 27001.
Esquema documental: Los documentos necesarios para poder certificar el sistema:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

Fase 3: Análisis de riesgos

Introducción: Debe identificarse aquello que queremos proteger y las amenazas que pueden tener.
Inventario de activos: Análisis de los activos vinculados a la información.
Valoración de los activos: Determinación del valor de los diferentes activos.
Dimensiones de seguridad: La criticidad de un activo se puede medir por las cinco dimensiones de seguridad de la información (ACIDA). Se especificará la escala en la que se realizarán las valoraciones (“Muy Alta”, “Alta”, “Media”, “Baja” o “Despreciable”) o [0-10]
Tabla resumen de valoración: Generación de la tabla donde se refleja tanto la valoración de activos como los aspectos críticos del mismo
Análisis de amenazas: Análisis de las amenazas que pueden afectar a los activos.
Impacto Potencial: Valoración del impacto potencial que puede suponer para la empresa la materialización de las amenazas.

Nivel de riesgo aceptable y riesgo residual: Establecer un límite a partir del cual decidir si asumir un riesgo o por el contrario no asumirlo o aplicar controles.

Fase 4: Análisis de riesgos

Introducción: Una vez conocido el nivel de riesgo actual en la Organización, deben plantearse los proyectos que mejoren el estado de la seguridad.
Propuestas: Planteamiento de los proyectos que mejoren el estado de la seguridad. La descripción de las mejoras propuestas deberá ayudar a mitigar el riesgo actual a la organización y evolucionar el cumplimiento ISO hasta un nivel adecuado.

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

Introducción: Ya identificados los activos de la empresa y evaluadas las amenazas. Se deben evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad.
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.
Evaluación de la madurez: Evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Para profundizar al máximo en el conocimiento de la organización.
Presentación de resultados: Evaluación del nivel de madurez porcentual de los diferentes controles.
Resultados: Visión del cumplimiento de los diferentes dominios de la ISO/IEC 27002:2013 y de sus posibles incumplimientos.

Fase 6: Presentación de Resultados y entrega de informes

Introducción: Es el momento de recopilar la información y darle el formato pertinente para su presentación.
Objetivo de la fase: El objetivo genérico de esta fase es la generación de la documentación que aborde todo el proceso de la implementación del SGSI.
Entregables: Listado de los documentos que es necesario presentar para superar el proyecto.

SITUACIÓN ACTUAL, CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

2.1 INTRODUCCIÓN

El actual proyecto fin de Master, como punto final del Master de Ciberseguridad y privacidad impartido por la UOC, se centra en la elaboración de un plan implementación de la seguridad en una organización basándose en la norma ISO/IEC 27001:2013. La información se trata de un elemento fundamental y de cuyo tratamiento y protección se depende cada vez más para el logro de los objetivos y metas. Así como para el desarrollo de la actividad propia de la organización.

La información junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una empresa. Las organizaciones y sus sistemas están expuestos a un gran número de amenazas, que pueden comprometer la confidencialidad, integridad y disponibilidad de la información acarreando graves perjuicios. Se trata de los tres pilares básicos de la seguridad de la información y sin los cuales no existe nada seguro. Para que se efectúe un correcto tratamiento de la información e intentar evitar fallos en estos elementos, también es muy importante concienciar al personal.

Por otra parte, para la implementación del SGSI, se ha tomado como base la norma ISO/IEC 27001:2013, evalúa el estado actual de los procesos relacionados con la seguridad de la información, elaborando un análisis de los riesgos e identificando los controles a generarse, así como las medidas de seguridad que prevengan posibles incidentes. La ISO/IEC 27002:2013, proporciona diferentes recomendaciones de las mejores prácticas para iniciar, implementar o mantener los sistemas de seguridad.

Basándonos en esto, el TFM se dividirá en las siguientes seis fases:
• Fase 1: Situación actual, contextualización, objetivos y análisis diferencial. El objetivo es caracterizar la organización y definir el o los procesos sobre los cuales se desarrollará el presente proyecto. Así como definir el alcance del TFM.
• Fase2: Sistema de gestión documental. Introducción, esquema documental y resultados.
• Fase 3: Análisis de Riesgos: El análisis de riesgos permitirá identificar la situación actual de la organización y definir los controles para mantener un nivel de riesgo aceptable en la organización. Se efectuará el inventario de activos, dimensiones de seguridad, análisis de amenazas, impacto potencial y nivel de riesgo.
• Fase 4: Propuestas de proyectos:
• Fase 5: Auditoría de cumplimiento: Metodología, evaluación de la madurez y presentación de resultados.
• Fase 6: Presentación de resultados y entrega de informes: Una vez realizado un diagnóstico del estado actual de seguridad y de definir el Plan Director de Seguridad, se procede a presentar los resultados a la alta dirección y a los diferentes sponsors para garantizar así el apoyo en todos los niveles de la organización.

2.2 CONOCIENDO LA ISO/IEC 27001 E ISO/IEC 27002

2.2.1 EVOLUCIÓN HISTÓRICA ISO/IEC 27001

La norma ISO 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional por primera vez en octubre de 2005 por ISO (International Organization for Standardization)y por la comisión International Electrotechnical Commission. Después, fue actualizado en 2013.
La norma ha evolucionado de otros estándares de seguridad de la información:

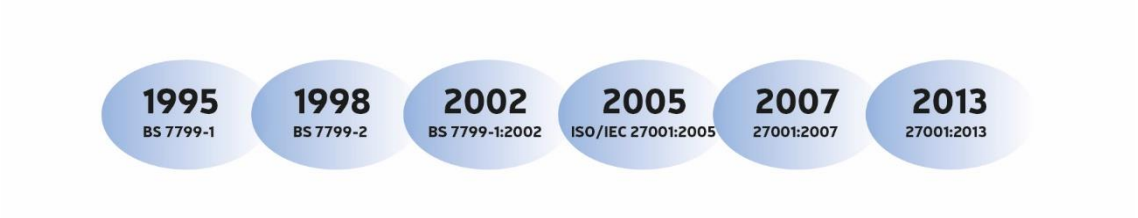


Ilustración 2. Evolución norma

• 1901 – Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional. Estas son el origen de normas actuales como ISO 9001, ISO 14001 u OHSAS 18001.
• 1995 - BS 7799-1:1995: Se define un estándar de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.
• 1998 – BS 7799-2:1999: Se trata de una revisión norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
• 1999 – BS 7799-1:1999: Se efectúa una revisión de la norma.
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 por una entidad certificadora en Reino Unido y en otros países.
• 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: 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. La ISO/IEC 27001:2007: Se publica la nueva versión de la norma.
• 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M: 2009.

2.2.2 CAMBIOS EN LA ÚLTIMA REVISIÓN ISO/IEC 27001:2013

La norma evoluciona a la ISO 27001:2013 con cambios significativos con respecto a la del 2005:

- Cambia su estructura aplicando una estructura de alto nivel, títulos de las sub-clausulas, texto, términos comunes y definiciones definidas conforme al Anexo SL.
- Cambios del Anexo A, se incrementan el número de dominios de seguridad de 11 a 14 y disminuye el número de controles pasando de 133 a 114. Criptografía y Relaciones con el Proveedor se han convertido en secciones separadas.
- Eliminación de la referencia al proceso de mejora continua PDCA dejando abierta la posibilidad de utilizarlo.
- Se incentiva el conocimiento de la organización definiendo el alcance, política, objetivos y análisis de riesgos.
- El análisis de riesgos, de forma más genérica, determina los controles necesarios se efectúan. En lugar de identificar primero los activos, las amenazas y sus vulnerabilidades.
- La Dirección adquiere mayor importancia en la gestión.

2.2.3 LA NORMA ISO/IEC 27001:2013

La ISO 27001:2013 define como organizar la información de cualquier tipo de empresa, independientemente de su tipo, tamaño o fines. Así como la forma de gestionar la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI, con el objeto de proteger la confidencialidad, integridad y disponibilidad de la información.
También permite que las organizaciones sean certificadas en este estándar, lo cual, conlleva que cumplan unos estándares comunes, garantiza unos elementos mínimos en materia de seguridad y favorece la competitividad entre ellas.

Ilustración 3. Norma ISO/IEC 27001:2013

2.2.4 ESTRUCTURA DE LA NORMA ISO/IEC 27001:2013

La norma se encuentra dividida en dos partes; la primera se compone de 11 puntos, del 0 al 3 de carácter introductorias, no obligadas para la implementación y del 4 al 10 obligatorias, deben ser efectuados todos sus requerimientos para cumplir con la norma. La segunda parte, está conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia.

0. Introducción. Explica el objetivo de la norma y su compatibilidad con otras normas.
1. Alcance. Trata el alcance aplicable de la norma a cualquier tipo de organización.
2. Referencias normativas. Referencia a la norma ISO/IEC 27000 como estándar.
3. Términos y definiciones. Referencia a la norma ISO/IEC 27000 como estándar.

Los siguientes puntos forman parte de la PDCA.

4. Contexto de la organización. Define los requerimientos para comprender cuestiones externas e internas, así como las partes interesadas, sus requisitos y el alcance del SGSI.

4.1. Conocimiento de la organización y de su contexto
4.2. Comprensión de las necesidades y expectativas de las partes interesadas
4.3. Determinación del alcance del Sistema de Gestión de la Seguridad de la Información.
4.4. Sistema de Gestión de Seguridad de la Información

5. Liderazgo. Define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades, así como el contenido de las políticas.

5.1. Liderazgo y compromiso.
5.2. Política.
5.3. Roles, responsabilidades y autoridades en la organización.

6. Planeación. Define los requerimientos para la evaluación de riesgos, el plan de tratamiento y la determinación de los objetivos de seguridad de la información.

6.1. Acciones para tratar riesgos y oportunidades.
6.2. Objetivos de Seguridad de la Información y planes para lograrlos.

7. Soporte. Define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

7.1. Recursos.
7.2. Competencia.
7.3. Toma de conciencia.
7.4. Comunicación.
7.5. Información documentada.

8. Operación. Evaluar los riesgos en materia de seguridad de la información, así como el tratamiento de dichos riesgos.

8.1. Planificación y control operacional.
8.2. Valoración de riesgos de la seguridad de la información.
8.3. Tratamiento de riesgos de la seguridad de la información.

9. Evaluación del desempeño. Procurar el seguimiento mediante el monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

9.1. Seguimiento, medición, análisis y evaluación.
9.2. Auditoría interna.
9.3. Revisión por la dirección.

10. Mejora. Trata las no conformidades, correcciones, medidas correctivas y mejora continua.

10.1. No conformidades y acciones correctivas.
10.2. Mejora continua.

Anexo A – Proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18) [3]

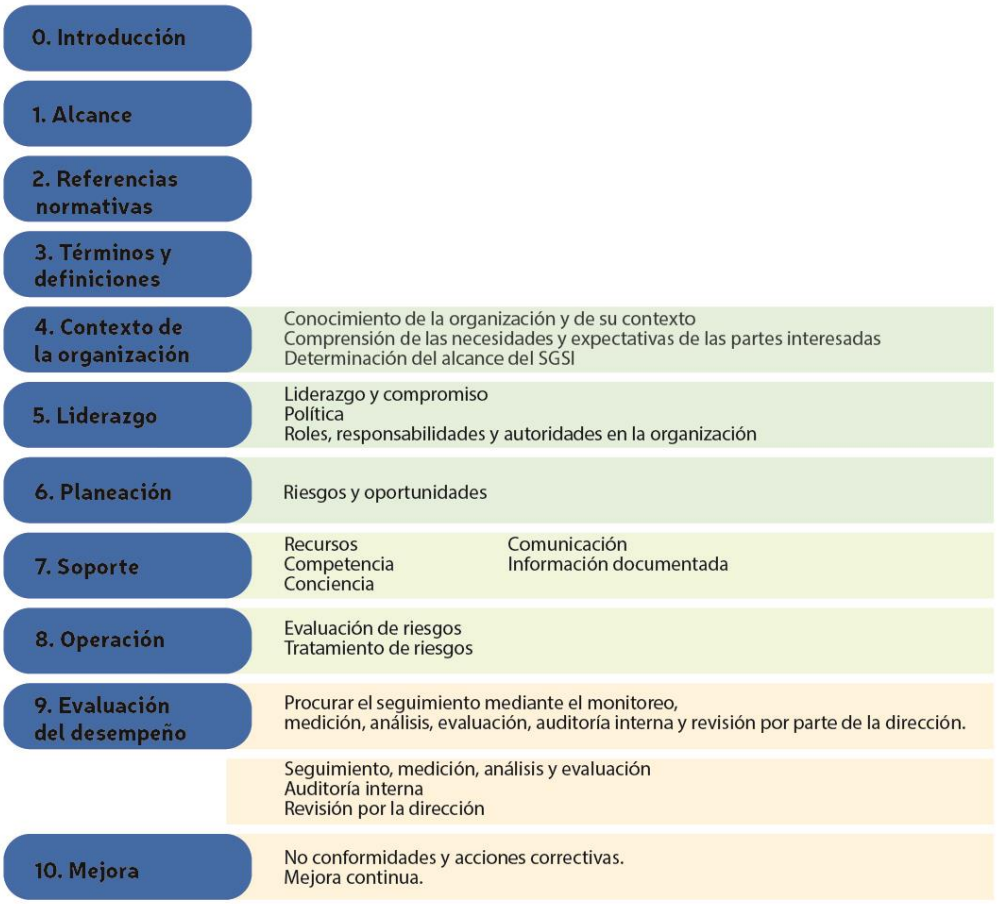


Ilustración 4. Estructura del estándar ISO/IEC 27001:2013

2.2.5 LA NORMA ISO/IEC 27002

La norma ISO 27002 es un estándar para la seguridad de la información publicada por la organización internacional de normalización y la comisión electrónica internacional. Su versión más reciente es la norma ISO 27002:2013.

2.2.6 EVOLUCIÓN HISTÓRICA ISO/IEC 27002

La ISO/IEC 27002 de igual forma que la ISO/IEC 27001 ha sufrido una evolución.

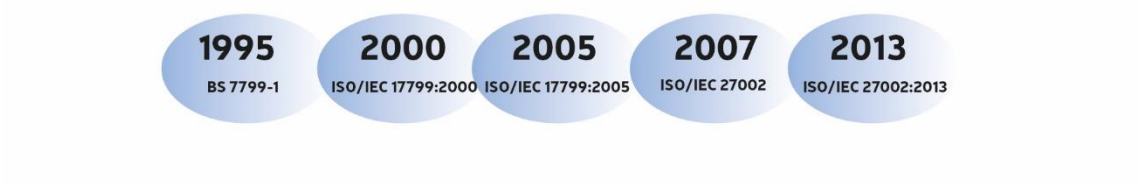


Ilustración 5. Evolución norma

Al principio se publicó como un cambio de nombre de la ISO17999.
• La ISO 17999 tiene su origen en el British Standard BS 7799-1 en 1995.
• Después, en el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, que fue

revisado y modificado en 2005 editando la ISO/IEC 17799:2005.
• Con la aprobación de la norma ISO/IEC 27001, el estándar ISO/IEC 17799:2005 pasó a renombrarse como ISO/IEC 27002 en el año 2007.
• Su versión más reciente data del 2013 ISO/IEC 27002:2013 con novedades asociadas al ANEXO A de la ISO/IEC 27001:2013.

2.2.7 LA NORMA ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 se trata de una guía de recomendaciones para las organizaciones que deseen implantar buenas prácticas en seguridad de la información y para la selección de controles de seguridad durante el proceso de implantación del SGSI en una organización. Esta norma no es certificable y simplemente sirve de apoyo a la norma ISO 27001.

2.2.8 ESTRUCTURA DE LA NORMA ISO/IEC 27002:2013

La norma ISO 27002 se encuentra estructurada en 14 dominios, 35 objetivos de control y 114 controles, y que pueden estar divididos en categorías en algunos casos, según el tipo de control.

Los dominios de la norma son los siguientes:
A5. Políticas de Seguridad. Trata la importancia de las directrices y políticas de seguridad. Así como la necesidad de revisión y actualización.
A.5.1 Directrices de la dirección en seguridad de la información
- A.5.1.1 Conjunto de políticas para la seguridad de la información
- A.5.1.2 Revisión de las políticas para la seguridad de la información

A6. Organización de la Seguridad de la Información. Controles sobre la organización interna; asignación de responsabilidades, funciones, contacto con las autoridades, etc.
A.6.1 Organización interna
- A.6.1.1 Asignación de responsabilidades para la seguridad de la información
- A.6.1.2 Segregación de tareas
- A.6.1.3 Contacto con las autoridades
- A.6.1.4 Contacto con grupo de especial interés
- A.6.1.5 Seguridad de la información en la gestión de proyectos.

A.6.2 Dispositivos móviles y teletrabajo
- A.6.2.1 Políticas de dispositivos móviles
- A.6.2.2 Teletrabajo

A7. Seguridad de los Recursos Humanos. Trata aspectos relativos a la contratación por parte de recursos humanos, investigación de antecedentes, condiciones de contrato, confidencialidad, etc. Así como la concienciación y formación de los empleados en la seguridad de la información. Y protocolo en caso de despido.
A.7.1 Antes de empleo
- A.7.1.1 Investigación de antecedentes
- A.7.1.2 Términos y condiciones de empleo

A.7.2 Durante el empleo
- A.7.2.1 Responsabilidades de gestión
- A.7.2.2 Conciencia de seguridad de la información y entrenamiento
  - A.7.2.3 Procedimiento disciplinario

A.7.3 Finalización del empleo o cambio en el puesto de trabajo
- A.7.3.1 Responsabilidades ante la finalización o cambio

A8. Gestión de los Activos. Establecer medidas adecuadas para proteger los activos,

establece medidas ante incidencias, quiebras de seguridad y alteraciones no deseadas de la información.

A.8.1 Responsabilidad de los activos
- A.8.1.1 Inventario de activos
- A.8.1.2 Propiedad de los activos
- A.8.1.3 Uso aceptable de los activos
- A.8.1.4 Retorno de los activos

A.8.2 Clasificación de la información
- A.8.2.1 Clasificación de la información
- A.8.2.2 Etiquetado de la información
- A.8.2.3 Manipulado de la información

A.8.3 Manejo de los soportes
- A.8.3.1 Gestión de soportes extraíbles
- A.8.3.2 Eliminación de soportes
- A.8.3.3 Soportes físicos en tránsito

A9. Control de Accesos. Requisitos de la organización para el control y gestión de acceso de los usuarios y responsabilidades.

A.9.1 Requisitos empresariales de control de acceso
- A.9.1.1 Política de control de acceso
- A.9.1.2 Acceso a las redes y servicios de red

A.9.2 Gestión de acceso de usuario
- A.9.2.1 Registro y baja de usuario
- A.9.2.2 Provisión de acceso de usuario
- A.9.2.3 Gestión de privilegiados de acceso
- A.9.2.4 Gestión de la información secreta de autentificación de los usuarios
- A.9.2.5 Revisión de los derechos de acceso de usuario
- A.9.2.6 Retirada o reasignación de los derechos de acceso

A.9.3 Responsabilidades del usuario
- A.9.3.1 Uso de información secreta de autenticación

A.9.4 Control de sistemas y acceso a las aplicaciones
- A.9.4.1 Restricción del acceso a la información
- A.9.4.2 Procedimiento de inicio de sesión seguro
- A.9.4.3 Sistema de gestión de contraseñas
- A.9.4.4 Uso de programas de servicios públicos privilegiados
- A.9.4.5 Control de acceso al código fuente del programa

A.10 Criptografía. Protección de la información crítica con técnicas criptográficas para proteger y garantizar la autenticidad, confidencialidad e integridad.

A.10.1 Controles criptográficos
- A.10.1.1 Políticas sobre el uso de controles criptográficos
- A.10.1.2 Gestión de claves.

A.11 Seguridad Física y Ambiental. Establecer seguridad no sólo de tipo tecnológico, sino también físico. Áreas seguras y seguridad física de los equipos.

A.11.1 Áreas seguras
- A.11.1.1 Perímetro de seguridad física
- A.11.1.2 Controles de entradas físicas
- A.11.1.3 Seguridad de oficina, despachos y recursos
- A.11.1.4 Protección contra amenazas externas y ambientales
- A.11.1.5 El trabajo en áreas seguras
- A.11.1.6 Zonas de entrega y carga

A.11.2 Seguridad de los equipos
- A.11.2.1 Emplazamiento y protección del equipo

A.11.2.2 Instalación de suministro
A.11.2.3 Seguridad del cableado
A.11.2.4 Mantenimiento de los equipos
A.11.2.5 Retirada de materiales propiedad de la empresa
A.11.2.6 Seguridad de los equipos fuera de las instalaciones
A.11.2.7 Reutilización o eliminación segura de equipos
A.11.2.8 Equipos de usuarios desatendidos
A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia

A.12 Seguridad de las Operaciones. Protección del software malicioso, copia de seguridad, control de software en explotación, gestión de vulnerabilidades, etc.
A.12.1 Procedimientos y responsabilidades en las operaciones
A.12.1.1 Procedimientos operativos documentales
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de la capacidad
A.12.1.4 Separación de los recursos de desarrollo, prueba y operación
A.12.2 Protección contra malware
A.12.2.1 Controles contra el malware
A.12.3 Copias de seguridad
A.12.3.1 Copia de seguridad de la información
A.12.4 Registro y seguimiento
A.12.4.1 Registro de eventos
A.12.4.2 Protección de la información de los registros
A.12.4.3 Registros de administración y operación
A.12.4.4 Sincronización del reloj
A.12.5 Control de software en explotación
A.12.5.1 Instalación de software en explotación
A.12.6 Técnico de gestión de vulnerabilidades
A.12.6.1 Gestión de vulnerabilidades técnicas
A.12.6.2 Restricciones de instalación de software
A.12.7 Consideraciones sobre la auditoria de sistemas de información
A.12.7.1 Controles de auditoría de sistemas de información

A.13 Seguridad de las Comunicaciones. Gestión de la seguridad de la red y gestión de la transferencia de información.
A.13.1 Gestión de la seguridad de la red
A.13.1.1 Controles de red
A.13.1.2 Seguridad de los servicios de red
A.13.1.3 Segregación en redes
A.13.2 Intercambio de información
A.13.2.1 Políticas y procedimientos de intercambio de información
A.13.2.2 Acuerdos de intercambio de información
A.13.2.3 Mensajería electrónica
A.13.2.4 Acuerdos de confidencialidad o de no revelación

A.14 Adquisición de sistemas, desarrollo y mantenimiento. Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
A.14.1 Requisitos de seguridad en los sistemas de información
A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas
A.14.1.3 Protección de las transacciones de servicios de aplicaciones
A.14.2 Seguridad en el desarrollo y en los procesos de soporte
A.14.2.1 Políticas de desarrollo seguro

A.14.2.2 Procedimientos de control de cambio del sistema
A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A.14.2.4 Restricciones a los cambios en los paquetes de software
A.14.2.5 Principios de ingeniería de sistemas seguros
A.14.2.6 Entorno de desarrollo seguro
A.14.2.7 Externalización del desarrollo de software
A.14.2.8 Pruebas funcionales de seguridad del sistema
A.14.2.9 Pruebas de aceptación del sistema

A.14.3 Datos de prueba
A.14.3.1 Protección de datos de prueba

A.15 Relaciones con los Proveedores. En la relación con terceras partes, como proveedores, se deben establecer medidas de seguridad.

A.15.1 Seguridad en las relaciones con proveedores
A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores
A.15.1.2 Requisitos de seguridad en contratos con terceros
A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

A.15.2 Gestión de la provisión de servicios del proveedor
A.15.2.1 Control y revisión de la provisión de servicios del proveedor
A.15.2.2 Gestión de cambios en la provisión del servicio de proveedor

A.16 Gestión de incidencias que afectan a la Seguridad de la Información. Deben establecerse procedimientos para la gestión de incidentes, de forma que se esté preparado ante posibles ataques y poder prevenirlos.

A.16.1 Gestión de incidentes de seguridad de la información y mejoras
A.16.1.1 Responsabilidades y procedimientos
A.16.1.2 Informar eventos de seguridad de la información
A.16.1.3 Informar las debilidades de seguridad de la información
A.16.1.4 Evaluación y decisión sobre eventos de seguridad de la información
A.16.1.5 Respuesta a incidentes de seguridad de la información
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
A.16.1.7 Recopilación de evidencias

A.17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad de Negocio. Continuidad de la información y redundancias.

A.17.1 Continuidad de la seguridad de la información
A.17.1.1 Planificación de la continuidad de la seguridad de la información
A.17.1.2 Implementación de la continuidad de la seguridad de la información
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

A.17.2 Redundancias
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información

A.18 Conformidad. Con los requisitos legales y contractuales y revisiones de la seguridad de la información.

A.18.1 Cumplimiento de requisitos legales y contractuales
A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales.
A.18.1.2 Derechos de propiedad intelectual
A.18.1.3 Protección de los registros de la organización
A.18.1.4 Protección y privacidad de la información de carácter personal
A.18.1.5 Regulación de controles criptográficos

A.18.2 Revisiones de seguridad de la información
A.18.2.1 Revisión independiente de seguridad de la información
A.18.2.2 Cumplimiento de políticas y estándares de seguridad
A.18.2.3 Revisión de cumplimiento técnico

Ilustración 6. Estructura ISO 27002:2013

2.3 CONTEXTUALIZACIÓN

En este apartado se realizará una descripción de la empresa ficticia sobre la que se basa el SGSI, indicando su actividad de negocio, su organigrama general, las funciones y cargos del personal, así como la arquitectura de los sistemas y tecnologías de la información.

2.3.1 DESCRIPCIÓN DE LA EMPRESA

La empresa objeto de estudio MASIAG es una agencia de marketing digital, su actividad consiste en diseñar estrategias de marketing online integral para los negocios y llevarlas a cabo. Se trata de una compañía innovadora, creada en 2011 que ha tenido un rápido crecimiento y hoy día es líder en el sector del marketing.

Con el auge de las nuevas tecnologías, las empresas han necesitado abrir sus posibilidades de desarrollo al negocio online para no quedarse descolgadas, lograr visibilidad en internet, estar a la última y ser competitivas. El propósito de MASIAG es asesorar y trabajar con los clientes para ayudarles a obtener los objetivos más acordes a su negocio.

La empresa MASIAG analiza las particulares propias del sector del cliente, se ajusta a sus necesidades y estudia a la competencia, con el objetivo de promover marca, productos y servicios a través de internet. Se procura optimizar el modelo de negocio para aprovechar las ventajas y oportunidades que ofrece el entorno digital.

Para poder aumentar la confianza de sus clientes y poder seguir creciendo, la empresa MASIAG necesita obtener la ISO 27001:2013. Por tanto, se realizarán distintas acciones que favorezcan la mejora de la calidad y seguridad en los sistemas de información, así como la obtención de la certificación.

2.3.2 ACTIVIDAD ESPECÍFICA

Las actividades que desarrollan y en las que se basa su negocio son las siguientes:

- **Auditoría de marketing digital**. Analiza la situación actual de una empresa mediante una auditoría de los canales y acciones de marketing de la empresa.

- **Posicionamiento en buscadores**. Servicios de SEO y SEM para incrementar la visibilidad de las empresas en los buscadores y conseguir generar tráfico de alta calidad a un sitio web.

- **Posicionamiento ASO**: Servicio de marketing para potenciar las apps e incrementar el número de descargas.

- **Campañas de Email marketing**. Campañas de marketing por correo electrónico.

- **Gestión de Redes Sociales.** Contenido y anuncios en redes sociales para llegar al mayor número de usuarios posible. Estudio de la situación en las redes sociales de la empresa para tener en cuenta el perfil de usuario y trabajar en consonancia.

- **Marketing** de contenidos. Creación de contenidos de valor, para atraer de manera natural a usuarios potencialmente interesados en la marca y convertirlos en clientes.

- **Comercio electrónico.** Plan de marketing para conseguir buenos resultados en la

web de compra/venta online.

- **Video marketing**. Comunicar de forma atractiva mediante videos de contenido que resulte popular para potenciar una marca.

- **Formación a medida**. Concienciación de los clientes sobre el marketing digital.

2.3.3 ESTRUCTURA Y JERARQUÍA DE LA ORGANIZACIÓN

La organización está estructura en tres áreas básicas (Comercial, Técnica y Financiera) con una serie de departamentos dependientes.

El personal vinculado a cada área es el siguiente:

- **Director general (1)**
- **Key Account Manager (1)**
- **Director comercial (1)**

  Dpto. Relaciones Públicas (1), Dpto. Marketing (1), Dpto. Ventas (1)
- **Director financiero (1)**

  Dpto Recursos humanos (2), Dpto Contabilidad (3), Dpto. Administración y compras (1)
- **Director técnico (1)**

  Content Manager (2), Community Manager (2), Especialista SEO/SEM (3), Diseñador UX/UI (2), Programador (3), Analista digital (2).

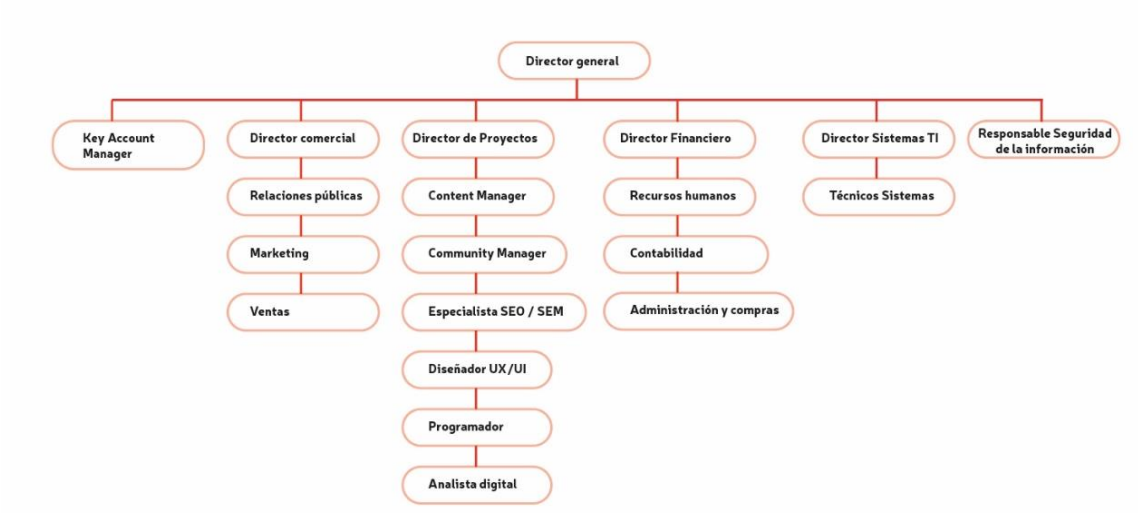


Ilustración 7. Organigrama empresa

2.3.4 FUNCIONES DE LOS CARGOS

Los perfiles del personal que trabaja en la agencia de marketing digital son los siguientes:
La dirección se conforma por el director general e inmediatamente después los directores de las tres áreas (director comercial, financiero y técnico), así como el ejecutivo de clave de cuentas. Del Director comercial, jerárquicamente dependen el personal de relaciones públicas, marketing y ventas. Del Director financiero dependen

Recursos humanos, Contabilidad y Administración y compras. Y del Director Técnico los empleados más técnicos.

Los perfiles más operativos son los siguientes:

- **Key Account Manager (Ejecutivo clave de cuentas)** Es la persona encargada de gestionar las cuentas de los clientes dentro de la agencia. Su labor principal es el trato con el cliente para conseguir buenas relaciones entre ellos y el negocio. Efectúa el diagnóstico inicial de toda la información precisa para emprender el proyecto y realiza el seguimiento.
- **SEO Manager (Especialista SEO)** El especialista SEO se encarga de la arquitectura de los sitios web y de la optimización de los contenidos. Asegura han sido redactados con las palabras clave adecuadas para maximizar el tráfico y la conversión
- **SEM Manager (Especialista SEM)** El especialista SEM es la persona que se encarga de gestionar todas las campañas de PPC o de pago de tus clientes en función de los objetivos de la estrategia.
- **Content Manager (Administrador de contenido)** Su función es crear los contenidos que se van a publicar en las redes sociales. Asegurando la calidad del contenido y acorde a la política y objetivos de la compañía. Así como estableciendo las plataformas más interesan al cliente.
- **Community Manager (Estratega de redes sociales)** Se encarga de llevar a cabo la estrategia de comunicación online a través de los medios digitales, posicionamiento de una organización en redes sociales.
- **Programador** Se encarga de crear los formatos tecnológicos. Desarrolla las aplicaciones, programas, aplicación móvil, web, etc. Trabaja de forma estrecha con el especialista en diseño UX/UI y el especialista SEO.
- **UX/UI Designer (Diseñador UX/UI)** Diseña la estructura de los sitios, con el objetivo de garantizar que su usabilidad y experiencia sean las mejores. Colabora sobre todo con programadores y especialistas SEO.
- **Data Analyst (Analista de datos)** Se encargan de analizar toda la información recogida para determinar cuán efectivas están siendo las estrategias, ya sean de conversión, tráfico, posicionamiento, etc. Para de esta forma trabajar nuevas estrategias.

2.3.5 INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA

La infraestructura tecnológica de la organización es básica para desarrollar los servicios que son objeto de negocio.
Dispone de una red LAN distribuida para usuarios de tareas administrativas y financieras, usuarios técnicos y para servidores. Además, cuenta con acceso wifi para dispositivos inalámbricos como portátiles, tablets y smartphones.
Por otra parte, dispone de conexión a internet para los trabajadores presencialmente en las instalaciones y en remoto. En la DMZ se albergan las DNS y la web de la organización.

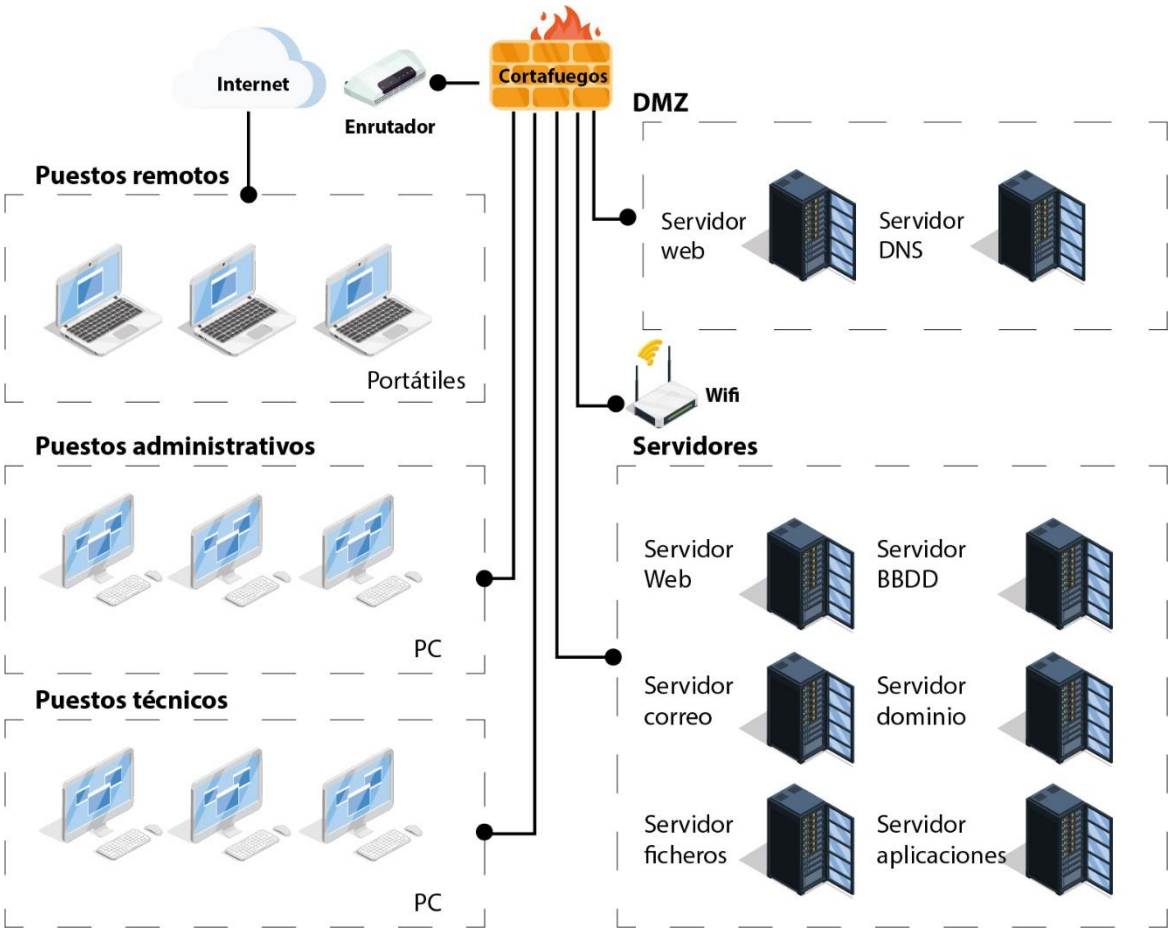


Ilustración 8. Infraestructura tecnológica

2.4 ALCANCE

El alcance del proyecto incluye la totalidad de los procesos y tratamientos de la información que se efectúa en la empresa. Afectará a todo el sistema, las instalaciones y el personal, así como a la información que pueda procesarse en la empresa, tanto si pertenece a ella como a terceros.

Por lo tanto, en este proceso se procurará la gestión de la seguridad en todos los niveles y capas de la organización. Procurando alinear los objetivos de seguridad con el negocio. Implicando a la alta dirección y procurando la concienciación del personal para que efectuar un correcto tratamiento de la información. Incluyendo la gestión de la seguridad tanto de los soportes físicos como lógicos de la seguridad. Así como el acceso a la información de forma remota o localmente.

2.5 ANÁLISIS DAFO

El análisis DAFO es una herramienta de estudio de la situación de una empresa, institución, proyecto o persona, analizando sus características internas y su situación externa, mostrando la información en forma de matriz.
Este análisis ayudará a identificar y contrastar las fortalezas y debilidades, contra las oportunidades y amenazas de la empresa.

	FORTALEZAS	DEBILIDADES
ANÁLISIS INTERNO	• **Equipo de trabajo altamente capacitado.** • **Baja rotación del personal.** • **Consciencia de la necesidad de la implementación de un SGSI.** • **Apoyo de la alta dirección en la implantación del SGSI.** • **Empresa altamente tecnológica.**	• **Falta de documentación de procesos de operación.** • **Falta de estrategia de continuidad de negocio.** • **Infraestructura en proceso de desarrollo.** • **Alto gasto para cumplir los compromisos del SGSI.**
	OPORTUNIDADES	AMENAZAS
ANÁLISIS EXTERNO	• **Ampliar servicios ofertados por la empresa.** • **Mejorar el prestigio y credibilidad a los clientes.** • **Ganar competitividad frente a otras empresas.**	• **Empresas con mayor experiencia en el mercado de la competencia.** • **Cambios en la estructura de la organización que pueden afectar al SGSI.** • **Cambio normativas legales.**

Tabla 1. Análisis DAFO

2.6 OBJETIVOS DEL PLAN DIRECTOR

Una vez conocido el marco normativo a aplicar, identificado el contexto y concretado el alcance el siguiente paso consiste en establecer los objetivos del Plan Director de Seguridad.

En el **ANEXO1_OBJETIVOS.pdf** se detallan los objetivos de Plan Director.

2.7 ANÁLISIS DIFERENCIAL

En este apartado se realizará un análisis diferencial de las medidas de seguridad y la normativa de la organización en relación, a la Seguridad de la Información para establecer su estado antes de iniciar las acciones de implementación del SGSI. Será el punto de partida para determinar la situación de la organización y de esta manera poder valorar los avances que a lo largo del proyecto se realicen.

El análisis diferencial se realizará con respecto la norma ISO/IEC 27001 y las mejores prácticas descritas en ISO/IEC 27002, y nos permitirá evaluar la capacidad actual y realizar las recomendaciones y oportunidades de mejora.

El análisis se ha efectuado empleando para la valoración de los controles el modelo de madurez definido por COBIT (Control Objectives for Information and related Technology) y basado en el CMM (Capability Marutity Model) desarrollado por la Carnegie Mellon School.

	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "best practice", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporciona mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "ad hoc" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

Tabla 2. Nivel de madurez

Para el establecimiento del nivel de madurez de cada uno de los controles y cláusulas, se realizaron entrevistas con el responsable de informática, técnicos informáticos, responsables de las áreas administrativas y representantes de la alta dirección. La información se completó con información de los procesos de trabajo propios de la organización.

Otro factor importante es el nivel medio de cumplimiento de cada uno de los controles para ello, se han tenido en cuenta los valores de 0 a 5 y su cumplimiento según el

siguiente baremo:

- Puntaje de madurez por debajo de 1.65: No cumple
- Puntaje de madurez entre 1.66 y 3.25: Cumple parcialmente
- Puntaje de madurez por encima de 3.26: Cumplimiento con requisitos de la Norma

MENOR 1.65	NO CUMPLE
ENTRE 1.66 Y 3.25	CUMPLE PARCIALMENTE
MAYOR 3.26	CUMPLE REQUISITOS NORMA

Tabla 3. Nivel de cumplimiento

2.8 RESULTADOS

En el análisis diferencial se muestra la evaluación de la organización con respecto a la norma ISO/IEC-27001:2013 y el anexo ISO/IEC-27002:2013 Este apartado está desarrollado en el **ANEXO2_ANALISISDIFERENCIAL.pdf.**

SISTEMA DE GESTIÓN DOCUMENTAL

3.1 INTRODUCCIÓN

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

- **Política de Seguridad de la Información:** Se trata de la normativa interna de la organización y de conocimiento y cumplimiento por parte del personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. La norma ISO 27001:2013 en el numeral 5.2 Política establece los requisitos para su definición.
    1) Ser adecuada al propósito de la organización.
    2) Incluir los objetivos de seguridad de la información o un marco de referencia para su establecimiento.
    3) Incluir el compromiso de cumplir requisitos aplicables relativos a seguridad de la información.
    4) La política debe estar documentada.
    5) Debe ser comunicada dentro de la organización.
    6) Debe estar disponible para las partes interesadas.

- **Procedimiento de auditorías Internas:** Documento sobre la planificación de las auditorías que se efectuarán durante la vigencia de la certificación. La ISO/IEC 27001:2013 establece en su apartado 9.2 la necesidad de llevar a cabo auditorías internas con el objeto de verificar que el Sistema de Gestión de Seguridad de la Información cumple con los requisitos propios de la organización y con los requisitos de la norma indicada.

- **Gestión de Indicadores:** Deben definirse los indicadores para medir la eficacia de los controles de seguridad implantados, así como el sistema de medición.

- **Gestión de Roles y Responsabilidades:** El Sistema de Gestión de la Seguridad de la Información debe contar con un equipo que se encargue de crear, mantener, supervisar y mejorar el sistema. Debe disponer personal técnico y de dirección, para que se puedan tomar decisiones consensuadas con la dirección.

- **Procedimiento de Revisión por la dirección:** La dirección debe efectuar revisiones sobre las cuestiones más importantes que han sucedido en relación a Sistema de Gestión de la Información.

- **Metodología de Análisis de Riesgos:** Establece el método para calcular el riesgo, incluyendo la identificación y valoración de los activos, amenazas y vulnerabilidades.

- **Declaración de Aplicabilidad:** Documento que incluye todos los controles de seguridad establecidos en la Organización, con el detalle de

su aplicabilidad, su estado actual y documentación relacionada.

3.2 ESQUEMA DOCUMENTAL

La información detallada del esquema documental se muestra en el **ANEXO6_ESQUEMADOCUMENTAL**.pdf.

3.3 RESULTADOS

Con la elaboración de los presentes documentos formados por política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por dirección, gestión de roles y responsabilidades, análisis de riesgos y declaración se aplicabilidad, se establece la estrategia y control del negocio, los requisitos legales y contractuales relativos a la seguridad de la información. Mediante la determinación de los indicadores se facilita la medición de la eficacia de los controles implantados. Para en base a los resultados iniciar las acciones y mejoras oportunas. Así, como la evaluación del impacto que supondría la pérdida de confidencialidad, integridad y disponibilidad para cada activo.

ANÁLISIS DE RIESGOS

4.1 INTRODUCCIÓN

El análisis de riesgo es un elemento fundamental para determinar las medidas de seguridad de un activo de información o sistema, ya que identifica los riesgos y estima el impacto potencial que supone su destrucción, la pérdida de información o la afectación de la disponibilidad, confidencialidad e integridad de la información.
El proceso tiene como resultado identificar las amenazas que pueden explotar las vulnerabilidades para mitigarlos, identificar los impactos potenciales que pudieran tener los incidentes y así aprovechar dichas vulnerabilidades encontradas, y determinar las recomendaciones para corregir o reducir las amenazas, de forma que implica determinar los activos que se necesitan proteger, de qué amenaza y cómo hacerlo.

Mediante el análisis de riesgos se deberán alcanzar los siguientes objetivos:

- Determinar los activos más significativos que posee la empresa.
- Establecer las amenazas a las que están expuestos cada activo.
- Escoger salvaguardas apropiadas para los activos.
- Estimar el impacto si se materializara alguna amenaza.

El análisis de riesgo ofrece beneficios a las organizaciones, los cuales varían en función del tipo, tamaño y van en acuerdo a las políticas de cada una.

- Asegurar la continuidad operacional de la empresa.
- Saber manejar las amenazas y riesgos críticos.
- Mantener una estrategia de protección y de reducción de riesgos.
- Justificar una mejora continua de la seguridad informática.
- Costos de seguridad justificados.
- Permitir que la seguridad se convierta en parte de la cultura de la organización.
- Apoyar la comunicación y facilitar la toma de decisiones, certeza económica/financiera.

El proceso de gestión de riesgos dispone de las siguientes medidas:

Ilustración 9. Proceso de análisis o gestión de riesgos

4.2 INVENTARIO DE ACTIVOS

En esta fase se identifican los activos de la empresa relacionados con la seguridad de la información cuyo objetivo del SGSI es protegerlos y se calcula su valor. Se inventarían todos los activos de la empresa a analizar agrupándolos según indica la metodología MAGERIT.
Se listarán todos los activos de información, entendiendo como activo de información cualquier dato, servicio, aplicación, equipo, soporte de información, equipamiento auxiliar, red de comunicación, instalación o persona que almacene, manipule, procese, transporte o genere información relacionada con el proceso, servicio o sistema de información objeto de análisis.
Los activos más relevantes tomados en cuenta para el análisis de riesgos se representan en forma de tabla y son los siguientes:

Las instalaciones son los entornos donde se desempeñan las actividades de la empresa.

AMBITO	ACTIVO	PROPIETARIO
INSTALACIONES [L]	[L-01] Oficina [L-02] CPD [L-03] Recepción	Director general Director sistemas Director general

Recursos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.

AMBITO	ACTIVO	PROPIETARIO
HARDWARE [HW]	[HW-01] Servidor de aplicaciones [HW-02] Servidor de desarrollo y pruebas [HW-03] Servidor de Web [HW-04] Servidor BBDD [HW-05] Servidor DNS/Proxy/Dominio [HW-06] Servidor de ficheros [HW-07] Servidor de Email [HW-08] Equipamiento de respaldo [HW-09] Enrutador de Internet [HW-10] Switch [HW-11] Cortafuegos [HW-12] Punto de acceso inalámbrico [HW-13] Equipos escritorio pc [HW-14] Portátiles [HW-15] Impresoras y escáneres [HW-16] Centralita [HW-17] Teléfono fijos [HW-18] Teléfonos móviles [HW-19] Cámaras de vigilancia	Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas

Soporte lógico que permite gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios.

AMBITO	ACTIVO	PROPIETARIO
APLICACIÓN [SW]	[[SW-01] Sistemas operativos [SW -02] Paquete ofimático [SW -03] Antivirus [SW -04] Software de desarrollo [SW -05] Software de contabilidad	Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica desarrollo Área técnica sistemas

	[SW -06] Email [SW -07] Servidores	Área técnica sistemas Área técnica sistemas

El activo que permite a la organización prestar sus servicios.

AMBITO	ACTIVO	PROPIETARIO
DATOS [D]	[D-01] Bases de datos [D-02] Datos de soporte y licencias [D-03] Desarrollos propios [D-04] Backups (copias de seguridad) [D-05] Correo electrónico [D-06] Logs de servidores y clientes [D-07] Credenciales y datos de control de acceso.	Responsable de sistemas Responsable de sistemas Responsable de sistemas Responsable de sistemas Responsable de sistemas Responsable de sistemas Responsable de sistemas

Instalaciones dedicadas como servicios de comunicaciones para medios de transporte que llevan datos de un sitio a otro.

AMBITO	ACTIVO	PROPIETARIO
RED [COM]	[COM-01] Internet [COM-02] Red inalámbrica [COM-03] Red cableada [COM-04] Telefonía fija [COM-05] Telefonía móvil	Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica desarrollo Área técnica sistemas

Funciones que satisfacen las necesidades de los usuarios prestados por el sistema.

AMBITO	ACTIVO	PROPIETARIO
SERVICIOS [SER]	[SER-01] Acceso remoto [SER -02] Red de control e instrumentación [SER -03] Acceso a internet [SER -04] Correo electrónico [SER -05] Servicio web [SER -06]Servicio aplicaciones [SER -07]Servicio ficheros	Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica sistemas Área técnica desarrollo Área técnica desarrollo Área técnica sistemas

Como equipamiento auxiliar se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

AMBITO	ACTIVO	PROPIETARIO
EQUIPAMIENTO AUXILIAR [AUX]	[AUX-01] Aire acondicionado [AUX -02 Archivadores [AUX -03] Consumibles varios [AUX -04] SAI [AUX -05] Corriente eléctrica	Director técnico Director técnico Director técnico Director técnico Director técnico

Las personas relacionadas con los sistemas de información.

AMBITO	ACTIVO	PROPIETARIO
PERSONAL [P]	[P-01] Director General [P-02] Director comercial [P-03] Director de proyectos [P-04] Director financiero	Director General Director comercial Director de proyectos Director financiero

	[P-05] Director Sistemas TI [P-06] Responsable seguridad de la información. [P-07] Key Account Manager [P-08] Técnicos de sistemas [P-09] Personal del departamento comercial [P-10] Personal del departamento de proyectos [P-11] Personal del departamento financiero	Director Sistemas TI Responsable seguridad de la información Key Account Manager Técnicos de sistemas Personal del departamento comercial Personal del departamento de proyectos Personal del departamento financiero

También podrían incluirse tres tipos de ámbitos adicionales, aunque no se van a tratar:

Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

AMBITO	ACTIVO
SOPORTES DE INFORMACIÓN [MEDIA]	[MEDIA-01] Almacenamiento en red [MEDIA-02] Almacenamiento en la nube [MEDIA -03] Cederrón (cd-rom) [MEDIA -04] DVD [MEDIA -05] Memorias USB [MEDIA -06] Material impreso

Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.

AMBITO	ACTIVO
SOPORTES DE INFORMACIÓN [ARCH]	[ARCH-01] Punto de acceso al servicio. [ARCH-02] Punto de interconexión.

La criptografía se emplea para proteger el secreto o autenticar a las partes.

AMBITO	ACTIVO
CLAVES CRIPTOGRÁFICAS[K]	[K-01] Cifrado de soportes de información. [K-02] Protección de la información. [K-03] Protección de las Comunicaciones.

4.3 VALORACIÓN DE ACTIVOS

Una vez se han identificado los activos relacionados con la seguridad de la información se efectuará la valoración de cada activo dentro de la organización. Con el objetivo final de garantizar la seguridad de los activos de la empresa. Para valorar el activo se han de tener en cuenta diferentes variables como son el coste de reposición, el valor del tiempo sin servicio, posibles penalizaciones, etc. Procurando que el coste de las medidas necesarias para garantizar la protección de los activos de la empresa no ha de superar el coste del activo que se tiene que proteger, en caso contrario, no sería rentable protegerlo y se consideraría más fácil sustituirlo.

Para la valoración de los activos, se utilizó la escala que propone MAGERIT en su Libro III (punto 2.1), completándolo con una estimación cuantitativa representada en términos monetarios para la organización.

El rango de la valoración económica:	RANGO	VALOR
Muy alta	Valor>50.000€	100.000€
Alta	10.000€<valor>50.000€	25.000€
Media	5.000€<valor>10.000€	7.500€
Baja	1.000€<valor>5.000€	2.500€
Muy baja	Valor<1.000€	1.000€

Tabla 4.Rango valoración económica

Análisis de dependencia de los Activos

Mediante los rangos establecidos en la tabla se podrá asignar una valoración de los activos en base a su valor económico.
Por otra parte, también se ha de tener en cuenta la jerarquización de los activos, identificando y valorando las dependencias entre activos. Un activo superior depende de otro activo inferior cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. De forma que en el caso de materializarse una amenaza en el activo inferior se perjudica sobre el activo superior. Esta información se puede representar en forma de árbol.

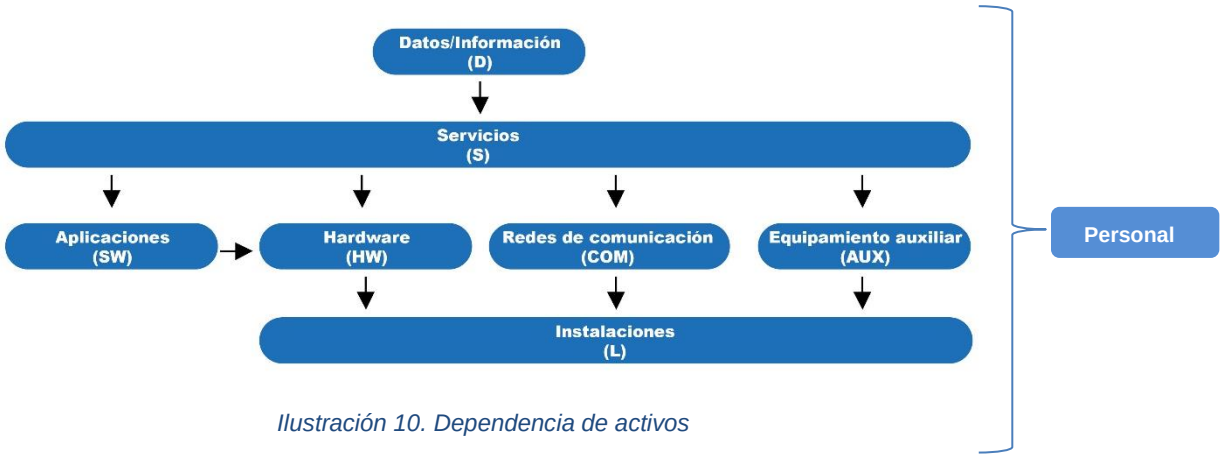


Ilustración 10. Dependencia de activos

En el árbol de dependencias se ubica en el nivel superior el activo más crítico de la empresa, la información. Por el contrario, el nivel inferior lo forma las Instalaciones, el cual no tiene dependencias. Y de forma transversal al resto de activos aparece el personal.

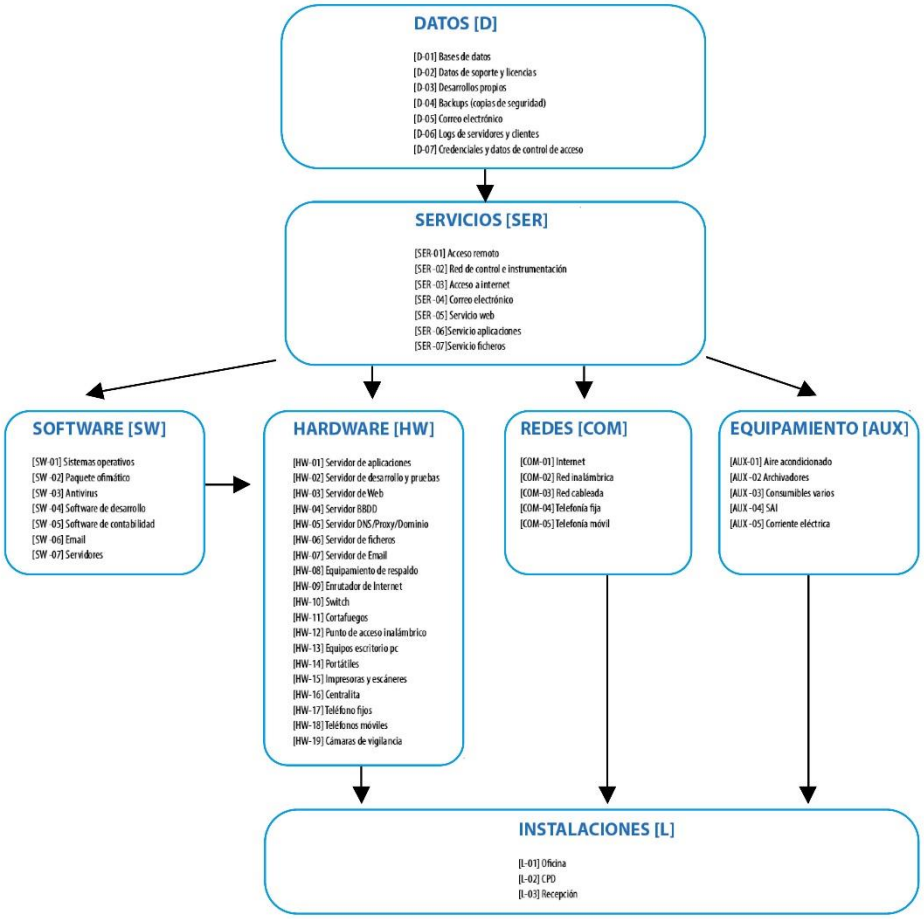


Ilustración 11.Dependencia de activos detallada

4.4 DIMENSIONES DE SEGURIDAD

Una vez identificados los activos se debe efectuar la valoración ACIDA de los mismos. Consiste en medir la criticidad del proceso de negocio en las cinco dimensiones de la seguridad de la información. Mediante esta valoración se podrá conocer el impacto que tendrá la materialización de una amenaza sobre el activo expuesto, sin salvaguardas. Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar.

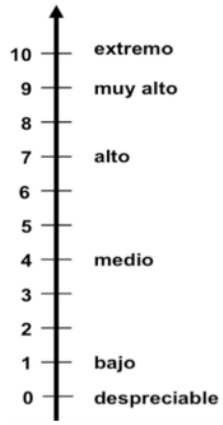
La valoración de Activos se realizará teniendo en cuenta las dimensiones de: Confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad definidas en Magerit como:

- Confiabilidad [C]: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Integridad [I]: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Autenticidad [A]: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Disponibilidad [D]: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo

requieren

- Trazabilidad [T]: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

El valor que reciba un activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Así pues, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar.
Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo).



Valor		Criterio
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

TABLA RESUMEN DE VALORACIÓN

A continuación se muestra la tabla resumen de valoración de las dimensiones de seguridad, Autenticidad, Criticidad, Integridad, Disponibilidad y Trazabilidad de los activos.

AMBITO	ACTIVO	NUMERO	VALOR	A	C	I	D	T
INSTALACIONES [L]	Oficina	[L-01]	Alto	7	8	8	9	5
	CPD	[L-02]	Muy Alto	9	9	9	9	9
	Recepción	[L-03]	Bajo	5	5	1	1	1
HARDWARE [HW]	Servidor de aplicaciones	[HW-01]	Alto	7	7	7	3	4
	Servidor de desarrollo y pruebas	[HW-02]	Medio	7	3	3	3	4
	Servidor de Web	[HW-03]	Alto	7	7	7	3	4
	Servidor BBDD	[HW-04]	Alto	9	5	5	9	4
	Servidor DNS/Proxy/Dominio	[HW-05]	Medio	7	1	3	3	4
	Servidor de ficheros	[HW-06]	Alto	9	5	5	9	4
	Servidor de Email	[HW-07]	Alto	9	5	5	9	4
	Equipamiento de respaldo	[HW-08]	Alto	7	7	7	3	4
	Enrutador de Internet	[HW-09]	Medio	5	5	5	5	5
	Switch	[HW-10]	Medio	5	5	5	5	5
	Cortafuegos	[HW-11]	Muy alto	9	9	9	9	9
	Punto de acceso inalámbrico	[HW-12]	Medio	5	3	3	3	3
	Equipos escritorio pc	[HW-13]	Medio	7	7	3	3	4
	Portátiles	[HW-14]	Medio	7	7	3	3	4
	Impresoras y escáneres	[HW-15]	Bajo	3	3	1	1	4
	Centralita	[HW-16]	Bajo	3	3	3	1	3
	Teléfonos fijos	[HW-17]	Bajo	3	3	3	1	3
	Teléfonos móviles	[HW-18]	Bajo	3	3	3	1	3
	Cámaras de vigilancia	[HW-19]	Medio	3	3	3	4	3
APLICACIÓN [SW]	Sistemas operativos	[SW-01]	Medio	3	7	7	3	3
	Paquete ofimático	[SW-02]	Bajo	3	3	3	1	
	Antivirus	[SW-03]	Medio	3	3	3	5	3
	Software de desarrollo	[SW-04]	Medio	5	7	5	5	3
	Software de contabilidad	[SW-05]	Medio	5	7	5	5	3
	Email	[SW-06]	Medio	3	3	3	5	3
	Servidores	[SW-07]	Alto	10	9	10	9	3
DATOS [D]	Bases de datos	[D-01]	Muy	10	9	10	9	10

			alto					
	Datos de soporte y licencias	[D-02]	Bajo	3	3	1	1	3
	Desarrollos propios	[D-03]	Medio	3	1	5	3	3
	Backups (copias de seguridad)	[D-04]	Alto	7	7	7	3	7
	Correo electrónico	[D-05]	Medio	3	1	5	3	3
	Logs de servidores y clientes	[D-06]	Medio	3	3	4	8	4
	Credenciales y datos de control de acceso.	[D-7]	Medio	3	3	4	8	4
RED [COM]	Internet	[COM-01]	Alto	3	9	9	3	7
	Red inalámbrica	[COM-02]	Medio	3	7	3	3	5
	Red cableada	[COM-03]	Alto	3	9	9	3	7
	Telefonía fija	[COM-04]	Medio	5	5	1	5	3
	Telefonía móvil	[COM-05]	Medio	5	5	1	5	3
SERVICIOS [SER]	Acceso remoto	[SER-01]	Bajo	1	3	1	1	0
	Red de control e instrumentación	[SER-02]	Bajo	0	0	0	1	0
	Acceso a internet	[SER-03]	Bajo	3	3	0	1	0
	Correo electrónico	[SER-04]	Bajo	3	3	5	3	7
	Servicio web	[SER-05]	Medio	5	5	5	5	5
	Servicio aplicaciones	[SER-06]	Medio	0	7	0	7	0
	Servicio ficheros	[SER-07]	Bajo	0	7	0	7	0
EQUIPAMIENTO AUXILIAR [AUX]	Aire acondicionado	[AUX-01]	Alto	9	9	9	9	0
	Archivadores	[AUX-02]	Bajo	3	1	1	3	0
	Consumibles varios	[AUX-03]	Bajo	1	1	1	3	0
	SAI	[AUX-04]	Alto	7	7	7	7	0
	Corriente eléctrica	[AUX-05]	Muy alto	9	9	9	9	0
PERSONAL [P]	Director General	[P-01]	Muy alto	9	3	3	3	3
	Director comercial	[P-02]	Medio	9	3	3	3	3
	Director de proyectos	[P-03]	Medio	9	3	3	3	3
	Director financiero	[P-04]	Medio	9	3	3	3	3
	Director Sistemas TI	[P-05]	Alto	9		7	7	9
	Responsable seguridad de la información.	[P-06]	Muy alto	9	7	7	7	7
	Key Account Manager	[P-07]	Medio	9	0	0	3	3
	Técnicos de sistemas	[P-08]	Medio	9	0	0	3	9
	Personal del departamento comercial	[P-09]	Bajo	3	0	0	3	3
	Personal del departamento de proyectos	[P-10]	Bajo	3	0	0	3	3
	Personal del departamento financiero	[P-11]	Bajo	3	0	0	1	3

Tabla 5. Resumen Valoración Activos

4.5 ANÁLISIS DE AMENAZAS

Una vez elaborado el inventario de los activos e identificado su valor. Se procede a analizar las amenazas utilizando la metodología MAGERIT. Los tipos de errores y amenazas pueden ser de diferentes tipos, según si se producen sin animosidad o deliberadamente. Un caso puede ser amenazas debidas a errores, nunca ataques deliberados; otro son amenazas debidos a ataques deliberados y el último modo, amenazas que pueden producirse tanto por error como deliberadamente. Se definen cuatro familias de amenazas:

[N] Desastres naturales. Amenazas naturales que pueden ocurrir.
[I] De origen industrial. Sucesos que pueden ocurrir en el desempeño de la actividad industrial. Pueden producirse de forma accidental o deliberada.
[E] Errores y fallos no intencionados.
[A] Ataques intencionados.

[N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen: Natural (accidental)

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. Ver: EBIOS: 01- INCENDIO	

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. Ver: EBIOS: 02- PERJUICIOS OCASIONADOS POR EL AGUA	

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. Ver: EBIOS: 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO	

09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN

[I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 01- INCENDIO	

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 02- PERJUICIOS OCASIONADOS POR EL AGUA	

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 04- SINIESTRO MAYOR	

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... Origen: Entorno (accidental) Humano (accidental o deliberado)	

Ver:
EBIOS: 03- CONTAMINACIÓN

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

[I.7] Condiciones inadecuadas de temperatura o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... Origen: Entorno (accidental) Humano (accidental o deliberado) Ver:	

EBIOS:
11- FALLAS EN LA CLIMATIZACIÓN

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: no disponible	

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [Media] soportes de información	Dimensiones: 1. [D] disponibilidad
Descripción: como consecuencia del paso del tiempo Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

[I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [C] confidencialidad
Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés “Transient Electromagnetic Pulse Standard”). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS	

[E] Errores y fallos no intencionados
Fallos no intencionales causados por las personas.
La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.
Origen:
Humano (accidental)

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. Ver: EBIOS: 38 - ERROR DE USO	

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación Ver: EBIOS: 38 - ERROR DE USO	

[E.3] Errores de monitorización (log)	
Tipos de activos: • [D.log] registros de actividad	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... Ver: EBIOS: no disponible	

[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	Dimensiones: 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	Dimensiones: 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.	

Acciones descoordinadas, errores por omisión, etc. Ver: EBIOS: no disponible

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	Dimensiones: 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Ver: EBIOS: no disponible	

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. Ver: EBIOS: no disponible	

[E.14] Escapes de información	
Tipos de activos: •	Dimensiones: 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Ver: EBIOS: no disponible	

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Ver: EBIOS: no disponible	

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	Dimensiones: 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. Ver: EBIOS: no disponible	

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	Dimensiones: 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Ver: EBIOS: no disponible	

[E.21] Errores de mantenimiento/actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	Dimensiones: 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. Ver: EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

[E.23] Errores de mantenimiento/actualización de programas (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. Ver: EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

[E.25] Pérdida de equipos	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Ver: EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... Ver: EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

[A] Ataques intencionados

Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:

Humano (deliberado)

[A.3] Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: Ver: EBIOS: no disponible	

[A.4] Manipulación de la configuración	
Tipos de activos: • [D.log] registros de actividad	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Ver:	

EBIOS: 40 - USURPACIÓN DE DERECHO

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Ver: EBIOS: 39 - ABUSO DE DERECHO	

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. Ver: EBIOS: no disponible	

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	Dimensiones: 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Ver: EBIOS: no disponible	

[A.9] Re-encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. Ver: EBIOS: no disponible	

[A.10] Alteración de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [I] integridad
Descripción:	

alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. Ver: EBIOS: 36 - ALTERACIÓN DE DATOS

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información 1. [C] confidencialidad • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

[A.12] Análisis de tráfico	
Tipos de activos: • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. Ver: EBIOS: no disponible	

[A.13] Repudio	
Tipos de activos: • [S] servicios • [D.log] registros de actividad	Dimensiones: 1. [I] integridad(trazabilidad)
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. Ver: EBIOS: 41 - NEGACIÓN DE ACCIONES	

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. Ver: EBIOS: 19 - ESCUCHA PASIVA	

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito)	Dimensiones: 1. [I] integridad

• [Media] soportes de información • [L] instalaciones	
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

[A.18] Destrucción de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

[A.19] Divulgación de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [C] confidencialidad
Descripción: revelación de información. Ver: EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (SW)	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Ver: EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

[A.23] Manipulación de los equipos	
Tipos de activos: • [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	Dimensiones: 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Ver: EBIOS: 25 - SABOTAJE DEL HARDWARE	

[A.24] Denegación de servicio	
Tipos de activos: • [S] servicios	Dimensiones: 1. [D] disponibilidad

• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Ver: EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. Ver: EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES	

[A.27] Ocupación enemiga	
Tipos de activos: • [L] instalaciones	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. Ver: EBIOS: no disponible	

[A.28] Indisposición del personal	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos... Ver: EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

[A.29] Extorsión	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [C] confidencialidad

	2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. Ver: EBIOS: no disponible	

[A.30] Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Ver: EBIOS: no disponible	

Para efectuar una valoración lo más exacta posible es necesario estimar la frecuencia de ocurrencia y el porcentaje de degradación.

- **Probabilidad de ocurrencia:** Representa la tasa anual de ocurrencia, es decir, cada cuanto se materializa una amenaza.

La frecuencia de ocurrencia se evalúa de acuerdo con los siguientes valores:

VALOR		CRITERIO	
Muy Alta [MA]	100	Una vez al día	Muy frecuente
Alta [A]	10	Una vez al mes	Frecuente
Media [M]	1	Una vez al año	Normal
Baja [B]	1/10	Una vez cada varios años	Poco frecuente
Muy baja [MB]	1/100	Cada muchos años.	Muy poco frecuente

Tabla 6. Valoración amenazas

- **Porcentaje de Degradación:** Significa el daño causado por un incidente. El grado de degradación se detalla para cada activo relacionándolos con amenaza y dimensión, se mide entre 0% y el 100%.

ACTIVO	FRECUENCIA		A	C	I	D	T
INSTALACIONES							
[L-01] – Oficina	Medio[M]	1	0%	100%	100%	100%	0%
[L-02] – CPD	Medio[M]	1	0%	100%	100%	100%	0%
[L-01] – Recepción	Medio[M]	1	0%	100%	100%	100%	0%
Listas de amenazas							
[N.1]Fuego	Muy baja [MB]	0,01				100%	
[N.2]Daños por agua	Baja[B]	0,1				75%	
[N.*]Desastres naturales	Baja[B]	0,1				75%	
[I.1] Fuego	Muy baja [MB]	0,01				100%	
[I.2] Daños por agua	Media[M]	1				100%	
[I.*]Desastres industriales	Baja[B]	0,1				100%	
[I.5] Avería de origen físico o lógico	Media[M]	1				75%	
[I.11] Emanaciones electromagnéticas	Baja[B]			40%			
[E.15] Alteración accidental de la información	Media[M]	1			100%		
[E.18] Destrucción de información	Alta[A]	10				100%	
[E.19] Fugas de información	Media[M]	1		100%			
[A.7] Uso no previsto	Media[M]	1		30%	30%	30%	
[A.11] Acceso no autorizado	Alta[A]	10		100%	100%		
[A.15] Modificación deliberada de la información	Media[M]	1			50%		
[A.19] Divulgación de la información	Media[M]	1		100%			
[A.26] Ataque destructivo	Media[M]	1				100%	
HARDWARE							
[HW – 01] Servidor de aplicaciones	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 02] Servidor de desarrollo y pruebas	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 03] Servidor web	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 04] Servidor BBDD	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 05] Servidor DNS/Proxy/Dominio	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 06] Servidor de ficheros	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 07] Servidor de email	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 08] Equipo de respaldo	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 09] Enrutador de Internet	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 10] Switch	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 11] Cortafuegos	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 12] Punto acceso wifi	Medio[M]	1	0%	100%	50%	100%	0%
[HW – 13] Ordenadores	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 14] Portátiles	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 15] Impresoras y escaneres	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 16] Centralita	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 17] Teléfono fijo	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 18] Teléfonos móviles	Medio[M]	1	0%	100%	30%	100%	0%
[HW – 19] Cámaras de vigilancia	Medio[M]	1	0%	100%	30%	100%	0%
Listas de amenazas							
[N.1]Fuego	Muy baja	0,01				100%	

	[MB]						
[N.2]Daños por agua	Muy baja [MB]	0,01				100%	
[N.*]Desastres naturales	Muy baja [MB]	0,01				100%	
[I.1] Fuego	Baja [MB]	0,1				100%	
[I.2] Daños por agua	Muy baja [MB]	0,01				50%	
[I.*] Desastres industriales	Muy baja [MB]	0,01				50%	
[I.3] Contaminación mecánica	Media[M]	1				50%	
[I.4] Contaminación electromagnética	Media[M]	1				50%	
[I.5] Avería de origen físico o lógico.	Baja[B]	0,1				50%	
[I.6] Corte de suministro eléctrico.	Media[M]	1				20%	
[I.7] Condiciones inadecuadas de temperatura o humedad.	Media[M]	1				100%	
[I.11] Emanaciones electromagnéticas	Baja[B]	0,1		100%			
[E.2] Errores del administrador	Media[M]	1		100%	30%	100%	
[E.23] Errores de mantenimiento	Media[M]	1				100%	
[E.24] Caída del sistema por agotamiento de recursos	Baja[B]	0,1				50%	
[E.25] Pérdida de equipos	Baja [MB]	0,1		100%		100%	
[A.7] Uso no previsto	Media[M]	1		100%	30%	100%	
[A.11]Acceso no autorizado	Media[M]	1		50%	30%		
[A.23]Manipulación de los equipos	Media[M]	1		50%		50%	
[A.24] Denegación de servicio	Media[M]	1				100%	
[A.25]Robo	Muy baja [MB]	0,01		100%		100%	
[A.26]Ataque destructivo	Muy baja [MB]	0,01				100%	
SOFTWARE							
[SW - 01] Sistemas operativos	Alta [A]	10	100%	100%	100%	100%	30%
[SW-02] – Paquete ofimático	Alta [A]	10	100%	100%	100%	100%	30%
[SW-03] - Antivirus	Alta [A]	10	100%	100%	100%	100%	30%
[SW-04] – Software desarrollo	Alta [A]	10	100%	100%	100%	100%	30%
[SW-05] – Software de contabilidad	Alta [A]	10	100%	100%	100%	100%	30%
[SW-06] – Email	Alta [A]	10	100%	100%	100%	100%	30%
[SW-07] – Servidores	Alta [A]	10	100%	100%	100%	100%	30%
Listas de amenazas							
[I.5] Avería de origen físico o lógico	Media[M]					100%	
[E.1] Errores de los usuarios	Alta [A]			100%	80%	100%	
[E.2]Errores del administrador	Alta [A]			100%	80%	100%	
[E.8]Difusión de SW dañino	Media[M]			75%	75%	75%	
[E.9] Errores de re-encaminamiento	Muy Baja [MB]			50%			
[E.15]Alteración accidental de la información	Alta [A]				20%		
[E.18]Destrucción de la información	Alta [A]					30%	30%
[E.19]Fugas de información	Media [M]			50%			

[E.20]Vulnerabilidades de los programas	Alta [A]			50%	20%	5%	
[E.21]Errores de mantenimiento	Alta [A]				5%	5%	
[A.5]Suplantación de la identidad del usuario	Media [M]		100%	100%	50%		
[A.6]Abuso de privilegios de acceso	Alta [A]			50%	20%	20%	
[A.7] Uso no previsto	Alta [A]			50%	20%	20%	
[A.8] Difusión de software dañino	Media [M]			100%	100%	100%	
[A.9] Re-encaminamiento de mensajes	Media [M]			50%			
[A.10] Alteración de secuencia	Media [M]				50%		
[A.11]Acceso no autorizado	Media [M]			50%	30%		
[A.15]Modificación deliberada de la información	Media [M]				50%		
[A.18]Destrucción de información	Media [M]					50%	
[A.19]Divulgación de información	Media [M]			50%			
[A.22]Manipulación de programas	Media [M]			50%	50%	50%	
DATOS							
[D-01] Bases de datos	Alta [A]	10	100%	100%	30%	100%	0%
[D-02] Datos de soporte y licencias	Alta [A]	10	100%	100%	30%	100%	0%
[D-03] Desarrollos propios	Alta [A]	10	100%	100%	30%	100%	0%
[D-04] Backups copias de seguridad)	Alta [A]	10	100%	100%	30%	100%	0%
[D-5] Correo electrónico	Alta [A]	10	100%	100%	30%	100%	0%
[D-06] Logs de servidores y clientes	Alta [A]	10	100%	100%	30%	100%	0%
[D-07] Credenciales y datos de control de acceso	Alta [A]	10	100%	100%	30%	100%	0%
Lista de amenazas							
[E.1]Errores de los usuarios	Muy Baja [MB]	0,01		20%	20%	20%	
[E.2]Errores del administrador	Baja[B]	0,1		20%	30%	30%	
[E.3] Errores de monitorización(log)	Baja[B]	0,1			30%		
[E.4] Errores de configuración (conf)	Alta[A]	10			20%		
[E.14] Escapes de información	Medio[M]	1		50%			
[E.15]Alteración accidental de la información	Alta[A]	10			20%		
[E.18]Destrucción de la información	Alta[A]	10				50%	
[E.19]Fugas de información	Media[M]	1		30%			
[A.3] Manipulación de los registros de actividad (log)	Baja[B]	0,1			30%		
[A.4] Manipulación de la configuración	Baja[B]	0,1		50%	20%	20%	
[A.5]Suplantación de la identidad del usuario	Media[M]	1	100%	50%	20%		
[A.6]Abuso de privilegios de acceso	Media[M]	1		30%	5%	5%	
[A.11] Acceso no autorizado	Media[M]	1		30%	30%		
[A.15]Modificación deliberada de la información	Media[M]	1			30%		
[A.18]Destrucción de información	Baja [MB]	0,1				100%	
[A.19]Divulgación de información	Baja [MB]	0,1		100%			
RED							

[COM-01] – Internet	Media[M]	1	50%	50%	30%	50%	0%
[COM-02] – Red inalámbrica	Media[M]	1	50%	50%	30%	50%	0%
[COM-03] – Red cableada	Media[M]	1	50%	50%	30%	50%	0%
[COM-04] – Telefonía fija	Media[M]	1	50%	50%	30%	50%	0%
[COM-05] – Telefonía móvil	Media[M]	1	50%	50%	30%	50%	0%
Listas de amenazas							
[E.2] Errores de administrador	Media[M]	1		20%	5%	50%	
[E.9] Errores de reencaminamiento	Muy baja [MB]	0,01		5%			
[E.14] Escapes de información	Muy baja [MB]	0,01		5%		5%	
[E.15] Alteración accidental de la información	Media[M]	1				5%	
[E.18] Destrucción de la información	Media[M]	1				50%	
[E.19] Fugas de información	Media[M]	1		50%			
[E.24] Caída del Sistema por agotamiento de recursos	Media[M]	1				50%	
[A.5] Suplantación de la identidad del usuario	Baja[B]	0,1	50%	30%	30%		
[A.6] Abuso de privilegios de acceso	Baja[B]	0,1		30%	30%	30%	
[A.7] Uso no previsto	Baja[B]	0,1		5%	50%	5%	
[A.9] Reencaminamiento de mensajes	Media[M]	1		5%			
[A.10] Alteración de secuencia	Media[M]	1			30%		
[A.11] Acceso no autorizado	Media[M]	1		50%	30%		
[A.12] Análisis de tráfico	Baja[B]	0,1		30%			
[A.14] Interceptación de información	Media[M]	1		50%			
[A.15] Modificación deliberada de la información	Media[M]	1			50%		
[A.19] Divulgación de la información	Baja[B]	0,1		50%			
[A.24] Denegación de servicio	Baja[B]	0,1				50%	
SERVICIOS							
[SER-01] – Acceso remoto	Alto[A]	10	100%	100%	50%	100%	0%
[SER-02] – Red de control e instrumentación	Alto[A]	10	100%	100%	50%	100%	0%
[SER-03] – Acceso a internet	Alto[A]	10	100%	100%	50%	100%	0%
[SER-04] – Correo electrónico	Alto[A]	10	100%	100%	50%	100%	0%
[SER-05] – Servicios web	Alto[A]	10	100%	100%	50%	100%	0%
[SER-06] – Servicio de aplicaciones	Alto[A]	10	100%	100%	50%	100%	0%
[SER-07] – Servicio ficheros	Alto[A]	10	100%	100%	50%	100%	0%
Listas de amenazas							
[E.1] Errores de los usuarios	Muy baja [MB]	0,01		5%	5%	5%	
[E.2] Errores de administrador	Baja[B]	0,1		5%	20%	20%	
[E.9] Errores de re-encaminamiento	Baja[B]	0,1		5%			
[E.15] Alteración accidental información	Muy baja [MB]	0,01			5%		
[E.18] Destrucción de información	Alta[A]	10				100%	
[E.19] Fugas de información	Alta[A]	10		20%			
[E.24] Caída del sistema por agotamiento de recursos	Media[M]	1				20%	

[A.5] Suplantación de identidad	Media[M]	1	100%	50%	20%		
[A.6] Abuso de privilegios	Alta[A]	10		20%	20%	50%	
[A.7] Uso no previsto	Alta[A]	10		5%	50%	5%	
[A.9] Re- encaminamiento de mensajes	Media[M]	1		50%			
[A.10] Alteración de secuencia	Baja[B]	0,1			30%		
[A.11] Acceso no autorizado	Media[M]	1		75%	50%		
[A.13] Repudio	Baja[B]	0,1			50%		
[A.15] Modificación deliberada de la información	Media[M]	1			50%		
[A.18] Destrucción de la información	Media[M]	1			50%		
[A.19] Divulgación de información	Media[M]	1		100%			
[A.24]Denegación de servicio	Media[M]	1				100%	
EQUIPAMIENTO AUXILIAR							
[AUX-01] – Aire acondicionado	Medio[M]	1	0%	50%	30%	100%	0%
[AUX-02] – Archivadores varios	Media[M]	1	0%	50%	30%	100%	0%
[AUX-03] – Consumibles varios	Media[M]	1	0%	50%	30%	100%	0%
[AUX-04] – SAI	Medio[M]	1	0%	50%	30%	100%	0%
[AUX-05] – Corriente eléctrica	Medio[M]	1	0%	50%	30%	100%	0%
Listas de amenazas							
[N.1]Fuego	Muy baja [MB]	0,01				100%	
[N.2]Daños por agua	Muy baja [MB]	0,01				100%	
[N.*]Desastres naturales	Muy baja [MB]	0,01				100%	
[I.1] Fuego	Muy baja [MB]	0,01				100%	
[I.2] Daños por agua	Muy baja [MB]	0,01				100%	
[I.*] Desastres industriales	Muy baja [MB]	0,01				100%	
[I.3] Contaminación mecánica	Baja[B]	0,1				100%	
[I.4] Contaminación electromagnética	Muy baja [MB]	0,01				5%	
[I.6] Corte de suministro eléctrico.	Media[M]	1				20%	
[I.7] Condiciones inadecuadas de temperatura o humedad.	Baja[B]	0,1				20%	
[I.9] Interrupción de otros servicios y suministros esenciales	Baja[B]	0,1				20%	
[I.11] Emanaciones electromagnéticas	Muy baja [MB]	0,01		20%			
[E.23] Errores de mantenimiento	Media[M]	1				50%	
[E.25] Pérdida de equipos	Media[M]	1		50%		50%	
[A.7] Uso no previsto	Alto[A]	10		50%	30%	50%	
[A.11]Acceso no autorizado	Media[M]	1		50%	30%		
[A.23]Manipulación de los equipos	Alto[A]	10		50%		75%	
[A.25]Robo	Medio[M]	1		50%		100%	
[A.26]Ataque destructivo	Bajo[B]	0,1				100%	
PERSONAL							
[P-01] - Director General	Alto[A]	10	0%	20%	30%	100%	0%
[P-02] - Director comercial	Alto[A]	10	0%	20%	30%	100%	0%

[P-03] - Director de proyectos	Alta[A]	10	0%	20%	30%	100%	0%
[P-04] - Director financiero	Alta[A]	10	0%	20%	30%	100%	0%
[P-05] - Director de Sistemas TI	Alta[A]	10	0%	20%	30%	100%	0%
[P-06] - Responsable de seguridad de la información	Alta[A]	10	0%	20%	30%	100%	0%
[P-07] - Key Account Manager	Alta[A]	10	0%	20%	30%	100%	0%
[P-08] - Técnicos de sistemas	Alta[A]	10	0%	20%	30%	100%	0%
[P-09] - Personal departamento comercial	Alta[A]	10	0%	20%	30%	100%	0%
[P-10] - Personal departamento proyectos	Alta[A]	10	0%	20%	30%	100%	0%
[P-11] - Personal departamento financiero	Alta[A]	10	0%	20%	30%	100%	
		Listas de amenazas					
[E.7] Deficiencias en la organización	Baja[B]	0,1				5%	
[E.19]Fugas de información	Baja[B]	0,1		20%			
[E.28] Indisponibilidad del personal	Alta[A]	10				100%	
[E.29]Extorsión	Muy Baja [MB]	0,01		20%	20%	20%	
[E.30]Ingeniería social(picaresca)	Media[M]	1		20%	30%	30%	

4.6 IMPACTO POTENCIAL

Una vez obtenidos los valores de los diferentes activos y la tabla de valoración de amenazas, se determina el impacto potencial que ocasionaría la materialización de dichas amenazas. En el cálculo, no se tienen en cuenta contramedidas, ni salvaguardas. El impacto y posteriormente el riesgo son datos relevantes, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen los controles.

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

Impacto potencial = valor del activo X valor del impacto

Entendido el valor del activo de cada dimensión y el impacto como la degradación en cada dimensión en la que se ve afectado el activo.

Según el método MAGERIT en su libro II apartado 2.1 se puede calcular el valor del impacto en base a la siguiente tabla sencilla.
La tabla para calcular el impacto:

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 7. Impacto

La estimación del impacto:

MA: Si el hecho se materializará tendría consecuencias o efectos desastrosos en la organización. Afecta a toda la organización. Multas por incumplimiento de la legislación. Suspensión de las actividades misionales de la organización.

A: Si el hecho se materializará tendría consecuencias o efectos muy graves en la organización.

M: Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización. Afecta un conjunto de datos personales o el proceso.

B: Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización. Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.

MB: Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización. Afecta a una actividad del proceso.

Seguidamente se muestra la tabla de cálculo del impacto en los activos.

			VALORACIÓN ACTIVOS					VALORACIÓN AMENAZAS					VALORACIÓN IMPACTO				
NUMERO	ACTIVO	VALOR	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
[L-01]	Oficina	Alto	7	8	8	9	5	0%	100%	100%	100%	0%	0	8	8	9	0
[L-02]	CPD	Muy Alto	9	9	9	9	9	0%	100%	100%	100%	0%	0	9	9	9	0
[L-03]	Recepción	Bajo	5	5	1	1	1	0%	100%	100%	100%	0%	0	5	1	1	0
[HW-01]	Servidor de aplicaciones	Alto	7	7	7	3	4	0%	100%	30%	100%	0%	0	7	2,1	3	0
[HW-02]	Servidor de desarrollo y pruebas	Medio	7	3	3	3	4	0%	100%	30%	100%	0%	0	3	0,9	3	0
[HW-03]	Servidor de Web	Alto	7	7	7	3	4	0%	100%	30%	100%	0%	0	7	2,1	3	0
[HW-04]	Servidor BBDD	Alto	9	5	5	9	4	0%	100%	30%	100%	0%	0	5	1,5	9	0
[HW-05]	Servidor DNS/Proxy/Dominio	Medio	7	1	3	3	4	0%	100%	30%	100%	0%	0	1	0,9	3	0
[HW-06]	Servidor de ficheros	Alto	9	5	5	9	4	0%	100%	30%	100%	0%	0	5	1,5	9	0
[HW-07]	Servidor de Email	Alto	9	5	5	9	4	0%	100%	30%	100%	0%	0	5	1,5	9	0
[HW-08]	Equipamiento de respaldo	Alto	7	7	7	3	4	0%	100%	30%	100%	0%	0	7	2,1	3	0
[HW-09]	Enrutador de Internet	Medio	5	5	5	5	5	0%	100%	30%	100%	0%	0	5	1,5	5	0
[HW-10]	Switch	Medio	5	5	5	5	5	0%	100%	30%	100%	0%	0	5	1,5	5	0
[HW-11]	Cortafuegos	Muy alto	9	9	9	9	9	0%	100%	30%	100%	0%	0	9	2,7	9	0
[HW-12]	Punto de acceso inalámbrico	Medio	5	3	3	3	3	0%	100%	50%	100%	0%	0	3	1,5	3	0
[HW-13]	Equipos escritorio pc	Medio	7	7	3	3	4	0%	100%	30%	100%	0%	0	7	0,9	3	0
[HW-14]	Portátiles	Medio	7	7	3	3	4	0%	100%	30%	100%	0%	0	7	0,9	3	0
[HW-15]	Impresoras y escáneres	Bajo	3	3	1	1	4	0%	100%	30%	100%	0%	0	3	0,3	1	0
[HW-16]	Centralita	Bajo	3	3	3	1	3	0%	100%	30%	100%	0%	0	3	0,9	1	0
[HW-17]	Teléfonos fijos	Bajo	3	3	3	1	3	0%	100%	30%	100%	0%	0	3	0,9	1	0
[HW-18]	Teléfonos móviles	Bajo	3	3	3	1	3	0%	100%	30%	100%	0%	0	3	0,9	1	0
[HW-19]	Cámaras de vigilancia	Medio	3	3	3	4	3	0%	100%	30%	100%	0%	0	3	0,9	4	0
[SW-01]	Sistemas operativos	Medio	3	7	7	3	3	100%	100%	100%	100%	30%	3	7	7	3	0,9
[SW-02]	Paquete ofimático	Bajo	3	3	3	1		100%	100%	100%	100%	30%	3	3	3	1	0
[SW-03]	Antivirus	Medio	3	3	3	5	3	100%	100%	100%	100%	30%	3	3	3	5	0,9
[SW-04]	Software de desarrollo	Medio	5	7	5	5	3	100%	100%	100%	100%	30%	5	7	5	5	0,9
[SW-05]	Software de contabilidad	Medio	5	7	5	5	3	100%	100%	100%	100%	30%	5	7	5	5	0,9
[SW-06]	Email	Medio	3	3	3	5	3	100%	100%	100%	100%	30%	3	3	3	5	0,9
[SW-07]	Servidores	Alto	10	9	10	9	3	100%	100%	100%	100%	30%	10	9	10	9	0,9
[D-01]	Bases de datos	Muy alto	10	9	10	9	10	100%	100%	30%	100%	0%	10	9	3	9	0
[D-02]	Datos de soporte y licencias	Bajo	3	3	1	1	3	100%	100%	30%	100%	0%	3	3	0,3	1	0

[D-03]	Desarrollos propios	Medio	3	1	5	3	3	100%	100%	30%	100%	0%	3	1	1,5	3	0
[D-04]	Backups (copias de seguridad)	Alto	7	7	7	3	7	100%	100%	30%	100%	0%	7	7	2,1	3	0
[D-05]	Correo electrónico	Medio	3	1	5	3	3	100%	100%	30%	100%	0%	3	1	1,5	3	0
[D-06]	Logs de servidores y clientes	Medio	3	3	4	8	4	100%	100%	30%	100%	0%	3	3	1,2	8	0
[D-7]	Credenciales y datos de control de acceso.	Medio	3	3	4	8	4	100%	100%	30%	100%	0%	3	3	1,2	8	0
[COM-01]	Internet	Alto	3	9	9	3	7	50%	50%	30%	50%	0%	1,5	4,5	2,7	1,5	0
[COM-02]	Red inalámbrica	Medio	3	7	3	3	5	50%	50%	30%	50%	0%	1,5	3,5	0,9	1,5	0
[COM-03]	Red cableada	Alto	3	9	9	3	7	50%	50%	30%	50%	0%	1,5	4,5	2,7	1,5	0
[COM-04]	Telefonía fija	Medio	5	5	1	5	3	50%	50%	30%	50%	0%	2,5	2,5	0,3	2,5	0
[COM-05]	Telefonía móvil	Medio	5	5	1	5	3	50%	50%	30%	50%	0%	2,5	2,5	0,3	2,5	0
[SER-01]	Acceso remoto	Bajo	1	3	1	1	0	100%	100%	50%	100%	0%	1	3	0,5	1	0
[SER-02]	Red de control e instrumentación	Bajo	0	0	0	1	0	100%	100%	50%	100%	0%	0	0	0	1	0
[SER-03]	Acceso a internet	Bajo	3	3	0	1	0	100%	100%	50%	100%	0%	3	3	0	1	0
[SER-04]	Correo electrónico	Bajo	3	3	5	3	7	100%	100%	50%	100%	0%	3	3	2,5	3	0
[SER-05]	Servicio web	Medio	5	5	5	5	5	100%	100%	50%	100%	0%	5	5	2,5	5	0
[SER-06]	Servicio aplicaciones	Medio	0	7	0	7	0	100%	100%	50%	100%	0%	0	7	0	7	0
[SER-07]	Servicio ficheros	Bajo	0	7	0	7	0	100%	100%	50%	100%	0%	0	7	0	7	0
[AUX-01]	Aire acondicionado	Alto	9	9	9	9	0	0%	50%	30%	100%	0%	0	4,5	2,7	9	0
[AUX-02]	Archivadores	Bajo	3	1	1	3	0	0%	50%	30%	100%	0%	0	0,5	0,3	3	0
[AUX-03]	Consumibles varios	Bajo	1	1	1	3	0	0%	50%	30%	100%	0%	0	0,5	0,3	3	0
[AUX-04]	SAI	Alto	7	7	7	7	0	0%	50%	30%	100%	0%	0	3,5	2,1	7	0
[AUX-05]	Corriente eléctrica	Muy alto	9	9	9	9	0	0%	50%	30%	100%	0%	0	4,5	2,7	9	0
[P-01]	Director General	Muy alto	9	3	3	3	3	0%	20%	30%	100%	0%	0	0,6	0,9	3	0
[P-02]	Director comercial	Medio	9	3	3	3	3	0%	20%	30%	100%	0%	0	0,6	0,9	3	0
[P-03]	Director de proyectos	Medio	9	3	3	3	3	0%	20%	30%	100%	0%	0	0,6	0,9	3	0
[P-04]	Director financiero	Medio	9	3	3	3	3	0%	20%	30%	100%	0%	0	0,6	0,9	3	0
[P-05]	Director Sistemas TI	Alto	9		7	7	9	0%	20%	30%	100%	0%	0	0	2,1	7	0
[P-06]	Responsable seguridad de la información.	Muy alto	9	7	7	7	7	0%	20%	30%	100%	0%	0	1,4	2,1	7	0
[P-07]	Key Account Manager	Medio	9	0	0	3	3	0%	20%	30%	100%	0%	0	0	0	3	0
[P-08]	Técnicos de sistemas	Medio	9	0	0	3	9	0%	20%	30%	100%	0%	0	0	0	3	0
[P-09]	Personal del departamento comercial	Bajo	3	0	0	3	3	0%	20%	30%	100%	0%	0	0	0	3	0
[P-10]	Personal del departamento de proyectos	Bajo	3	0	0	3	3	0%	20%	30%	100%	0%	0	0	0	3	0

[P-11]	Personal del departamento financiero	Bajo	3	0	0	1	3	0%	20%	30%	100%	0%	0	0	0	1	0

4.7 NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Una vez calculado el nivel del Impacto Potencial por cada activo, de igual forma se deberá calcular el nivel del riesgo al cual se encuentra sometida la empresa. Para obtener el riesgo se debe integrar la frecuencia con que se puede dar un hecho concreto en nuestros sistemas. Se debe designar un límite a partir del cual podamos decidir si asumir o no un riesgo para determinado activo.
Para ello usaremos el siguiente cálculo:

Riesgo = Impacto Potencial * Frecuencia

Los niveles de evaluación del riesgo nos indicarán el estado actual de seguridad de la empresa y ayudará a decidir si se implementan controles o no, estableciendo un nivel de riesgo aceptable, de tal manera que se puedan designar recursos para implementar controles que ayuden a minimizar los riegos sobre los activos que superen los niveles de riesgo aceptable.

Según el método MAGERIT en su libro II apartado 2.1 se puede calcular el valor del impacto en base a la siguiente tabla sencilla.

Impacto, probabilidad y riesgo se modelan por medio de escalas cualitativas:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo.

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

A continuación, aparece la tabla de cálculo del riesgo de los activos.

					VALORACIÓN IMPACTO					VALORACIÓN RIESGO				
NUMERO	ACTIVO	VALOR	FRECUENCIA		A	C	I	D	T	A	C	I	D	T
[L-01]	Oficina	Alto	Medio[M]	1	0	8	8	9	0	0	8	8	9	0
[L-02]	CPD	Muy Alto	Medio[M]	1	0	9	9	9	0	0	9	9	9	0
[L-03]	Recepción	Bajo	Medio[M]	1	0	5	1	1	0	0	5	1	1	0
[HW-01]	Servidor de aplicaciones	Alto	Medio[M]	1	0	7	2,1	3	0	0	7	2,1	3	0
[HW-02]	Servidor de desarrollo y pruebas	Medio	Medio[M]	1	0	3	0,9	3	0	0	3	0,9	3	0
[HW-03]	Servidor de Web	Alto	Medio[M]	1	0	7	2,1	3	0	0	7	2,1	3	0
[HW-04]	Servidor BBDD	Alto	Medio[M]	1	0	5	1,5	9	0	0	5	1,5	9	0
[HW-05]	Servidor DNS/Proxy/Dominio	Medio	Medio[M]	1	0	1	0,9	3	0	0	1	0,9	3	0
[HW-06]	Servidor de ficheros	Alto	Medio[M]	1	0	5	1,5	9	0	0	5	1,5	9	0
[HW-07]	Servidor de Email	Alto	Medio[M]	1	0	5	1,5	9	0	0	5	1,5	9	0
[HW-08]	Equipamiento de respaldo	Alto	Medio[M]	1	0	7	2,1	3	0	0	7	2,1	3	0
[HW-09]	Enrutador de Internet	Medio	Medio[M]	1	0	5	1,5	5	0	0	5	1,5	5	0
[HW-10]	Switch	Medio	Medio[M]	1	0	5	1,5	5	0	0	5	1,5	5	0
[HW-11]	Cortafuegos	Muy alto	Medio[M]	1	0	9	2,7	9	0	0	9	2,7	9	0
[HW-12]	Punto de acceso inalámbrico	Medio	Medio[M]	1	0	3	1,5	3	0	0	3	1,5	3	0
[HW-13]	Equipos escritorio pc	Medio	Medio[M]	1	0	7	0,9	3	0	0	7	0,9	3	0
[HW-14]	Portátiles	Medio	Medio[M]	1	0	7	0,9	3	0	0	7	0,9	3	0
[HW-15]	Impresoras y escáneres	Bajo	Medio[M]	1	0	3	0,3	1	0	0	3	0,3	1	0
[HW-16]	Centralita	Bajo	Medio[M]	1	0	3	0,9	1	0	0	3	0,9	1	0
[HW-17]	Teléfonos fijos	Bajo	Medio[M]	1	0	3	0,9	1	0	0	3	0,9	1	0
[HW-18]	Teléfonos móviles	Bajo	Medio[M]	1	0	3	0,9	1	0	0	3	0,9	1	0
[HW-19]	Cámaras de vigilancia	Medio	Medio[M]	1	0	3	0,9	4	0	0	3	0,9	4	0
[SW-01]	Sistemas operativos	Medio	Alta [A]	10	3	7	7	3	0,9	30	70	70	30	9
[SW-02]	Paquete ofimático	Bajo	Alta [A]	10	3	3	3	1	0	30	30	30	10	0
[SW-03]	Antivirus	Medio	Alta [A]	10	3	3	3	5	0,9	30	30	30	50	9
[SW-04]	Software de desarrollo	Medio	Alta [A]	10	5	7	5	5	0,9	50	70	50	50	9
[SW-05]	Software de contabilidad	Medio	Alta [A]	10	5	7	5	5	0,9	50	70	50	50	9
[SW-06]	Email	Medio	Alta [A]	10	3	3	3	5	0,9	30	30	30	50	9
[SW-07]	Servidores	Alto	Alta [A]	10	10	9	10	9	0,9	100	90	100	90	9
[D-01]	Bases de datos	Muy alto	Alta [A]	10	10	9	3	9	0	100	90	30	90	0
[D-02]	Datos de soporte y licencias	Bajo	Alta [A]	10	3	3	0,3	1	0	30	30	3	10	0
[D-03]	Desarrollos propios	Medio	Alta [A]	10	3	1	1,5	3	0	30	10	15	30	0
[D-04]	Backups (copias de seguridad)	Alto	Alta [A]	10	7	7	2,1	3	0	70	70	21	30	0
[D-05]	Correo electrónico	Medio	Alta [A]	10	3	1	1,5	3	0	30	10	15	30	0
[D-06]	Logs de servidores y clientes	Medio	Alta [A]	10	3	3	1,2	8	0	30	30	12	80	0
[D-7]	Credenciales y datos de control de acceso.	Medio	Alta [A]	10	3	3	1,2	8	0	30	30	12	80	0
[COM-01]	Internet	Alto	Media[M]	1	1,5	4,5	2,7	1,5	0	1,5	4,5	2,7	1,5	0
[COM-02]	Red inalámbrica	Medio	Media[M]	1	1,5	3,5	0,9	1,5	0	1,5	3,5	0,9	1,5	0

[COM-03]	Red cableada	Alto	Media[M]	1	1,5	4,5	2,7	1,5	0	1,5	4,5	2,7	1,5	0
[COM-04]	Telefonía fija	Medio	Media[M]	1	2,5	2,5	0,3	2,5	0	2,5	2,5	0,3	2,5	0
[COM-05]	Telefonía móvil	Medio	Media[M]	1	2,5	2,5	0,3	2,5	0	2,5	2,5	0,3	2,5	0
[SER-01]	Acceso remoto	Bajo	Alto[A]	10	1	3	0,5	1	0	10	30	5	10	0
[SER-02]	Red de control e instrumentación	Bajo	Alto[A]	10	0	0	0	1	0	0	0	0	10	0
[SER-03]	Acceso a internet	Bajo	Alto[A]	10	3	3	0	1	0	30	30	0	10	0
[SER-04]	Correo electrónico	Bajo	Alto[A]	10	3	3	2,5	3	0	30	30	25	30	0
[SER-05]	Servicio web	Medio	Alto[A]	10	5	5	2,5	5	0	50	50	25	50	0
[SER-06]	Servicio aplicaciones	Medio	Alto[A]	10	0	7	0	7	0	0	70	0	70	0
[SER-07]	Servicio ficheros	Bajo	Alto[A]	10	0	7	0	7	0	0	70	0	70	0
[AUX-01]	Aire acondicionado	Alto	Medio[M]	1	0	4,5	2,7	9	0	0	4,5	2,7	9	0
[AUX-02]	Archivadores	Bajo	Media[M]	1	0	0,5	0,3	3	0	0	0,5	0,3	3	0
[AUX-03]	Consumibles varios	Bajo	Media[M]	1	0	0,5	0,3	3	0	0	0,5	0,3	3	0
[AUX-04]	SAI	Alto	Medio[M]	1	0	3,5	2,1	7	0	0	3,5	2,1	7	0
[AUX-05]	Corriente eléctrica	Muy alto	Medio[M]	1	0	4,5	2,7	9	0	0	4,5	2,7	9	0
[P-01]	Director General	Muy alto	Alto[A]	10	0	0,6	0,9	3	0	0	6	9	30	0
[P-02]	Director comercial	Medio	Alto[A]	10	0	0,6	0,9	3	0	0	6	9	30	0
[P-03]	Director de proyectos	Medio	Alta[A]	10	0	0,6	0,9	3	0	0	6	9	30	0
[P-04]	Director financiero	Medio	Alta[A]	10	0	0,6	0,9	3	0	0	6	9	30	0
[P-05]	Director Sistemas TI	Alto	Alta[A]	10	0	0	2,1	7	0	0	0	21	70	0
[P-06]	Responsable seguridad de la información.	Muy alto	Alta[A]	10	0	1,4	2,1	7	0	0	14	21	70	0
[P-07]	Key Account Manager	Medio	Alta[A]	10	0	0	0	3	0	0	0	0	30	0
[P-08]	Técnicos de sistemas	Medio	Alta[A]	10	0	0	0	3	0	0	0	0	30	0
[P-09]	Personal del departamento comercial	Bajo	Alta[A]	10	0	0	0	3	0	0	0	0	30	0
[P-10]	Personal del departamento de proyectos	Bajo	Alta[A]	10	0	0	0	3	0	0	0	0	30	0
[P-11]	Personal del departamento financiero	Bajo	Alta[A]	10	0	0	0	1	0	0	0	0	10	0

La valoración del nivel de riesgo existente para cada activo, así como la comparación de los resultados con el umbral de riesgo y los resultados se detallan en el **ANEXO3_ANALISISRIESGOS.pdf.**

4.8 RESULTADOS

El análisis de riesgos proporciona información sobre la seguridad de la empresa en relación, a sus sistemas de información.
Se consigue obtener una visión clara y objetiva de los activos de la información de la organización y su nivel de seguridad. Mediante el análisis se conocen las amenazas a las que se exponen los activos de la información y el grado de impacto que se sufriría en la organización en caso de materializarse las amenazas.
Por otra parte, la dirección de la organización define el nivel de riesgo que se asume como aceptable y por el contrario, aquel que debe ser tratado mediante los controles de seguridad adecuados.
El análisis de riesgos es el estudio a partir del cual se propone en la siguiente fase el listado de proyectos y acciones a acometer para poder mejorar el estado de seguridad de la organización.

PROPUESTAS DE PROYECTOS

5.1 INTRODUCCIÓN

Una vez realizado el análisis de riesgos y definidas las amenazas, el impacto y los riesgos de los activos, se conoce de forma más exacta el estado de la organización en materia de seguridad. El estudio muestra como necesario reducir el riesgo existente, procurando mitigar el impacto de las amenazas hasta conseguir el estado de cumplimiento de madurez óptimo de los diferentes dominios de la ISO 27001:2013.
En esta fase se efectuará el planeamiento de los diferentes proyectos. Bien sean proyectos que la empresa aceptó tratar para mitigar los riesgos y/o amenazas hasta niveles aceptables (Proyectos del Plan de Tratamiento de Riesgos). O proyectos planteados para mejorar los niveles de seguridad de la organización y entrar en cumplimiento de la norma ISO 27001:2013 (Proyectos para el Cumplimiento de la norma).
Los progresos podrán ser evaluados de acuerdo a las normas establecidas por la ISO, así como el seguimiento de sus mejoras, con la finalidad de continuar la optimización del sistema de seguridad.
Todos los proyectos identificados tendrán información sobre el valor económico, planificación requerida, recursos y tiempo necesario para la ejecución.

La lista de los proyectos propuestos se indica a continuación:
Proyecto 1: Definir políticas de seguridad de la información
Proyecto 2 – Mejora del CPD
Proyecto 3 – Control de acceso
Proyecto 4 – Plan de contingencia de datos – Backups y Restores
Proyecto 5 – Monitoreo SGSI
Proyecto 6 – Concienciación sobre la importancia de la información Proyecto 7 – Criptografía
Proyecto 8 – Plan de clasificación de la información y tratamiento del mismo.
Proyecto 9 – Mantenimiento, control y protección equipos informáticos Proyecto 10 – Proyecto Desarrollo de software
Proyecto 11 – Plan de contingencia y continuidad de negocio
Proyecto 12 – Procedimiento Gestión de incidentes

Cada proyecto de seguridad tiene la siguiente información:

- Identificador y nombre.
- Responsable
- Prioridad
- Activos del sistema de información afectados.
- Objetivos del proyecto.
- Descripción del proyecto y tareas que realizar para su puesta en funcionamiento.
- Controles y medidores para medir la efectividad de las medidas implantadas.
- Estimación de costes, tanto económicos como de esfuerzo.

5.2 PROPUESTA

Los proyectos planteados, su detalle de coste económico, la planificación temporal y su impacto sobre el cumplimiento normativo de la ISO/IEC 27002:2013 en los diferentes dominios, se encuentra detallado en el **ANEXO5_PROYECTOS**.pdf.

5.3 RESULTADOS

La propuesta de proyectos debe ir alineada con un análisis del impacto sobre la seguridad. La puesta en marcha de los proyectos produce una evolución del riesgo y el impacto, así como del nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002. El objetivo es evolucionar hacia un nivel de madurez optimizado.

Seguidamente se muestran los valores de cumplimiento antes de la implementación de los proyectos y de forma posterior. También se indican de forma gráfica la evolución de los diferentes dominios y su cumplimiento antes y después de la realización de los diferentes proyectos.

CONTROL	Valor	Cumplimiento	Valor	Cumplimiento esperado con la implementación de los proyectos
A.5 Política de seguridad de la información	1,5	30%	5	100%
A.6 Organización de la seguridad de la información	1,6	32%	3	60%
A.7 Seguridad de recursos humanos	1,44	29%	4	80%
A.8 Gestión de activos	1,47	29%	4	80%
A.9 Control de acceso	1,92	38%	4	80%
A.10 Criptografía	1	20%	4,5	90%
A.11 Seguridad física y del entorno	1,56	31%	4	80%
A.12 Operaciones de seguridad	1,26	25%	4	80%
A.13 Seguridad de las comunicaciones	1,46	29%	4	80%
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	1,48	30%	4	80%
A.15 Relación con proveedores	1,42	28%	3	60%
A.16 Gestión de incidentes de seguridad de la información	0,71	14%	4,5	90%
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	2	40%	4	80%
A.18 Cumplimiento	1,4	28%	4	80%

Tabla 8.Comparativa cumplimiento norma

Mediante los 12 proyectos planteados se mejorará prácticamente todos los dominios de la norma, subsanando aspectos graves y ante los cuales un eventual incidente podría ocasionar un gran perjuicio a la empresa. Se consigue mejorar desde la política de seguridad al sistema de copias de seguridad o la gestión de logs.

A continuación, se muestra de forma gráfica la evolución de los diferentes dominios y su cumplimiento antes de la realización de los diferentes proyectos.

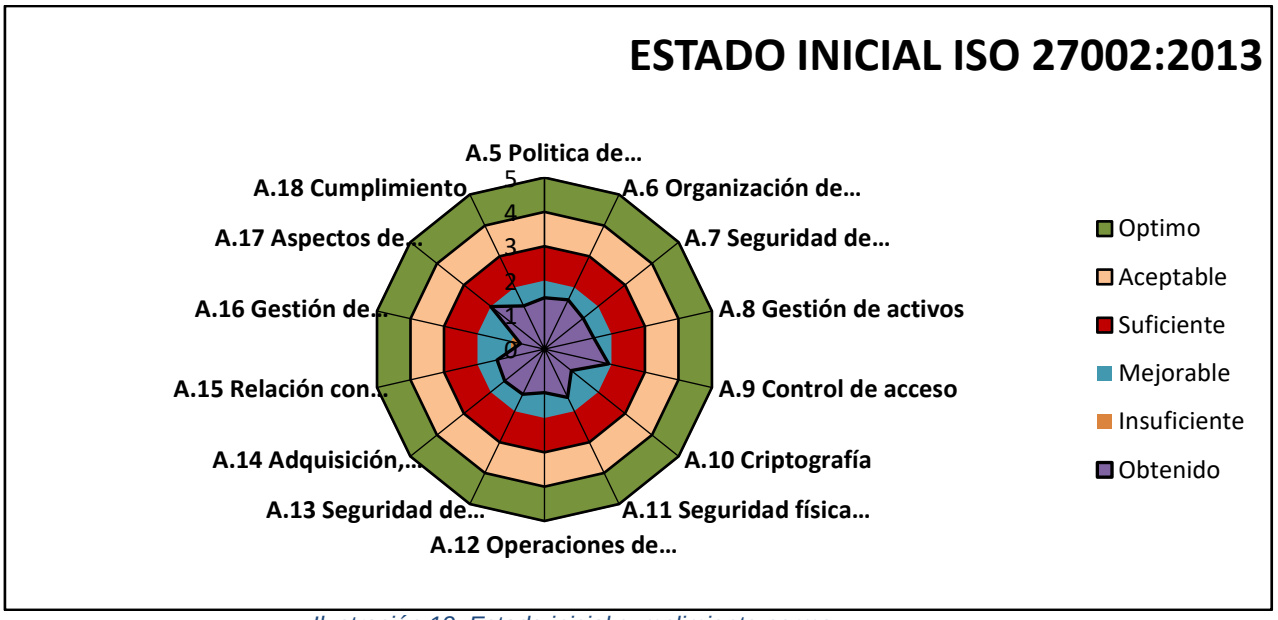


Ilustración 12. Estado inicial cumplimiento norma

Seguidamente, aparece el gráfico de la evolución de los diferentes dominios y su cumplimiento después de la realización de los proyectos.

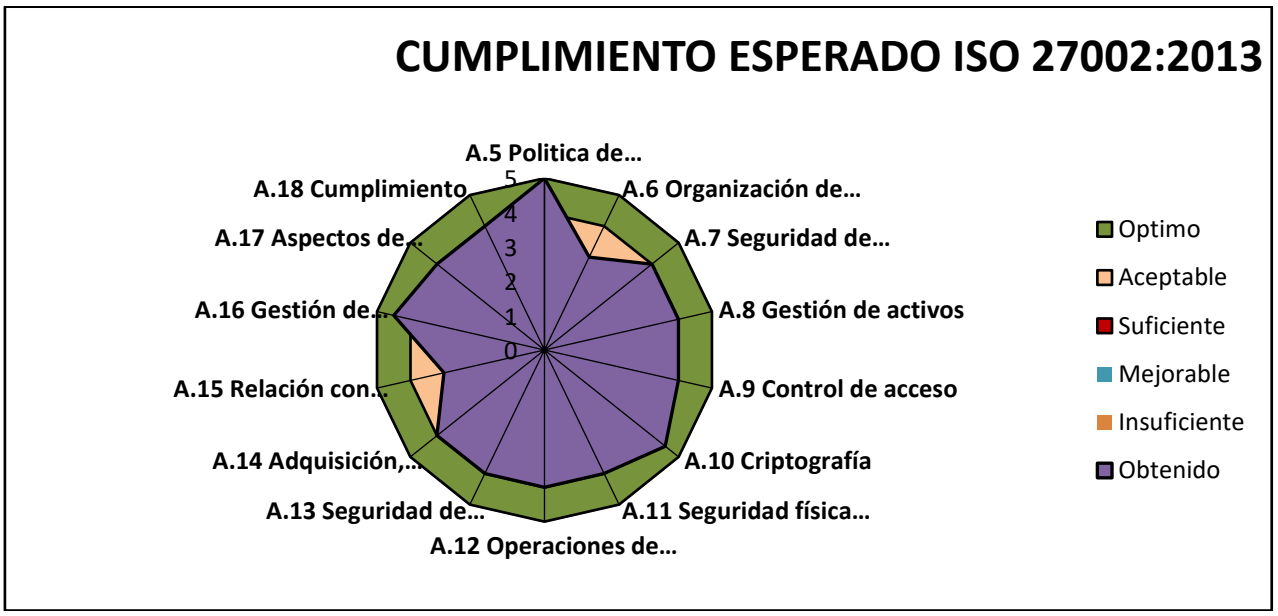


Ilustración 13. Estado esperado cumplimiento norma

Los proyectos planificados modificarán los niveles de riesgo identificados como críticos y altos de los activos, con el objeto de conseguir niveles aceptables para la organización.

NUMERO	ACTIVO	VALOR	RIESGO	RIESGO ESPERADO CON LA IMPLEMENTACIÓN DE LOS PROYECTOS
[SW-07]	Servidores	Alto	100	10
[D-01]	Bases de datos	Muy alto	100	10

NUMERO	ACTIVO	VALOR	RIESGO	RIESGO ESPERADO CON LA IMPLEMENTACIÓN DE LOS PROYECTOS
[SW-01]	Sistemas operativos	Medio	70	7
[SW-04]	Software de desarrollo	Medio	70	7
[SW-05]	Software de contabilidad	Medio	70	7
[D-04]	Backups (copias de seguridad)	Alto	70	7
[D-06]	Logs de servidores y clientes	Medio	80	8
[D-7]	Credenciales y datos de control de acceso.	Medio	80	8
[SER-06]	Servicio aplicaciones	Medio	70	7
[SER-07]	Servicio ficheros	Bajo	70	7
[P-05]	Director Sistemas TI	Alto	70	7
[P-06]	Responsable seguridad de la información.	Muy alto	70	7

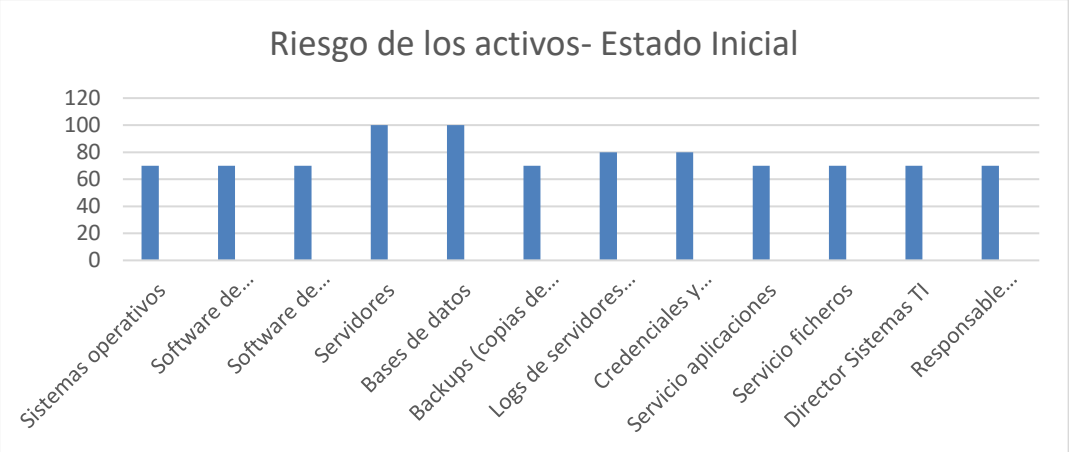


Ilustración 14. Estado inicial riesgo de los activos

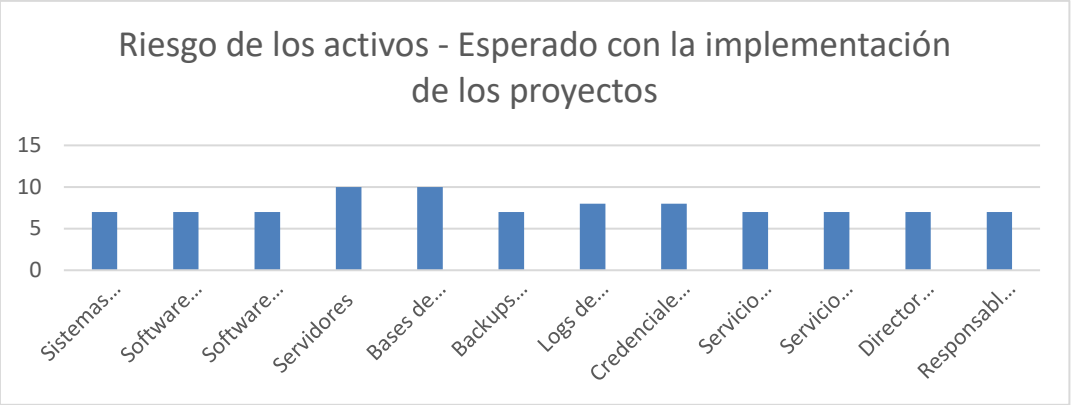


Ilustración 15. Estado esperado después de la implementación proyectos

AUDITORÍA DE CUMPLIMIENTO

6.1 INTRODUCCIÓN

Una vez efectuada la identificación de los activos, las amenazas y riesgos asociados, se plantearon y planificaron una serie de proyectos a implementar en el plazo de tres años, con el propósito de reducir el impacto de las amenazas.
La auditoría de cumplimiento analiza la evolución y estado de la seguridad de la información. Son una herramienta importante en el análisis y revisión de la gestión de la seguridad de la información, como forma de obtener conocimiento del estado real de la empresa y las posibles acciones a implantar o mejorar.
En esta fase se realizará nuevamente un análisis del estado de la empresa, en relación, a los distintos controles de la ISO/IEC 27002:2013 para poder comprobar si efectivamente tras la consecución de los distintos proyectos realizados y los controles que se han añadido, han producido efectos en el SGSI.

6.2 METODOLOGÍA

En esta fase, se evaluará la madurez de la seguridad en lo que respecta a los 14 dominios de control y los 114 controles planteados por la norma ISO/IEC 27002:2013 para cumplir con los diferentes objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de las organizaciones.

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo como son:
• 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 una combinación de salvaguardas sobre cada uno de los aspectos.

La estimación se realizará según la tabla del Modelo de Madurez de la Capacidad (CMM),

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 9.Modelo de Madurez de la Capacidad CMM

6.3 EVALUACIÓN DE LA MADUREZ

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

De forma resumida, los dominios que deben analizarse son:
• Política de seguridad
• Organización de la seguridad de la información.
• Gestión de activos.
• Seguridad en los recursos humanos
• Seguridad física y ambiental
• Gestión de comunicaciones y operaciones.
• Control de acceso.
• Adquisición, desarrollo y mantenimiento de Sistemas de Información
• Gestión de incidentes
• Gestión de continuidad de negocio
• Cumplimiento

En primer lugar, se verificó el nivel de implementación de los requisitos de la norma y se agregaron las observaciones correspondientes:

SECCIÓN	DESCRIPCIÓN	ESTADO	OBSERVACIONES
4	Contexto de la organización	En cumplimiento	Se ha documentado el contexto de la organización, la identificación de necesidades, el alcance y el establecimiento del SGSI.
5	Liderazgo	En cumplimiento	La dirección se ha involucrado activamente en la creación, divulgación y documentación de las políticas de seguridad y la definición de roles y responsabilidades.
6	Planificación	En cumplimiento	Se evidencia la existencia de un plan de implementación del Sistema, objetivos de seguridad medibles y concretos.
7	Soporte	En cumplimiento	Se han determinado y proporcionado recursos para el establecimiento del SGSI. Además, se ha efectuado formación al personal para su sensibilización en relación, a la seguridad. Se mantiene información documentada de los temas de seguridad de la información.
8	Operación	En cumplimiento	Se ha evidenciado el funcionamiento del procedimiento de gestión de riesgos y la existencia de planes concretos de tratamiento de los riesgos identificados.
9	Evaluación del desempeño	En cumplimiento	Se evidencia la evaluación del desempeño del sistema mediante indicadores,

			monitorización, seguimiento del cumplimiento de los objetivos y la revisión de los objetivos en conjunto con la dirección para tomar las medidas adecuadas con respecto al desempeño.
10	Mejora	En cumplimiento	Existen procedimientos de revisión y mejora continua. Así como atención de las no conformidades y acciones correctivas.

Tabla 10. Nivel de cumplimiento por cláusula de la Norma

Seguidamente, se evaluaron los 14 dominios y 114 controles de la norma según el Modelo de Madurez de la Capacidad (CMM). En el **ANEXO4_CUMPLIMIENTO.xlsx** se detalla toda esta información.

CONTROL			NIVEL	ESTADO	TOTAL	OBSERVACIÓN
A.5 Política de seguridad de la información					80,00%	
A.5.1 Directrices de la dirección en seguridad de la información					80,00%	
	A.5.1.1		L4 – Gestionado y medible	En cumplimiento	80,00%	Las políticas de seguridad de la información se han establecido y documentado. Pero se encuentra en proceso la propagación de la documentación.
	A.5.1.2		L4 – Gestionado y medible	En cumplimiento	80,00%	Existe un procedimiento de Revisión de las políticas de seguridad por parte de la Dirección de forma periódica. Sin embargo, no hay registro de revisiones de las políticas hasta este momento.
A.6 Organización de la seguridad de la información					53,00%	
A.6.1 Organización interna					56,00%	
	A.6.1.1		L3- Proceso definido	En cumplimiento	60%	Se han definido, asignado y documentado los roles y las responsabilidades para la seguridad de la información. Pero los usuarios todavía no tienen claro el canal de notificación.
	A.6.1.2		L3- Proceso definido	En cumplimiento	60%	Hay unos procedimientos de gestión de autorizaciones a la información que facilitan que no se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. Debe mejorarse porque hay solicitudes aprobadas por la misma persona y no por el director de área.
	A.6.1.3		L3- Proceso definido	En cumplimiento	60%	La dirección y el responsable de seguridad tienen los contactos apropiados sobre la autoridad pertinente en materia de seguridad con la que se debería contactar en caso de sufrir algún tipo de ataque. Hay documentación asociada al respecto.
	A.6.1.4		L2- Reproducible, pero intuitivo	No conformidad menor	40%	El contacto con grupos de interés no se encuentra formalmente definido, aunque el responsable de seguridad está en contacto con grupos de interés u asociaciones profesionales especializados en seguridad.
	A.6.1.5		L3- Proceso definido	En cumplimiento	60%	Existe un proceso formal de gestión de proyectos en el cual se contemplan los requisitos de seguridad de la información.
A.6.2 Dispositivos móviles y teletrabajo					50,00%	
	A.6.2.1		L3- Proceso definido	En cumplimiento	60%	Las medidas de seguridad para la protección contra los riesgos de la utilización de dispositivos móviles están documentadas, se cuenta con una política formalmente definida.

		A.6.2.2		L2- Reproducible, pero intuitivo	No conformidad menor	40%	Los usuarios conocen el uso que deben realizar sobre la información a la que se accede, trata o almacenada en emplazamientos de teletrabajo. Falta mejorarse estableciendo procedimientos y manuales al respecto.
A.7 Seguridad de recursos humanos						80,00%	
	A.7.1 Antes de empleo					80,00%	
		A.7.1.1		L4 – Gestionado y medible	En cumplimiento	80,00%	Existe un procedimiento formalmente definido para la selección del personal donde se contemplan los aspectos de seguridad de la información. La responsabilidad es de la dirección y de recursos humanos.
		A.7.1.2		L4 – Gestionado y medible	En cumplimiento	80,00%	En los términos y condiciones del contrato de trabajo se reflejan las políticas de seguridad de la organización en forma de documento de confidencialidad. Al empleado se le procura informar sobre el tratamiento que deben dar a la información en materia de seguridad.
	A.7.2 Durante el empleo					80,00%	
		A.7.2.1		L4 – Gestionado y medible	En cumplimiento	80,00%	Los empleados y contratistas conocen las normas en la gestión del trabajo. Se ha establecido la responsabilidad de la alta dirección en relación con el liderazgo en la gestión de seguridad de la información. Se efectúan reuniones de seguimiento y sensibilización por parte de la alta dirección.
		A.7.2.2		L4 – Gestionado y medible	En cumplimiento	80,00%	Se cuenta con un programa de capacitación y sensibilización para todos los empleados, sobre la importancia de la seguridad de la información en la organización.
		A.7.2.3		L4 – Gestionado y medible	En cumplimiento	80,00%	Existe un procedimiento disciplinario documentado y acorde a los requisitos legales, en el cual se contemplan los incidentes relacionados con la protección de la información.
	A.7.3 Finalización del empleo o cambio en el puesto de trabajo					80,00%	
		A.7.3.1		L4 – Gestionado y medible	En cumplimiento	80,00%	Existe un procedimiento publicado y aprobado para el cambio de responsabilidades o terminación de empleo. Recursos humanos contempla las medidas de seguridad para la terminación o cambio de empleo. Pero no se efectúa medición o mejora.
A.8 Gestión de activos						63,00%	
	A.8.1 Responsabilidad de los activos					75,00%	

	A.8.1.1		L4 – Gestionado y medible	En cumplimiento	80%	Existe un inventario de los activos asociados a la información y a los recursos para el tratamiento de la información. Cuneta con un procedimiento que evidencia la actualización del inventario.
	A.8.1.2		L4 – Gestionado y medible	En cumplimiento	80%	La propiedad de los activos de información del inventario está documentada, y se dispone de evidencia con respecto al conocimiento de los propietarios y su responsabilidad.
	A.8.1.3		L3- Proceso definido	En cumplimiento	60%	Los usuarios son conscientes del uso responsable de la información y de los activos de la organización. Se cuenta con una política de uso aceptable de activos, divulgada a todo el personal de la empresa.
	A.8.1.4		L4 – Gestionado y medible	En cumplimiento	80%	Existe control por parte de la organización y compromiso por parte de los empleados, una vez finaliza el empleo o acuerdo para devolver los activos de la organización. Existe un documento o procedimiento de desvinculación estipulado en el contrato y que es un requisito legal para la empresa.
A.8.2 Clasificación de la información					66,67%	
	A.8.2.1		L4 – Gestionado y medible	En cumplimiento	80%	La dirección ha aprobado una política y un procedimiento de clasificación de la información. Hay evidencia de la medición del control y de mejora a través del tiempo.
	A.8.2.2		L3- Proceso definido	En cumplimiento	60%	La información es etiqueta por la persona responsable de informática pero faltan procedimientos para efectuar dicha etiquetación.
	A.8.2.3		L3- Proceso definido	En cumplimiento	60%	Existe un conjunto adecuado de procedimientos para la manipulación de la información. No hay evidencia de su medición.
A.8.3 Manejo de los soportes					47,33%	
	A.8.3.1		L1 – Inicial/Ad-hoc	No conformidad menor	22%	Existen procedimientos para la gestión de soportes extraíbles. Pero no se pide autorización para extraer soportes de la organización, no se almacenan en lugar seguro y no se utilizan técnicas criptográficas para proteger los datos.
	A.8.3.2		L3- Proceso definido	En cumplimiento	60%	Eliminación de forma segura de los soportes cuando ya no son necesarios, especialmente en el caso de contener información sensible, que pueda ser confidencial. La eliminación de los medios sigue prácticas documentas y aunque se eliminan de forma segura los soportes cuando ya no son necesarios, depende del personal a cargo que

							lo efectúe.
		A.8.3.3		L3- Proceso definido	En cumplimiento	60%	Se utiliza siempre el mismo servicio de mensajería y se lleva a cabo un registro de las transferencias. Los empleados conocen los protocolos seguros para la transferencia. Pero no se efectúan mediciones.
A.9 Control de acceso						69,33%	
	A.9.1 Requisitos empresariales de control de acceso					60,00%	
		A.9.1.1		L3- Proceso definido	En cumplimiento	60%	Existe una política de control de acceso lógico y físico documentada que ha sido divulgada a todo el personal de la empresa, de lo cual se tiene evidencia.
		A.9.1.2		L3- Proceso definido	En cumplimiento	60%	Los usuarios solamente tienen acceso a las redes y a los servicios en red para los que están autorizados. Se cuenta con un procedimiento para el control de acceso a la red y el acceso a los servicios.
	A.9.2 Gestión de acceso de usuario					73,33%	
		A.9.2.1		L4 – Gestionado y medible	En cumplimiento	80%	Los usuarios disponen de un identificador que les proporciona derechos de acceso y les hace responsables de sus acciones. Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
		A.9.2.2		L4 – Gestionado y medible	En cumplimiento	80%	Existe un procedimiento formal para asignar o revocar los derechos de acceso a los usuarios en todos los sistemas y servicios. Se registran todos los cambios de acceso.
		A.9.2.3		L4 – Gestionado y medible	En cumplimiento	80%	La política de control de acceso controla la asignación de derechos de acceso privilegiados. Están establecidos los procedimientos para registrar y cancelar usuarios cuando corresponda. Se tiene registro de los cambios de acceso.
		A.9.2.4		L3- Proceso definido	En cumplimiento	60%	Se ha requerido a los usuarios el compromiso de mantener su información de autenticación de forma secreta. Se han generado directrices para su gestión.
		A.9.2.5		L3- Proceso definido	En cumplimiento	60%	Existe la revisión a intervalos regulares del acceso de los usuarios y el cambio de rol al reasignarse funciones. Se tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.
		A.9.2.6		L4 – Gestionado y medible	En cumplimiento	80%	Los derechos de acceso de los empleados a la información y los recursos de tratamiento de la información son retirados a la finalización del empleo o ajustados. Se tienen definidas directrices para registrar y cancelar usuarios cuando corresponda.

A.9.3 Responsabilidades del usuario					60,00%	
	A.9.3.1		L3- Proceso definido	En cumplimiento	60,00%	Existe una política por la cual los usuarios son responsables del uso de la información secreta. Este procedimiento está documentado y obliga.
A.9.4 Control de sistemas y acceso a las aplicaciones					84,00%	
	A.9.4.1		L3- Proceso definido	En cumplimiento	60%	Se controla y restringe el acceso a la información y a las funciones de las aplicaciones de forma informal, el responsable de seguridad lo decide. La dirección cuenta con procedimientos de control de acceso para ejecutarlas. No se lleva registro.
	A.9.4.2		L5 – Optimizado	En cumplimiento	100%	El procedimiento de inicio de sesión que controla el acceso a los sistemas y a las aplicaciones es seguro. Se han añadido técnicas más robustas, medios criptográficos, tarjetas inteligentes, doble autenticación, etc.
	A.9.4.3		L5 – Optimizado	En cumplimiento	100%	El sistema de gestión de contraseñas es implementado para conseguir la seguridad de las aplicaciones. Existen directrices para la gestión del control para manejar autenticación secreta en varias de sus aplicaciones.
	A.9.4.4		L3- Proceso definido	En cumplimiento	60%	Control establecido para manejar autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión. Se implementa un sistema que restringe y controla el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de las aplicaciones.
	A.9.4.5		L5 – Optimizado	En cumplimiento	100%	El código fuente del software propio que utiliza la organización tiene restringido su acceso. Existen políticas de restricción de acceso a los códigos fuente de los programas. Están planificadas las intervenciones que se desarrollan.
A.10 Criptografía					60,00%	
A.10.1 Controles criptográficos					60,00%	
	A.10.1.1		L3- Proceso definido	En cumplimiento	60%	Existe el establecimiento y comunicación de la política de uso de controles criptográficos. Se están desarrollando controles técnicos robustos para dar seguimiento a la gestión de estos controles.
	A.10.1.2		L3- Proceso definido	En cumplimiento	60%	Se han desarrollado e implementado políticas de uso. Se efectúa gestión de las claves criptográficas en todo el ciclo de vida.
A.11 Seguridad física y del entorno					66,83%	

A.11.1 Áreas seguras					53,67%	
	A.11.1.1		L3- Proceso definido	En cumplimiento	60%	El edificio cuenta con medidas de control del perímetro de seguridad, barrera física, cámaras de seguridad, sistema de alarma, etc. Existe evidencia de documentación de los planos y la definición de las áreas seguras.
	A.11.1.2		L3- Proceso definido	En cumplimiento	60%	Existe un control de seguridad para acceder al edificio. Se evidencia el uso de controles de acceso físico y la documentación de los visitantes a las instalaciones y las áreas seguras. Para acceder al CPD es necesario el uso de tarjeta, está protegido mediante controles de entrada adecuados, para asegurar el acceso a personal autorizado.
	A.11.1.3		L3- Proceso definido	En cumplimiento	60%	Existe un modelo de diseño y aplicación. Aunque todavía existen deficiencias que podrían ser mejoradas con respecto al control de acceso a las oficinas y despachos.
	A.11.1.4		L4- Gestionado y medible	En cumplimiento	80%	El edificio dispone de algunas medidas de protección física contra desastres naturales, ataques provocados por el hombre o accidentes. Generador eléctrico para caídas de corriente eléctrica o pararrayos.
	A.11.1.5		L1 – Inicial/Ad-hoc	No conformidad menor	22%	No se evidencian prácticas o procedimientos para el trabajo en las zonas que se han identificado como de alta seguridad. No se evidencia que estas zonas sean protegidas de forma especial con respecto al resto de las instalaciones.
	A.11.1.6		L2 – Reproducible pero intuitivo	No conformidad menor	40%	Existen puntos de acceso tales como áreas de carga y descarga u otros puntos debidamente señalizados pero se desconoce si la empresa de seguridad los controla de forma correcta. No hay evidencia de documentación.
A.11.2 Seguridad de los equipos					80,00%	
	A.11.2.1		L5 – Optimizado	En cumplimiento	100%	Está establecida la protección de los equipos según lo estableció en la política de seguridad. Hay evidencia de la implementación de controles orientados a garantizar la seguridad de estos equipos.
	A.11.2.2		L5 – Optimizado	En cumplimiento	100%	El edificio dispone de sistemas contra fallos en el suministro eléctrico. El área de mantenimiento del edificio se ocupa de su mantenimiento y gestión.
	A.11.2.3		L5 – Optimizado	En cumplimiento	100%	El edificio dispone de eficientes sistemas de cableado y telecomunicaciones. El área de mantenimiento se ocupa de su gestión y mantenimiento.

		A.11.2.4		L5 – Optimizado	En cumplimiento	100%	Los equipos de sobremesa y portátiles de los usuarios reciben un mantenimiento anual para asegurar su disponibilidad e integridad. Se lleva un registro del mantenimiento preventivo y correctivo que se efectúa, así como tampoco de los fallos, reparaciones e incidencias. Se lleva un registro de todo ello.
		A.11.2.5		L3- Proceso definido	En cumplimiento	60%	Están identificados los usuarios pueden sacar de las instalaciones activos. Se lleva a cabo registro de salida de equipos fuera de los locales de la organización, así como de su retorno. Se ha centralizado la autorización de retirar activos físicos o tecnológicos de su sitio.
		A.11.2.6		L3- Proceso definido	En cumplimiento	60%	Los usuarios que sacan equipos o cualquier otro tipo de información fuera de las oficinas tienen conocimiento del riesgo de seguridad que conlleva, en caso de daño, robo o escucha. Conectan utilizando conexiones seguras VPN. Pero no se mantiene un registro que defina la cadena de custodia de los equipos y no se realizan controles. Se han realizado cursos básicos de concienciación.
		A.11.2.7		L2 – Reproducible, pero intuitivo	Observación	40%	Se comprueba que los soportes de almacenamiento no guardan información sensible o software bajo licencia de la organización cuando van a ser destruidos o dados de baja. Los soportes con información sensible o con derechos de autor son destruidos físicamente o por medio de formateo que impida la recuperación de la información original. En el procedimiento existen deficiencias, ya que no se documenta la forma de actuar y tampoco los soporte sobre los que se ha intervenido.
		A.11.2.8		L4 – Gestionado y medible	En cumplimiento	80%	Los usuarios mediante el código de conducta informático son conscientes de los requisitos y procedimientos que se deben seguir para proteger el equipo desatendido. Se han implantado los procedimientos de seguridad y se les ha asesorado.
		A.11.2.9		L4 – Gestionado y medible	En cumplimiento	80%	Existe política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables. Así como políticas de pantalla limpia. A los usuarios se les ha concienciado.
A.12 Operaciones de seguridad						67,76%	
	A.12.1 Procedimientos y responsabilidades en las operaciones					73,33%	

	A.12.1.1		L5 – Optimizado	En cumplimiento	100%	El personal conoce los procedimientos operativos para las actividades del sistema asociadas a los recursos de tratamiento y comunicación de la información, tal como encendido y apagado ordenadores, copias de respaldo, etc. Se han documentado los procedimientos de operación y los usuarios lo tienen a su disposición para consulta.
	A.12.1.2		L2 – Reproducible, pero intuitivo	Observación	40%	Un técnico informático se encarga de efectuar el control sobre la seguridad de la información en cambios que se producen en la organización, procesos de negocio, instalaciones o tratamiento de la información y los sistemas. Pero no está definido un protocolo a seguir.
	A.12.1.3		L2 – Reproducible, pero intuitivo	Observación	40%	Se aplica un sistema de control y de ajuste básico para asegurar donde es necesario la mejora de la disponibilidad y de la eficiencia de los sistemas. Los controles para la detección de problemas son rudimentarios. Debería elaborarse un plan documentado de gestión de la capacidad para los sistemas de misión crítica.
	A.12.1.4		L2 – Reproducible, pero intuitivo	Observación	40%	Existe pero con deficiencias la separación entre entornos de operación, de prueba y de desarrollo con respecto al software a medida que necesita la organización para el desarrollo de su actividad.
A.12.2 Protección contra malware					100,00%	
	A.12.2.1		L5 – Optimizado	En cumplimiento	100,00%	Los equipos llevan protección contra código malicioso, software de detección de código malicioso y de reparación. Los usuarios asumen su responsabilidad al respecto a la seguridad. Hay implementadas políticas y controles de detección para la prevención y recuperación, también hay procedimientos de concienciación del usuario.
A.12.3 Copias de seguridad					100,00%	
	A.12.3.1		L5 – Optimizado	En cumplimiento	100,00%	Se realizan copias de seguridad de la información, del software y de los sistemas de acuerdo a una planificación periódica acordada. Están documentadas las políticas de respaldo y definidos los requisitos de conservación y protección.
A.12.4 Registro y seguimiento					50,00%	
	A.12.4.1		L2 – Reproducible, pero intuitivo	Observación	40%	Existe registro de eventos para la protección y revisión de las actividades de los usuarios pero no es controlado por ningún responsable de la organización.

	A.12.4.2		L2 – Reproducible, pero intuitivo	Observación	40%	El responsable de informática de la organización lleva el control contra manipulaciones indebidas y accesos no autorizados. Se deberían mejorar los mecanismos para proteger contra cambios no autorizados y problemas operacionales relativos a los dispositivos e información de registro.
	A.12.4.3		L2 – Reproducible, pero intuitivo	Observación	40%	El administrador del sistema tiene privilegios para manipular los registros en las instalaciones de la organización. Supervisa las actividades del sistema y el cumplimento de las actividades de administración de la red.
	A.12.4.4		L4 - Gestionado	En cumplimiento	80%	Los relojes de todos los sistemas de tratamiento de la información dentro del dominio están sincronizados con una fuente única de tiempo.
A.12.5 Control de software en explotación					60,00%	
	A.12.5.1		L3- Proceso definido	En cumplimiento	60,00%	En el procedimiento de despliegue de sistemas se han definido políticas y actividades específicas para la instalación de software, se dispone de una lista de software permitido y un inventario de licenciamiento adquirido.
A.12.6 Técnico de gestión de vulnerabilidades					41,00%	
	A.12.6.1		L1 – Inicial/Ad-hoc	No conformidad menor	22%	Se realiza de manera básica la gestión de las vulnerabilidades técnicas de los sistemas de información utilizados. Se deberían evaluar la exposición de la organización a dichas vulnerabilidades, así como adoptar las medidas adecuadas para afrontar el riesgo asociado.
	A.12.6.2		L3- Proceso definido	En cumplimiento	60%	El personal tiene claro el tipo de software que está permitido instalar y conoce las reglas con respecto a ese tema. La organización tiene definidas unas normas para decidir el tipo de software pueden instalar los usuarios y los privilegios. Existe documentación al respecto.
A.12.7 Consideraciones sobre la auditoria de sistemas de información					100,00%	
	A.12.7.1		L5 – Optimizado	En cumplimiento	100,00%	Se cumplen los requisitos de auditoría exigidos para las auditorias de gestión y las auditorías internas a sistema de gestión.
A.13 Seguridad de las comunicaciones					55,33%	
A.13.1 Gestión de la seguridad de la red					40,67%	

		A.13.1.1		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	Las redes son controladas de forma básica para proteger la información en los sistemas y las aplicaciones. Deberían establecerse las responsabilidades y procedimientos para la gestión de equipos de red, así como controles para salvaguardar la confidencialidad e integridad de los datos.
		A.13.1.2		L3- Proceso definido	En cumplimiento	60%	Están implementados mecanismos de seguridad, niveles y gestión de los servicios de red que solamente el responsable de seguridad de la organización conoce. Existen deficiencias en cuanto a los procedimientos y gestión del cortafuego o de los sistemas de detección de intrusiones.
		A.13.1.3		L1 – Inicial/Ad-hoc	No conformidad menor	22%	No existe segregación de redes, solamente hay una única red en la que se conectan todos los equipos y no hay ninguna política para impedir que equipos externos se conecten a dicha red. La red inalámbrica es meramente de cortesía y no accede a la red de trabajo.
	A.13.2 Intercambio de información					70,00%	
		A.13.2.1		L3- Proceso definido	En cumplimiento	60%	Se conoce por parte del personal los procedimientos para el intercambio de información de forma básica. Se han documentado los controles sobre el uso de técnicas criptográficas, directrices para la retención, eliminación de la correspondencia e información sensible.
		A.13.2.2		L3- Proceso definido	En cumplimiento	60%	El intercambio de información de negocio y de software entre la organización y terceros se realiza de forma segura. Se cuida especialmente el tratamiento de datos personales. Pero no existen políticas, procedimientos o normas aprobadas por la dirección.
		A.13.2.3		L3- Proceso definido	En cumplimiento	60%	Solamente se utiliza como tipo de mensajería el correo electrónico y están implementados mecanismos de fiabilidad y disponibilidad del servicio. Así como de protección frente a accesos no autorizados.
		A.13.2.4		L5 – Optimizado	En cumplimiento	100%	Existen acuerdos de confidencialidad y de no revelación en la organización con respecto a negocios con otras organizaciones. Están identificados, documentados y revisados regularmente dichos acuerdos.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información						57,85%	
	A.14.1 Requisitos de seguridad en los sistemas de información					53,33%	

	A.14.1.1		L3- Proceso definido	En cumplimiento	60%	Existen procedimientos para el análisis de seguridad del software a adquirir, así como con un listado de requerimientos generales para cualquier caso que se evalúa y se toma en cuenta al momento de seleccionar un proveedor.
	A.14.1.2		L3- Proceso definido	En cumplimiento	60%	Se utilizan métodos de control en las aplicaciones utilizadas que pasan información a través de redes públicas. Hacen uso de autenticación seguro basado en certificado electrónico y firmas digitales. Se encuentra protegida ante actividades fraudulentas o no autorizadas.
	A.14.1.3		L2 – Reproducible, pero intuitivo	Observación	40%	Se tiene en cuenta una serie de consideraciones sobre la seguridad de la información en las transacciones de servicios de aplicaciones para prevenir las transmisiones incompletas, alteración del mensaje, etc. Pero debería mejorarse mediante protocolos seguros, rutas de comunicación cifrada.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte					60,22%	
	A.14.2.1		L3- Proceso definido	En cumplimiento	60%	Se han establecido reglas con respecto al desarrollo de aplicaciones y sistemas. Su implementación está en curso dentro de los planes.
	A.14.2.2		L3- Proceso definido	En cumplimiento	60%	La incorporación de nuevos sistemas y los cambios importantes en los existentes se han realizado mediante un proceso formal de documentación, especificaciones y pruebas. Se han documentado los procedimientos formales de control de cambios.
	A.14.2.3		L3- Proceso definido	En cumplimiento	60%	La aplicación interna de negocio que se utiliza en el servicio de llamadas telefónicas es revisada y aprobadas sus modificaciones antes del cambio del sistema operativo. Hay políticas para garantizar que no existen efectos adversos en las funcionalidades o en la seguridad de la organización.
	A.14.2.4		L2 – Reproducible, pero intuitivo	Observación	40%	Se controlan los paquetes de software suministrados por proveedores. No se ha dado el caso de ser necesaria la modificación del software original, se instalan los parches y actualizaciones aprobadas por éste.
	A.14.2.5		L1 – Inicial/Ad-hoc	Observación	22%	Para la actividad de la organización no es necesario aplicar los principios de ingeniería seguros.

		A.14.2.6		L3- Proceso definido	En cumplimiento	60%	Se efectúan controles de seguridad en la organización, diferenciación de entornos, control de accesos, etc. Está documentado convenientemente.
		A.14.2.7		L4 - Gestionado	En cumplimiento	80%	El desarrollo del software propio que utiliza la organización es supervisado y controlado por personal interno. Se formalizan acuerdos con referencia a las licencias, código, derechos de propiedad intelectual, etc. Es consensuado con el proveedor en acuerdos firmados y consensuados. Están regulados y revisados los acuerdos.
		A.14.2.8		L4 - Gestionado	En cumplimiento	80%	El personal informático de la organización dispone de un plan de pruebas funcionales de seguridad y se prueba y revisa periódicamente.
		A.14.2.9		L4 - Gestionado	En cumplimiento	80%	El personal informático de la organización ha establecido un programa de pruebas de aceptación relacionados con nuevos sistemas de información, actualizaciones y nuevas versiones. Hay una política aprobada por la dirección al respecto.
	A.14.3 Datos de prueba					60,00%	
		A.14.3.1		L3- Proceso definido	En cumplimiento	60,00%	En el desarrollo del software propio de la organización se utilizan datos no reales con los que se realizan las pruebas posteriores de los sistemas. Se encuentra ambientes por separado para desarrollo, test y producción. Está documentado convenientemente.
A.15 Relación con proveedores						40,00%	
	A.15.1 Seguridad en las relaciones con proveedores					40,00%	
		A.15.1.1		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	Existen acuerdos entre la organización y los proveedores sobre el acceso a los activos. Falta la divulgación de la política de seguridad en las relaciones con los proveedores.
		A.15.1.2		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	Las condiciones de seguridad de la información no se reflejan en los contratos de forma explícita. Se efectúa de manera informal. Se deberían establecer y documentar los acuerdos con los proveedores para asegurar no haya malentendidos y además, el proveedor respete las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información.
		A.15.1.3		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	El suministro de tecnología de la información y de las comunicaciones tiene lugar mediante la contratación de otras

						empresas.
A.15.2 Gestión de la provisión de servicios del proveedor					40,00%	
	A.15.2.1		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	Se revisa y supervisa de forma básica los servicios de los proveedores en los términos y condiciones de seguridad de la información acordados. Pero no hay políticas ni procedimientos acordados por la dirección para ello.
	A.15.2.2		L2 – Reproducible, pero intuitivo	No conformidad menor	40%	Los cambios en la provisión de un servicio no se documentan, ni se lleva control. Depende de la gestión del líder del proyecto área relacionada.
A.16 Gestión de incidentes de seguridad de la información					80,00%	
A.16.1 Gestión de incidentes de seguridad de la información y mejoras					80,00%	
	A.16.1.1		L5 - Optimizado	En cumplimiento	100%	Se han establecidos las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada ante incidentes de seguridad. Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, así como la medición de ellos.
	A.16.1.2		L5 - Optimizado	En cumplimiento	100%	El responsable informático conoce la forma de informar de eventos de seguridad además, están implementados los canales de comunicación adecuados para notificar los eventos de seguridad. Existe y es de conocimiento por parte de todos los implicados de los procedimientos para la gestión de incidentes.
	A.16.1.3		L4 - Gestionado	En cumplimiento	80%	Los empleados son conscientes de la importancia de notificar los puntos débiles que observen o sospechen en los sistemas. Saben los procedimientos para ponerlo en conocimiento de su responsable.
	A.16.1.4		L4 - Gestionado	En cumplimiento	80%	Se lleva un registro de los eventos que se producen, se evalúan y se decide si se clasifican como incidentes de seguridad de la información. Existe un procedimiento al respecto.
	A.16.1.5		L4 - Gestionado	En cumplimiento	80%	Existen procedimientos documentados para dar respuesta a incidentes de seguridad de la información. El personal ha sido formado sobre la forma de actuar ante este tipo de situaciones.
	A.16.1.6		L2 – Reproducible, pero intuitivo	En cumplimiento	40%	Se evalúa la necesidad de mejorar o añadir controles que limiten incidentes. Pero no están implementados mecanismos para cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la

							información.
		A.16.1.7		L4 - Gestionado	En cumplimiento	80%	La organización tiene definidos procedimientos para la recogida, adquisición y preservación de la información que puede servir de evidencia.
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio						70,00%	
	A.17.1 Continuidad de la seguridad de la información					80,00%	
		A.17.1.1		L4 - Gestionado	En cumplimiento	80%	El plan de continuidad de negocio ante contratiempos y situaciones de parada de los distintos servicios (energía, comunicaciones, red, etc.) está desarrollado en profundidad para situaciones adversas.
		A.17.1.2		L4 - Gestionado	En cumplimiento	80%	El responsable de informática tiene establecidas una serie de medidas para restablecer la disponibilidad de la información en caso de situaciones inesperadas. Además, está documentado todo el proceso.
		A.17.1.3		L4 - Gestionado	En cumplimiento	80%	Se efectúan por parte del responsable informático controles a intervalos regulares que verifiquen que los procesos, procedimientos y controles para la seguridad de la información son válidos y eficaces durante situaciones adversas. Hay procedimientos establecidos, ni documentación aprobada por la dirección al respecto.
	A.17.2 Redundancias				60,00%		
		A.17.2.1		L3- Proceso definido	En cumplimiento	60,00%	Están implementados mecanismos de redundancia de la información. Se ha llegado a un acuerdo con otra empresa, en el uso como centro alternativo con estaciones de trabajo que proporcionen servicio aceptable para el negocio en caso de contingencia. Pero todavía no sido probado su funcionamiento.
A.18 Cumplimiento						62,00%	
	A.18.1 Cumplimiento de requisitos legales y contractuales					44,00%	
		A.18.1.1		L2 – Reproducible, pero intuitivo	Observación	40%	El asesor jurídico y el responsable de informática conocen los requisitos pertinentes en cuanto a la legislación pero no se encuentran definidos y documentados los controles específicos y las responsabilidades individuales.

		A.18.1.2		L2 – Reproducible, pero intuitivo	Observación	40%	Se respetan los derechos de propiedad intelectual y de los productos de software patentado pero no hay implementados procedimientos adecuados para garantizar el cumplimiento de los requisitos legales.
		A.18.1.3		L2 – Reproducible, pero intuitivo	Observación	40%	Existe protección para los registros de la organización contra la pérdida, destrucción, falsificación o acceso no autorizados pero con muchas deficiencias. No se hace en relación con unos requisitos legales, regulatorios y de negocio documentados.
		A.18.1.4		L2 – Reproducible, pero intuitivo	Observación	40%	Debería mejorarse la garantía y privacidad de los datos, según se requiere en la legislación y la reglamentación aplicables. Es necesario contar con una buena política de privacidad y protección de la información de carácter personal.
		A.18.1.5		L3- Proceso definido	En cumplimiento	60%	Existe una política respecto a los controles criptográficos. Su implementación está en curso.
	A.18.2 Revisiones de seguridad de la información				80,00%		
		A.18.2.1		L4 - Gestionado	En cumplimiento	80%	Se están realizando revisiones sobre la gestión de la seguridad de la información y su implantación en la organización. Se cuenta con un plan de auditoria y revisión interna de la operación de los controles y del SGSI.
		A.18.2.2		L4 - Gestionado	En cumplimiento	80%	La dirección y el responsable determinan cómo revisar los requisitos definidos en las políticas, normas y otra reglamentación. Se revisan periódicamente los indicadores con respecto al desempeño de los controles y el cumplimiento de las políticas por parte de la dirección.
		A.18.2.3		L4 - Gestionado	En cumplimiento	80%	El responsable de informática realiza revisiones de cumplimiento técnico de las normas de seguridad. Se efectúan pruebas de intrusión, evaluación de vulnerabilidades, planificadas, documentadas y repetidas.

5.4 PRESENTACIÓN DE RESULTADOS

La evaluación del nivel de madurez indica que los proyectos y controles que se han aplicado han generado una mejoría general en todas las áreas. Se ha procurado involucrar a la dirección en la toma de decisiones que conciernen a la seguridad y se ha producido una considerable mejoría en todos los dominios aunque todavía hay puntos en los que debería reforzarse la seguridad.

Después de efectuar los proyectos, el mayor número de controles se encuentran en un nivel L3 (39 controles) y L4 (31 controles). Son proyectos definidos y gestionados, muchos de ellos con documentación, aprobados por la dirección y definidas las responsabilidades. Concretamente, de los 114 controles; 16 controles L5; 31 controles L4, 39 controles L3, 23 controles L2 y 5 controles L1. En relación con los 14 dominios, 8 se encuentran en fase de cumplimiento y 6 cumplimiento parcial.

De forma resumida se presenta en la siguiente tabla la situación de cada uno de los dominios de la norma:

CONTROL	Situación actual	Objetivo	Óptimo
A.5 Política de seguridad de la información	80%	100%	100%
A.6 Organización de la seguridad de la información	53%	60%	100%
A.7 Seguridad de recursos humanos	80%	80%	100%
A.8 Gestión de activos	63%	80%	100%
A.9 Control de acceso	69,33%	80%	100%
A.10 Criptografía	60%	90%	100%
A.11 Seguridad física y del entorno	66,83%	80%	100%
A.12 Operaciones de seguridad	67,76%	80%	100%
A.13 Seguridad de las comunicaciones	55,33%	80%	100%
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	57,85%	80%	100%
A.15 Relación con proveedores	40%	60%	100%
A.16 Gestión de incidentes de seguridad de la información	80%	90%	100%
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	70%	80%	100%
A.18 Cumplimiento	62%	80%	100%

Tabla 11.Comparativa madurez de los dominios

Podemos ver la representación gráfica por dominios de la siguiente forma:

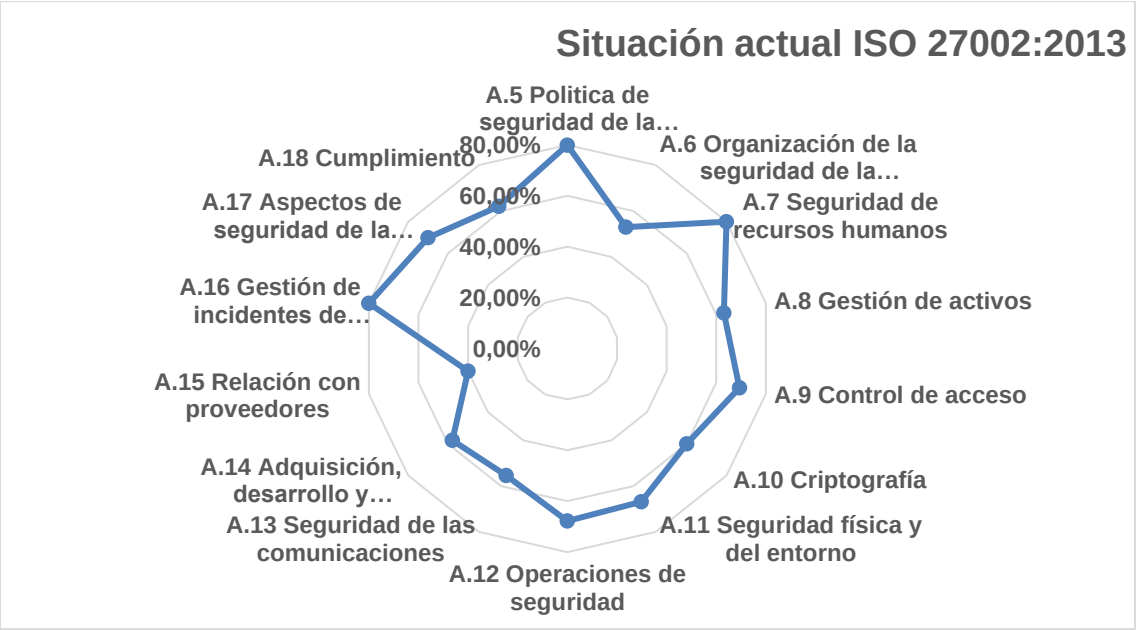


Ilustración 16. Situación actual nivel de madurez

Seguidamente se muestran los gráficos correspondientes a la situación actual de la organización, el nivel objetivo que estaba previsto y el nivel óptimo que se quiere conseguir.

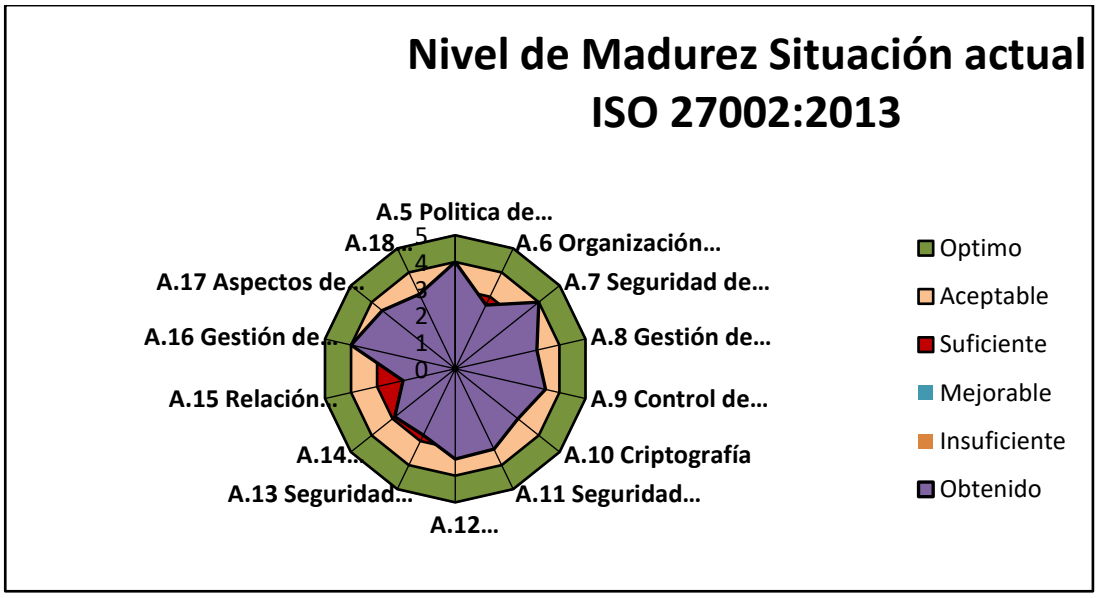


Ilustración 17.Situación actual nivel madurez

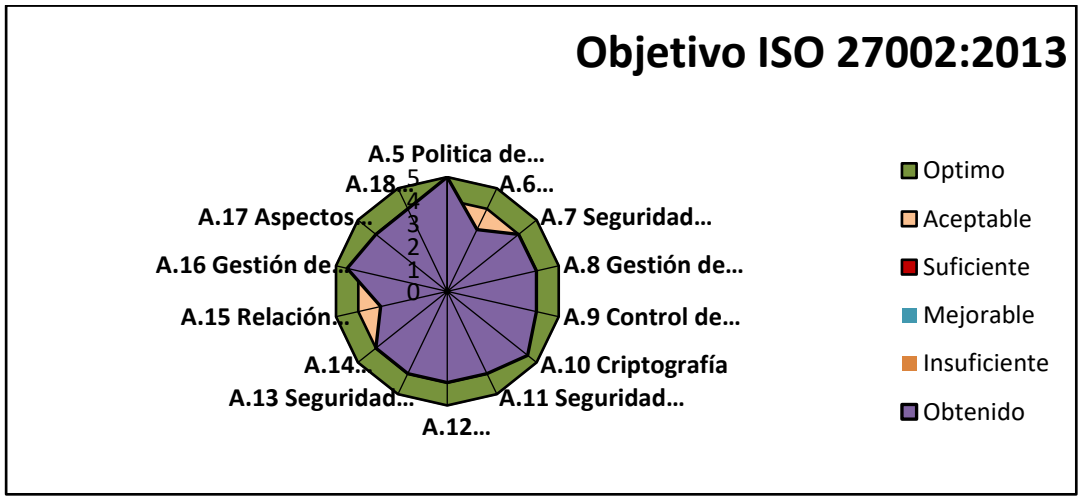


Ilustración 18. Objetivos nivel madurez

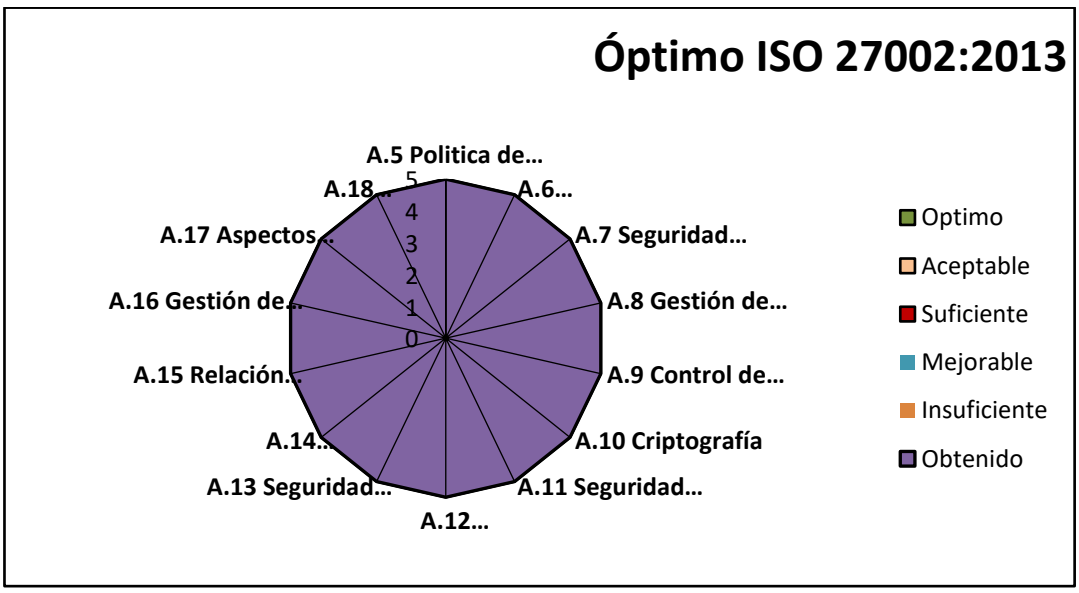


Ilustración 19. Nivel óptimo madurez

Como se puede observar, se han producido importantes mejoras en la situación de la seguridad de la información de la organización. Se ha definido la política de seguridad de la información, se han documentado normas y procedimientos y se han establecido procedimientos de medición que permiten detectar desviaciones frente a la evolución prevista. Por otra parte, ningún control de la norma figura en un nivel de madurez calificado como “0 – Inexistente”.

Han tenido una mejora considerable respecto a la situación inicial los controles de “A.5 Políticas de la seguridad de la información” y “A.16 Gestión de incidentes de la información”. En el primero, se han definido las políticas de seguridad y establecido los procedimientos documentados para su revisión. En cuanto a la gestión de incidentes, también se han documentado los procedimientos de gestión y respuesta.
El apartado “A.7 Seguridad relativa a los recursos humanos” también alcanza una mejora considerable. Se han establecido procedimientos que inciden en el entrenamiento y la formación del personal, que ayudan a su concienciación en seguridad de la información. Además, se cuidan los aspectos relativos a los procedimientos a seguir en caso de cese o cambio de puesto de trabajo.

A continuación, se puede ver de forma más detallada el resumen de controles por nivel de madurez. La situación inicial era la siguiente:

CONTROL	NÚMERO
0 - No existente	14
1 - Inicial	35
2 - Repetible	62
3 - Definido	1
4 - Gestionado	2
5 - Optimizado	0

Tabla 12.Resumen controles situación inicial

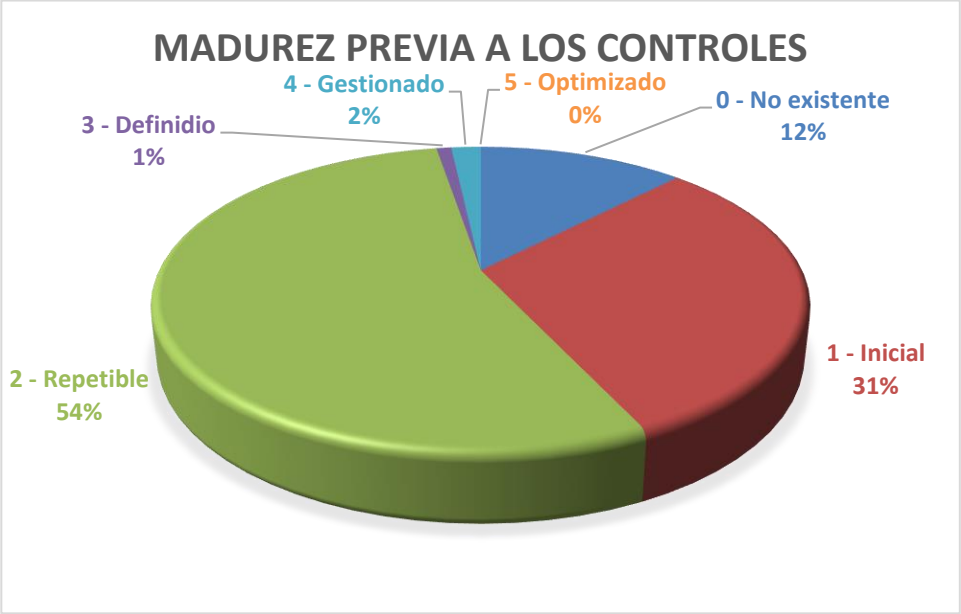


Ilustración 20. Madurez previa a los controles

Tras la aplicación de los proyectos se ha mejorado la situación de la organización de la siguiente manera:

Resumen controles por nivel de madurez	Número
L0 Inexistente	0
L1 Inicial / Ad-hoc	5
L2 Reproducible, pero intuitivo	23
L3 Proceso definido	39
L4 Gestionado y medible	33
L5 Optimizado	14

Tabla 13.Resumen controles situación actual

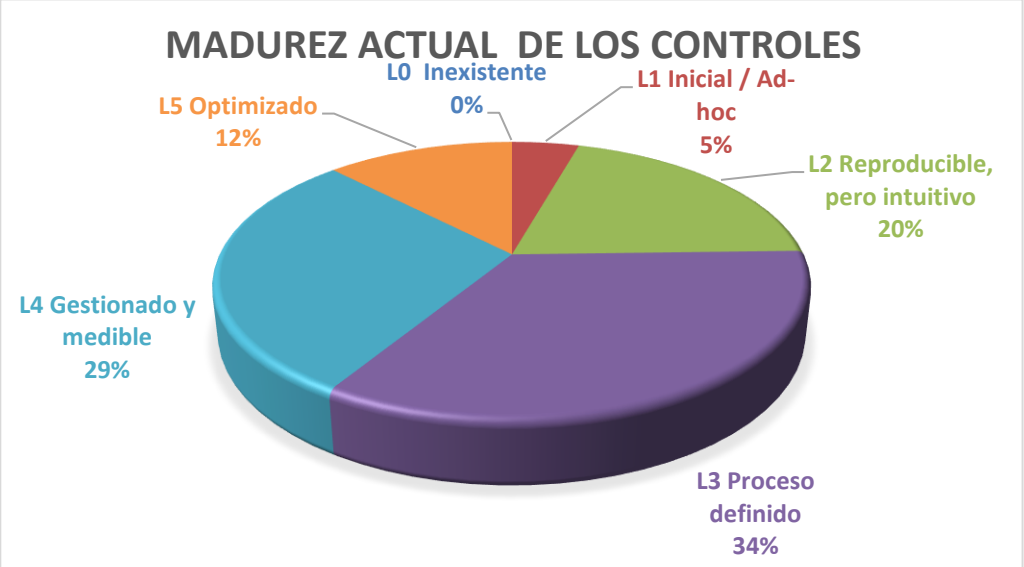


Tabla 14.Madurez actual de los controles

6.5 RESULTADOS

Una vez presentado el estudio y la representación gráfica de la evolución de la madurez de los 14 dominios y 114 controles de la norma ISO 27002:2013.
Se procede a la revisión del cumplimiento normativo de la organización relativo a la identificación de los diferentes tipos de desviaciones. En el análisis del estado se han detectado controles con no conformidad menor y en observación.
Sus diferencias son:

- 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.

Dominio	**A.6. Organización de la seguridad de la información**
Punto de control	6.1.4 (L2) y 6.2.2 (L2)
Comentarios	6.1.4 (L2) El contacto con grupos de interés no se encuentra formalmente definido, aunque el responsable de seguridad está en contacto con grupos de interés u asociaciones profesionales especializados en seguridad. 6.2.2 (L2) Los usuarios conocen el uso que deben realizar sobre la información a la que se accede, trata o almacenada en emplazamientos de teletrabajo. Falta mejorarse estableciendo procedimientos y manuales al respecto.
Tipo de no conformidad	No conformidad menor No conformidad menor
Acción correctora	6.1.4 (L2) El responsable de seguridad debe definir formalmente y documentar los contactos con grupos de interés y asociaciones profesionales especializados en seguridad. 6.2.2 (L2) Deben establecerse los procedimientos y manuales con relación a la información a la que acceden, tratan y almacenan los usuarios en teletrabajo.

Dominio	**A.8. Gestión de activos**
Punto de control	8.3.1 (L1)
Comentarios	8.3.1 (L1) Existen procedimientos para la gestión de soportes extraíbles. Pero no se pide autorización para extraer soportes de la organización, no se almacenan en lugar seguro y no se utilizan técnicas criptográficas para proteger los datos.
Tipo de no conformidad	No conformidad menor
Acción correctora	8.3.1 (L1) Es necesario implementar y mejorar los procedimientos creados para la gestión de soportes extraíbles, mediante la autorización de extracción, almacenamiento seguro y uso de técnicas criptográficas.

Dominio	**A.11. Seguridad física y del entorno**
Punto de control	A.11.1.5(L1), A.11.1.6(L2) y A.11.2.7(L2)
Comentarios	A.11.1.5(L1) No se evidencian prácticas o procedimientos para el trabajo en las zonas

	que se han identificado como de alta seguridad. No se evidencia que estas zonas sean protegidas de forma especial con respecto al resto de las instalaciones A.11.1.6(L2) Existen puntos de acceso tales como áreas de carga y descarga u otros puntos debidamente señalizados pero se desconoce si la empresa de seguridad los controla de forma correcta. No hay evidencia de documentación. A.11.2.7(L2) Se comprueba que los soportes de almacenamiento no guardan información sensible o software bajo licencia de la organización cuando van a ser destruidos o dados de baja. Los soportes con información sensible o con derechos de autor son destruidos físicamente o por medio de formateo que impida la recuperación de la información original. En el procedimiento existen deficiencias, ya que no se documenta la forma de actuar y tampoco los soporte sobre los que se ha intervenido.
Tipo de no conformidad	No conformidad menor No conformidad menor Observación
Acción correctora	A.11.1.5(L1) Debe establecerse zonas de alta seguridad, protegidas de forma especial con respecto al resto de las instalaciones. A.11.1.6(L2) Deben crearse protocolos y documentación con relación a los puntos de acceso de carga y descarga. A.11.2.7(L2) Existen procedimientos sobre la forma de actuar con respecto a los soportes de almacenamiento que guardan información sensible, con derechos de autor, etc. Pero debe mejorarse con documentación adecuada sobre la forma de manejarlos y un registro de los soportes intervenidos.

Dominio	**A.12.Operaciones de seguridad**
Punto de control	A.12.6.1(L1)
Comentarios	A.12.6.1(L1) Se realiza de manera básica la gestión de las vulnerabilidades técnicas de los sistemas de información utilizados. Se deberían evaluar la exposición de la organización a dichas vulnerabilidades, así como adoptar las medidas adecuadas para afrontar el riesgo asociado.
Tipo de no conformidad	No conformidad menor
Acción correctora	A.12.6.1(L1) Debe completarse la gestión de las vulnerabilidades técnicas de los sistemas de información con herramientas y procedimientos más detallados y completos. Así como adoptar las medidas adecuadas para reducir el riesgo de ellas.

Dominio	**A.13.Seguridad de las comunicaciones**
Punto de control	A.13.1.1(L2)
Comentarios	A.13.1.1(L2) Las redes son controladas de forma básica para proteger la información en los sistemas y aplicaciones. Deberían establecerse las responsabilidades y procedimientos para la gestión de equipos de red, así como controles para salvaguardar la confidencialidad e integridad de los datos.
Tipo de no conformidad	No conformidad menor

Acción correctora	A.13.1.1(L2) Deben establecerse las responsabilidades y procedimientos de la gestión de la seguridad de las comunicaciones, así como de las redes y equipos conectados a ella. Deben habilitarse controles para salvaguardar la confidencialidad e integridad de los datos.

Dominio	**A.14.Adquisición, desarrollo y mantenimiento de los sistemas de información.**
Punto de control	A.14.1.3(L2), A.14.2.4(L2) y A.14.2.5(L1)
Comentarios	A.14.1.3(L2) Se tiene en cuenta una serie de consideraciones sobre la seguridad de la información en las transacciones de servicios de aplicaciones para prevenir las transmisiones incompletas, alteración del mensaje, etc. Pero debería mejorarse mediante protocolos seguros, rutas de comunicación cifrada. A.14.2.4(L2) Se controlan los paquetes de software suministrados por proveedores. No se ha dado el caso de ser necesaria la modificación del software original, se instalan los parches y actualizaciones aprobadas por éste. A.14.2.5(L1) Se conocen los principios de ingeniería seguros para la organización pero de manera informal. Debe completarse con procedimientos y manuales.
Tipo de no conformidad	No conformidad menor. Observación Observación
Acción correctora	A.14.1.3(L2) Las transacciones de servicios de aplicaciones deben mejorarse mediante protocolos seguros, rutas de comunicación cifrada. Y además, documentarse todo correctamente. A.14.2.4(L2) Debe crearse un protocolo de actuación, instalación de parches y actualizaciones ante la posibilidad de modificación de software original en alguna circunstancia. A.14.2.5(L2) Es necesario la creación de un procedimiento con los principios de ingeniería seguros.

Dominio	**A.15.Relación con proveedores**
Punto de control	A.15.1.1(L2), A.15.1.2(L2), A.15.1.3(L2), A.15.2.1(L2) y A.15.2.2(L2)
Comentarios	A.15.1.1(L2) Existen acuerdos entre la organización y los proveedores sobre el acceso a los activos. Falta la divulgación de la política de seguridad en las relaciones con los proveedores. A.15.1.2(L2) Las condiciones de seguridad de la información no se reflejan en los contratos de forma explícita. Se efectúa de manera informal. Se deberían establecer y documentar los acuerdos con los proveedores para asegurar no haya malentendidos y además, el proveedor respete las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información. A.15.1.3(L2) El suministro de tecnología de la información y de las comunicaciones tiene lugar mediante la contratación de otras empresas. A.15.2.1(L2) Se revisa y supervisa de forma básica los servicios de los proveedores en los términos y condiciones de seguridad de la información acordados. Pero no hay políticas ni procedimientos acordados por la dirección para ello.

	A.15.2.2(L2) Los cambios en la provisión de un servicio no se documentan, ni se lleva control. Depende de la gestión del líder del proyecto área relacionada.
Tipo de no conformidad	No conformidad menor No conformidad menor No conformidad menor No conformidad menor No conformidad menor
Acción correctora	A.15.1.1(L2) Es necesaria la comunicación y publicidad de la política de seguridad en las relaciones con los proveedores. A.15.1.2(L2) Debe establecerse y documentarse de manera formal los acuerdos con los proveedores para obligar a ambas partes con el cumplimiento de los requisitos de seguridad de la información. A.15.1.3(L2) Debe establecerse una cadena de suministro con garantías, proveedores de confianza y exigir a los proveedores un control de seguridad a sus propios proveedores. A.15.2.1(L2) Se necesitan políticas y procedimientos acordados por la dirección para la revisión y supervisión de los servicios de los proveedores en materia de seguridad de la información. A.15.2.2(L2) Se debe controlar y documentar los cambios en la provisión de un servicio.

Dominio	**A.16.Gestión de incidentes de seguridad de la información**
Punto de control	A.16.1.6(L2)
Comentarios	A.16.1.6(L2) Se evalúa la necesidad de mejorar o añadir controles que limiten incidentes. Pero no están implementados mecanismos para cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.
Tipo de no conformidad	No conformidad menor
Acción correctora	A.16.1.6(L2) Es importante contar con un mecanismo para cuantificar y supervisar la gestión de incidentes de seguridad de la información. De manera que se pueda tener conocimiento real del coste que suponen.

Dominio	**A.18.Cumplimiento**
Punto de control	A.18.1.1(L2), A.18.1.2(L2), A.18.1.3(L2) y A.18.1.4(L2)
Comentarios	A.18.1.1(L2) El asesor jurídico y el responsable de informática conocen los requisitos pertinentes en cuanto a la legislación pero no se encuentran definidos y documentados los controles específicos y las responsabilidades individuales. A.18.1.2(L2) Se respetan los derechos de propiedad intelectual y de los productos de software patentado pero no hay implementados procedimientos adecuados para garantizar el cumplimiento de los requisitos legales. A.18.1.3(L2) Existe protección para los registros de la organización contra la pérdida, destrucción, falsificación o acceso no autorizados pero con muchas deficiencias. No se hace en relación con unos requisitos legales, regulatorios y de negocio documentados.

	A.18.1.4(L2) Debería mejorarse la garantía y privacidad de los datos, según se requiere en la legislación y la reglamentación aplicables. Es necesario contar con una buena política de privacidad y protección de la información de carácter personal.
Tipo de no conformidad	Observación Observación Observación Observación
Acción correctora	A.18.1.1(L2) Se deben definir y documentar los controles específicos y las responsabilidades legales relacionados al cumplimiento. A.18.1.2(L2) Es necesario implementar los procedimientos adecuados para garantizar el cumplimiento de los requisitos legales con relación a los derechos de la propiedad intelectual y de los productos de software patentado. A.18.1.3(L2) Es necesario adecuar el método de protección de los registros de la organización con los requisitos legales y regulatorios de la empresa. A.18.1.4(L2) Deben desarrollarse con mayor profundización las políticas de privacidad y protección de la información de carácter personal.

PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

7.1 INTRODUCCIÓN

Seguidamente se recopila la información y documentación de la puesta en funcionamiento del Plan de Implementación de un SGSI. Se le dará el formato pertinente para su presentación.

7.2 OBJETIVOS DE LA FASE

La documentación que se incluirá será la siguiente:

• Resumen ejecutivo: breve descripción en que se incluye la motivación, enfoque del proyecto y principales conclusiones extraídas.
• Memoria descriptiva: incluye un detalle del proceso, la descripción de la empresa en estudio, el análisis de riesgos realizado, el nivel de cumplimiento de la empresa actualmente, un plan de acción para mejorar la seguridad, la cuantificación de la mejora que supondrá el plan y los aspectos organizativos que conviene abordar para hacer viable el plan.
• La presentación a la dirección exponiendo los principales resultados del estudio, el plan de acción planteado y los aspectos organizativos relevantes.

7.3 ENTREGABLES

Se entregarán los siguientes documentos:
• Resumen ejecutivo

• Memoria de Proyecto. Figurarán como anexos:
  - Objetivos del Plan Director e Informe Análisis Diferencial
  - Resultados del análisis de riesgos
  - Nivel de cumplimiento de la ISO basado en el análisis de los 114 controles planteados por la norma.
  - Proyectos planteados a la dirección, detallando el coste económico de los mismos, su planificación temporal y su impacto sobre el cumplimiento normativo de la ISO/IEC 27002:2013 en los diferentes dominios.
  - Esquema documental indicado en el apartado 2.2

Adicionalmente, se incluirán también:

• Presentación del estado de cumplimiento de los controles de seguridad y del objetivo de la compañía a corto y medio plazo, basándonos en la realización de los proyectos que se proponen para mejorar el estado de la seguridad. El objetivo de esta presentación sirve de base para la aprobación de los proyectos que en ella se detallan.

• Una presentación a la dirección planteada exponiendo los principales resultados del estudio, planteamiento claro del plan de acción y los aspectos organizativos relevantes, así como el resumen del impacto de la ejecución de los proyectos en el estado de la seguridad.

8. CONCLUSIONES

La ejecución del presente proyecto supone una mejora en el nivel de madurez de seguridad de la información en la compañía. Se ha tomado conciencia sobre la importancia de los sistemas de gestión de la seguridad, para garantizar el tratamiento y seguridad de la información, hacer la empresa más competitiva tanto a nivel nacional como internacional, cumplir con la normativa legal y ofrecer una imagen de buenas prácticas a clientes y proveedores.
Se ha efectuado un análisis real de la empresa, en base a la norma ISO 27001:2013, identificando potenciales riesgos que afecten a la organización, estableciendo la estrategia a tomar para cada uno de ellos, ya sea asumir, traspasar a terceros o gestionar el riesgo. Así como una serie de proyectos para resolver los problemas de seguridad.

Mediante la mejora continua se seguirá trabajando para mantener el nivel de madurez en aquellos dominios que cumplen con los requisitos de la norma y alcanzar un nivel de madurez lo óptimo posible del resto. Se seguirá trabajando en la toma de conciencia por parte de los empleados sobre la importancia de la seguridad, como elemento clave para la consecución de los objetivos de la compañía y permitir el crecimiento de esta acorde a las estrategias definidas por la dirección.

9. GLOSARIO

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo proactivo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo, si sólo incluye una parte de la organización.

Alerta: Notificación formal de un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

Lista de Chequeo: 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.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén 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. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

DAFO: Es una herramienta de estudio de la situación de una empresa, institución, proyecto o persona, analizando sus características internas (Debilidades y Fortalezas) y su situación externa (Amenazas y Oportunidades) en una matriz cuadrada.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Desastre: 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: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Entidad de acreditación: 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)...

Entidad de certificación: (Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27000, ISO 9000, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Evaluación de riesgos: Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: 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 seguridad de la información.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.
Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Impacto: 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: 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: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, 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 organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. Es certificable. Publicación 2013.

IT: Information technology, Tecnología de la Información

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

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

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

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Política de escritorio despejado: La política de la empresa que indica a los empleados que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Requerimiento: Es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de

organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

SI: Seguridad de la información.

Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: 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.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

10. REFERENCIAS

ISO ISO27000
http://www.iso27000.es/

https://www.iso27000.es/iso27000.html

https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

Definición, evolución y características ISO 27001
https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

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

https://www.iso27001security.com/html/27001.html

https://es.wikipedia.org/wiki/ISO/IEC_27001

Controles de ISO 27002
http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Definición, evolución y características ISO 27002
http://www.iso27000.es/iso27002.html

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

INCIBE
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html

MAGERIT
Portal de Administración electrónica gobierno de España

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

LIBRO 3 MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
LIBRO 2 MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874#:~:text=Es%20importante%20establecer%20una%20metodolog%C3%ADa,el%20prop%C3%B3sito%20de%20evaluar%20el

11. ANEXOS

ANEXO1_OBJETIVOS.pdf
ANEXO2_ANALISISDIFERENCIAL.pdf
ANEXO2_ANALISISDIFERENCIAL.xlsx
ANEXO3_ANALISISRIESGOS.pdf
ANEXO3_ANALISISRIESGOS.xlsx
ANEXO4_CUMPLIMIENTO.xlsx
ANEXO5_PROYECTOS.pdf
ANEXO5_PROYECTOS_GANTT.xlsx
ANEXO6_ESQUEMADOCUMENTAL.pdf
AUDITORIA.pdf
DOCUMENTACION_AUDITORIA.pdf