Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

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

Alumno: Cristóbal Garrido Camargo

Director: Antonio José Segovia Henares

Diciembre 2018

RESUMEN

Hoy en día la información es uno de los principales activos en buena parte de las organizaciones. La correcta gestión de la seguridad de la información se ha convertido en una necesidad básica para protegerla frente a las amenazas que acechan a las organizaciones en un mundo ampliamente interconectado.

La implantación de un Sistema de Gestión de la Seguridad (SGSI) es el modo más eficaz de proteger la información de las organizaciones y gestionar los riesgos a los que se expone. Para su puesta en marcha es conveniente seguir estándares y guías de buenas prácticas que hayan demostrado sus bondades y que faciliten su implantación.

La norma ISO/IEC 27001 es una norma internacional ampliamente reconocida que, además, permite la certificación de las organizaciones y que se acompaña habitualmente de la guía de buenas prácticas que se recogen en la norma ISO/IEC 27002.

Este trabajo muestra el proceso realizado para elaboración del Plan de Implementación de la ISO/IEC 27001:2013 en una multinacional dedicada al reciclaje de residuos industriales que, aunque concienciada con la necesidad de asegurar adecuadamente sus sistemas de información, no contaba hasta el momento con un SGSI.

El proyecto recoge las tareas realizadas para sentar las bases para la implantación del SGSI, y genera una serie de entregables que formarán parte del sistema de gestión documental del SGSI. Además, muestra la evolución y mejora de la seguridad de la información conseguida con la puesta en marcha del SGSI.

SUMMARY

Nowadays, information is one of the main assets in a significant part of organizations. The correct information security management has become a basic need, in order to protect this information from the threats that threaten any organization in a widely interconnected world.

An Information Security Management System (ISMS) implementation is the most effective way to protect the information of organizations and to manage the risks to which it is exposed. For its implementation, it is advisable to follow standards and guides to good practices that have proven their benefits and that facilitate their implementation.

ISO/IEC 27001 is a widely recognized international standard that, in addition, allows organizations to be certified, and is usually accompanied by the guide to good practices that is included in ISO/IEC 27002.

This document shows the process carried out to elaborate the ISO/IEC 27001: 2013 Implementation Plan in a multinational engaged in industrial waste recycling that, although aware of the need to ensure adequately its information systems, did not have ISMS yet.

The project includes the tasks performed to lay the foundations for the ISMS implementation, generating a number of deliverables, which are part of the ISMS document management system. Besides it shows the information security evolution and improvement achieved with its implementation.

Tabla de Contenido

RESUMEN **2**

SUMMARY **2**

1 INTRODUCCIÓN **7**

2 SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL8

2.1 Introducción 8
2.1.1 ISO/IEC 27001:2013 9
2.1.2 ISO/IEC 27002:2013 12
2.2 Contextualización 13
2.2.1 DESCRIPCIÓN GENERAL DE LA ORGANIZACIÓN 13
2.2.2 ESTRUCTURA ORGANIZATIVA 14
2.2.3 ESTRUCTURA DEL SERVICIO DE IT 15
2.2.4 USUARIOS Y SEDES 17
2.2.5 INFRAESTRUCTURA TECNOLÓGICA 18
2.2.5.1 PUESTOS DE TRABAJO 18
2.2.5.2 DISPOSITIVOS MÓVILES 19
2.2.5.3 TELEFONÍA IP 20
2.2.5.4 APLICACIONES CORPORATIVAS 21
2.2.5.5 INFRAESTRUCTURA DE SERVIDORES 22
2.2.5.6 RED DE COMUNICACIONES 24
2.2.6 ALCANCE 26
2.3 Objetivos del Plan Director de Seguridad 26
2.4 Análisis diferencial 28
2.4.1 EVALUACIÓN DE EFECTIVIDAD DE LOS CONTROLES ISO/IEC 27002:2013 28
2.4.2 EVALUACIÓN DE SITUACIÓN NORMA ISO/IEC 27001:2013 30

3 SISTEMA GESTIÓN DOCUMENTAL **31**

3.1 Introducción 31
3.2 Política de Seguridad 32
3.3 Procedimiento de Auditorías Internas 33
3.4 Gestión de Indicadores 34
3.5 Procedimiento de Revisión por la Dirección 35
3.6 Gestión de Roles y Responsabilidades 36
3.7 Metodología de Análisis de Riesgos 38
3.8 Declaración de Aplicabilidad 39

4 ANÁLISIS DE RIESGOS **40**

4.1 Introducción 40
4.2 Inventario de Activos 41
4.3 Valoración de los Activos 44
4.4 Dimensiones de la seguridad 45
4.5 Tabla resumen de la seguridad 46
4.6 Análisis de amenazas 47
4.7 Impacto potencial 48
4.8 Nivel de riesgo aceptable y riesgo residual 50
4.9 Resultados 51

5 PROPUESTAS DE PROYECTOS 53

5.1 Introducción 53
5.2 Proyectos de ámbito tecnológico 54
5.3 Proyectos de ámbito organizativo y de gestión 62
5.4 Planificación propuesta 70
5.5 Resultados esperados 72
5.5.1 EVOLUCIÓN DE RIESGOS 72
5.5.2 EVOLUCIÓN ANÁLISIS DIFERENCIAL 74

6 AUDITORÍA DE CUMPLIMIENTO 77

6.1 Introducción 77
6.2 Declaración de aplicabilidad 77
6.3 Revisión de requerimientos ISO/IEC 27001:2013 78
6.4 Revisión de cumplimiento de los controles 78
6.5 Informe de Auditoría 78

7 CONCLUSIONES Y PRESENTACIÓN DE RESULTADOS 79

7.1 Introducción 79
7.2 Conclusiones 79
7.2.1 OBJETIVOS ALCANZADOS 79
7.2.2 ASPECTOS PENDIENTES: SIGUIENTES PASOS 80
7.3 Presentación de resultados 80

8 TÉRMINOS Y DEFINICIONES 81

9 REFERENCIAS Y BIBLIOGRAFÍA 82

10 ANEXOS 83

Anexo A. Efectividad de los controles ISO/IEC 27002:2013 84
Anexo B. Política de Seguridad 89
Anexo C. Procedimiento de auditorías Internas 92
Anexo D. Gestión de Indicadores 96
Anexo F. Procedimiento de Revisión por la Dirección 104
Anexo G. Gestión de Roles y Responsabilidades 107
Anexo H. Metodología de Análisis de Riesgos 112
Anexo I. Plantilla Declaración de Aplicabilidad 116
Anexo J. Tabla de amenazas Magerit 119
Anexo K. Tabla de análisis amenazas/activos 120
Anexo L. Tabla de Análisis amenazas/activos tras ejecución de Proyectos. 123
Anexo M. Efectividad de los controles ISO/IEC 27002:213 tras implantación de proyectos 126
Anexo N. Declaración aplicabilidad 131
Anexo O. Cumplimiento Requerimientos ISO/IEC 27001:2013 136
Anexo P. Cumplimiento controles 137
Anexo Q. Informe de Auditoría 141

Índice de ilustraciones

Ilustración 1. Ciclo de Deming aplicado a los SGSI. 9
Ilustración 2. Organigrama RecycleSA..... 14
Ilustración 3. Organigrama departamento IT RecycleSA. 15
Ilustración 4. Estructura del servicio de soporte IT de RecycleSA. 16
Ilustración 5. Topología global de comunicaciones RecycleSA. 24
Ilustración 6. Esquema de red de CPD principal de RecycleSA. 24
Ilustración 7. Esquema de comunicaciones en sedes y proveedores de RecyclesA. 25
Ilustración 8. Evaluación de la implantación de los controles ISO/IEC 27002:2013 29
Ilustración 9. Evaluación de madurez de los controles ISO/IEC 27002:2013 29
Ilustración 10. ISO 31000 - Marco de trabajo para la gestión de riesgos 38
Ilustración 11. Planificación de proyectos propuesta. 71
Ilustración 12. Evaluación esperada de controles ISO/IEC 27002:2013 tras proyectos..... 75
Ilustración 13. Evaluación esperada de madurez de los controles ISO/IEC 27002:2013 tras proyectos ... 76

Índice de Tablas

Tabla 1. Usuarios por sede. 17
Tabla 2. Distribución de puestos de trabajo por sede. 18
Tabla 3.Distribución de dispositivos móviles por sede. 19
Tabla 4. Distribución de dispositivos ToIP por sede. 20
Tabla 5. Distribución de uso de aplicaciones de usuarios por sede. 21
Tabla 6. Distribución servidores físicos por sede. 22
Tabla 7. Distribución servidores virtuales por sede 22
Tabla 8. Distribución de servicios de servidor por ubicación. 23
Tabla 9. Modelo de madurez. 28
Tabla 10. Evaluación de efectividad de los controles ISO/IEC 27002:2013. 28
Tabla 11. Evaluación de situación ISO/IEC 27001:2013 30
Tabla 12. Estructura organizativa de la Seguridad de la Información 36
Tabla 13. Tipos de activo 41
Tabla 14. Activos 43
Tabla 15. Valoración de activos 44
Tabla 16. Dimensiones de la seguridad 45
Tabla 17. Escala de valoración de dimensiones de la seguridad 45
Tabla 18. Valoración de activos 46
Tabla 19. Grupos de amenazas Magerit 47
Tabla 20. Tipificación de frecuencias de amenazas 47
Tabla 21. Valoración de impactos de amenazas 47
Tabla 22. Escala de valoración de dimensiones de la seguridad 48
Tabla 23. Valoración de impacto potencial sobre cada activo 49
Tabla 24. Escala de riesgos 50
Tabla 25. Cálculo de riesgo en base a impacto y frecuencia 50
Tabla 26. Estimación de riesgos 51
Tabla 27. Proyectos Propuestos. 53
Tabla 28. PRY1. Migración infraestructura CPD a modelo IaaS. 56
Tabla 29. PRY2. Securización dispositivos portátiles. 57
Tabla 30. PRY3. Eliminación infraestructura de servidores sedes. 59
Tabla 31. PRY4. Implantación solución MDM. 61
Tabla 32. PRY5. Políticas de seguridad. 63
Tabla 33. PRY6. Plan de Formación. 64
Tabla 34. PRY7. Política de dispositivos móviles. 65
Tabla 35. PRY8. Política y auditoría de control de accesos. 67
Tabla 36. PRY9. Plan de continuidad de negocio. 68
Tabla 37. PRY10. Procedimientos de gestión de incidentes de seguridad. 69
Tabla 38. Escala de valoración de dimensiones de la seguridad tras implantación proyectos 72
Tabla 39. Estimación de riesgos tras ejecución de proyectos 73
Tabla 40. Relación controles/proyectos 74
Tabla 41. Evaluación esperada de efectividad de los controles ISO/IEC 27002:2013 tras proyectos. 75
Tabla 42. Codificación de cumplimiento y no conformidades. 78

1 INTRODUCCIÓN

El Trabajo de Fin de Máster que se describe en esta memoria, tiene por objetivo establecer las bases para la implementación de un Sistema de Gestión de la Seguridad (SGSI) en una multinacional dedicada al reciclaje de residuos industriales.

La implantación del SGSI debe permitir a la organización mejorar la seguridad de su información que, como para buena parte de las compañías actuales, se ha convertido en uno de sus mayores activos.

La organización es consciente de la necesidad de proteger adecuadamente su información, pero hasta ahora no cuenta con un sistema de gestión definido para conseguirlo. Es por ello que se plantea la implantación de su SGSI de acuerdo con los planteamientos y requisitos definidos por la norma ISO/IEC 27001, pues es ésta una norma ampliamente reconocida que, además, y llegado el caso, les permitiría certificar la organización, con las ventajas adicionales que ello conlleva en cuanto a mejora de su imagen corporativa.

Para conseguir los objetivos descritos, se ha realizado este proyecto fin de máster mediante la ejecución de las siguientes fases:

1. Determinación de la situación actual: contextualización de la organización, definición de los objetivos del SGSI y realización del análisis diferencial con respecto a los requerimientos de la norma ISO/IEC 27001:2013 a implantar.
2. Definición del sistema de gestión documental del SGSI. Para ello se han definido los siguientes documentos:
   - Política de Seguridad
   - Procedimiento de Auditorías Internas
   - Gestión de Indicadores
   - Procedimiento de Revisión por la Dirección
   - Metodología de Análisis de Riesgos
   - Declaración de Aplicabilidad
3. Análisis de riesgos. Siguiendo la metodología de análisis de riesgos definida en la fase anterior, basada en Magerit, para la identificación de activos y amenazas y la posterior evaluación de riesgos.
4. Propuestas de proyectos orientados a mitigar los riesgos de la organización. Para la elección de los proyectos se tienen en cuenta fundamentalmente el análisis de riesgos, las amenazas detectadas previamente y el análisis diferencial realizado al inicio de este trabajo.
5. Auditoría de cumplimiento. Se trata de valuar la seguridad de la organización y su grado de cumplimiento respecto a la ISO/IEC 27001:0113, identificando las no conformidades y proponiendo las mejoras necesarias, que quedan reflejadas en el informe de auditoría generado.

Tras la realización de todas estas tareas, se extraen las conclusiones y se determinan los objetivos alcanzados y los aspectos a mejorar, que se deberán abordar dentro de la mejora continua que todo SGSI de contemplar.

2 SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

2.1 INTRODUCCIÓN

La información siempre ha sido un valor importante en las organizaciones. Hoy en día, con la gran revolución de las tecnologías de la información, para muchas compañías se ha convertido en su principal activo. Es, por tanto, un valor que hay que proteger.

La seguridad de la información hay que contemplarla en un sentido amplio, entendiendo que afecta a todos los estamentos de las organizaciones y que debe gestionarse de manera adecuada para protegerla en todas sus dimensiones, que tradicionalmente comprenden, al menos:

- **Confidencialidad.** Sólo las personas autorizadas deben tener acceso a la información sensible o privada.
- **Integridad.** La información de la organización debe ser fiable y no manipulable, de manera que sólo las personas autorizadas puedan registrar la información.
- **Disponibilidad.** La información debe estar disponible cuando lo necesiten los usuarios autorizados.

La implementación de un Sistema de Gestión de la Seguridad de la Información[1] es el mecanismo natural que tenemos para proteger la información de las organizaciones.

Para la puesta en marcha de un SGSI, como se describe en el manual de la asignatura *Sistemas de Gestión de la Seguridad de la Información* [1], que forma parte del Máster Interuniversitario en Seguridad de las TIC (MISTIC) [2], es necesario:

- **Conocer el negocio:** lo que permitirá identificar sus procesos críticos, cuya seguridad se habrá de priorizar.
- **Analizar la situación de partida**, con el objetivo de establecer un plan definido que permita alcanzar los objetivos deseados desde la situación actual.
- **El contexto en el que se trabaja**, lo que permitirá identificar y analizar los correspondientes riesgos para el negocio, que el SGSI debe tener en cuenta
- **Identificar las leyes de aplicación a la organización**, que podrán incluir medidas de seguridad que obligatoriamente deberá incluirse en el SGSI.

Para la puesta en marcha de cualquier SGSI es conveniente utilizar normas o referencias que hayan demostrado su eficacia pues existen múltiples estándares relativos a la gestión de la seguridad de la información. La familia ISO27000 es una de las más importantes y reconocidas, y la que utilizaremos para desarrollar este trabajo.

En concreto el plan de implementación del SGSI lo desarrollaremos siguiendo las directrices de la norma ISO/IEC 27001:2013 y el código de buenas prácticas que describe la norma ISO/IEC 27002:2013, que pasamos a describir.

[1] En adelante SGSI

2.1.1 ISO/IEC 27001:2013

La norma ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad.

Para ello plantea un sistema de gestión basado en el Ciclo de Deming: Plan, Do, Check, Act, conocido como PDCA y que podemos traducir como Planificar, Hacer, Comprobar y Mejorar.

Así pues, el plan de proyecto para la implantación de la ISO 27001 debe desarrollar un ciclo de Deming que garantice la actualización del sistema de gestión de la seguridad y su mejora continua.

El ciclo de Deming aplicado a los sistemas de gestión de la seguridad constaría de las fases y tareas que se describen a continuación y muestra en el siguiente gráfico:

- Planificar: Establecer el SGSI

  En esta fase se analizará la actividad que realiza la compañía, la información que trata, las directrices corporativas y los requisitos legales que le son aplicables.

- Hacer: Implantar y operar el SGSI

  En esta fase se desarrollará e implantará el plan de seguridad que evite o atenúe los posibles riesgos para la seguridad de la información de la organización.

- Verificar: Monitorizar y revisar el SGSI.

  En esta fase se realiza el seguimiento y revisión de los controles y medidas implantados, para verificar la eficacia de SGSI y su mejora continua

- Actuar: Mantener y mejorar el SGSI.

  El objetivo de esta fase es mantener y mejorar constantemente el SGSI. Para ello, cuando se detecten deficiencias se deberán tomar las medidas correctoras que garanticen la seguridad y protección de la información.

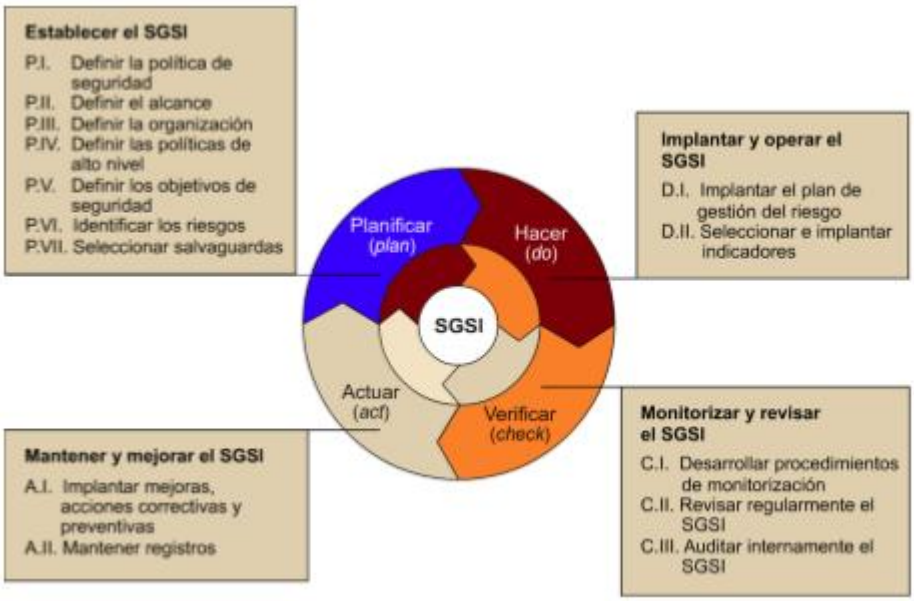

Ilustración 1. Ciclo de Deming aplicado a los SGSI.

Fuente: manual de la asignatura *Sistemas de Gestión de la Seguridad de la Información* [1] del *Máster Interuniversitario en Seguridad de las TIC (MISTIC)*[2]

La norma ISO/EIC 27001:2013, que es una norma certificable, establece como obligatorios los siguientes documentos[2]:

- El alcance del sistema de gestión de seguridad de la información (apartado 4.3)

  Este documento debe mostrar el alcance definir los límites y la aplicabilidad del SGSI determinados por la organización, en la que se deben de tener en cuenta:

- Los aspectos externos e internos relevantes para el SGSI
- Los requisitos, necesidades y expectativas de las partes interesadas.
- Los interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones.

  Suele ser un documento corto e independiente, aunque a veces se unifica con el documento de política de seguridad de la información.

- Política de seguridad de la información y objetivos (apartados 5.2 y 6.2)

  Es un documento de alto nivel que debe detallar la política de seguridad de información establecida para la organización por la alta dirección. Igualmente se deben detallar los objetivos principales del SGSI, que deben ser consistentes con la política, medibles y tener en cuenta los requisitos y los resultados del análisis de riesgos.

  Igualmente debe definir la planificación prevista para lograr los objetivos.

- Metodología de evaluación y tratamiento de riesgos (apartado 6.1.2)

  Este documento debe plasmar la información sobre el proceso de valoración de riesgos que se realiza en la organización, incluyendo los criterios de utilizados para la identificación, valoración, análisis, evaluación y aceptación de riesgos.

  La metodología utilizada debe ser redactada antes de que se realice la evaluación y el tratamiento de los riesgos, cuyo informe se realizará posteriormente.

- Declaración de aplicabilidad (apartado 6.1.3 d)

  Este documento, que se basa en los resultados del tratamiento del riesgo, describe los controles que son aplicables (que se pueden tomar del Anexo A o incluir controles adicionales), cómo se implantaran dichos controles y su estado actual.

- Plan de tratamiento de riesgo (apartado 6.1.3 e y 6.2)

  Este documento define el plan de acción establecido para implementar los distintos controles establecidos en el documento de declaración de aplicabilidad.

  Se basa, por tanto, en la declaración de aplicabilidad y se actualiza durante todo el proceso de implantación del SGSI.

- Informe sobre evaluación de riesgos (apartado 8.2, 8.3)

  Este documento debe plasmar las evaluaciones de riesgos realizadas siguiendo los criterios y metodologías de evaluación tratamiento de riesgos recogidas en el documento correspondiente.

  Igualmente debe reflejar los resultados del tratamiento de los riesgos realizado.

  El documento se actualiza a intervalos planificados o cuando ocurran cambios significativos en relación a los riesgos.

[2] Los documentos del Anexo A son obligatorios únicamente si existen riegos que obliguen a su implantación.

- Definición de roles y responsabilidades de seguridad (apartados A.7.1.2 y A.13.2.4)

  Este documento debe reflejar las funciones y responsabilidades de seguridad de los empleados y contratistas que se definir en contratos. Dichas funciones y responsabilidades deben describirse de la manera más precisa posible.

  También debe contener los requisitos para los acuerdos de confidencialidad y no divulgación que reflejen las necesidades de la organización para la protección de la información, que deben ser identificados, revisados y documentados periódicamente.

- Inventario de activos (apartado A.8.1.1)

  Este documento debe identificar los activos de la organización y definir las responsabilidades de su protección. Debe mantener actualizado adecuadamente.

- Uso aceptable de los activos (apartado A.8.1.3)

  Este documento debe reflejar las reglas para el uso aceptable de los activos asociados con la información.

- Política de control de acceso (apartado A.9.1.1)

  Este documento debe mostrar la política de control de acceso definida por la organización en base a los requisitos de negocio y seguridad de la información.

  Puede incluir reglas de acceso lógico y/o físico y debe revisarse periódicamente.

- Procedimientos de operación para gestión de TI (apartado A.12.1.1)

  Este documento debe reflejar los procedimientos operativos de gestión de TI, como, entre otros, los incluidos en los puntos A.12 Seguridad de las operaciones y A.13 Seguridad de las comunicaciones, como puede ser la gestión de copias de seguridad, seguridad y monitorización de red, gestión de código malicioso, etc.

- Principios de ingeniería de sistemas seguros (apartado A.14.2.5)

  Este documento debe definir cómo se debe incorporar principios y técnicas para la construcción de sistemas seguros en cualquier actividad o área implicada en la implantación de sistemas de información: negocio, datos, aplicaciones, etc.

- Política de seguridad para proveedores (apartado A.15.1.1)

  Este documento debe reflejar la política de seguridad para la relación con los proveedores. Esta política puede incluir múltiples controles, como cláusulas a incluir en los contratos, mecanismos de verificación de su cumplimiento, evaluación de riesgos de un proveedor, etc.

- Procedimiento para gestión de incidentes (apartado A.16.1.5)

  Este documento debe definir como se notifican y gestionan los incidentes de seguridad. Además debe contemplar cómo se estudian posteriormente para aprender de ellos y tratar de evitarlos en un futuro.

- Procedimientos de Continuidad de negocio (apartado A.17.1.2)

  Este documento debe reflejar los procedimientos definidos para garantizar la continuidad del negocio como los planes de contingencia y procedimientos de recuperación ante desastres.

- Requerimientos legales, regulatorios y contractuales (apartado A.18.1.1)

  Este documento debe incluir todos los requisitos impuestos por la legislación aplicable y por las obligaciones contractuales.

2.1.2 ISO/IEC 27002:2013

A diferencia de la norma ISO/IEC 27001:2013 que, como hemos indicado es una norma certificable, la ISO/IEC 27002:2013 es un conjunto de buenas prácticas para la gestión de la seguridad de la información.

Se estructura a través de 14 capítulos de controles de seguridad que contienen 35 categorías principales y 114 controles de seguridad.

Los controles de seguridad que establece la norma son:

- A5. Políticas de seguridad de la información
- A6. Organización de la seguridad de la información
- A7. Seguridad relativa a los recursos humanos
- A8. Gestión de activos
- A9. Control de acceso
- A10. Criptografía
- A11. Seguridad física y del entorno
- A12. Seguridad de las operaciones
- A13. Seguridad de las comunicaciones
- A14. Adquisición, desarrollo y mantenimiento de los sistemas de información
- A15. Relación con proveedores
- A16. Gestión de incidentes de seguridad de la información
- A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
- A18. Cumplimiento

El detalle de las categorías principales y de los controles de cada capítulo de seguridad se puede consultar en el punto *Anexo A. Efectividad de los controles ISO/IEC 27002:2013* de este documento.

2.2 CONTEXTUALIZACIÓN

Para la realización del Plan Director de seguridad que se abordará en este proyecto hemos seleccionado una multinacional dedicada a prestar servicios medioambientales, actualmente especializada en el reciclaje de residuos industriales, que, a efectos de este Trabajo Final de Máster, denominaremos *RecycleSA.*

2.2.1 DESCRIPCIÓN GENERAL DE LA ORGANIZACIÓN

RecycleSA es una multinacional formada por distintas sociedades, con sedes distribuidas en múltiples países, fundamentalmente en Europa. Durante sus ya más de 25 años de historia, siempre ha prestado servicios relacionados con la gestión medioambiental, con el objetivo prioritario de ser líderes y tecnológicamente competitivos para ofrecer sus servicios en la industria del reciclaje.

Los principios que rigen RecycleSA son:

- Misión.

  Prestar servicios medioambientales y soluciones sostenibles de gestión y reciclaje de residuos peligrosos de las industrias del acero y aluminio.

- Visión:

  Aportar soluciones y servicios para la gestión y el reciclaje de residuos industriales teniendo muy presente su responsabilidad social para contribuir a crear un mundo sostenible.

- Valores:
  - Liderazgo en prevención de riesgos laborales y protección medioambiental.
  - Excelencia en sus operaciones y los servicios que ofrece.
  - Cumplimiento, integridad y transparencia.

A lo largo de su historia, han ido variando las sociedades que la componen, las sedes que la integran y los países en los que opera. Actualmente se encuentra en proceso de reorganización tras la venta de algunas sociedades y la incorporación de nuevas sedes en nuevos continentes.

RecycleSA también se encuentra actualmente en un proceso de importante cambio tecnológico, en lo referente a las tecnologías de la Información. Entre esos cambios podemos destacar los siguientes:

- Cambios en su estructura de comunicaciones en buena parte de sus sedes.
- Migración de la infraestructura de servidores centralizados, actualmente localizados en un CPD en España, hacia infraestructura IaaS.
- Cambio del servicio ERP principal desde SAP a Navision.

2.2.2 ESTRUCTURA ORGANIZATIVA

RecycleSA se organiza alrededor de sus dos grandes unidades de negocio:

- Servicios de reciclaje de acero.
- Servicios de reciclaje de aluminio.

Adicionalmente, como toda organización, requiere de infraestructura y servicios adicionales para su funcionamiento. Entre los más importantes se encuentran:

- Servicios financieros.
- Recursos Humanos.
- Legal.
- Seguridad y Medio Ambiente.
- Tecnologías de la información.
- Desarrollo de negocio
- …

Para prestar todos estos servicios, la compañía se estructura según el organigrama que se muestra en la siguiente figura:

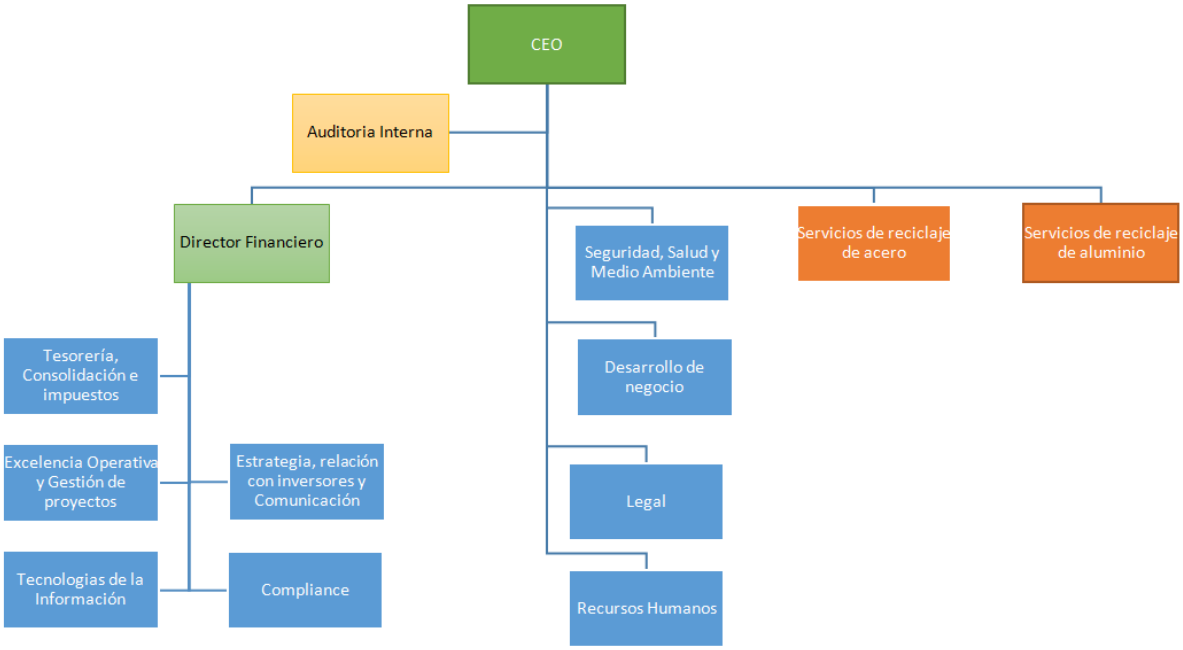

Ilustración 2. Organigrama RecycleSA

2.2.3 ESTRUCTURA DEL SERVICIO DE IT

RecycleSA mantiene externalizado la mayor parte de sus servicios de TI, por lo que el departamento de Tecnologías de la información cuenta únicamente con 4 integrantes.

El organigrama y responsabilidades del equipo de Servicios IT se muestra en la siguiente figura.

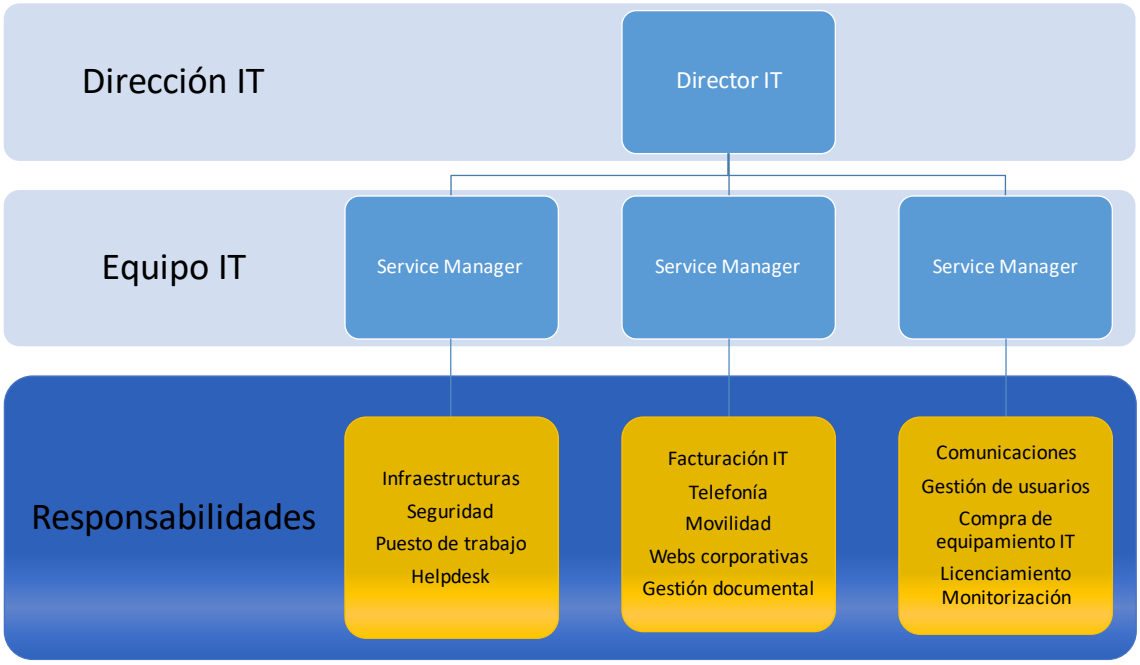

Ilustración 3. Organigrama departamento IT RecycleSA.

Los integrantes del departamento de TI se encargan de definir los servicios de TI a proporcionar a la organización, así como establecer las políticas de gestión que deben aplicar los diferentes proveedores de servicio de TI. Igualmente son responsables de la correcta coordinación de los distintos servicios y proveedores, así como del seguimiento y control de los distintos servicios contratados.

Básicamente, los servicios de TI prestados en RecycleSA son:

- Servicios de infraestructuras: servidores y almacenamiento.
- Servicios de comunicaciones y redes.
- Servicios de seguridad.
- Servicios de despliegue al puesto de trabajo.
- Servicios Office 365: Correo y Sharepoint.
- Servicios ERP: SAP y Navision.
- Servicios de telefonía.
- Servicios de soporte remoto al puesto de usuario.
- Servicios de soporte on-site.
- Servicios de Helpdesk.

El servicio de soporte IT de RecycleSA se estructura como se muestra en el siguiente gráfico:

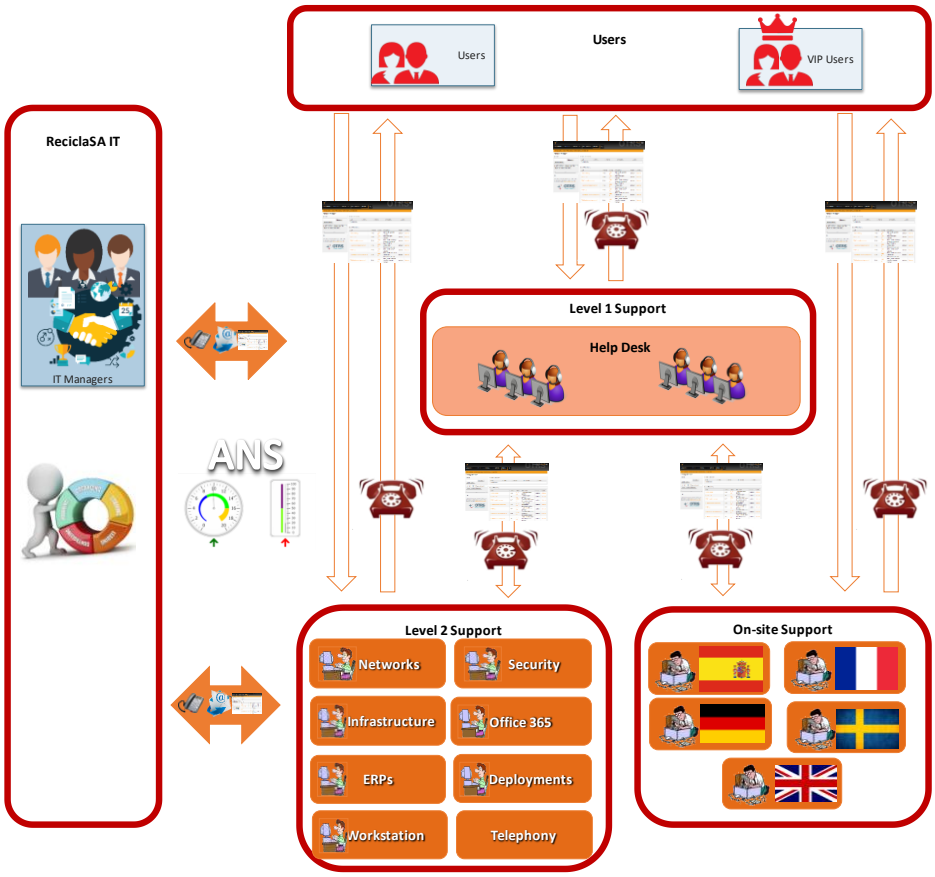

Ilustración 4. Estructura del servicio de soporte IT de RecycleSA.

2.2.4 USUARIOS Y SEDES

Actualmente RecycleSA proporciona servicios de información a aproximadamente 450 usuarios, distribuidos en los distintos países y sedes como se muestra en la siguiente tabla:

Sedes	Usuarios
Alemania	**160**
Alemania-Sede 1	28
Alemania-Sede 2	28
Alemania-Sede 3	16
Alemania-Sede 4	35
Alemania-Sede 5	12
Alemania-Sede 6	41
China	**3**
China-Sede 1	3
Corea	**18**
Corea-Sede 1	18
España	**199**
España-Sede 1	5
España-Sede 2	61
España-Sede 3	62
España-Sede 4	26
España-Sede 5	7
España-Sede 6	8
España-Sede 7	30
Francia	**42**
Francia-Sede 1	42
Reino Unido	**21**
Reino Unido-Sede 1	21
Total general	**443**

Tabla 1. Usuarios por sede.

Todos estos usuarios disponen de una cuenta en el Directorio Activo de RecyleSA mediante la cual se gestiona el acceso a la mayor parte de los sistemas de información de la organización.

2.2.5 INFRAESTRUCTURA TECNOLÓGICA

A pesar de que RecycleSA mantiene algunos de sus servicios, como el correo y video-conferencia, en la modalidad SaaS, muchos otros servicios se gestionan con infraestructuras propias, que deben ser adecuadamente gestionadas y securizadas.

RecyleSA tiene en proyecto la migración de su infraestructura de servicios a la modalidad IasS, por lo que la infraestructura descrita en este apartado cambiará notablemente en los próximos meses. En todo caso, este apartado refleja la situación actual de RecycleSA.

2.2.5.1 PUESTOS DE TRABAJO

Los empleados de RecycleSA que necesitan acceso a los sistemas de información disponen de 2 tipos de puestos de trabajo:

- PCs, para aquellos usuarios que no requieren movilidad en su puesto de trabajo.
- Portátiles, para aquellos usuarios que si requieren movilidad.

Los usuarios con portátiles tienen la posibilidad, previa autorización, de conectarse en remoto a las infraestructuras de RecycleSA a través de una conexión VPN.

La distribución de los PCs y portátiles en las distintas sedes se muestra en la siguiente tabla.

Sedes	PC	Portátil	Total
Alemania	**83**	**81**	**164**
Alemania-Sede 1	16	8	24
Alemania-Sede 2	15	10	25
Alemania-Sede 3	13	5	18
Alemania-Sede 4	14	11	25
Alemania-Sede 5	11	4	15
Alemania-Sede 6	14	43	57
Corea	**17**	**1**	**18**
Corea-Sede 1	17	1	18
España	**113**	**125**	**238**
España-Sede 1		7	7
España-Sede 2	35	44	79
España-Sede 3	31	34	65
España-Sede 4	20	7	27
España-Sede 5	10	15	25
España-Sede 6	3	4	7
España-Sede 7	14	14	28
Francia	**33**	**16**	**49**
Francia-Sede 1	33	16	49
Reino Unido	**14**	**10**	**24**
Reino Unido-Sede 1	14	10	24
Total	**260**	**233**	**493**

Tabla 2. Distribución de puestos de trabajo por sede.

2.2.5.2 DISPOSITIVOS MÓVILES

Hoy en día los dispositivos móviles son un medio de acceso habitual a la información de cualquier organización. En RecycleSA, se proporciona dispositivos móviles corporativos a determinados usuarios en función de sus necesidades y responsabilidades.

Adicionalmente se permite que el resto de usuarios utilice sus propios dispositivos para el acceso a la información corporativa, en lo que denominamos BYOD.

Actualmente no se utilizan soluciones para la gestión de estos dispositivos móviles, más allá de las funcionalidades de gestión que proporciona el servicio de Exchange Online para el acceso al correo desde este tipo de dispositivos.

Sin embargo, está prevista la implantación de la solución Microsoft Intune para mejorar la gestión de los dispositivos móviles.

En la siguiente tabla se muestra la distribución de uso de dispositivos móviles en las distintas sedes, catalogadas por tecnología (Android/iphone/Ipad) y por la propietario del dispositivo (corporativo o personal).

Sedes	Corp Android/Win	Corp iPhone	Corp IPAD	BYOD Android/Win	BYOD iPhone	BYOD - iPad
Alemania	**54**	**12**	**11**	**6**	**9**	
Alemania-Sede 1	9					
Alemania-Sede 2	10	1	1			
Alemania-Sede 3	7	2		1		
Alemania-Sede 4	6			1	4	
Alemania-Sede 5	3			3		
Alemania-Sede 6	19	9	10	1	5	
China	**1**					
China-Sede 1	1					
Corea				**10**		
Corea-Sede 1				10		
España	**71**	**12**	**12**	**1**		**1**
España-Sede 1	4	1				
España-Sede 2	29	6	6			
España-Sede 3	11	3	3			1
España-Sede 4	7					
España-Sede 5	3	2	3	1		
España-Sede 6	3					
España-Sede 7	14					
Francia	**18**	**1**			**2**	**1**
Francia-Sede 1	18	1			2	1
Reino Unido	**12**					
Reino Unido-Sede 1	12					
Total general	**156**	**25**	**23**	**17**	**11**	**2**

Tabla 3.Distribución de dispositivos móviles por sede.

2.2.5.3 TELEFONÍA IP

En determinadas sedes se ha implantado telefonía IP para las comunicaciones fijas de voz de los usuarios. Estas comunicaciones utilizan la red de datos de RecycleSA, por lo que es importante su correcto control para el Sistema de Gestión de la Seguridad de la Información.

A continuación se muestran los usuarios que utilizan tecnología IP para sus comunicaciones de voz:

Sedes	ToIP
Alemania	**95**
Alemania-Sede 1	13
Alemania-Sede 2	
Alemania-Sede 3	14
Alemania-Sede 4	17
Alemania-Sede 5	10
Alemania-Sede 6	41
China	
China-Sede 1	
Corea	
Corea-Sede 1	
España	**137**
España-Sede 1	
España-Sede 2	55
España-Sede 3	48
España-Sede 4	13
España-Sede 5	6
España-Sede 6	
España-Sede 7	15
Francia	
Francia-Sede 1	
Reino Unido	
Reino Unido-Sede 1	
Total general	**232**

Tabla 4. Distribución de dispositivos ToIP por sede.

2.2.5.4 APLICACIONES CORPORATIVAS

Todos los usuarios de los sistemas de información de RecycleSA utilizan, en mayor o menor medida, aplicaciones corporativas.

Podemos destacar 2 grandes grupos:

- Aplicaciones ERPs.

  RecycleSA está compuesta por diversas sociedades. La mayor parte de ellas utilizan actualmente el ERP del fabricante SAP. Sin embargo, algunas sociedades utilizan Navision como aplicación ERP. Además, residualmente, se utiliza contaplus.

- Servicios de correo, ofimática y colaboración.

  RecycleSA utiliza los servicios en la nube que Microsoft ofrece bajo su plataforma Office 365. En concreto de todos los servicios que incluye esta plataforma, actualmente se utilizan:
  - La suite de aplicaciones Office, que se utiliza habitualmente en local en los puestos de trabajo.
  - Correo Outlook. Se utiliza tanto en local como en la nube.
  - Sharepoint
  - Onedrive
  - Skype

La siguiente tabla muestra la distribución de uso por parte de los usuarios de las aplicaciones comentadas anteriormente.

Sedes	Navision	SAP	Contaplus	Office 365	Correo
Alemania	**60**	**4**		**150**	**152**
Alemania-Sede 1	25			25	25
Alemania-Sede 2				26	28
Alemania-Sede 3				15	15
Alemania-Sede 4	20			32	32
Alemania-Sede 5	12			11	11
Alemania-Sede 6	3	4		41	41
China				**3**	**3**
China-Sede 1				3	3
Corea				**18**	**18**
Corea-Sede 1				18	18
España	**91**	**68**	**9**	**182**	**183**
España-Sede 1		5		5	5
España-Sede 2		49	9	57	58
España-Sede 3	50	3		57	57
España-Sede 4	17			20	20
España-Sede 5	1	7		7	7
España-Sede 6		4		8	8
España-Sede 7	23			28	28
Francia		**23**		**39**	**39**
Francia-Sede 1		23		39	39
Reino Unido	**18**	**2**		**19**	**19**
Reino Unido-Sede 1	18	2		19	19
Total general	**169**	**97**	**9**	**411**	**414**

Tabla 5. Distribución de uso de aplicaciones de usuarios por sede.

2.2.5.5 INFRAESTRUCTURA DE SERVIDORES

Como ya se ha comentado, RecycleSA utiliza algunos servicios en la nube, como el servicio de correo y de videoconferencia. Pero buena parte de los servicios utilizan infraestructuras propias que se gestionan por su propio departamento IT a través de la contratación de proveedores externos.

La mayor de los servidores que alojan estos servicios se alojan en servidores ubicados en un DataCenter contratado para ello. Todos ellos son servidores virtualizados mediante un hipervisor.

Sin embargo, en algunas de las sedes de mayor dimensión, también se ubican servidores distribuidos para dar algunos de los servicios básicos de red, como puede ser el servicio de ficheros. En este caso encontramos tanto servidores físicos como virtuales.

Esta deslocalización de la infraestructura de servidor en distintas sedes genera unos riesgos relacionados con la seguridad física que deben ser tenidos en cuenta.

La distribución de los servidores físicos y virtuales en las distintas sedes se muestra en la siguiente tabla.

Ubicación	Servidores físicos
Alemania	**13**
Alemania-Sede 1	2
Alemania-Sede 2	3
Alemania-Sede 3	2
Alemania-Sede 4	2
Alemania-Sede 5	2
Alemania-Sede 6	2
Corea	**2**
Corea-Sede 1	2
España	**12**
CPD Principal	8
España-Sede 2	4
Francia	**2**
Francia-Sede 1	2
Reino Unido	**2**
Reino Unido-Sede 1	2
Suecia	**2**
Suecia-Sede 1	2
Total general	**33**

Tabla 6. Distribución servidores físicos por sede.

Ubicación	Servidores Virtuales
Alemania	**18**
Alemania-Sede 1	3
Alemania-Sede 2	2
Alemania-Sede 3	3
Alemania-Sede 4	3
Alemania-Sede 5	3
Alemania-Sede 6	4
Corea	**3**
Corea-Sede 1	3
España	**64**
CPD Principal	56
España-Sede 2	2
España-Sede 4	6
Francia	**4**
Francia-Sede 1	4
Reino Unido	**3**
Reino Unido-Sede 1	3
Suecia	**2**
Suecia-Sede 1	2
Total general	**94**

Tabla 7. Distribución servidores virtuales por sede

La distribución de los servicios en los distintos servidores y ubicaciones es la siguiente:

Ubicación	Servidor Ficheros	Directorio Activo	Herramientas	Aplicaciones/Servicios	BBDD	Otros
Linux			**13**	**1**	**1**	**14**
Alemania-Sede 6			1			1
CPD Principal			12	1	1	13
Otros			**1**	**4**		**5**
CPD Principal			1	4		5
Windows	**13**	**7**	**38**	**9**	**16**	**75**
Alemania-Sede 1	1		1		1	3
Alemania-Sede 2	1		1			2
Alemania-Sede 3	1		2		1	3
Alemania-Sede 4	1		1		1	3
Alemania-Sede 5	1		1		1	3
Alemania-Sede 6	1	1	2			3
Corea-Sede 1	1	1	3			3
CPD Principal	4	5	22	3	4	38
España-Sede 2			1			2
España-Sede 4				6	5	6
Francia-Sede 1	1		1		2	4
Reino Unido-Sede 1	1		1		1	3
Suecia-Sede 1			2			2
Total general	**13**	**7**	**52**	**14**	**17**	**94**

Tabla 8. Distribución de servicios de servidor por ubicación.

2.2.5.6 RED DE COMUNICACIONES

El esquema global de la red de comunicaciones de RecycleSA se muestra en la siguiente figura.

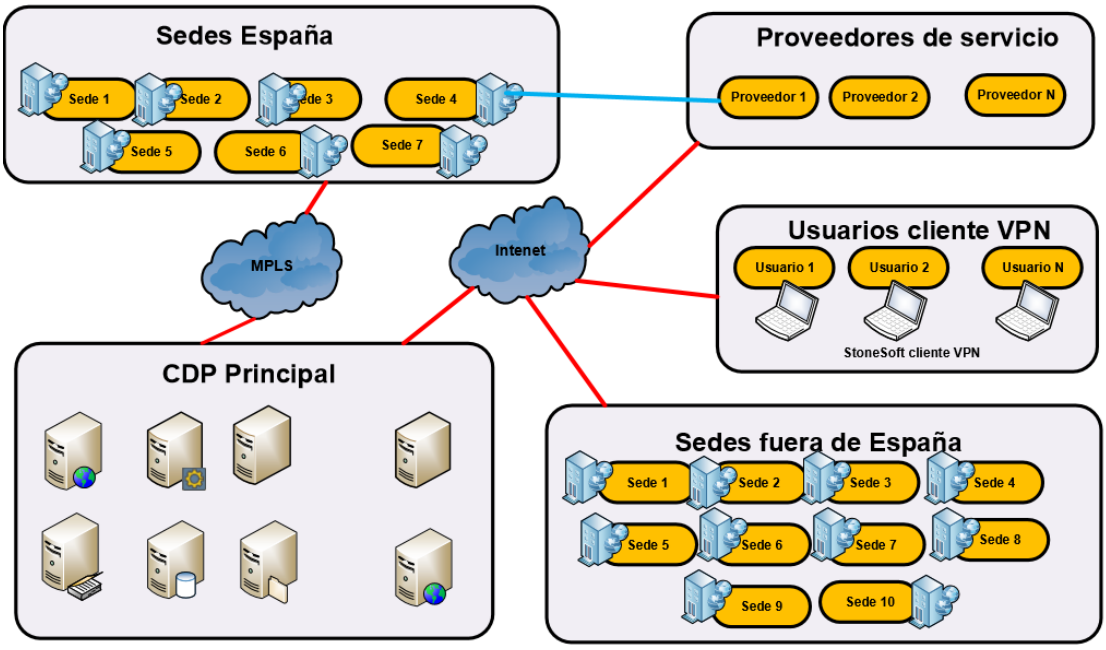

Ilustración 5. Topología global de comunicaciones RecycleSA.

Los elementos de interconexión y la topología de red del CPD principal es la que se muestra a continuación.

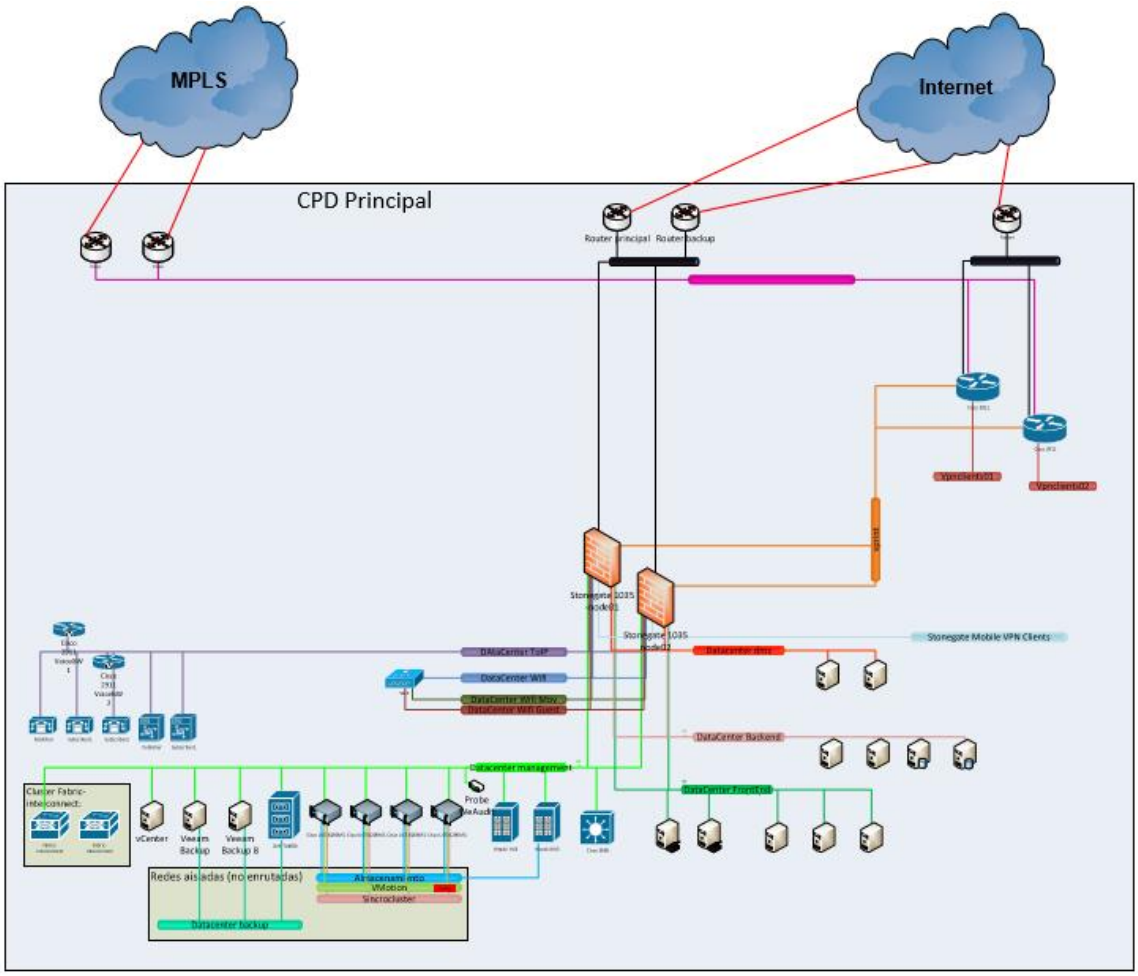

Ilustración 6. Esquema de red de CPD principal de RecycleSA.

Finalmente, la estructura de conexión para las distintas sedes y proveedores de servicio son los mostrados a continuación.

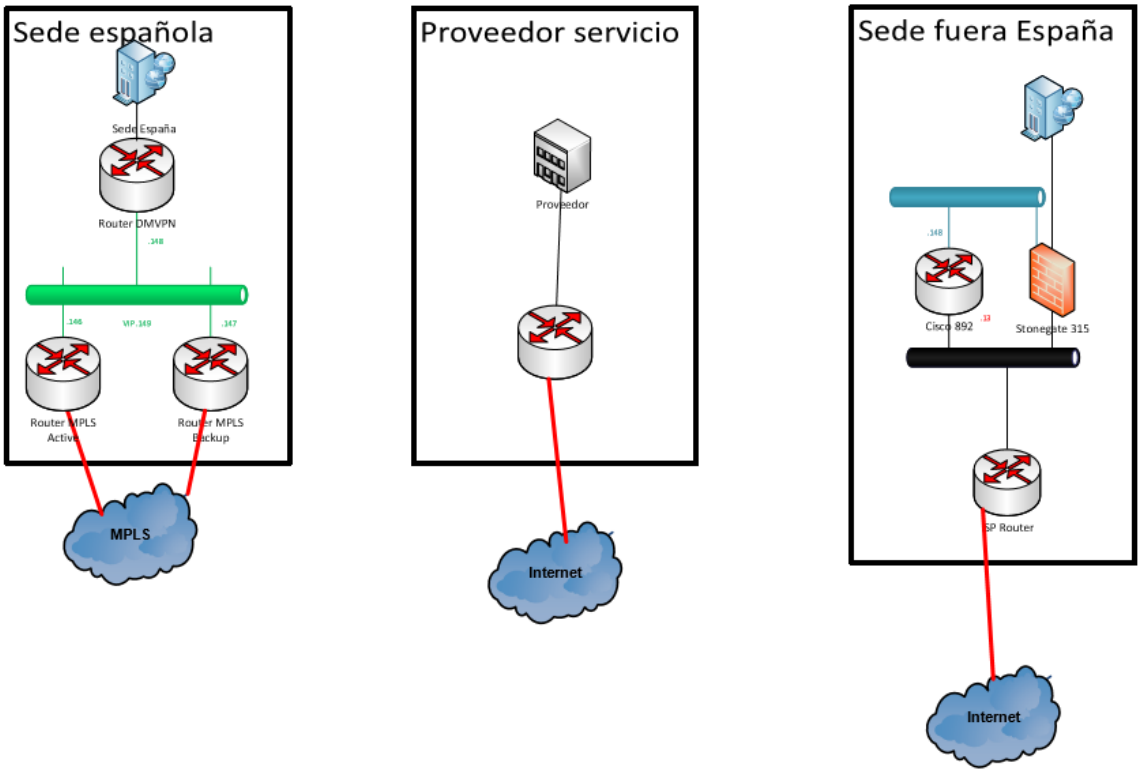

Ilustración 7. Esquema de comunicaciones en sedes y proveedores de RecyclesA.

2.2.6 ALCANCE

El Plan Director de Seguridad que se desea implantar en RecycleSA pretende adecuar a la norma ISO/IEC 27001:2013 todos los procesos y procedimientos, tanto organizativos como técnicos, relacionados con los Sistemas de Información de la organización.

Los Sistemas de Información contemplados abarcan:

- Sistemas relativos a los procesos productivos de RecycleSA: Servicios de reciclaje.
- Servicios financieros.
- Recursos Humanos.
- Legal.
- Seguridad y Medio Ambiente.
- Desarrollo de negocio.
- Tecnologías de la información.

Por todo ello, se incluye en el alcance:

- Todos los activos relacionados con la información relativa a los servicios que presta a terceros y con los propios procesos internos de la empresa, que ésta utiliza para su correcto funcionamiento.
- Todos los procesos de negocio y de organización interna que requieran de la gestión de información.
- Todos los procedimientos que el personal, tanto interno como externo, deben aplicar para la gestión de la información de la organización.

Como parte de los Sistemas de Información se incluye toda la infraestructura tecnológica para gestionar información de RecycleSA, independientemente de la ubicación física de la misma (instalaciones locales, CPD central o servicios en la nube) y del proveedor encargado de su gestión, pues, como se ha visto, RecycleSA mantiene externalizado buena parte de los servicios de TI.

En el alcance no se contempla, sin embargo, la seguridad física de los elementos que residen físicamente fuera de las instalaciones de RecycleSA, como pueden ser su CPD principal, y las infraestructuras que residen en la nube (en este caso de Microsoft).

Igualmente, tampoco se contemplan los activos, y procesos relacionados con sociedades ya vendidas, aunque todavía mantengan dependencias de los sistemas de información de RecycleSA

2.3 OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

El departamento de IT de RecycleSA es plenamente consciente de la importancia de definir un SGSI que permita mejorar los niveles de seguridad de los Sistemas de Información de su organización.

De hecho, el departamento IT siempre tiene en cuenta las consideraciones relativas a la seguridad en la gestión de los distintos servicios y en la implantación de nuevos proyectos IT.

Pero es plenamente consciente de que, para conseguir los niveles adecuados de seguridad, ésta se debe abordar de acuerdo a normas y principios estandarizados que ya hayan demostrado su bondad y eficacia.

Es por ello que considera que la elaboración de un Plan de implementación de la ISO/IEC 27001:2013 es el mecanismo idóneo para conseguirlo.

Considera, además, que como establece la norma descrita anteriormente, la seguridad de la información se debe abordar de manera integral, involucrando no sólo al departamento IT, sino a todos los

departamentos y empleados de la organización. Además, debe contar con el compromiso y el liderazgo de la alta dirección como requisito indispensable para conseguir alcanzar los objetivos marcados.

Es por ello que se plantea la elaboración del Plan Director de Seguridad que permita implantar un SGSI para la organización acorde a la norma ISO/IEC 27001:2013.

Los objetivos principales que se desean conseguir mediante la implantación del SGSI son:

- Promover la cultura de la seguridad en toda la organización, involucrando a la Alta Dirección y concienciando al conjunto del personal en lo relativo a la seguridad de la información, que actualmente se percibe como responsabilidad casi exclusiva del departamento de IT.
- Mejorar en la concienciación y formación del personal en cuanto a la seguridad de la información.
- Identificar los riesgos y amenazas a los que se encuentra expuesta la organización.
- Definir los procesos y controles necesarios para garantizar la seguridad de los sistemas de información bajo los umbrales de riesgo aceptables por la organización.
- Reducir el riesgo general para los activos de la organización, mejorando la disponibilidad de los servicios esenciales y la confidencialidad de la información, evitando fugas y/o robos de información.
- Definir los roles y responsabilidades de la organización en materia de seguridad.
- Adecuar todos los procesos y sistemas al Reglamento Europeo de Protección de Datos Personales (RGPD).
- Extender la visión y mecanismos de seguridad de la información, que actualmente se aplican básicamente desde el punto de vista IT, a todos los ámbitos de la organización.
- Conseguir la madurez necesaria en los procesos que permita la expansión de la compañía sin poner en riesgo su seguridad.
- Establecer las bases necesarias para conseguir una mejora continua en lo relativo a la seguridad de información.
- Alcanzar la madurez suficiente en los procesos de gestión de la seguridad de la información que faciliten a la organización superar auditorias de segundas partes que puedan requerir clientes e inversores.

De este modo, el objetivo principal a conseguir mediante el Plan Director de Seguridad es identificar los proyectos que se deberían abordar para la puesta en marcha efectiva del SGSI. Estos proyectos deben conseguir que la seguridad se tenga en cuenta en todos los procesos, técnicos o no, que afecten a los sistemas de información.

2.4 ANÁLISIS DIFERENCIAL

El objetivo del análisis diferencial que se presenta en esta apartado es conocer, de manera global, el estado actual de la Organización en relación con la Seguridad de la Información.

Para medir dicho estado actual de la Organización, utilizaremos el Modelo de Madurez de Capacidades o CMM (*Capability Maturity Model*) que permite evaluar los procesos de una organización.

En la tabla siguiente se muestra los distintos niveles que establece el modelo, y su descripción.

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	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	Gestionable 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.

Adicionalmente, se muestran en la tabla anterior los niveles de "efectividad" que utilizaremos para evaluar cuantitativamente los distintos niveles de cada control o proceso.

2.4.1 EVALUACIÓN DE EFECTIVIDAD DE LOS CONTROLES ISO/IEC 27002:2013

Tras la evaluación de la efectividad para los controles definidos por la norma, que se muestra en el apartado *0*, obtenemos los resultados que se muestran en la siguiente tabla:

Controles de Seguridad de la Información	Madurez	Implantados
A5. Políticas de seguridad de la información	**10%**	**2/2**
A6. Organización de la seguridad de la información	**6%**	**3/7**
A7. Seguridad relativa a los recursos humanos	**0%**	**0/6**
A8. Gestión de activos	**13%**	**3/10**
A9. Control de acceso	**38%**	**12/14**
A10. Criptografía	**0%**	**0/2**
A11. Seguridad física y del entorno	**1%**	**2/15**
A12. Seguridad de las operaciones	**49%**	**13/14**
A13. Seguridad de las comunicaciones	**43%**	**3/7**
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**0%**	**0/14**
A15. Relación con proveedores	**0%**	**0/5**
A16. Gestión de incidentes de seguridad de la información	**0%**	**/7**
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**0%**	**0/4**
A18. Cumplimiento	**0%**	**0/7**

Tabla 10. Evaluación de efectividad de los controles ISO/IEC 27002:2013.

Es decir, la organización tiene implantados 38 de los 114 controles que define la norma ISO/IEC 27002:2013. Gráficamente lo podemos ver en la siguiente ilustración.

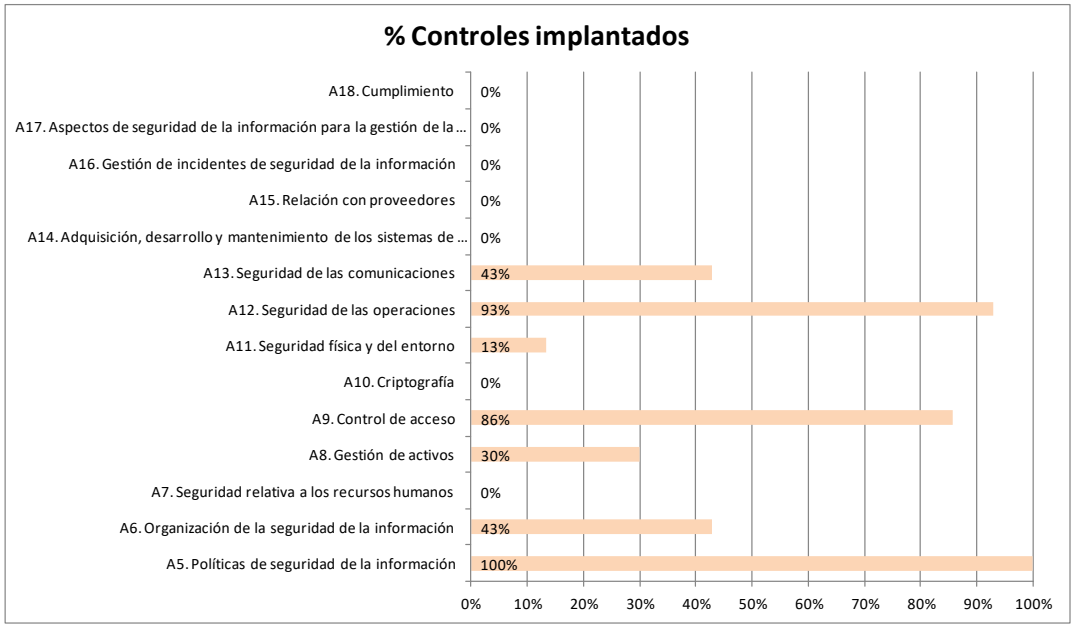

Ilustración 8. Evaluación de la implantación de los controles ISO/IEC 27002:2013

Por otro lado la madurez de los distintos controles es bastante desigual, como se muestra en el siguiente gráfico.

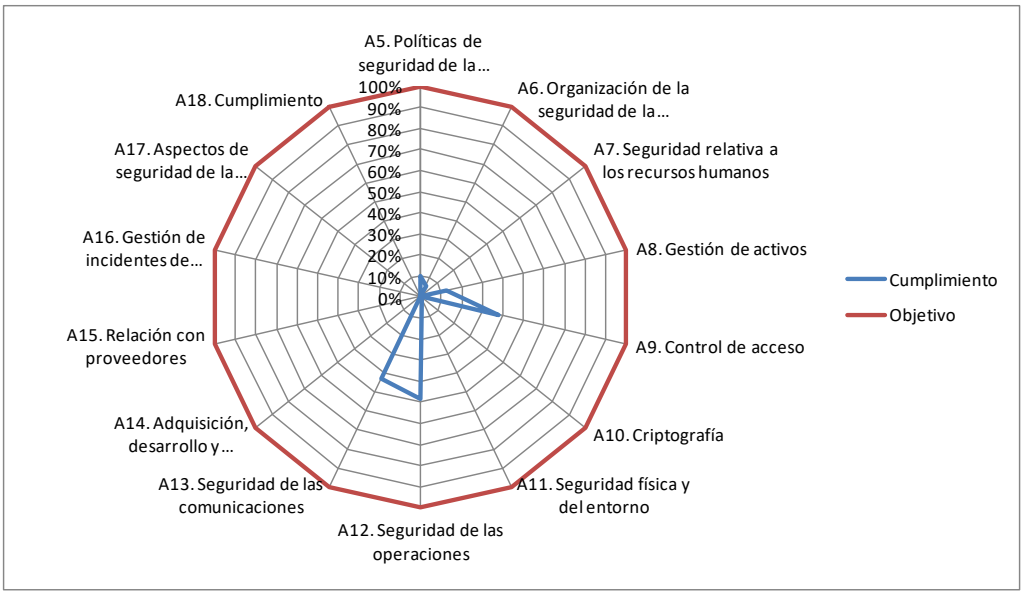

Ilustración 9. Evaluación de madurez de los controles ISO/IEC 27002:2013

2.4.2 EVALUACIÓN DE SITUACIÓN NORMA ISO/IEC 27001:2013

Aunque el departamento IT de RecicleSA tiene implantado, como hemos visto, múltiples controles de seguridad, la organización en su conjunto no dispone de un SGSI que involucre a todos sus estamentos, ni dispone de la documentación y mecanismos formales que establece la norma ISO/IEC 27001:2013 en sus distintos aspectos.

Es por ello que, como muestra la siguiente tabla, podemos considerar que los requerimientos que establece la norma son básicamente inexistentes.

Sección	Requerimientos ISO 27001	Estado	Cumplimiento
4	**Contexto de la organización**		**0%**
4.1	Comprensión de la organización y de su contexto	L0 - Inexistente	0%
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	L0 - Inexistente	0%
4.3	Determinación del alcance del SGSI	L0 - Inexistente	0%
4.4	SGSI	L0 - Inexistente	0%
5	**Liderazgo**		**0%**
4.1	Liderazgo y compromiso	L0 - Inexistente	0%
5.2	Política	L0 - Inexistente	0%
5.3	Roles, responsabilidades y autoridades en la organización	L0 - Inexistente	0%
6	**Planificación**		**0%**
6.1	Acciones para tratar los riesgos y oportunidades	L0 - Inexistente	0%
6.2	Objetivos de seguridad de la información y planificación para su consecución	L0 - Inexistente	0%
7	**Soporte**		**0%**
7.1	Recursos	L0 - Inexistente	0%
7.2	Competencia	L0 - Inexistente	0%
7.3	Concienciación	L0 - Inexistente	0%
7.4	Comunicación	L0 - Inexistente	0%
7.5	Información documentada	L0 - Inexistente	0%
8	**Operación**		**0%**
8.1	Planificación y control operacional	L0 - Inexistente	0%
8.2	Apreciación de los riesgos de seguridad de la información	L0 - Inexistente	0%
8.3	Tratamiento de los riesgos de seguridad de la información	L0 - Inexistente	0%
9	**Evaluación del desempeño**		**0%**
9.1	Seguimiento, medición, análisis y evaluación	L0 - Inexistente	0%
9.2	Auditoría interna	L0 - Inexistente	0%
9.3	Revisión por la dirección	L0 - Inexistente	0%
10	**Mejora**		**0%**
10.1	No conformidad y acciones correctivas	L0 - Inexistente	0%
10.2	Mejora continua	L0 - Inexistente	0%

Tabla 11. Evaluación de situación ISO/IEC 27001:2013

3 SISTEMA GESTIÓN DOCUMENTAL

3.1 INTRODUCCIÓN

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo.
En el caso de los SGSI que se rigen por la norma ISO/IEC 27001, los documentos necesarios para su buen funcionamiento e imprescindibles para la certificación del sistema vienen claramente recogidos en dicha norma.

El listado de los documentos obligatorios para la certificación se detalla en el apartado 2.1.1. ISO/IEC 27001:2013 de este documento, pero en este TFM dejaremos fuera los documentos del Anexo A y nos centraremos únicamente los siguientes documentos:

- **Política de Seguridad**: Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.
- **Procedimiento de Auditorías Internas**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.
- **Gestión de Indicadores**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.
- **Procedimiento Revisión por Dirección**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.
- **Metodología de Análisis de Riesgos**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.
- **Declaración de Aplicabilidad**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

En los siguientes apartados pasamos a describir en detalle el contenido y función de dichos documentos.

3.2 POLÍTICA DE SEGURIDAD

El apartado 5.2. Política de la norma ISO/IEC 27001:2013 indica que la Alta Dirección debe establecer una política de seguridad que:

a) Sea adecuada al propósito de la organización

b) Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información

c) Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información

d) Incluya el compromiso de mejora continua del gestión de la seguridad de la información

También indica que la seguridad de la información debe:

e) Estar disponible como información documentada

f) Comunicarse dentro de la organización

g) Estar disponible para las partes interesadas, según sea apropiado.

Tal como se indica en la web isotools.org [3]), :

> *…la política de Seguridad de la Información* ***no debe ser un documento extenso que contenga los pormenores de los procesos, las verificaciones o las auditorías del sistema****. Estos propósitos los cumplen otros documentos accesorios del sistema, como la política de control de acceso, la de uso aceptable o la de clasificación.* ***Mayor brevedad, a veces, como en este caso, puede representar mayor precisión y claridad****.*

A partir de estas directrices que marca la norma y a la documentación consultada (ver [4][5][3]), se ha generado el documento de Política de Seguridad de RecycleSA, que se incluye en el *Anexo* B *Política de Seguridad* de este documento.

3.3 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

En el apartado 9.2 de la norma ISO/IEC27001:2013, que forma parte de las medidas de evaluación del desempeño, se establece que:

> *La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de de la seguridad de la información:*
>
> *a) Es conforme con:*
>
> *b) Los propios requisitos de la organización para su sistema de gestión de la seguridad de la información y*
>
> *c) Los requisitos de esta norma*
>
> *d) Esta implementado y mantenido eficazmente*
>
> *La organización debe:*
>
> *e) Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas.*
>
> *f) Para cada auditoria, definir los criterios y el alcance de ésta*
>
> *g) Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría*
>
> *h) Asegurarse de que los resultados de las auditorías se informan a la dirección pertinente*
>
> *i) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.*

Para satisfacer estos requerimientos se ha elaborado un documento que define el procedimiento a realizar para la ejecución de las auditorías internas en ReycleSA, que se muestra en el *Anexo C. Procedimiento de auditorías Internas*.

Para la elaboración de dicho procedimiento se ha tomado como base la documentación del manual de la asignatura de *Auditoria técnica y de certificación*[6], que forma parte del Máster Interuniversitario en Seguridad de las TIC (MISTIC) [2], y de otras fuentes de internet [7] adaptándolo a las características de de RecycleSA.

Así, para la definición del perfil de auditor interno necesario se han tenido en cuenta, además del manual de la asignatura de *Auditoria técnica y de certificación*[6], las características definidas en la web de ISOTOOLS [8]

3.4 GESTIÓN DE INDICADORES

La implantación y mantenimiento de un SGSI exige la evaluación de la eficacia de los controles de seguridad implantados de manera continua.

Para realizar dicha evaluación es necesario definir una serie de indicadores que permitirán controlar el funcionamiento real y la eficacia de las medidas de seguridad implantadas.

Cada indicador debe incluir, al menos:

- **Descripción del indicador**, explicando el objetivo a medir.
- **Fórmula de cálculo.** Descripción de la fórmula aplicada para obtener la medición. Es primordial que la fórmula sea suficientemente clara y no se preste a ambigüedad.
- **Frecuencia.** Periodo de tiempo durante el cual se debe realizar la medición.
- **Valor objetivo.** Es el valor que la organización desea conseguir
- **Valor umbral.** Es el valor por debajo del cual se debería levantar una alarma.

En el *Anexo D. Gestión de Indicadores* de este documento se detallan los indicadores que se plantean para el SGSI de RecycleSA

3.5 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

Para que la puesta en marcha de un Sistema de Gestión de la Información sea exitosa, es necesario el impulso y apoyo incondicional de la Dirección de la organización, que debe, además, proveer los medios y recursos necesarios para su implantación.

Como resultado palpable de ese apoyo, la dirección de la organización debe revisar periódicamente los aspectos más relevantes ocurridos en relación al Sistema de Gestión de la Seguridad de la Información, para asegurarse de su eficacia.

Para ello, la norma ISO/IEC 27001:2013, en su apartado *9.3 Revisión por la Dirección*, establece que:

> *La revisión por la dirección debe incluir consideraciones sobre:*
>
> *a) El estado de las acciones con relación a las revisiones previas por la dirección*
>
> *b) Los cambios en las cuestiones externas en internas que sean pertinentes al sistema de gestión de seguridad de la información*
>
> *c) Retroalimentación sobre el desempeño de la seguridad e la información, incluidas las tendencias relativas a:*
>
> *1) No conformidades y acciones correctivas*
>
> *2) Seguimiento y resultados de las mediciones*
>
> *3) Resultados de la auditoría*
>
> *4) Cumplimiento de los objetivos de la seguridad de la información*
>
> *d) Retroalimentación de las partes interesadas*
>
> *e) Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos*
>
> *f) Oportunidades de mejora continua*

Para plasmar de manera formal las actividades y procesos a realizar, así como las entradas y salidas a obtener durante la revisión por parte de la Dirección, se elabora el documento que se incluye en *el Anexo F. Procedimiento de Revisión por la Dirección*.

3.6 GESTIÓN DE ROLES Y RESPONSABILIDADES

Para que cualquier SGSI se implante, mantenga, supervise y mejore adecuadamente es necesario que se definan correctamente las responsabilidades de cada uno de los roles que intervienen en el mismo.

Así, la norma ISO/IEC 27001 indica, en su apartado 5.3 Roles, responsabilidades y autoridades en la organización, lo siguiente:

> *La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.*
>
> *La alta dirección debe asignar la responsabilidad y autoridad para:*
>
> *a) Asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta norma.*
>
> *b) Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.*

Para el establecimiento de los comités y roles necesarios para la gestión de la seguridad en RecycleSA, así como para la definición de las responsabilidades de cada uno de ellos, se ha partido de la estructura organizativa habitual que se describe en el manual de la asignatura *Sistemas de Gestión de la Seguridad de la Información* [1], que forma parte del Máster Interuniversitario en Seguridad de las TIC (MISTIC) [2], adaptándolo a la estructura organizativa de RecycleSA.

Como resultado, se plantea la siguiente organización de la seguridad de la información de RecycleSA:

Nivel	Órgano/Departamento	Aportación/Implicación	Miembros
Estratégico	Comité de Dirección	Visión estratégica Aportación de recursos	▪ CEO. ▪ Director Financiero. ▪ Director Servicios de Reciclaje de Acero. ▪ Director Servicios de Reciclaje de Aluminio. ▪ Director Tecnologías de la Información.
Táctico	Comité de Seguridad de la Información	Liderazgo Gestión del riesto Comunicación	▪ CEO. ▪ Director Financiero. ▪ Director Servicios de Reciclaje de Acero. ▪ Director Servicios de Reciclaje de Aluminio. ▪ Director Tecnologías de la Información. ▪ Responsable de Seguridad. ▪ Posibles invitados según temática.
Operativo	Responsable de Seguridad de la Información	Coordinación y Gestión Lenguaje común	▪ Responsable de Seguridad.
Operativo	Departamento de Tecnologías de la Información	Implanta en los SI los controles de seguridad	▪ Director de Tecnologías de la Información. ▪ Service Managers. ▪ Proveedores de servicio de TI.
Operativo	Recursos Humanos	Informa sobre los cambios de personal y aplica procedimientos disciplianarios	▪ Personal del departamento de Recursos Humanos.
Operativo	Legal	Colabora en definición de normas y políticas	▪ Personal del departamento de Legal.
Operativo	Personal general	Confidencialidad y uso adecuado de los recursos	▪ Personal de la organización ▪ Personal de proveedores de servicios con acces a información de la organización

Tabla 12. Estructura organizativa de la Seguridad de la Información

La descripción detalla de los comités y roles, así como las responsabilidades de cada uno de ellos, se describe en el *Anexo G. Gestión de Roles y Responsabilidades* de este documento.

En todo caso, de la estructura organizativa definida, cabe resaltar:

- Como se observa en la tabla anterior, dado el pequeño tamaño de RecycleSA, el Comité de Seguridad está formado básicamente por los mismos miembros que el Comité de Dirección, al que se añade el Responsable de Seguridad. Además, en función de la temática tratada, se podrán añadir miembros invitados, como puede ser el Director del Departamento Legal o de Recursos Humanos
- El Responsable de Seguridad puede delegar algunas de sus funciones en otras personas, pero continúa siendo responsable de las mismas y debe seguir velando porque se realicen correctamente.
- Puesto que buena parte de los servicios de TI de RecycleSA se encuentran externalizados en proveedores de servicio, éstos deben asumir las responsabilidades definidas para el departamento de Tecnologías de la Información de RecycleSA. Los gestores de servicio del departamento de TI deben velar por el cumplimiento de dichas responsabilidades de los proveedores de servicio que gestionan.

3.7 METODOLOGÍA DE ANÁLISIS DE RIESGOS

El análisis de riesgos es una parte fundamental en la implantación de cualquier SGSI, que se debe contemplar dentro del proceso global de gestión del riesgo. Existen múltiples metodologías que permiten abordar la realización del análisis de riesgos para la implantación del SGSI y, de hecho, la norma ISO/IEC 27001:2013 no impone ninguna metodología concreta para ello.

Por ello podemos elegir cualquier metodología o guía de buenas prácticas o bien definir una propia que esté acorde con las necesidades de la organización. En realidad, cualquier metodología proporcionará resultados similares si se aplica de forma correcta.

Para la implantación del SGSI de RecycleSA se ha decidido utilizar la Metodología MAGERIT[9] elaborada por el Consejo Superior de Administración Electrónica, ampliamente utilizada en las administraciones públicas españolas. Esta Metodología persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

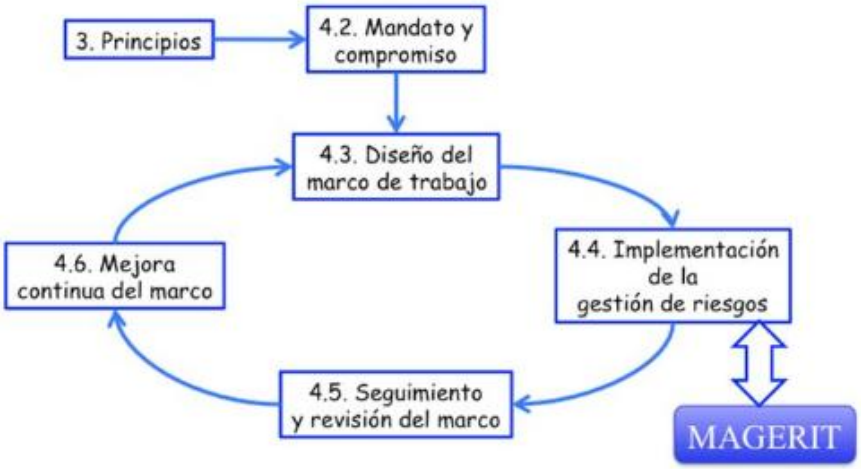

Ilustración 10. ISO 31000 - Marco de trabajo para la gestión de riesgos

La versión actual de MAGERIT es la versión 3 se estructura en tres libros: "Método"[10], "Catálogo de Elementos"[11] y "Guía de Técnicas"[12].

La descripción de la metodología de análisis de riesgos de MAGERIT que se utilizará para la implantación del SGSI de RecycleSA se describe en el *Anexo H. Metodología de Análisis de Riesgos* de este documento, que básicamente resume los principios, conceptos y fases que se desarrollan en el libro I – Método [10] que desarrolla la metodología MAGERIT.

Adicionalmente, y aunque la metodología Magerit no lo contempla, la norma ISO/IEC 27001, desde su versión de 2013 contempla, en el apartado 6.1.2.c)2) la necesidad de identificar a los propietarios de los riesgos.

El propietario o **dueño del riesgo** es la persona o entidad con la responsabilidad para gestionar el riesgo, y se adopta para dotar de autoridad a los encargados de tomar decisiones relacionadas con el tratamiento de los riesgos de seguridad de la información.

El concepto de propietario del riesgo es, por tanto, diferente al de propietario del activo, que en la norma ISO/IEC 27001:2013 sigue apareciendo, pero ya únicamente en el control A.8.1.2 del Anexo A.

Es por todo ello que, en el análisis de riesgo que se realizará utilizando la metodología Magerit, una vez se identifiquen los riesgos a tratar, se contemplará también al propietario del riesgo para cumplir con los requisitos de la norma ISO/IEC 27001:2013.

3.8 DECLARACIÓN DE APLICABILIDAD

La norma ISO/IEC 27001:2013 establece, en el apartado 6.1.3 de Tratamiento de riesgos de seguridad de la información, la necesidad de elaborar una "Declaración de Aplicabilidad" que contenga los controles necesarios y la justificación de las inclusiones, estén implementadas o no, de las exclusiones de los controles del Anexo A.

La declaración de aplicabilidad debería incluir:

- Control
- Dominio del control: A5. Políticas de seguridad, A6. Organización de la seguridad,…
- Aplica. Indicas si es necesaria la aplicación del control o no.
- Justificación de la aplicabilidad del control.
- Estado de implementación del control.
- Origen del control: análisis de riesgos, cumplimiento legal o normativo, requerimiento interno,…

En el *Anexo I. Plantilla Declaración de* Aplicabilidad de este documento se recoge una posible plantilla a utilizar para la declaración de aplicabilidad.

4 ANÁLISIS DE RIESGOS

4.1 INTRODUCCIÓN

La gestión de riesgos es fundamental en la gestión de la seguridad de la información y, por ello, es una pieza clave en la noma ISO/IEC 27001:2013. De hecho, ya en la introducción de dicha norma se indica:

> *El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información* ***mediante la aplicación de un proceso de gestión de riesgos*** *y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.*

En el apartado *6.1 Acciones para tratar los riegos y oportunidades* de la norma ISO 27001:2013, se definen las directrices que marca la norma para dicha gestión de riesgos, aunque no se impone ninguna metodología para el análisis de riesgos.

En nuestro caso, como ya se ha indicado, se utilizará la Metodología MAGERIT[9] elaborada por el Consejo Superior de Administración Electrónica, que describimos someramente en el *Anexo H. Metodología de Análisis de Riesgos* y desarrollamos a continuación para realizar el análisis de riesgos de RecycleSA.

4.2 INVENTARIO DE ACTIVOS

Tal como se detalla en el *Anexo H. Metodología de Análisis de Riesgos* de este documento, la metodología Magerit comienza por determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

Para Magerit, según se indica en el punto 3.1.1. del Libro 1 [10], un activo es:

> *Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]*

Igualmente, la metodología Magerit en su Libro 1 [10] establece que:

En un sistema de información hay 2 cosas esenciales:

- La información que maneja
- Los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- **Datos** que materializan la información.
- **Servicios auxiliares** que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- **Los equipos informáticos (hardware)** y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas que explotan u operan** todos los elementos anteriormente citados.

En base a todo ello, agruparemos los activos de RecycleSA en los grupos que mostramos en la siguiente tabla, que refleja también el identificador que utilizaremos para cada tipo de activo:

Tipo Activo	Identificador
Instalaciones	L
Hardware	HW
Aplicación/Software	SW
Datos/Información	D
Redes de comunicación	COM
Servicios	S
Soportes de información	M
Equipamiento auxiliar	AUX
Personal	P

Tabla 13. Tipos de activo

Tras el análisis de los activos de RecycleSA, obtenemos la siguiente tabla, que refleja los activos que contemplaremos para el análisis de riesgos, así como su tipo, de acuerdo con la tabla anterior.

Tipo Activo	ID Activo	Activo
Instalaciones [L]	[L.1]	CPD
	[L.2]	Sala Técnica Sede
	[L.3]	Despacho Directivo
	[L.4]	Oficinas
Hardware [HW]	[HW.1]	Servidores hypervisor CPD
	[HW.2]	Firewall CPD
	[HW.3]	Swithes CPD
	[HW.4]	Servidores hypervisor Sedes
	[HW.5]	Switches/routers Sedes
	[HW.6]	Puntos de acceso Wifi
	[HW.7]	PCs usuarios
	[HW.8]	Portátiles usuarios
	[HW.9]	Dispositivos móviles corporativos
	[HW.10]	Dispositivos móviles personales
	[HW.11]	Teléfonos IPs
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare
	[SW.2]	Sistema operativos Windows Server
	[SW.3]	Sistema operativos Linux Server
	[SW.4]	Software backup: Veeam backup
	[SW.5]	Sistema operativo Windows 7
	[SW.6]	Sistema operativo Windows 10
	[SW.7]	Sistema operativo android
	[SW.8]	Sistema operativo IOS
	[SW.9]	Directorio Activo Microsoft
	[SW.10]	BBDD Microsoft SQL Server
	[SW.11]	BBDD Oracle
	[SW.12]	Microsoft SCCM
	[SW.13]	Herramienta de ticketing: OTRS
	[SW.14]	Antivirus Symantec
	[SW.15]	Intranet corporativa
	[SW.16]	Web corporativa
	[SW.17]	SAP
	[SW.18]	Navision
	[SW.19]	Contaplus
	[SW.20]	Software puesto usuario: office 365, antivirus, acrobat
	[SW.21]	Aplicaciones Office 365: Correo, one drive, skype,…
	[SW.22]	Aplicaciones Sharepoint Office 365
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus
	[D.3]	Bases de datos RRHH
	[D.4]	LDAP: Directorio Activo Microsoft
	[D.5]	Copias de seguridad

Comunicaciones [D]	[COM.1]	Red internet
	[COM.2]	Red MPLS
	[COM.3]	Red local CPD
	[COM.4]	Red local sedes
	[COM.5]	Red wifi invitados sedes
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)
	[COM.7]	Red wifi usuarios
	[COM.8]	Red telefonía IP
	[COM.9]	Red telefonía móvil
Servicios [S]	[S.1]	Servicio ERP
	[S.2]	Servicio correo
	[S.3]	Servicio de telefonía
	[S.4]	Servicio de ficheros
	[S.5]	Servicio de acceso remoto
	[S.6]	Servicio de backup
Soportes de Información [M]	[M.1]	Almacenamiento CPD
	[M.2]	Almacenamiento Sedes
	[M.3]	Memorias USB
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico
	[AUX.2]	Aire acondicionado Salas técnicas
	[AUX.3]	Sistemas antiincidencios
	[AUX.4]	Cableado LAN
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Financiero
	[P.2]	Personal TI
	[P.3]	Personal Proveedor TI
	[P.4]	Resto de personal

Tabla 14. Activos

4.3 VALORACIÓN DE LOS ACTIVOS

Una vez identificados los activos relacionados con la seguridad de la información, se les debe asignar un valor.

Para la metodología Magerit, la valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Entre los factores que Magerit indica que hay que considerar, se encuentran:

- Coste de reposición: adquisición e instalación.
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.
- Lucro cesante: pérdida de ingresos.
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos.
- Daño a personas.
- Daños medioambientales.

La experiencia ha demostrado la conveniencia de utilizar métodos simples mediante tablas que permitan identificar la importancia relativa de los diferentes activos.

Por ello utilizaremos la tipificación del valor que se define en el libro III de Magerit [12] y que se muestra en la siguiente tabla.

,

ID	Valoración
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Tabla 15. Valoración de activos

4.4 DIMENSIONES DE LA SEGURIDAD

Además de la valoración en sí del activo que se describe en el apartado anterior, desde el punto de vista de la seguridad, es necesario indicar el aspecto de la seguridad más crítico de cada activo.

Para ello se debe valorar cada una de las 5 dimensiones de la seguridad, que se detallan en la siguiente tabla, tal como se describen en el punto *3. Dimensiones de valoración* del libro II de Magerit[11].

Dimensión	Descripción
[A] autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
[C] confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[I] integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[D] disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[T] trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Tabla 16. Dimensiones de la seguridad

La valoración que se proporcione a cada activo en una determinada dimensión se realizará en base al perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Dicha valoración se realizará de manera cualitativa, utilizando la escala de 10 valores que se describe en la siguiente tabla, según se propone en el punto *4. Criterios de valoración* del libro II de Magerit [11].

Valor Numérico	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 17. Escala de valoración de dimensiones de la seguridad

4.5 TABLA RESUMEN DE LA SEGURIDAD

Realizado el análisis y valoración de los activos de RecycleSA para las distintas dimensiones y conforme a las escalas descritas anteriormente, obtenemos la siguiente tabla de valoración de los activos.

			Aspectos críticos				
Tipo Activo	ID Activo	Activo	A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	9	9	9	10	8
	[L.2]	Sala Técnica Sede	9	7	7	10	3
	[L.3]	Despacho Directivo	8	9	8	7	5
	[L.4]	Oficinas	2	6	7	7	2
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	9	9	9	9	7
	[HW.2]	Firewall CPD	9	9	9	9	7
	[HW.3]	Swithes CPD	8	7	9	9	7
	[HW.4]	Servidores hypervisor Sedes	7	7	7	7	6
	[HW.5]	Switches/routers Sedes	6	6	7	7	6
	[HW.6]	Puntos de acceso Wifi	5	6	5	3	4
	[HW.7]	PCs usuarios	7	7	5	5	6
	[HW.8]	Portátiles usuarios	7	7	5	5	6
	[HW.9]	Dispositivos móviles corporativos	6	6	4	3	6
	[HW.10]	Dispositivos móviles personales	5	6	4	3	6
	[HW.11]	Teléfonos IPs	3	2	2	3	4
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	8	8	8	9	5
	[SW.2]	Sistema operativos Windows Server	8	8	8	8	5
	[SW.3]	Sistema operativos Linux Server	7	8	7	6	5
	[SW.4]	Software backup: Veeam backup	8	9	8	2	7
	[SW.5]	Sistema operativo Windows 7	6	7	4	7	3
	[SW.6]	Sistema operativo Windows 10	6	7	4	7	3
	[SW.7]	Sistema operativo android	5	6	3	3	3
	[SW.8]	Sistema operativo IOS	5	7	3	3	3
	[SW.9]	Directorio Activo Microsoft	6	6	9	9	6
	[SW.10]	BBDD Microsoft SQL Server	7	8	8	6	7
	[SW.11]	BBDD Oracle	7	8	8	8	7
	[SW.12]	Microsoft SCCM	5	6	4	6	6
	[SW.13]	Herramienta de ticketing: OTRS	5	6	4	8	7
	[SW.14]	Antivirus Symantec	3	3	5	7	6
	[SW.15]	Intranet corporativa	7	8	7	7	7
	[SW.16]	Web corporativa	7	6	9	6	8
	[SW.17]	SAP	8	9	8	8	8
	[SW.18]	Navision	8	9	8	8	8
	[SW.19]	Contaplus	6	7	6	5	5
	[SW.20]	Software puesto usuario: office 365, antivirus,	3	7	5	5	3
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	6	8	5	7	6
	[SW.22]	Aplicaciones Sharepoint Office 365	7	8	6	7	6
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	8	9	8	7	6
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	9	9	9	8	8
	[D.3]	Bases de datos RRHH	9	9	8	8	8
	[D.4]	LDAP: Directorio Activo Microsoft	7	7	8	9	7
	[D.5]	Copias de seguridad	7	9	7	3	7
Comunicaciones [D]	[COM.1]	Red internet	7	8	8	9	7
	[COM.2]	Red MPLS	7	8	8	8	7
	[COM.3]	Red local CPD	8	9	9	9	7
	[COM.4]	Red local sedes	6	7	7	7	6
	[COM.5]	Red wifi invitados sedes	2	3	3	3	2
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	3	3	3	4	3
	[COM.7]	Red wifi usuarios	3	7	3	5	3
	[COM.8]	Red telefonía IP	0	0	2	7	0
	[COM.9]	Red telefonía móvil	0	0	2	8	0
Servicios [S]	[S.1]	Servicio ERP	8	9	9	8	7
	[S.2]	Servicio correo	7	9	8	9	7
	[S.3]	Servicio de telefonía	0	3	0	8	0
	[S.4]	Servicio de ficheros	7	8	8	7	7
	[S.5]	Servicio de acceso remoto	6	8	6	6	6
	[S.6]	Servicio de backup	8	9	8	6	8
Soportes de Información [M]	[M.1]	Almacenamiento CPD	9	9	9	9	7
	[M.2]	Almacenamiento Sedes	7	7	7	7	6
	[M.3]	Memorias USB	2	6	3	2	2
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	0	0	8	9	0
	[AUX.2]	Aire acondicionado Salas técnicas	0	0	7	6	0
	[AUX.3]	Sistemas antiincidencios	0	0	8	8	0
	[AUX.4]	Cableado LAN	0	0	6	9	0
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	0	0	0	9	0
	[P.2]	Personal TI	0	0	0	8	0
	[P.3]	Personal Proveedor TI	0	0	0	7	0
	[P.4]	Resto de personal	0	0	0	3	0

Tabla 18. Valoración de activos

4.6 ANÁLISIS DE AMENAZAS

Una vez identificados los activos de la organización, es necesario determinar las amenazas a las que se encuentran expuestos, de manera que se pueda cuantificar la vulnerabilidad de los distintos activos a las distintas amenazas.

Para realizar esta evaluación con un enfoque metodológico adecuado, es conveniente utilizar tablas con las amenazas más comunes. En concreto, Magerit, en el apartado 5 del libro II [11], define un catálogo de amenazas, en el que se describen las amenazas para cada tipo de activo y las dimensiones de seguridad a las que afecta.

Este catálogo clasifica las amenazas en los grupos que se describen en la siguiente tabla::

Grupo	Identificador
Desastres Naturales	[N]
De origen Industrial	[I]
Errores y fallos no intencionados	[E]
Ataques Intencionados	[A]

Tabla 19. Grupos de amenazas Magerit

El detalle de las amenazas que se incluyen en cada grupo se muestra en el *Anexo J. Tabla de amenazas Magerit*

Para cada amenaza se debe tipificar su probabilidad. Es habitual modelarla como frecuencia de ocurrencia. En nuestro caso utilizaremos 5 posibles valores, correspondientes a la frecuencia que se muestra en la siguiente tabla

ID	Vulnerabiliad	Frecuencia
MA	Muy Alta	A diario
A	Alta	Mensualmente
M	Media	Cada 6 meses
B	Baja	Cada año
MB	Muy Baja	Cada 5 años

Tabla 20. Tipificación de frecuencias de amenazas

Adicionalmente se debe tipificar la degradación que provoca cada amenaza en las distintas dimensiones de cada activo. Para ello utilizaremos la tabla de valoración de impactos que figura en el manual de la asignatura SGSI[1], en el capítulo de Análisis de riesgos.

Impacto	ID	Valor
Muy Alto	MA	100%
Alto	A	75%
Medio	M	50%
Bajo	B	20%
Muy Bajo	MB	5%

Tabla 21. Valoración de impactos de amenazas

A partir de esta modelización de probabilidad e impacto se obtiene la tabla que muestra la valoración de cada amenaza para los distintos grupos de activos, que se incluye en el *Anexo K. Tabla de análisis amenazas/activos* de este documento.

De dicho análisis obtenemos los impactos máximos para cada uno de los grupos de activos de la organización, que se muestran en la siguiente tabla:

	Impacto				
Activo	A	C	I	D	T
Aplicación/Software [SW]	75%	100%	100%	100%	
Datos/Información [D]	100%	100%	100%	100%	100%
Equipamiento auxiliar [AUX]		20%	20%	100%	
Hardware [HW]		100%	50%	100%	
Instalaciones [L]		20%	20%	100%	
Personal [P]		75%	20%	100%	
Redes de comunicación [COM]	75%	100%	75%	100%	
Servicios [S]	75%	75%	75%	100%	75%
Soportes de información [M]		100%	50%	100%	

Tabla 22. Escala de valoración de dimensiones de la seguridad

4.7 IMPACTO POTENCIAL

A partir del impacto identificado en la tabla anterior para cada grupo de activos, podemos obtener una tabla resumen con el impacto potencial que puede suponer para la organización la materialización de las distintas amenazas sobre cada activo.

El impacto potencial, para cada una de las dimensiones, se calcula de la siguiente manera:

Impacto potencial = Valor del activo x Valor del impacto de la amenaza

Para el cálculo del impacto potencial no se tiene en cuenta posibles contramedidas y su resultado nos permitirá extraer valores de referencia que nos ayuden a priorizar los planes de acción a ejecutar.

La tabla resultante obtenida es la siguiente:

			Aspectos críticos					Impacto					Impacto potencial				
Tipo Activo	ID Activo	Activo	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	9	9	9	10	8	0%	20%	20%	100%	0%	0,00	1,80	1,80	10,00	0,00
	[L.2]	Sala Técnica Sede	9	7	7	10	3	0%	20%	20%	100%	0%	0,00	1,40	1,40	10,00	0,00
	[L.3]	Despacho Directivo	8	9	8	7	5	0%	20%	20%	100%	0%	0,00	1,80	1,60	7,00	0,00
	[L.4]	Oficinas	2	6	7	7	2	0%	20%	20%	100%	0%	0,00	1,20	1,40	7,00	0,00
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	9	9	9	9	7	0%	100%	50%	100%	0%	0,00	9,00	4,50	9,00	0,00
	[HW.2]	Firewall CPD	9	9	9	9	7	0%	100%	50%	100%	0%	0,00	9,00	4,50	9,00	0,00
	[HW.3]	Swithes CPD	8	7	9	9	7	0%	100%	50%	100%	0%	0,00	7,00	4,50	9,00	0,00
	[HW.4]	Servidores hypervisor Sedes	7	7	7	7	6	0%	100%	50%	100%	0%	0,00	7,00	3,50	7,00	0,00
	[HW.5]	Switches/routers Sedes	6	6	7	7	6	0%	100%	50%	100%	0%	0,00	6,00	3,50	7,00	0,00
	[HW.6]	Puntos de acceso Wifi	5	6	5	3	4	0%	100%	50%	100%	0%	0,00	6,00	2,50	3,00	0,00
	[HW.7]	PCs usuarios	7	7	5	5	6	0%	100%	50%	100%	0%	0,00	7,00	2,50	5,00	0,00
	[HW.8]	Portátiles usuarios	7	7	5	5	6	0%	100%	50%	100%	0%	0,00	7,00	2,50	5,00	0,00
	[HW.9]	Dispositivos móviles corporativos	6	6	4	3	6	0%	100%	50%	100%	0%	0,00	6,00	2,00	3,00	0,00
	[HW.10]	Dispositivos móviles personales	5	6	4	3	6	0%	100%	50%	100%	0%	0,00	6,00	2,00	3,00	0,00
	[HW.11]	Teléfonos IPs	3	2	2	3	4	0%	100%	50%	100%	0%	0,00	2,00	1,00	3,00	0,00
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	8	8	8	9	5	75%	100%	100%	100%	0%	6,00	8,00	8,00	9,00	0,00
	[SW.2]	Sistema operativos Windows Server	8	8	8	8	5	75%	100%	100%	100%	0%	6,00	8,00	8,00	8,00	0,00
	[SW.3]	Sistema operativos Linux Server	7	8	7	6	5	75%	100%	100%	100%	0%	5,25	8,00	7,00	6,00	0,00
	[SW.4]	Software backup: Veeam backup	8	9	8	2	7	75%	100%	100%	100%	0%	6,00	9,00	8,00	2,00	0,00
	[SW.5]	Sistema operativo Windows 7	6	7	4	7	3	75%	100%	100%	100%	0%	4,50	7,00	4,00	7,00	0,00
	[SW.6]	Sistema operativo Windows 10	6	7	4	7	3	75%	100%	100%	100%	0%	4,50	7,00	4,00	7,00	0,00
	[SW.7]	Sistema operativo android	5	6	3	3	3	75%	100%	100%	100%	0%	3,75	6,00	3,00	3,00	0,00
	[SW.8]	Sistema operativo IOS	5	7	3	3	3	75%	100%	100%	100%	0%	3,75	7,00	3,00	3,00	0,00
	[SW.9]	Directorio Activo Microsoft	6	6	9	9	6	75%	100%	100%	100%	0%	4,50	6,00	9,00	9,00	0,00
	[SW.10]	BBDD Microsoft SQL Server	7	8	8	6	7	75%	100%	100%	100%	0%	5,25	8,00	8,00	6,00	0,00
	[SW.11]	BBDD Oracle	7	8	8	8	7	75%	100%	100%	100%	0%	5,25	8,00	8,00	8,00	0,00
	[SW.12]	Microsoft SCCM	5	6	4	6	6	75%	100%	100%	100%	0%	3,75	6,00	4,00	6,00	0,00
	[SW.13]	Herramienta de ticketing: OTRS	5	6	4	8	7	75%	100%	100%	100%	0%	3,75	6,00	4,00	8,00	0,00
	[SW.14]	Antivirus Symantec	3	3	5	7	6	75%	100%	100%	100%	0%	2,25	3,00	5,00	7,00	0,00
	[SW.15]	Intranet corporativa	7	8	7	7	7	75%	100%	100%	100%	0%	5,25	8,00	7,00	7,00	0,00
	[SW.16]	Web corporativa	7	6	9	6	8	75%	100%	100%	100%	0%	5,25	6,00	9,00	6,00	0,00
	[SW.17]	SAP	8	9	8	8	8	75%	100%	100%	100%	0%	6,00	9,00	8,00	8,00	0,00
	[SW.18]	Navision	8	9	8	8	8	75%	100%	100%	100%	0%	6,00	9,00	8,00	8,00	0,00
	[SW.19]	Contaplus	6	7	6	5	5	75%	100%	100%	100%	0%	4,50	7,00	6,00	5,00	0,00
	[SW.20]	Software puesto usuario: office 365, antivirus,	3	7	5	5	3	75%	100%	100%	100%	0%	2,25	7,00	5,00	5,00	0,00
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	6	8	5	7	6	75%	100%	100%	100%	0%	4,50	8,00	5,00	7,00	0,00
	[SW.22]	Aplicaciones Sharepoint Office 365	7	8	6	7	6	75%	100%	100%	100%	0%	5,25	8,00	6,00	7,00	0,00
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	8	9	8	7	6	100%	100%	100%	100%	100%	8,00	9,00	8,00	7,00	6,00
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	9	9	9	8	8	100%	100%	100%	100%	100%	9,00	9,00	9,00	8,00	8,00
	[D.3]	Bases de datos RRHH	9	9	8	8	8	100%	100%	100%	100%	100%	9,00	9,00	8,00	8,00	8,00
	[D.4]	LDAP: Directorio Activo Microsoft	7	7	8	9	7	100%	100%	100%	100%	100%	7,00	7,00	8,00	9,00	7,00
	[D.5]	Copias de seguridad	7	9	7	3	7	100%	100%	100%	100%	100%	7,00	9,00	7,00	3,00	7,00
Comunicaciones [D]	[COM.1]	Red internet	7	8	8	9	7	75%	100%	75%	100%	0%	5,25	8,00	6,00	9,00	0,00
	[COM.2]	Red MPLS	7	8	8	8	7	75%	100%	75%	100%	0%	5,25	8,00	6,00	8,00	0,00
	[COM.3]	Red local CPD	8	9	9	9	7	75%	100%	75%	100%	0%	6,00	9,00	6,75	9,00	0,00
	[COM.4]	Red local sedes	6	7	7	7	6	75%	100%	75%	100%	0%	4,50	7,00	5,25	7,00	0,00
	[COM.5]	Red wifi invitados sedes	2	3	3	3	2	75%	100%	75%	100%	0%	1,50	3,00	2,25	3,00	0,00
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	3	3	3	4	3	75%	100%	75%	100%	0%	2,25	3,00	2,25	4,00	0,00
	[COM.7]	Red wifi usuarios	3	7	3	5	3	75%	100%	75%	100%	0%	2,25	7,00	2,25	5,00	0,00
	[COM.8]	Red telefonía IP	0	0	2	7	0	75%	100%	75%	100%	0%	0,00	0,00	1,50	7,00	0,00
	[COM.9]	Red telefonía móvil	0	0	2	8	0	75%	100%	75%	100%	0%	0,00	0,00	1,50	8,00	0,00
Servicios [S]	[S.1]	Servicio ERP	8	9	9	8	7	75%	75%	75%	100%	75%	6,00	6,75	6,75	8,00	5,25
	[S.2]	Servicio correo	7	9	8	9	7	75%	75%	75%	100%	75%	5,25	6,75	6,00	9,00	5,25
	[S.3]	Servicio de telefonía	0	3	0	8	0	75%	75%	75%	100%	75%	0,00	2,25	0,00	8,00	0,00
	[S.4]	Servicio de ficheros	7	8	8	7	7	75%	75%	75%	100%	75%	5,25	6,00	6,00	7,00	5,25
	[S.5]	Servicio de acceso remoto	6	8	6	6	6	75%	75%	75%	100%	75%	4,50	6,00	4,50	6,00	4,50
	[S.6]	Servicio de backup	8	9	8	6	8	75%	75%	75%	100%	75%	6,00	6,75	6,00	6,00	6,00
Soportes de Información [M]	[M.1]	Almacenamiento CPD	9	9	9	9	7	0%	100%	50%	100%	0%	0,00	9,00	4,50	9,00	0,00
	[M.2]	Almacenamiento Sedes	7	7	7	7	6	0%	100%	50%	100%	0%	0,00	7,00	3,50	7,00	0,00
	[M.3]	Memorias USB	2	6	3	2	2	0%	100%	50%	100%	0%	0,00	6,00	1,50	2,00	0,00
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	0	0	8	9	0	0%	20%	20%	100%	0%	0,00	0,00	1,60	9,00	0,00
	[AUX.2]	Aire acondicionado Salas técnicas	0	0	7	6	0	0%	20%	20%	100%	0%	0,00	0,00	1,40	6,00	0,00
	[AUX.3]	Sistemas antiincidencios	0	0	8	8	0	0%	20%	20%	100%	0%	0,00	0,00	1,60	8,00	0,00
	[AUX.4]	Cableado LAN	0	0	6	9	0	0%	20%	20%	100%	0%	0,00	0,00	1,20	9,00	0,00
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	0	0	0	9	0	0%	75%	20%	100%	0%	0,00	0,00	0,00	9,00	0,00
	[P.2]	Personal TI	0	0	0	8	0	0%	75%	20%	100%	0%	0,00	0,00	0,00	8,00	0,00
	[P.3]	Personal Proveedor TI	0	0	0	7	0	0%	75%	20%	100%	0%	0,00	0,00	0,00	7,00	0,00
	[P.4]	Resto de personal	0	0	0	3	0	0%	75%	20%	100%	0%	0,00	0,00	0,00	3,00	0,00

Tabla 23. Valoración de impacto potencial sobre cada activo

4.8 NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

Una vez determinado el impacto potencial de cada activo estamos en condiciones de determinar el riesgo, que podemos calcular como:

Nivel de riesgo = Impacto potencial x frecuencia de la amenaza.

En nuestro análisis de riesgos utilizaremos escalas cualitativas, tanto para el impacto como para la frecuencia y el riesgo, tal como se describe en el apartado 2.1 Análisis mediante tablas del libro III de Magerit [12].

En concreto, utilizaremos los valores ya definidos en la *Tabla 20. Tipificación de frecuencias de amenazas y en la Tabla 21. Valoración de impactos de amenazas* para la frecuencia e impacto. Para la valoración cualitativa del riesgo utilizaremos la siguiente escala:

Riesgo
Muy Alto
Alto
Medio
Bajo
Muy Bajo

Tabla 24. Escala de riesgos

En este modelo la combinación de impacto y frecuencia nos determina el riesgo conforme a lo establecido en la siguiente tabla:

Riesgo			Frecuencia				
			Muy Alta	Alta	Media	Baja	Muy Baja
			MA	A	M	B	MB
Impacto	Muy Alto	MA	MA	MA	MA	MA	A
	Alto	A	MA	MA	A	A	M
	Medio	M	A	A	M	M	B
	Bajo	B	M	M	B	B	MB
	Muy Bajo	MB	B	B	MB	MB	MB

Tabla 25. Cálculo de riesgo en base a impacto y frecuencia

La Dirección de RecycleSA deberá decidir el nivel de riesgo que considera aceptable, de manera que aquellos que tengan un nivel aceptable no se tratarán. Los riesgos que, sin embargo, se tipifiquen con un nivel superior al aceptable deberán ser reducidos mediante el establecimiento de los controles y medidas necesarias.

Para ello se deberá identificar el responsable de cada riesgo que deberá tomar todas las medidas necesarias para el correcto tratamiento del riesgo.

Una vez se establezcan las medidas de salvaguarda, los niveles de riesgo se reducirán, a lo que denominamos riesgo residual. El cálculo de dicho riesgo residual es sencillo, ya que sólo cambia la magnitud de la degradación y la probabilidad de ocurrencia de la amenaza, pero no cambian ni los activos ni sus dependencias.

4.9 RESULTADOS

En la siguiente tabla se muestra el resultado del análisis de riegos para los distintos activos, según el modelo establecido en el apartado anterior.

			Impacto potencial					Impacto potencial (cualitativo)					Frecuencia	Riesgo				
Tipo Activo	ID Activo	Activo	A	C	I	D	T	A	C	I	D	T		A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	0,00	1,80	1,80	10,00	0,00	MB	MB	MB	MA	MB	B	MB	MB	MB	MA	MB
	[L.2]	Sala Técnica Sede	0,00	1,40	1,40	10,00	0,00	MB	MB	MB	MA	MB	B	MB	MB	MB	MA	MB
	[L.3]	Despacho Directivo	0,00	1,80	1,60	7,00	0,00	MB	MB	MB	M	MB	B	MB	MB	MB	M	MB
	[L.4]	Oficinas	0,00	1,20	1,40	7,00	0,00	MB	MB	MB	M	MB	B	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	0,00	9,00	4,50	9,00	0,00	MB	A	M	A	MB	A	B	MA	A	MA	B
	[HW.2]	Firewall CPD	0,00	9,00	4,50	9,00	0,00	MB	A	M	A	MB	A	B	MA	A	MA	B
	[HW.3]	Swithes CPD	0,00	7,00	4,50	9,00	0,00	MB	M	M	A	MB	A	B	A	A	MA	B
	[HW.4]	Servidores hypervisor Sedes	0,00	7,00	3,50	7,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	0,00	6,00	3,50	7,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	0,00	6,00	2,50	3,00	0,00	MB	M	B	B	MB	A	B	A	M	M	B
	[HW.7]	PCs usuarios	0,00	7,00	2,50	5,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.8]	Portátiles usuarios	0,00	7,00	2,50	5,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.9]	Dispositivos móviles corporativos	0,00	6,00	2,00	3,00	0,00	MB	M	MB	B	MB	A	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	0,00	6,00	2,00	3,00	0,00	MB	M	MB	B	MB	A	B	A	B	M	B
	[HW.11]	Teléfonos IPs	0,00	2,00	1,00	3,00	0,00	MB	MB	MB	B	MB	A	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	6,00	8,00	8,00	9,00	0,00	M	A	A	A	MB	A	A	MA	MA	MA	B
	[SW.2]	Sistema operativos Windows Server	6,00	8,00	8,00	8,00	0,00	M	A	A	A	MB	A	A	MA	MA	MA	B
	[SW.3]	Sistema operativos Linux Server	5,25	8,00	7,00	6,00	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	6,00	9,00	8,00	2,00	0,00	M	A	A	MB	MB	A	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	4,50	7,00	4,00	7,00	0,00	M	M	B	M	MB	A	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	4,50	7,00	4,00	7,00	0,00	M	M	B	M	MB	A	A	A	M	A	B
	[SW.7]	Sistema operativo android	3,75	6,00	3,00	3,00	0,00	B	M	B	B	MB	A	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	3,75	7,00	3,00	3,00	0,00	B	M	B	B	MB	A	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	4,50	6,00	9,00	9,00	0,00	M	M	A	A	MB	A	A	A	MA	MA	B
	[SW.10]	BBDD Microsoft SQL Server	5,25	8,00	8,00	6,00	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	5,25	8,00	8,00	8,00	0,00	M	A	A	A	MB	A	A	MA	MA	MA	B
	[SW.12]	Microsoft SCCM	3,75	6,00	4,00	6,00	0,00	B	M	B	M	MB	A	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	3,75	6,00	4,00	8,00	0,00	B	M	B	A	MB	A	M	A	M	MA	B
	[SW.14]	Antivirus Symantec	2,25	3,00	5,00	7,00	0,00	B	B	M	M	MB	A	M	M	A	A	B
	[SW.15]	Intranet corporativa	5,25	8,00	7,00	7,00	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.16]	Web corporativa	5,25	6,00	9,00	6,00	0,00	M	M	A	M	MB	A	A	A	MA	A	B
	[SW.17]	SAP	6,00	9,00	8,00	8,00	0,00	M	A	A	A	MB	A	A	MA	MA	MA	B
	[SW.18]	Navision	6,00	9,00	8,00	8,00	0,00	M	A	A	A	MB	A	A	MA	MA	MA	B
	[SW.19]	Contaplus	4,50	7,00	6,00	5,00	0,00	M	M	M	M	MB	A	A	A	A	A	B
	[SW.20]	Software puesto usuario: office 365, antivirus,	2,25	7,00	5,00	5,00	0,00	B	M	M	M	MB	A	M	A	A	A	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	4,50	8,00	5,00	7,00	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	5,25	8,00	6,00	7,00	0,00	M	A	M	M	MB	A	A	MA	A	A	B
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	8,00	9,00	8,00	7,00	6,00	A	A	A	M	M	A	MA	MA	MA	A	A
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	9,00	9,00	9,00	8,00	8,00	A	A	A	A	A	A	MA	MA	MA	MA	MA
	[D.3]	Bases de datos RRHH	9,00	9,00	8,00	8,00	8,00	A	A	A	A	A	A	MA	MA	MA	MA	MA
	[D.4]	LDAP: Directorio Activo Microsoft	7,00	7,00	8,00	9,00	7,00	M	M	A	A	M	A	A	A	MA	MA	A
	[D.5]	Copias de seguridad	7,00	9,00	7,00	3,00	7,00	M	A	M	B	M	A	A	MA	A	M	A
Comunicaciones [D]	[COM.1]	Red internet	5,25	8,00	6,00	9,00	0,00	M	A	M	A	MB	A	A	MA	A	MA	B
	[COM.2]	Red MPLS	5,25	8,00	6,00	8,00	0,00	M	A	M	A	MB	A	A	MA	A	MA	B
	[COM.3]	Red local CPD	6,00	9,00	6,75	9,00	0,00	M	A	M	A	MB	A	A	MA	A	MA	B
	[COM.4]	Red local sedes	4,50	7,00	5,25	7,00	0,00	M	M	M	M	MB	A	A	A	A	A	B
	[COM.5]	Red wifi invitados sedes	1,50	3,00	2,25	3,00	0,00	MB	B	B	B	MB	A	B	M	M	M	B
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	2,25	3,00	2,25	4,00	0,00	B	B	B	B	MB	A	M	M	M	M	B
	[COM.7]	Red wifi usuarios	2,25	7,00	2,25	5,00	0,00	B	M	B	M	MB	A	M	A	M	A	B
	[COM.8]	Red telefonía IP	0,00	0,00	1,50	7,00	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[COM.9]	Red telefonía móvil	0,00	0,00	1,50	8,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
Servicios [S]	[S.1]	Servicio ERP	6,00	6,75	6,75	8,00	5,25	M	M	M	A	M	A	A	A	A	MA	A
	[S.2]	Servicio correo	5,25	6,75	6,00	9,00	5,25	M	M	M	A	M	A	A	A	A	MA	A
	[S.3]	Servicio de telefonía	0,00	2,25	0,00	8,00	0,00	MB	B	MB	A	MB	A	B	M	B	MA	B
	[S.4]	Servicio de ficheros	5,25	6,00	6,00	7,00	5,25	M	M	M	M	M	A	A	A	A	A	A
	[S.5]	Servicio de acceso remoto	4,50	6,00	4,50	6,00	4,50	M	M	M	M	M	A	A	A	A	A	A
	[S.6]	Servicio de backup	6,00	6,75	6,00	6,00	6,00	M	M	M	M	M	A	A	A	A	A	A
Soportes de Información [M]	[M.1]	Almacenamiento CPD	0,00	9,00	4,50	9,00	0,00	MB	A	M	A	MB	A	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	0,00	7,00	3,50	7,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[M.3]	Memorias USB	0,00	6,00	1,50	2,00	0,00	MB	M	MB	MB	MB	A	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	0,00	0,00	1,60	9,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	0,00	0,00	1,40	6,00	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[AUX.3]	Sistemas antiincidencios	0,00	0,00	1,60	8,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[AUX.4]	Cableado LAN	0,00	0,00	1,20	9,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	0,00	0,00	0,00	9,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[P.2]	Personal TI	0,00	0,00	0,00	8,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[P.3]	Personal Proveedor TI	0,00	0,00	0,00	7,00	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[P.4]	Resto de personal	0,00	0,00	0,00	3,00	0,00	MB	MB	MB	B	MB	A	B	B	B	M	B

Tabla 26. Estimación de riesgos

Del análisis de la tabla anterior, podemos concluir que:

- La dimensión que se ve afectada por mayor riesgo es la confidencialidad
- La mayor parte de los activos tienen alguna dimensión con riesgo alto o muy alto.
- Los grupos de activos con riesgos más altos son: datos, software comunicaciones y servicios.

5 PROPUESTAS DE PROYECTOS

5.1 INTRODUCCIÓN

En base al análisis realizado en los apartados anteriores, se proponen una serie de proyectos que deben ayudar a mitigar el riesgo actual de la organización.

Para la elección de los proyectos tendremos en cuenta fundamentalmente el análisis de riesgos, las amenazas detectadas previamente y el análisis diferencial realizado al inicio de este trabajo.

Además, se ha tenido en cuenta que los recursos de RecycleSA en el ámbito de la IT y la seguridad de la Información son reducidos, por lo que se deben plantear proyectos realistas y abordables con los recursos disponibles.

Por otro lado, RecycleSA aborda sus presupuestos anualmente, por lo que se plantean proyectos para su ejecución en un espacio temporal de aproximadamente un año.

En base a todo ello, se proponen 10 proyectos que cubrirán tanto cambios tecnológicos, que ayuden a mejorar la seguridad, como proyectos para mejorar la organización de los procesos de gestión de RecycleSA y se alineen con la ISO/IEC 27001:2013 y las mejoras prácticas que define la ISO/IEC 27002:2013.

La siguiente tabla muestra dichos proyectos:

Ámbto	ID	Proyecto
Tecnológico	PRY1	Migración infraestructura CPD a modelo IaaS
	PRY2	Securización dispositivos portátiles
	PRY3	Eliminación infraestructura de servidores sedes
	PRY4	Implantación solución MDM
Organizativo/Gestión	PRY5	Políticas de seguridad
	PRY6	Plan de Formación
	PRY7	Política de dispositivos móviles
	PRY8	Política y auditoría de control de accesos
	PRY9	Plan de continuidad de negocio
	PRY10	Procedimientos de gestión de incidentes de seguridad

Tabla 27. Proyectos Propuestos.

En los siguientes apartados se describen en detalle cada uno de esos proyectos, su planificación global y los resultados que se esperan conseguir con su ejecución.

5.2 PROYECTOS DE ÁMBITO TECNOLÓGICO

A continuación se describen diversos proyectos tecnológicos que se proponen para la mejora de la seguridad de ReycleSA.

Es de notar que, durante la realización de este TFM, RecycleSA ha abordado un proyecto para la migración a la nube de su infraestructura de servidores. Dadas las implicaciones y mejoras que este proyecto supondrá para el SGSI, se refleja en este apartado de propuestas de mejoras, pues posteriormente se contemplará su impacto en el SGSI.

Igualmente RecycleSA abordó hace algún tiempo la implantación de una solución MDM para la gestión de sus dispositivos móviles. Sin embargo, debido a consideraciones de tipo legal, aún no se ha puesto en marcha. Consideramos que es muy importante para la mejora del SGSI su implantación efectiva cuanto antes, por lo que también se refleja en este documento.

PRY1	**Migración infraestructura CPD a modelo IaaS**
Objetivos	Migrar toda la infraestructura del CPD principal de RecycleSA a infraestructura en la nube.
Descripción	Como se mostraba en el apartado *2.2.5 Infraestructura tecnológica* de este documento, RecycleSA mantiene actualmente su infraestructura de servidores en un Datacenter contratado al efecto. El hardware de servidores, almacenamiento y comunicaciones es propiedad de RecycleSA y aloja una infraestructura de virtualización basada en VMWare. La gestión y administración de todos estos elementos (hardware y software) es responsabilidad directa de RecycleSA, que lo gestiona a través de un proveedor de servicio contratado al efecto. Igualmente toda la gestión de compra y mantenimiento en garantía de todos los elementos es responsabilidad de RecycleSA. Con este proyecto se pretende pasar la gestión del CPD a un modelo IaaS del fabricante Microsoft, que se encargará de proveer y gestionar toda la infraestructura necesaria. Con ello se garantiza unos muy altos niveles de disponibilidad que difícilmente se pueden conseguir para el hardware y las instalaciones con medios propios, que como se ha visto, mantienen actualmente un riesgo muy alto.
Actividades	▪ Análisis de la infraestructura de servidores actual ▪ Análisis de las relaciones entre los distintos servidores ▪ Análisis de los cambios de comunicaciones necesarios ▪ Análisis de los distintos mecanismos de migración en función de la tipología de servidores a migrar: SSOO, BBDD,…. ▪ Definición de plan de migración ▪ Preparación de infraestructura de comunicaciones ▪ Realización de piloto de migración ▪ Ejecución de la migración según planificación previa ▪ Adecuación de documentación y procesos del SGSI a nueva infraestructura

Controles relacionados	▪ A15.1.1 Política de seguridad de la información en las relaciones con los proveedores. ▪ A15.1.2 Requisitos de seguridad en contratos con terceros. ▪ A15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones. ▪ A15.2.1 Control y revisión de la provisión de servicios del proveedor. ▪ A15.2.2 Gestión de cambios en la provisión del servicio del proveedor. ▪ A16.1.1 Responsabilidades y procedimientos. ▪ A17.1.1 Planificación de la continuidad de la seguridad de la información. ▪ A17.1.2 Implementar la continuidad de la seguridad de la información. ▪ A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. ▪ A17.2.1 Disponibilidad de los recursos de tratamiento de la información
Activos involucrados	▪ [L.1] CPD ▪ [HW.1] Servidores hypervisor CPD ▪ [HW.2] Firewall CPD ▪ [HW.3] Swithes CPD ▪ [SW.1] Software virtualizacion VMWare ▪ [SW.2] Sistema operativos Windows Server ▪ [SW.3] Sistema operativos Linux Server ▪ [SW.4] Software backup: Veeam backup ▪ [SW.9] Directorio Activo Microsoft ▪ [SW.10] BBDD Microsoft SQL Server ▪ [SW.11] BBDD Oracle ▪ [SW.12] Microsoft SCCM ▪ [SW.13] Herramienta de ticketing: OTRS ▪ [SW.14] Antivirus Symantec ▪ [SW.15] Intranet corporativa ▪ [SW.16] Web corporativa ▪ [SW.17] SAP ▪ [SW.18] Navision ▪ [SW.19] Contaplus ▪ [SW.21] Aplicaciones Office 365: Correo, one drive, skype,… ▪ [SW.22] Aplicaciones Sharepoint Office 365 ▪ [COM.3] Red local CPD ▪ [M.1] Almacenamiento CPD ▪ [AUX.1] Sistema eléctrico ▪ [AUX.2] Aire acondicionado Salas técnicas ▪ [AUX.3] Sistemas antiincidendios ▪ [AUX.4] Cableado LAN

Riesgos a mitigar	▪ [D] disponibilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora en la disponibilidad de los servicios que aloja: fabricantes como Microsoft ofrecen una disponibilidad que difícilmente se conseguirá con medios propios. ▪ Mejoras en la disponibilidad de los sistemas auxiliares que proporcionan los CPDS de grandes fabricantes: Sistema eléctrico, aire acondicionado, sistemas anti-incendios, etc. ▪ Mejoras en las soluciones de backup que se proporciona también como servicio. Otros Beneficios: ▪ Eliminación de inversión para renovación de infraestructura hardware de servidores ▪ Disminución de costes globales ▪ Reducción de gestión compras a cargo de RecycleSA, que ya no deberá gestionar la compra de todos los elementos hardware y de software de virtualización del CPD. ▪ Disminución en la gestión de toda la infraestructura contratada ahora como un servicio (IaaS), liberando al departamento IT ▪ Mejoras globales en la percepción del servicio por parte de los usuarios.
Planificación	6 meses
Coste	El cambio de modelo de servicio de la infraestructura de CPD conlleva un cambio en el modelo de costes que van mucho más allá del propio proyecto de implantación y puesta en marcha: ▪ Eliminación de compra y/o renovación de hardware ▪ Eliminación de compra y /o renovación de software de virtualización ▪ Administración y gestión de toda la infraestructura ▪ Nuevas necesidades de líneas de comunicación Es por ello una valoración económica muy compleja. En todo caso, RecycleSA ya ha abordado la implantación de este proyecto y, por tanto, su valoración, que se ha dejado fuera de este TFM.

Tabla 28. PRY1. Migración infraestructura CPD a modelo IaaS.

PRY2	**Securización dispositivos portátiles**
Objetivos	Implantación de políticas de securización de los dispositivos portátiles.
Descripción	Aunque RecicleSA ha implantado mecanismos de cifrados para todos sus portátiles, mejorando por tanto la confidencialidad de sus datos, mantiene una política de seguridad para los puestos de trabajo que distingue claramente entre PCs y portátiles.

	En los PCs los usuarios no son administradores del sistema. Sin embargo, en los portátiles todos los usuarios si son administradores, debido a que se considera que pueden necesitar realizar tareas que requieren privilegios de administración cuando no están en la red corporativa y, por tanto, no disponen de soporte remoto. Con este proyecto se eliminaría los privilegios de administración de los usuarios de portátiles para mejorar la seguridad de los mismos y mantener homogénea la plataforma de puesto de usuario, con las ventajas que esto tiene para su correcta administración y gestión.
Actividades	▪ Análisis de los requerimientos de los aplicativos corporativos. ▪ Análisis de las necesidades específicas de los usuarios. ▪ Definición de mecanismos para la instalación de software por parte de los usuarios. ▪ Diseño de las políticas necesarias en el Directorio Activo. ▪ Diseño de plan de comunicación a los usuarios: refuerzo en concienciación en seguridad de los usuarios. ▪ Planificación del proyecto. ▪ Ejecución del proyecto.
Controles relacionados	▪ A9.4.4 Uso de utilidades con privilegios del sistema. ▪ A11.2.6 Seguridad de los equipos fuera de las instalaciones ▪ A12.2.1 Controles contra el código malicioso. ▪ A12.5.1 Instalación del software en explotación. ▪ A12.6.1 Gestión de las vulnerabilidades técnicas. ▪ A12.6.2 Restricción en la instalación de software.
Activos involucrados	▪ [HW.8] Portátiles usuarios
Riesgos a Mitigar	▪ [C] confidencialidad ▪ [I] integridad ▪ [D] Disponibilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora de la disponibilidad de los puestos de trabajo. ▪ Mejora en la confidencialidad e integridad, al impedir que los usuarios accedan a perfiles de otros usuarios de los portátiles. ▪ Limitación de la instalación de malware. Otros Beneficios: ▪ Homogenización de la plataforma de puesto de usuario. ▪ Reducción de la tasa de incidencias del puesto de trabajo. ▪ Mejora de la productividad de los usuarios. ▪ Minimizar instalación de software no corporativo ▪ Limitar problemas de licenciamiento
Planificación	2 meses
Coste	Se estima un coste aproximado de 9.000 €

Tabla 29. PRY2. Securización dispositivos portátiles.

PRY3	Eliminación infraestructura de servidores sedes
Objetivos	Eliminar, en la medida de lo posible, la infraestructura de servidores existente en las diversas sedes de RecycleSA.
Descripción	Como se describe en el apartado *2.2.5.5 Infraestructura de Servidores* de este documento, RecycleSA mantiene múltiples servidores distribuidos en las distintas sedes. Estos servidores proporcionan fundamentalmente servicios de ficheros. El mantenimiento de dicha infraestructura en sus correspondientes salas técnicas provoca diversos problemas para su gestión y mantenimiento de seguridad, como pueden ser: ▪ Control de acceso a dichas salas técnicas. ▪ Disponibilidad de la infraestructura. ▪ Mantenimiento de backups. ▪ Gestión remota. Tanto desde el punto de vista de la gestión como de la seguridad, es conveniente adoptar una solución de servicio de ficheros centralizada, que se debe abordar en este proyecto. El proyecto debe tener en cuenta diversas opciones tecnológicas, como puede ser la utilización de los servicios que ofrece Office 365, ya contratado por RecycleSA, relativos al servicio de ficheros.
Actividades	▪ Análisis de las necesidades de cada sede. ▪ Análisis de alternativas. ▪ Análisis de necesidades de comunicaciones. ▪ Diseño de solución en la nube ▪ Formación a los usuarios ▪ Migración de datos a la nube
Controles relacionados	▪ A11.1.2 Controles físicos de entrada. ▪ A11.2.1 Emplazamiento y protección de equipos. ▪ A11.2.2 Instalaciones de suministro. ▪ A12.3.1 Copias de seguridad de la información. ▪ A16.1.1 Responsabilidades y procedimientos. ▪ A17.1.1 Planificación de la continuidad de la seguridad de la información. ▪ A17.1.2 Implementar la continuidad de la seguridad de la información. ▪ A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. ▪ A17.2.1 Disponibilidad de los recursos de tratamiento de la información
Activos involucrados	▪ [L.2] Sala Técnica Sede ▪ [HW.4] Servidores hypervisor Sedes ▪ [HW.5] Switches/routers Sedes ▪ [D.1] Servidores de ficheros corporativos

	▪ [SW.1] Software virtualizacion VMWare ▪ [SW.2] Sistema operativos Windows Server ▪ [M.2] Almacenamiento Sedes ▪ [AUX.1] Sistema eléctrico ▪ [AUX.2] Aire acondicionado Salas técnicas ▪ [AUX.3] Sistemas antiincidencios ▪ [AUX.4] Cableado LAN
Riesgos a Mitigar	▪ [D] disponibilidad ▪ [C] confidencialidad ▪ [I] integridad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora de la disponibilidad del servicio de ficheros de las sedes ▪ Mejoras en la confidencialidad, limitando acceso físicos no autorizados ▪ Mejoras en la integridad, evitando acceso físico directo a los sistemas ▪ Mejoras en la gestión mediante la gestión centralizada de permisos. Otros Beneficios: ▪ En función de la solución adoptada, se podría mejorar: ▪ Colaboración entre los distintos usuarios de la organización. ▪ Mejorar la productividad.
Planificación	2 meses
Coste	Puesto que inicialmente se debe realizar un análisis de posibles alternativas, en función del cual se podrán adoptar diversas soluciones tecnológicas, con costes muy diversos, en este apartado se estima únicamente el coste de dicho análisis inicial. Se estima el coste del análisis inicial en 2.000 €.

Tabla 30. PRY3. Eliminación infraestructura de servidores sedes.

PRY4	Implantación solución MDM
Objetivos	Implantación de solución MDM que permita gestionar adecuadamente la seguridad de los dispositivos móviles.
Descripción	Como se describe en el apartado *2.2.5.2. Dispositivos móviles* de este documento, RecycleSA mantiene múltiples usuarios que acceden al correo corporativo desde dispositivos móviles. Además, se permite dicho acceso tanto desde dispositivos corporativos como desde dispositivos personales (BYOD). Esto supone un elevado riesgo de seguridad en distintas dimensiones (confidencialidad, autenticidad,..), sobre todo ante la pérdida o robo del dispositivo. Por todo ello, además definir políticas adecuada para los dispositivos móviles, que se tratarán en otro proyecto adicional, es necesario implantar de manera efectiva una solución MDM que permita gestionar el dispositivo de manera remota y, en caso necesario, eliminar toda la información corporativa del mismo.
Actividades	▪ Análisis de requisitos ▪ Diseño de políticas MDM Definiendo: ○ Política de contraseñas ○ Encriptación del dispositivo ○ Mecanismos de restauración y borrado Distinguiendo: ○ Por tipo de dispositivo: BYOD, personal ○ Por tecnología: Android, IOS ○ Por tipo de usuario: VIP, IT,… ▪ Realización de Piloto ▪ Implantación en producción. ▪ Documentación
Controles relacionados	▪ A6.2.1 Política de dispositivos móviles. ▪ A6.2.2 Teletrabajo. ▪ A11.2.1 Emplazamiento y protección de equipos. ▪ A11.2.6 Seguridad de los equipos fuera de las instalaciones. ▪ A12.2.1 Controles contra el código malicioso. ▪ A12.5.1 Instalación del software en explotación. ▪ A12.6.1 Gestión de las vulnerabilidades técnicas. ▪ A12.6.2 Restricción en la instalación de software.
Activos involucrados	▪ [HW.9] Dispositivos móviles corporativos ▪ [HW.10] Dispositivos móviles personales ▪ [S.2] Servicio correo
Riesgos a Mitigar	▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad

Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora de la disponibilidad de los dispositivos móviles. ▪ Mejora en la confidencialidad de información corporativa ▪ Mejoras en la protección de la información personal ▪ Mejora de la seguridad "legal" (dispositivos personales/corporativos) Otros Beneficios: ▪ Homogenización de la plataforma de dispositivos móviles. ▪ Reducción de la tasa de incidencias del puesto de trabajo. ▪ Mejora de la productividad de los usuarios.
Planificación	5 meses
Coste	Se estima un coste de implantación de 10.000 € A este coste habría que añadir el coste anual de la solución tecnológica finalmente implantada.

Tabla 31. PRY4. Implantación solución MDM.

5.3 PROYECTOS DE ÁMBITO ORGANIZATIVO Y DE GESTIÓN

PRY5	Políticas de seguridad
Objetivos	Definición y puesta en marcha de la política de seguridad.
Descripción	Al inicio de estos trabajos RecycleSA disponía de un documento "Corporate IT Security Policy". Sin embargo, este documento no comprende todos los elementos que la norma ISO/IEC 27001:2013 establece como necesarios. En el *Anexo B Política de Seguridad*de este documento se ha definido la política de RecycleSA conforme a los requisitos que establece dicha norma en su apartado 5.2. En este proyecto se abordará la actualización y aprobación de la Política de Seguridad conforme al resultado de los análisis realizados y se pondrá en marcha, creando las estructuras organizativas necesarias. Finalmente se comunicará a toda la organización.
Actividades	▪ Actualización de la Política. ▪ Aprobación por la Alta Dirección ▪ Documentación formal y publicación. ▪ Puesta en marcha de la estructura organizativa, incluyendo: ▪ Designación del Comité de Seguridad ▪ Asignación de roles y responsabilidades ▪ Comunicación de la política a toda la organización
Controles relacionados	▪ A5.1.1. Políticas de seguridad de la Información ▪ A5.1.2 Revisión de las políticas de seguridad de la Información.
Activos involucrados	▪ Todos los activos del SGSI
Riesgos a Mitigar	▪ [A] autenticidad ▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad ▪ [T] trazabilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejor organización en los procesos relativos a la Seguridad de la Información. ▪ Optimización de recursos y procesos asociados a la Seguridad de la Información. ▪ Concienciación de todos los empleados de la organización Otros Beneficios: ▪ Mejora de la imagen corporativa
Planificación	1 mes

Coste	Para la ejecución de este proyecto se debería contratar un servicio externo de consultoría. Se estima su coste en 6.000 €.

Tabla 32. PRY5. Políticas de seguridad.

PRY6	**Plan de Formación**
Objetivos	Definición y puesta en marcha de un plan de formación continua en Seguridad de la Información.
Descripción	La formación de los usuarios de cualquier organización es fundamental para mantener adecuadamente la Seguridad de la Información. Por ello se debe definir y ejecutar un programa de formación continua dirigido a todos los usuarios de la organización. La formación debe incluir diversos aspectos, como son: ▪ Política de Seguridad de la Organización. ▪ Riesgos y amenazas. ▪ Mecanismos seguros de intercambio de información. ▪ Acuerdos de confidencialidad. ▪ Responsabilidades legales. Leyes y normas (RGPD) ▪ Medidas disciplinarias.
Actividades	▪ Definición del plan de formación. Contenidos ▪ Planificación periódica anual. ▪ Ejecución de la formación. ▪ Evaluación y control de la formación.
Controles relacionados	▪ A9.3.1 Uso de información secreta de autenticación. ▪ A12.5.1 Instalación del software en explotación. ▪ A13.2.1 Políticas y procedimientos de intercambio de información. ▪ A13.2.2 Acuerdos de intercambio de información ▪ A13.2.3 Mensajería electrónica ▪ A13.2.4 Acuerdos de confidencialidad o no revelación ▪ A15.1.1 Política de seguridad de la información en las relaciones con los proveedores
Activos involucrados	▪ [P.1] Personal Dirección: CEO, Auditor, Director Financiero ▪ [P.2] Personal TI ▪ [P.3] Personal Proveedor TI ▪ [P.4] Resto de personal

Riesgos a Mitigar	▪ [A] autenticidad ▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora de la concienciación de los usuarios de la organización ▪ Reducción de riesgos por desconocimiento de los usuarios. Otros Beneficios: ▪ Mejora de la imagen corporativa
Planificación	Se estima que se necesitarán 3 meses para la ejecución de este proyecto
Coste	Se estima un coste de 12.000 €

Tabla 33. PRY6. Plan de Formación.

PRY7	**Política de dispositivos móviles**
Objetivos	Revisión de la política de dispositivos móviles
Descripción	RecycleSA tiene definida una política de dispositivos móviles (Mobile device policy). Sin embargo, dado que aún no tiene implantado una solución MDM que permita gestionar adecuadamente los dispositivos móviles, no puede garantizar, ni siquiera determinar, el grado cumplimiento de dicha política. En paralelo al proyecto de implantación de la solución MDM que se propone en este documento, se debe actualizar dicha política para adecuarla tanto a las necesidades de RecycleSA como a la solución tecnológica de MDM adoptada.
Actividades	▪ Actualización de la Política. ▪ Aprobación por la Alta Dirección ▪ Documentación formal y publicación. ▪ Comunicación de la política a toda la organización
Controles relacionados	▪ A6.2.1 Política de dispositivos móviles. ▪ A6.2.2 Teletrabajo. ▪ A9.3.1 Uso de la información secreta de autenticación ▪ A11.2.1 Emplazamiento y protección de equipos. ▪ A11.2.6 Seguridad de los equipos fuera de las instalaciones. ▪ A12.6.1 Gestión de las vulnerabilidades técnicas. ▪ A12.6.2 Restricción en la instalación de software.
Activos involucrados	▪ [HW.9] Dispositivos móviles corporativos ▪ [HW.10] Dispositivos móviles personales

Riesgos a Mitigar	▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Concienciación de los usuarios en materia de confidencialidad de la información en los dispositivos móviles. ▪ Mejoras en la integridad de la información manipulada desde dispositivos móviles ▪ Mejoras en la confidencialidad de la información accesible desde los dispositivos móviles Otros Beneficios: ▪ Mejora de la imagen corporativa.
Planificación	2 semanas. A realizar en paralelo a la implantación del MDM
Coste	Se realizará por el propio departamento IT por lo que no se valora coste.

Tabla 34. PRY7. Política de dispositivos móviles.

PRY8	**Política y auditoría de control de accesos**
Objetivos	Definir, implementar y auditar una política de control de acceso para limitar el mismo a los recursos y a la información, basada en los requisitos de negocio y la seguridad de la información.
Descripción	Se debe definir, aprobar y publicar una política de control de accesos que contemple todos los aspectos relacionados con la seguridad en la gestión de los accesos de los usuarios, externo o internos, de la organización a los diversos servicios, aplicaciones e información de RecycleSA. Adicionalmente, se debe realizar una **auditoría completa inicial** de todos los usuarios que determine el grado de cumplimiento con dicha política de control de accesos. La auditoría debe incluir diversos aspectos, como son: ▪ Detección de usuarios con privilegios excesivos. ▪ Detección de usuarios de baja en la organización que no se han eliminado de los servicios IT. ▪ Detección de servicios con control de accesos deficientes o que no cumplen con la política definida. La auditoría debe comprender, todos los servicios y aplicaciones de RecycleSA: ▪ Servicio de Directorio ▪ Servicio de ficheros. ▪ Servicios de acceso remoto (VPN) ▪ Aplicaciones ERP: SAP, Navision, Contaplus.

	▪ Servicios Office 365 ▪ Servicios de comunicaciones y redes. La auditoría debe analizar con especial cuidado a los usuarios de los distintos proveedores IT de RecycleSA que mantienen privilegios de administración sobre los sistemas para los que prestan servicios.
Actividades	▪ Definición de la Política. ▪ Aprobación por la Alta Dirección ▪ Documentación formal y publicación. ▪ Comunicación de la política a toda la organización ▪ Auditoria de todos los usuarios del sistema y de los servicios a los que tienen acceso.
Controles relacionados	▪ A9.1.1 Política de control de acceso. ▪ A9.1.2 Acceso a las redes y a los servicios de red ▪ A9.2.1 Registro y baja de usuario. ▪ A9.2.2 Provisión de acceso de usuario. ▪ A9.2.3 Gestión de privilegios de acceso. ▪ A9.2.4 Gestión de la información secreta de autenticación de los usuarios. ▪ A9.2.5 Revisión de los derechos de acceso de usuario. ▪ A9.2.6 Retirada o reasignación de los derechos de acceso ▪ A9.3.1 Uso de la información secreta de autenticación ▪ A9.4.1 Restricción del acceso a la información. ▪ A9.4.2 Procedimientos seguros de inicio de sesión. ▪ A9.4.3 Sistema de gestión de contraseñas. ▪ A9.4.4 Uso de utilidades con privilegios del sistema. ▪ A9.4.5 Control de acceso al código fuente de los programas
Activos involucrados	▪ Todos los activos del SGSI
Riesgos a Mitigar	▪ [A] autenticidad ▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad ▪ [T] trazabilidad
Beneficios	Asociados a la Seguridad de la Información: ▪ Mejora de la concienciación de los usuarios ▪ Mejora de la confidencialidad, integridad y disponibilidad de la información ▪ Reducción de riesgos por desconocimiento de los usuarios. ▪ Reducción de riesgos de accesos no autorizados. Otros Beneficios: ▪ Mejora de la imagen corporativa

Planificación	Se estima un plazo de 2 meses para la realización del proyecto
Coste	Se estima un coste de 6.000 €

Tabla 35. PRY8. Política y auditoría de control de accesos.

PRY9	**Plan de continuidad de negocio**
Objetivos	Definir un plan de continuación de negocio para la gestión de la seguridad de la información en situaciones adversas.
Descripción	Se definirá un plan de continuidad que permita reaccionar adecuadamente ante incidentes que puedan interrumpir la actividad de la organización, y que debe permitir: ▪ Recuperar las funciones críticas en el menor tiempo posible ▪ Disponer de procedimientos documentados y probados para su ejecución cuando sea necesaria ▪ Reducir las pérdidas económicas por indisponibilidad de funciones de negocio. Como resultado del plan de continuidad de negocio es posible se surjan nuevos proyectos, para mejorar la disponibilidad global de los sistemas IT de RecycleSA.
Actividades	▪ Identificación de los activos críticos en base a su disponibilidad ▪ Identificación y priorización de amenazas ▪ Análisis de impacto de negocio (BIA) ▪ Identificar a los responsables de cada servicio ▪ Definir la estrategia de recuperación ▪ Crear el plan de respuesta y recuperación ▪ Pruebas de funcionamiento.
Controles relacionados	▪ A17.1.1 Planificación de la continuidad de la seguridad de la información. ▪ A17.1.2 Implementar la continuidad de la seguridad de la información. ▪ A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. ▪ A17.2.1 Disponibilidad de los recursos de tratamiento de la información
Activos involucrados	▪ Todos los activos necesarios para el funcionamiento de los servicios identificados como críticos en el plan de continuidad.
Riesgos a Mitigar	▪ [I] integridad ▪ [D] disponibilidad

Beneficios	▪ Mejora de la disponibilidad de los servicios críticos. ▪ Reducir las pérdidas económicas y de imagen corporativa ante incidentes críticos. ▪ Mejora del conocimiento de todos los aspectos involucrados en la operación de los sistemas de la organización.
Planificación	El plan de continuidad estará muy condicionado por las infraestructura de CPD que albergan los servicios críticos de RecycleSA. Puesto que también se abordará un proyecto para pasar a modelo IaaS dichas infraestructuras, será conveniente definir el plan de continuidad tras la ejecución del proyecto de migración a IaaS. 3 meses
Coste	Se estima un coste de 15.000 €

Tabla 36. PRY9. Plan de continuidad de negocio.

PRY10	**Procedimientos de gestión de incidentes de seguridad**
Objetivos	Definir procedimientos de gestión de los incidentes de seguridad que agilicen y mejoren la respuesta ante incidentes de seguridad.
Descripción	Una correcta gestión de los incidentes de seguridad ayudará a mitigar los efectos causados y, con la correspondiente documentación y análisis posterior, reducir su frecuencia, mejorando la seguridad global de los sistemas de información. Como se describe en el apartado *2.2.3. Estructura del servicio de IT* de este documento, RecycleSA mantiene externalizado la mayor parte de sus servicios de TI, lo que facilita que se diluyan las responsabilidades ante incidentes de seguridad. Es por ello especialmente importante que RecycleSA mantenga procedimientos de gestión de incidentes de seguridad que involucre a todos sus proveedores de servicios, asignándoles las responsabilidades adecuadas y que permita la coordinación fluida de todos ellos.
Actividades	▪ Identificar y tipificar los posibles incidentes, con su gravedad. ▪ Identificar los roles participantes en el proceso. ▪ Definir las responsabilidades de cada uno de los proveedores de servicios IT ▪ Definir procedimiento de actuación ante cada tipo de incidente. ▪ Publicar a los usuarios procedimientos de actuación ▪ Publicar a los proveedores de servicio IT sus tareas y responsabilidades.
Controles relacionados	▪ A16.1.1 Responsabilidades y procedimientos. ▪ A16.1.2 Notificación de los eventos de seguridad de la información. ▪ A16.1.3 Notificación de puntos débiles de la seguridad. ▪ A16.1.4 Evaluación y decisión sobre los eventos de seguridad de información

	▪ A16.1.5 Respuesta a incidentes de seguridad de la información ▪ A16.1.6 Aprendizaje de los incidentes de seguridad de la información ▪ A16.1.7 Recopilación de evidencias
Activos involucrados	▪ Todos los activos del SGSI
Riesgos a Mitigar	▪ [A] autenticidad ▪ [C] confidencialidad ▪ [I] integridad ▪ [D] disponibilidad ▪ [T] trazabilidad
Beneficios	▪ Mejora en la rapidez y calidad de la respuesta ante incidentes de seguridad. ▪ Creación de registro de incidentes que facilite análisis posteriores para la mejora de la seguridad de la información ▪ Mejora de la interlocución entre los proveedores de servicios involucrados.
Planificación	El plan de continuidad estará muy condicionado por las infraestructura de CPD que albergan los servicios críticos de RecycleSA. Puesto que también se abordará un proyecto para pasar a modelo IaaS dichas infraestructuras, será conveniente definir el plan de continuidad tras la ejecución del proyecto de migración a IaaS. Se estiman 1,5 meses.
Coste	Se estima un coste de 9.000 € para este proyecto.

Tabla 37. PRY10. Procedimientos de gestión de incidentes de seguridad.

5.4 PLANIFICACIÓN PROPUESTA

Una vez identificados los proyectos que se considera conviene abordar inicialmente es necesario realizar una planificación adecuada que permita lograr los objetivos cuanto antes con los medios y recursos disponibles.

Para la planificación de ejecución de los diversos proyectos propuestos se ha tenido en cuenta que el departamento IT cuenta con escasos recursos, por lo que se ha planteado que solo se aborden dos proyectos simultáneamente.

Para su priorización y secuenciación se han seguido los siguientes principios y condicionantes:

- La implantación del proyecto *Migración infraestructura CPD a modelo IaaS* se ha abordado por RecycleSA durante la relación de este TFM, por lo que es ya una tarea en ejecución, que se contempla al inicio de esta planificación.
- Al finalizar la migración anterior, se podría abordar el proyecto técnico de *Eliminación de infraestructura de servidores*, que en función de la tecnología elegida para su sustitución, podrá afectar a las rutinas de trabajo de los usuarios. Dado que el proyecto previo es de larga duración, la ejecución de este se realizará cuando ya los usuarios estén correctamente formados.
- Se considera esencial para la correcta gestión de la Seguridad de la Información la definición de la *Política de Seguridad* acorde a la ISO/IECI 27001:2013 y la puesta en marcha de los mecanismos que ésta define: Comité de Dirección, asignación de roles y responsabilidades, etc.. Finalmente se debería aprobar formalmente por la Alta Dirección y difundirse a toda la organización. Es por ello que se aborda al inicio de esta planificación
- Una vez definida y aprobada la Política de Seguridad, es conveniente abordar la definición de la política de control de accesos, lo que permitirá auditar el grado de cumplimiento de los distintos sistemas de RecycleSA de dicha política y, en su caso, solventar los problemas de seguridad detectados.
- A continuación debe definirse la Política de dispositivos móviles, lo que permitirá abordar posteriormente la implantación de los mecanismos de seguridad para dichos dispositivos mediante la implantación de la herramienta MDM.
- Una vez definidas correctamente las políticas, y antes de abordar proyectos tecnológicos que afectarán directamente a los usuarios, es conveniente abordar el plan de formación de todos ellos, lo que permitirá su concienciación previa, lo que redundará en mejor aceptación de los proyectos que afectarán a su forma de trabajo habitual hasta el momento, facilitando reducir su resistencia al cambio.
- Una vez los usuarios estén formados en materia de seguridad, se podrá abordar la implantación del proyecto de implantación de MDM. Como se ha visto, previamente se habrán definido las políticas asociadas.
- La securización de los portátiles es un proyecto que generalmente genera una fuerte resistencia al cambio por parte de los usuarios, por lo que se aborda en este momento, en el que ya han recibido la formación necesaria que les permitirá comprender mejor las razones que justifican este proyecto.
- Una vez la infraestructura de servidores, tanto del CPD como la existente previamente en las sedes se han migrado, es el momento de abordar la definición de los procedimientos de gestión de incidentes de seguridad.
- Para finalizar se puede abordar el plan de continuidad de negocio, que ya tendrá en cuenta todos los elementos previamente implantados.

En base a lo establecido en este punto, se establece el diagrama de Gantt que se propone y se muestra en la siguiente ilustración:

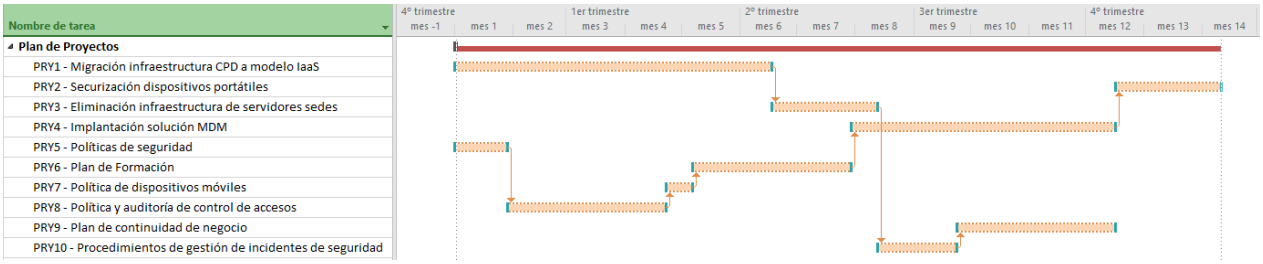

Ilustración 11. Planificación de proyectos propuesta.

5.5 RESULTADOS ESPERADOS

Los proyectos propuestos anteriormente tienen como objetivo disminuir los riesgos de nuestro SGSI evolucionándolo hacia el cumplimiento de las directrices que establece la norma ISO/IEC 27001:2013.

En los siguientes apartados, se evaluará el grado de evolución que se espera conseguir tras la ejecución de los proyectos propuestos.

5.5.1 EVOLUCIÓN DE RIESGOS

Una vez ejecutados los proyectos propuestos, el riesgo se podrá ver disminuido para cada activo tanto por la reducción de la frecuencia de las amenazas como por la disminución su impacto si finalmente se materializa.

Así, por ejemplo, la frecuencia de la materialización de las amenazas se puede reducir gracias a la formación impartida a los usuarios de la organización que permitirá minimizar su malos hábitos que puedan comprometer la seguridad de la información de RecycleSA.

Del mismo modo, otros proyectos reducirán el impacto de la materialización de las amenazas, como, por ejemplo, la implantación de los procedimientos de gestión de incidencias y los planes de continuidad de negocio.

En el Anexo L. Tabla de Análisis amenazas/activos tras ejecución de Proyectos.se muestra el análisis de amenazas realizado actualizadas según lo esperado tras la ejecución de los proyectos propuestos.

De ese análisis, al igual que en el apartado *4.6. Análisis de amenazas* de este documento, obtenemos la siguiente tabla de impactos por activo, actualizada tras la ejecución de los proyectos.

	Impacto				
Activo	A	C	I	D	T
Aplicación/Software [SW]	75%	100%	100%	75%	
Datos/Información [D]	100%	100%	100%	100%	100%
Equipamiento auxiliar [AUX]		20%	20%	100%	
Hardware [HW]		75%	50%	75%	
Instalaciones [L]		20%	20%	75%	
Personal [P]		75%	20%	75%	
Redes de comunicación [COM]	75%	100%	75%	100%	
Servicios [S]	75%	75%	75%	75%	75%
Soportes de información [M]		100%	50%	100%	

Tabla 38. Escala de valoración de dimensiones de la seguridad tras implantación proyectos

Finalmente, aplicando los mismos procedimientos descritos en el apartado *4. Análisis de Riesgos* de este documento, obtenemos una nueva tabla de estimación de riesgos, que se muestra a continuación.

			Impacto potencial					Impacto potencial (cualitativo)					Frecuencia	Riesgo				
Tipo Activo	ID Activo	Activo	A	C	I	D	T	A	C	I	D	T		A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	0,00	1,80	1,80	7,50	0,00	MB	MB	MB	A	MB	B	MB	MB	MB	A	MB
	[L.2]	Sala Técnica Sede	0,00	1,40	1,40	7,50	0,00	MB	MB	MB	A	MB	B	MB	MB	MB	A	MB
	[L.3]	Despacho Directivo	0,00	1,80	1,60	5,25	0,00	MB	MB	MB	M	MB	B	MB	MB	MB	M	MB
	[L.4]	Oficinas	0,00	1,20	1,40	5,25	0,00	MB	MB	MB	M	MB	B	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	0,00	6,75	4,50	6,75	0,00	MB	M	M	M	MB	A	B	A	A	A	B
	[HW.2]	Firewall CPD	0,00	6,75	4,50	6,75	0,00	MB	M	M	M	MB	A	B	A	A	A	B
	[HW.3]	Swithes CPD	0,00	5,25	4,50	6,75	0,00	MB	M	M	M	MB	A	B	A	A	A	B
	[HW.4]	Servidores hypervisor Sedes	0,00	5,25	3,50	5,25	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	0,00	4,50	3,50	5,25	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	0,00	4,50	2,50	2,25	0,00	MB	M	B	B	MB	A	B	A	M	M	B
	[HW.7]	PCs usuarios	0,00	5,25	2,50	3,75	0,00	MB	M	B	B	MB	A	B	A	M	M	B
	[HW.8]	Portátiles usuarios	0,00	5,25	2,50	3,75	0,00	MB	M	B	B	MB	A	B	A	M	M	B
	[HW.9]	Dispositivos móviles corporativos	0,00	4,50	2,00	2,25	0,00	MB	M	MB	B	MB	A	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	0,00	4,50	2,00	2,25	0,00	MB	M	MB	B	MB	A	B	A	B	M	B
	[HW.11]	Teléfonos IPs	0,00	1,50	1,00	2,25	0,00	MB	MB	MB	B	MB	A	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	6,00	8,00	8,00	6,75	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.2]	Sistema operativos Windows Server	6,00	8,00	8,00	6,00	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.3]	Sistema operativos Linux Server	5,25	8,00	7,00	4,50	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	6,00	9,00	8,00	1,50	0,00	M	A	A	MB	MB	A	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	4,50	7,00	4,00	5,25	0,00	M	M	B	M	MB	A	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	4,50	7,00	4,00	5,25	0,00	M	M	B	M	MB	A	A	A	M	A	B
	[SW.7]	Sistema operativo android	3,75	6,00	3,00	2,25	0,00	B	M	B	B	MB	A	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	3,75	7,00	3,00	2,25	0,00	B	M	B	B	MB	A	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	4,50	6,00	9,00	6,75	0,00	M	M	A	M	MB	A	A	A	MA	A	B
	[SW.10]	BBDD Microsoft SQL Server	5,25	8,00	8,00	4,50	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	5,25	8,00	8,00	6,00	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.12]	Microsoft SCCM	3,75	6,00	4,00	4,50	0,00	B	M	B	M	MB	A	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	3,75	6,00	4,00	6,00	0,00	B	M	B	M	MB	A	M	A	M	A	B
	[SW.14]	Antivirus Symantec	2,25	3,00	5,00	5,25	0,00	B	B	M	M	MB	A	M	M	A	A	B
	[SW.15]	Intranet corporativa	5,25	8,00	7,00	5,25	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.16]	Web corporativa	5,25	6,00	9,00	4,50	0,00	M	M	A	M	MB	A	A	A	MA	A	B
	[SW.17]	SAP	6,00	9,00	8,00	6,00	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.18]	Navision	6,00	9,00	8,00	6,00	0,00	M	A	A	M	MB	A	A	MA	MA	A	B
	[SW.19]	Contaplus	4,50	7,00	6,00	3,75	0,00	M	M	M	B	MB	A	A	A	A	M	B
	[SW.20]	Software puesto usuario: office 365, antivirus,	2,25	7,00	5,00	3,75	0,00	B	M	M	B	MB	A	M	A	A	M	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	4,50	8,00	5,00	5,25	0,00	M	A	M	M	MB	A	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	5,25	8,00	6,00	5,25	0,00	M	A	M	M	MB	A	A	MA	A	A	B
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	8,00	9,00	8,00	7,00	6,00	A	A	A	M	M	M	A	A	A	M	M
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	9,00	9,00	9,00	8,00	8,00	A	A	A	A	A	M	A	A	A	A	A
	[D.3]	Bases de datos RRHH	9,00	9,00	8,00	8,00	8,00	A	A	A	A	A	M	A	A	A	A	A
	[D.4]	LDAP: Directorio Activo Microsoft	7,00	7,00	8,00	9,00	7,00	M	M	A	A	M	M	M	M	A	A	M
	[D.5]	Copias de seguridad	7,00	9,00	7,00	3,00	7,00	M	A	M	B	M	M	M	A	M	B	M
Comunicaciones [D]	[COM.1]	Red internet	5,25	8,00	6,00	9,00	0,00	M	A	M	A	MB	M	M	A	M	A	MB
	[COM.2]	Red MPLS	5,25	8,00	6,00	8,00	0,00	M	A	M	A	MB	M	M	A	M	A	MB
	[COM.3]	Red local CPD	6,00	9,00	6,75	9,00	0,00	M	A	M	A	MB	M	M	A	M	A	MB
	[COM.4]	Red local sedes	4,50	7,00	5,25	7,00	0,00	M	M	M	M	MB	M	M	M	M	M	MB
	[COM.5]	Red wifi invitados sedes	1,50	3,00	2,25	3,00	0,00	MB	B	B	B	MB	M	MB	B	B	B	MB
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	2,25	3,00	2,25	4,00	0,00	B	B	B	B	MB	M	B	B	B	B	MB
	[COM.7]	Red wifi usuarios	2,25	7,00	2,25	5,00	0,00	B	M	B	M	MB	M	B	M	B	M	MB
	[COM.8]	Red telefonía IP	0,00	0,00	1,50	7,00	0,00	MB	MB	MB	M	MB	M	MB	MB	MB	M	MB
	[COM.9]	Red telefonía móvil	0,00	0,00	1,50	8,00	0,00	MB	MB	MB	A	MB	M	MB	MB	MB	A	MB
Servicios [S]	[S.1]	Servicio ERP	6,00	6,75	6,75	6,00	5,25	M	M	M	M	M	M	M	M	M	M	M
	[S.2]	Servicio correo	5,25	6,75	6,00	6,75	5,25	M	M	M	M	M	M	M	M	M	M	M
	[S.3]	Servicio de telefonía	0,00	2,25	0,00	6,00	0,00	MB	B	MB	M	MB	M	MB	B	MB	M	MB
	[S.4]	Servicio de ficheros	5,25	6,00	6,00	5,25	5,25	M	M	M	M	M	M	M	M	M	M	M
	[S.5]	Servicio de acceso remoto	4,50	6,00	4,50	4,50	4,50	M	M	M	M	M	M	M	M	M	M	M
	[S.6]	Servicio de backup	6,00	6,75	6,00	4,50	6,00	M	M	M	M	M	M	M	M	M	M	M
Soportes de Información [M]	[M.1]	Almacenamiento CPD	0,00	9,00	4,50	9,00	0,00	MB	A	M	A	MB	A	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	0,00	7,00	3,50	7,00	0,00	MB	M	B	M	MB	A	B	A	M	A	B
	[M.3]	Memorias USB	0,00	6,00	1,50	2,00	0,00	MB	M	MB	MB	MB	A	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	0,00	0,00	1,60	9,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	0,00	0,00	1,40	6,00	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[AUX.3]	Sistemas antiincidencios	0,00	0,00	1,60	8,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
	[AUX.4]	Cableado LAN	0,00	0,00	1,20	9,00	0,00	MB	MB	MB	A	MB	A	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	0,00	0,00	0,00	6,75	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[P.2]	Personal TI	0,00	0,00	0,00	6,00	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[P.3]	Personal Proveedor TI	0,00	0,00	0,00	5,25	0,00	MB	MB	MB	M	MB	A	B	B	B	A	B
	[P.4]	Resto de personal	0,00	0,00	0,00	2,25	0,00	MB	MB	MB	B	MB	A	B	B	B	M	B

Tabla 39. Estimación de riesgos tras ejecución de proyectos

Vemos que, aunque aún existen activos con riesgos importantes, se conseguiría una disminución global de los riesgos frente a los riesgos estimados en la fase inicial, que se mostrábamos en el *apartado 4.9. Resultados* de este documento.

5.5.2 Evolución Análisis Diferencial

Por otro lado, la implantación de los proyectos propuestos deberá tener un impacto positivo en la adecuación del SGSI de RecycleSA a lo definido para los diferentes dominios que establece la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

En la siguiente tabla se muestran los controles de la ISO/IEC 27002:2013 que, de alguna manera, se verán afectados por los proyectos propuestos para su implantación.

CONTROL /PROYECTO	PRY1	PRY2	PRY3	PRY4	PRY5	PRY6	PRY7	PRY8	PRY9	PRY10
A5.1.1. Políticas de seguridad de la Información					✓					
A5.1.2 Revisión de las políticas de seguridad de la Información.					✓					
A6.2.1 Política de dispositivos móviles.				✓			✓			
A6.2.2 Teletrabajo.				✓			✓			
A9.1.1 Política de control de acceso.								✓		
A9.1.2 Acceso a las redes y a los servicios de red								✓		
A9.2.1 Registro y baja de usuario.								✓		
A9.2.2 Provisión de acceso de usuario.								✓		
A9.2.3 Gestión de privilegios de acceso.								✓		
A9.2.4 Gestión de la información secreta de autenticación de los usuarios.								✓		
A9.2.5 Revisión de los derechos de acceso de usuario.								✓		
A9.2.6 Retirada o reasignación de los derechos de acceso								✓		
A9.3.1 Uso de la información secreta de autenticación						✓	✓	✓		
A9.4.1 Restricción del acceso a la información.								✓		
A9.4.2 Procedimientos seguros de inicio de sesión.								✓		
A9.4.3 Sistema de gestión de contraseñas.								✓		
A9.4.4 Uso de utilidades con privilegios del sistema.		✓						✓		
A11.1.2 Controles físicos de entrada.			✓							
A11.2.1 Emplazamiento y protección de equipos.			✓	✓			✓			
A11.2.2 Instalaciones de suministro.			✓							
A11.2.6 Seguridad de los equipos fuera de las instalaciones		✓		✓			✓			
A12.2.1 Controles contra el código malicioso.		✓		✓						
A12.3.1 Copias de seguridad de la información.			✓							
A12.5.1 Instalación del software en explotación.		✓		✓		✓				
A12.6.1 Gestión de las vulnerabilidades técnicas.		✓		✓						
A12.6.2 Restricción en la instalación de software.		✓		✓			✓			
A13.2.1 Políticas y procedimientos de intercambio de información.						✓				
A13.2.2 Acuerdos de intercambio de información						✓				
A13.2.3 Mensajería electrónica						✓				
A13.2.4 Acuerdos de confidencialidad o no revelación						✓				
A15.1.1 Política de seguridad de la información en las relaciones con los proveedores	✓					✓				
A15.1.2 Requisitos de seguridad en contratos con terceros.	✓									
A15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones.	✓									
A15.2.1 Control y revisión de la provisión de servicios del proveedor.	✓									
A15.2.2 Gestión de cambios en la provisión del servicio del proveedor.	✓									
A16.1.1 Responsabilidades y procedimientos.	✓		✓							✓
A16.1.2 Notificación de los eventos de seguridad de la información.										✓
A16.1.3 Notificación de puntos débiles de la seguridad.										✓
A16.1.4 Evaluación y decisión sobre los eventos de seguridad de información										✓
A16.1.5 Respuesta a incidentes de seguridad de la información										✓
A16.1.6 Aprendizaje de los incidentes de seguridad de la información										✓
A16.1.7 Recopilación de evidencias										✓
A17.1.1 Planificación de la continuidad de la seguridad de la información.	✓		✓						✓	
A17.1.2 Implementar la continuidad de la seguridad de la información.	✓		✓						✓	
A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	✓		✓						✓	
A17.2.1 Disponibilidad de los recursos de tratamiento de la información	✓		✓						✓	

Tabla 40. Relación controles/proyectos

La tabla anterior refleja el impacto de la implantación de los proyectos sobre los distintos controles en diversos sentidos. Así, algunos proyectos técnicos pueden mejorar la seguridad reduciendo el riesgo, sin que, en sí mismos mejoren los controles. Los proyectos de organización y gestión (5 a 10), sin embargo, si incidirán en la implantación y/o mejora de los controles a los que afecta.

Si realizamos un análisis diferencial, como el realizado en el apartado *2.4.1. Evaluación de efectividad de los controles ISO/IEC 27002:2013* de este documento, en base a que la ejecución de los proyectos se ha realizado cumpliendo sus objetivos, obtendríamos una nueva tabla de evaluación, que se muestra en el *Anexo L. Tabla de Análisis amenazas/activos tras ejecución de Proyectos.*

Del análisis comparativo de la evaluación de efectividad inicial y la obtenida tras la implantación de los proyectos, obtenemos la siguiente tabla:

	Inicial		Tras implantación proyectos	
Controles de Seguridad de la Información	**Madurez.**	**Implantados.**	**Madurez**	**Implantados**
A5. Políticas de seguridad de la información	10%	2/2	10%	2/2
A6. Organización de la seguridad de la información	6%	3/7	64%	5/7
A7. Seguridad relativa a los recursos humanos	0%	0/6	0%	0/6
A8. Gestión de activos	13%	3/10	13%	3/10
A9. Control de acceso	38%	12/14	90%	13/14
A10. Criptografía	0%	0/2	0%	0/2
A11. Seguridad física y del entorno	1%	2/15	4%	3/15
A12. Seguridad de las operaciones	49%	13/14	54%	13/14
A13. Seguridad de las comunicaciones	43%	3/7	43%	3/7
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información	0%	0/14	0%	0/14
A15. Relación con proveedores	0%	0/5	0%	0/5
A16. Gestión de incidentes de seguridad de la información	0%	0/7	90%	7/7
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	0%	0/4	90%	4/4
A18. Cumplimiento	0%	0/7	0%	0/7

Tabla 41. Evaluación esperada de efectividad de los controles ISO/IEC 27002:2013 tras proyectos.

De igual modo, tras la implantación de los proyectos anteriores, la organización pasaría de 38 a 60 controles implantados, como se muestra en la siguiente ilustración.

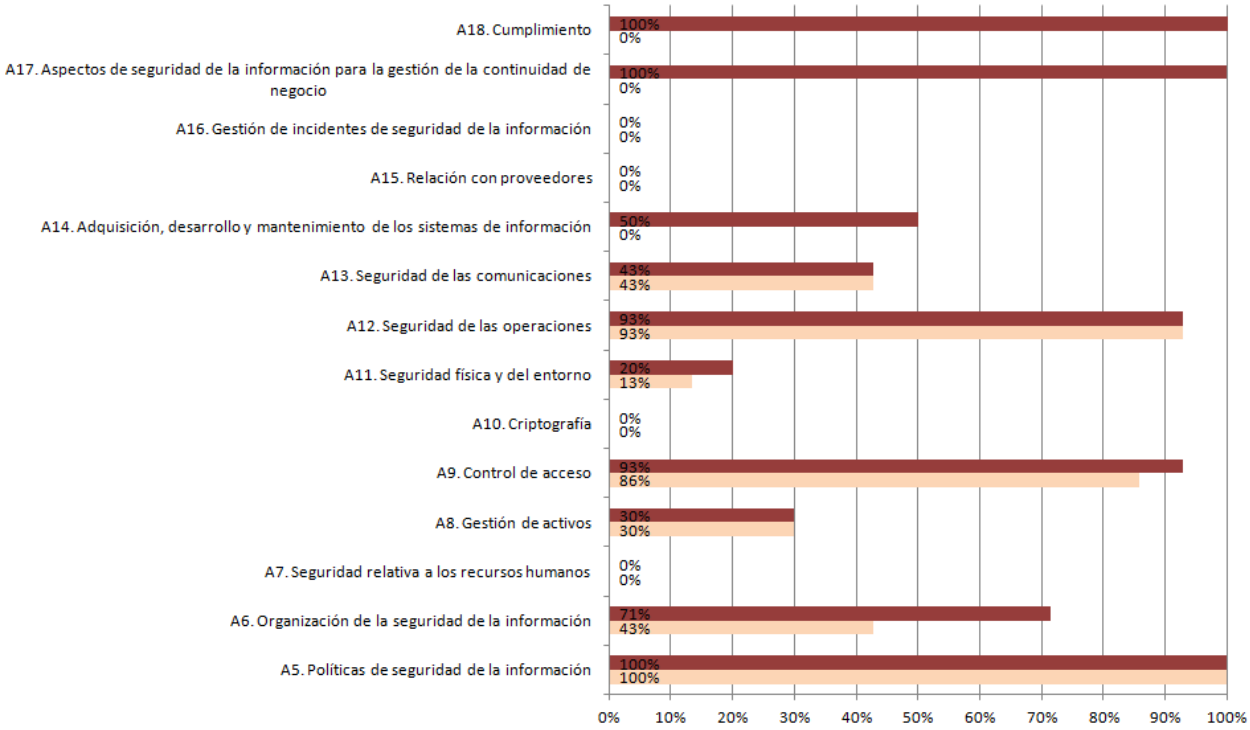

Ilustración 12. Evaluación esperada de controles ISO/IEC 27002:2013 tras proyectos

Y la madurez de los controles que se podría alcanzar tras la ejecución de estos proyectos mejoraría notablemente en algunos dominios, como se puede observar en el siguiente gráfico.

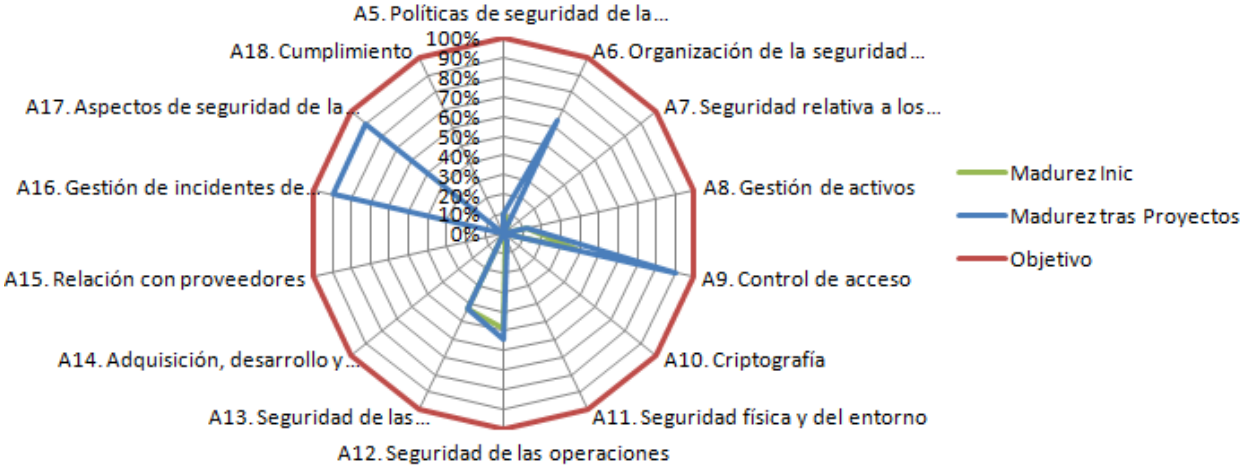

Ilustración 13. Evaluación esperada de madurez de los controles ISO/IEC 27002:2013 tras proyectos

6 AUDITORÍA DE CUMPLIMIENTO

6.1 INTRODUCCIÓN

Tras la realización de las tareas descritas en los puntos anteriores, estamos en condiciones de evaluar la seguridad actual de la organización, pues conocemos sus activos y hemos evaluado sus amenazas.

Por tanto, podemos realizar una auditoría para determinar el grado de cumplimiento de seguridad con respecto a la norma ISO/IEC 27001:2013. Este tipo de auditoría se denomina auditoría de cumplimiento.

Esta auditoría se aborda tras la ejecución de los proyectos descritos en el apartado *5. Propuestas de Proyectos* de este documento, cuyo objetivo era mitigar el riesgo inicial de la organización.

Dichos proyectos se propusieron para su realización en un marco temporal de un año, por lo que, teniendo en cuenta el estado inicial de la seguridad y la escasez de recursos de la organización, no abordaron buena parte de los elementos de seguridad que plantea ISO/IEC 27001:2013.

Por todo ello es previsible que la auditoría de cumplimiento arroje un alto número de no conformidades o incumplimientos, cuya corrección se deberá abordar en el proceso de mejora continua del SGSI que se describe en el apartado *2.1.1. ISO/IEC 27001:2013* de este documento.

Finalmente indicar que, aunque la planificación de auditorías descrito en el punto *6* del *Procedimiento de auditorías Internas (Anexo C),* indica que las auditorías internas se realizan anualmente en 2 fases sobre dominios de control diferentes, por sencillez en este TFM se muestra un único informe con el resultado global de la auditoría de cumplimiento que se incluye en el *Anexo Q. Informe de Auditoría*

El conjunto de tareas que los auditores deberán abordar para la realización de la auditoría de cumplimiento se describen el punto *5.Actividades* del *Anexo C. Procedimiento de auditorías Internas*. En este apartado simplemente describiremos con más detalle alguna de esas tareas y el resultado final obtenido.

6.2 DECLARACIÓN DE APLICABILIDAD

Como paso previo a la auditoría, es necesario realizar la declaración de aplicabilidad, que utilizarán los auditores como “guía” para saber qué controles aplican a la organización y cuáles no.

La declaración de aplicabilidad se realiza en base el análisis de los riesgos de la organización y su contexto y utiliza *la* plantilla definida en el Anexo I. Plantilla Declaración de Aplicabilidad de este documento.

Aunque los controles necesarios ya se ha definido previamente, definir la declaración de aplicabilidad es importante porque, como se indica en [13]:

- Debe indicar qué controles son necesarios no sólo en función de los riesgos, sino también por otros motivos, como legales, contractuales, etc.
- Es un documento breve, que permite ser actualizado fácilmente y presentado a la gerencia.
- Debe indicar si cada control aplicable está ya implementado o no.

El resultado obtenido se muestra en el *Anexo N. Declaración aplicabilidad* de este documento.

6.3 REVISIÓN DE REQUERIMIENTOS ISO/IEC 27001:2013

Para la realización de la auditoría, se revisan todos los requerimientos que establece la norma ISO/IEC 27001:2013, que se detallan en los puntos 4 a 10 de la norma.

En el *Anexo O. Cumplimiento Requerimientos ISO/IEC 27001:2013* de este documento se muestra la tabla final resultante de dicho análisis en la que, para cada requerimiento, se ha codificado su cumplimiento con los siguientes criterios:

Código	Valor	Descripción
OK	Cumplimiento	Cumplimiento de los requisitos normativos
NC-	No Conformidad Menor	Desviación minima en relación a los requisitos normativos que no afecta a la eficienca e integraidad del Sistema de Gestión
NC+	No Conformidad Mayor	Incumplimiento de un requisito normativo que vulnera o pone en serio riesgo la integriad del sistema de Gestión

Tabla 42. Codificación de cumplimiento y no conformidades.

Para cada requerimiento se justifica, en el campo comentarios, la razón que ha determinado la evaluación realizada por el auditor.

6.4 REVISIÓN DE CUMPLIMIENTO DE LOS CONTROLES

Adicionalmente, se revisan todos los controles definidos en la declaración de aplicabilidad y se evalúa su cumplimiento conforme a la norma.

En el *Anexo P. Cumplimiento controles* de este documento se muestra la tabla final resultante de dicho análisis en la que, para cada control, se ha codificado su cumplimiento de acuerdo a los criterios establecidos anteriormente en la Tabla 42. Codificación de cumplimiento y no conformidades.

Para cada control se justifica, en el campo comentarios, la razón que ha determinado la evaluación realizada por el auditor.

6.5 INFORME DE AUDITORÍA

Una vez auditada toda la documentación del SGSI y los controles que establece la norma, se redacta el informe de auditoría, que debe mostrar, como resultados principales:

- Hallazgos de auditoría: No conformidades, ya sean mayores o menores.
- Posibles Mejoras

Igualmente debe mostrarla planificación prevista para la próxima auditoría.

Una vez finalizado, el informe de auditoría se entrega al Responsable de Seguridad del SGSI.

En el Anexo Q. Informe de Auditoría se muestra el informe de auditoría resultante de la realización de la auditoría de cumplimento en RecycleSA.

7 CONCLUSIONES Y PRESENTACIÓN DE RESULTADOS

7.1 INTRODUCCIÓN

Tras la realización de las tareas encaminadas a la puesta en marcha del SGSI y la realización de la auditoría de cumplimento, es el momento de extraer conclusiones, identificando los objetivos conseguidos y los puntos pendientes a desarrollar.

Los resultados obtenidos se presentarán mediante la generación y entrega de los documentos a la Dirección de la organización, de manera que les permitirá conocer el estado de la seguridad de la organización que dirigen y las acciones necesarias para mejorarla.

7.2 CONCLUSIONES

Como evidencia el análisis diferencial realizado al inicio de este proyecto, la organización, aunque contaba con múltiples controles de seguridad específicos, no se englobaban en un SGSI que involucrara a todos sus estamentos, ni disponía de buena parte de los mecanismos formales que se deben contemplar un sistema de gestión de la seguridad de la información.

Tras la realización de todas las actividades descritas en este proyecto, se puede concluir que su objetivo principal, que es la puerta en marcha efectiva del SGSI, de manera que la seguridad se tenga en cuenta en todos los procesos de la organización y, por tanto, mejorar la seguridad global de la organización, ha sido plenamente conseguido.

La implementación del SGSI de RecycleSA se ha realizado siguiendo las directrices de la norma ISO/IEC 27001:2013 y el código de buenas prácticas que describe la norma ISO/IEC 27002:2013, que establece una serie de puntos a desarrollar y cumplir. Buena parte de esos puntos se han alcanzado, pero como muestra la auditoría de cumplimiento realizada, es necesario desarrollar algunos puntos que aún no se han contemplador.

A continuación mostramos los objetivos concretos conseguidos y los aspectos pendientes de desarrollar.

7.2.1 OBJETIVOS ALCANZADOS

Entre los objetivos concretos alcanzados podemos indicar:

- Se ha definido y puesto en marcha un SGSI del que carecía inicialmente la organización.
- Se ha definido y desarrollado el esquema documental necesario para sustentar el SGSI.
- Se ha definido la metodología y se ha realizado el análisis de riesgos necesario para evaluar las amenazas que afectan a los distintos activos de la organización.
- Se han definido y ejecutado diversos proyectos, tanto tecnológicos como organizativos y de gestión, que han permitido mejorar la seguridad global de la organización.
- Se ha mejorado la formación y concienciación de todos los empleados de la organización, lo que a su vez contribuye a disminuir los riesgos y mejorar la seguridad de la organización.
- Se han definido los roles y las responsabilidades relativas a la seguridad de la información.
- Se ha definido los indicadores que permitirán evaluar el cumplimiento de los controles de seguridad definidos.

7.2.2 ASPECTOS PENDIENTES: SIGUIENTES PASOS

A pesar de lo indicado en el párrafo anterior, aún quedan aspectos importantes a mejorar, como refleja la auditoría de cumplimiento realizada. En este sentido, es necesario avanzar en el desarrollo del SGSI en los siguientes aspectos:

- Definir e implementar la política de seguridad de proveedores. Su definición y desarrollo permitirá cumplir con los controles relativos al dominio *A15.Relación con proveedores* actualmente inexistentes.
- Definir e implementar procedimientos para la correcta gestión de la seguridad desde el punto de vista de los recursos humanos. Su definición y desarrollo permitirá que el SGSI cumpla con los controles relativos al *dominio A7. Seguridad relativa a los recursos humanos*.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información: recursos humanos, TI, etc.
- Identificar las distintas áreas físicas y clasificarlas en función de sus necesidades en cuanto a la seguridad. Definir procedimientos de identificación y acceso en base a la clasificación realizada.
- Definir e implementar procedimientos para la autorización de retirada de materiales de las oficinas.

Adicionalmente, no se debe olvidar que todo SGSI se debe contemplar bajo un modelo de mejora continua, de manera que se debe revisar y evaluar periódicamente y, cuando se detecten deficiencias, se deberán tomar las medidas correctoras que garanticen la seguridad y protección de la información.

7.3 PRESENTACIÓN DE RESULTADOS

Como resultado de este trabajo de Fin de Máster se han generado los siguientes entregables:

- Este documento con la **memoria del proyecto.** Incluye todos los anexos referenciados en la memoria.
- **Resumen ejecutivo.** Documento adicional en el que se muestran las principales conclusiones del proyecto.
- **Presentación a la dirección**. Documento adicional, en formato en formato PPT, en el que se incluyen conceptos de seguridad con el objetivo de concienciar y sensibilizar al personal en materia de seguridad de la información.
- Presentación con el resumen del **estado de los proyectos** propuestos en el *punto 5. Propuestas de Proyectos* de este documento.
- **Video de presentación del proyecto**, dirigido al tribunal del TFM. Describe las distintas etapas y el proceso llevado a cabo para la realización de este Trabajo Fin de Máster.

8 TÉRMINOS Y DEFINICIONES

A continuación se definen algunos términos, en orden alfabético, que se utilizan en este trabajo.

Activo	Es cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección.
Amenaza.	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
CSI	Comité de Seguridad de la Información
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
ISO/IEC	Comité de Seguridad de la Información
PDCA.	Ciclo de Deming. Indica Plan (planear) – Do (hacer) – Check (comprobar) – Act (actuar).
RGPD	El Reglamento General de Protección de Datos es un sistema regulador a nivel europeo cuya finalidad es proteger y controlar el tratamiento de los datos personales que las empresas y organizaciones llevan a cabo en favor de los derechos fundamentales de las personas. Su fin es prevenir que dichos datos puedan usarse de forma que vulneren la intimidad y la libertad de las personas o que se puedan usar con fines criminales. [13]
Riesgo	Probabilidad de que una amenaza determinada se materialice produciendo un impacto negativo sobre los activos
RSI	Responsable de Seguridad de la Información.
Salvaguarda	Procedimiento o mecanismo tecnológicos que reduce el riesgo.
Seguridad de la Información	Es el conjunto de medidas preventivas y reactivas que permite resguardar y proteger la información. Se ocupa de la información en todas sus formas (oral, impresa, electrónica,…), a diferencia de la seguridad informática, que se ocupa únicamente de la seguridad de los sistemas de información.
SGSI	Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. [14]
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

9 REFERENCIAS Y BIBLIOGRAFÍA

[1] UOC, «Manual Asignatura "Sistemas de Gestión de la Seguridad de la Información",» *MISTIC.*

[2] UOC, «Máster Interuniversitario en Seguridad de las TIC (MISTIC),» *http://estudios.uoc.edu/es/masters-universitarios/seguridad-tecnologias-informacion-comunicaciones/presentacion.*

[3] «https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/».

[4] «Política de Seguridad ISO 27001,» *https://isowin.org/blog/politica-seguridad-ISO-27001/.*

[5] «Política de seguridad en la nomra ISO 27001,» *https://www.pmg-ssi.com/2016/06/que-debe-incluir-en-su-politica-de-seguridad-de-la-informacion-basado-en-la-norma-iso-27001/.*

[6] UOC, «Manual de la asitnatura "Auditoria técnica y de certificación"».

[7] «https://www.pmg-ssi.com/2017/09/iso-27001-mejorar-las-auditorias-internas-sgssi/».

[8] ISOTOOLS, «https://www.isotools.com.mx/cuales-las-cualidades-auditor-iso-27001/».

[9] «MAGERIT,» *https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8ixx2gzaM-.*

[10] «MAGERIT - Libro I- Método,» *https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pd.*

[11] «MAGERIT - Libro II - Catálogo de elementos,» *https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf.*

[12] «MAGERIT - Libro III - Guía de Técnicas,» *https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e17-9cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf.*

[13] «https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/».

[14] «RGPD: Reglamento General de Protección de Datos,» *https://www.boe.es/doue/2016/119/L00001-00088.pdf.*

[15] «El portal de ISO 27001 en Español,» *http://www.iso27000.es/.*

[16] rgpd.es, «Reglamento General de Protección de Datos,» *https://rgpd.es/.*

10 ANEXOS

Anexo A. EFECTIVIDAD DE LOS CONTROLES ISO/IEC 27002:2013

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A5	**Políticas de seguridad de la información**		**10%**
A5.1	**Directrices de gestión de la seguridad de la información**		**10%**
A5.1.1	Políticas para la seguridad de la información	L1 - Inicial	10%
A5.1.2	Revisión de las políticas para la seguridad de la información	L1 - Inicial	10%
A6	**Organización de la seguridad de la información**		**6%**
A6.1	**Organización interna**		**2,00%**
A6.1.1	Roles y responsabilidades en seguridad de la información	L1 - Inicial	10%
A6.1.2	Segregación de tareas	L0 - Inexistente	0%
A6.1.3	Contacto con las autoridades	L0 - Inexistente	0%
A6.1.4	Contacto con grupos de interés especial	L0 - Inexistente	0%
A6.1.5	Seguridad de la información en la gestión de proyectos	L0 - Inexistente	0%
A6.2	**Los dispositivos móviles y el teletrabajo**		**10%**
A6.2.1	Política de dispositivos móviles	L1 - Inicial	10%
A6.2.2	Teletrabajo	L1 - Inicial	10%
A7	**Seguridad relativa a los recursos humanos**		**0%**
A7.1	**Antes del empleo**		**0%**
A7.1.1	Investigación de antecedentes	L0 - Inexistente	0%
A7.1.2	Términos y condiciones del empleo	L0 - Inexistente	0%
A7.2	**Durante el empleo**		**0%**
A7.2.1	Responsabilidades de gestión	L0 - Inexistente	0%
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	L0 - Inexistente	0%
A7.2.3	Proceso disciplinario	L0 - Inexistente	0%
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		**0%**
A7.3.1	Responsabilidades ante la finalización o cambio	L0 - Inexistente	0%
A8	**Gestión de activos**		**13%**
A8.1	**Responsabilidad sobre los activos**		**38%**
A8.1.1	Inventario de activos	L3 - Definido	90%
A8.1.2	Propiedad de los activos	L1 - Inicial	10%
A8.1.3	Uso aceptable de los activos	L0 - Inexistente	0%
A8.1.4	Devolución de activos	L2 - Repetible	50%
A8.2	**Clasificación de la información**		**0%**
A8.2.1	Clasificación de la información	L0 - Inexistente	0%
A8.2.2	Etiquetado de la información	L0 - Inexistente	0%
A8.2.3	Manipulado de la información	L0 - Inexistente	0%
A8.3	**Manipulación de los soportes**		**0%**
A8.3.1	Gestión de soportes extraíbles	L0 - Inexistente	0%
A8.3.2	Eliminación de soportes	L0 - Inexistente	0%
A8.3.3	Soportes físicos en tránsito	No Aplica	#N/A

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A9	**Control de acceso**		**38,13%**
A9.1	**Requisitos de negocio para el control de acceso**		**45%**
A9.1.1	Política de control de acceso	L0 - Inexistente	0%
A9.1.2	Acceso a las redes y a los servicios de red	L3 - Definido	90%
A9.2	**Gestión de acceso de usuario**		**50%**
A9.2.1	Registro y baja de usuario	L3 - Definido	90%
A9.2.2	Provisión de acceso de usuario	L3 - Definido	90%
A9.2.3	Gestión de privilegios de acceso	L2 - Repetible	50%
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	L1 - Inicial	10%
A9.2.5	Revisión de los derechos de acceso de usuario	L1 - Inicial	10%
A9.2.6	Retirada o reasignación de los derechos de acceso	L2 - Repetible	50%
A9.3	**Responsabilidades del usuario**		**10%**
A9.3.1	Uso de la información secreta de autenticación	L1 - Inicial	10%
A9.4	**Control de acceso a sistemas y aplicaciones**		**48%**
A9.4.1	Restricción del acceso a la información	L2 - Repetible	50%
A9.4.2	Procedimientos seguros de inicio de sesión	L2 - Repetible	50%
A9.4.3	Sistema de gestión de contraseñas	L3 - Definido	90%
A9.4.4	Uso de utilidades con privilegios del sistema	L0 - Inexistente	0%
A9.4.5	Control de acceso al código fuente de los programas	No Aplica	#N/A
A10	**Criptografía**		**0%**
A10.1	**Controles criptográficos**		**0%**
A10.1.1	Política de uso de los controles criptográficos	L0 - Inexistente	0%
A10.1.2	Gestión de claves	L0 - Inexistente	0%
A11	**Seguridad física y del entorno**		**1%**
A11.1	**Áreas seguras**		**0%**
A11.1.1	Perímetro de seguridad física	L0 - Inexistente	0%
A11.1.2	Controles físicos de entrada	L0 - Inexistente	0%
A11.1.3	Seguridad de oficinas, despachos y recursos	L0 - Inexistente	0%
A11.1.4	Protección contra las amenazas externas y ambientales	L0 - Inexistente	0%
A11.1.5	El trabajo en áreas seguras	L0 - Inexistente	0%
A11.1.6	Áreas de carga y descarga	L0 - Inexistente	0%
A11.2	**Seguridad de los equipos**		**2%**
A11.2.1	Emplazamiento y protección de equipos	L0 - Inexistente	0%
A11.2.2	Instalaciones de suministro	L0 - Inexistente	0%
A11.2.3	Seguridad del cableado	L0 - Inexistente	0%
A11.2.4	Mantenimiento de los equipos	L0 - Inexistente	0%
A11.2.5	Retirada de materiales propiedad de la empresa	L0 - Inexistente	0%
A11.2.6	Seguridad de los equipos fuera de las instalaciones	L1 - Inicial	10%
A11.2.7	Reutilización o eliminación segura de equipos	L0 - Inexistente	0%
A11.2.8	Equipo de usuario desatendido	L1 - Inicial	10%
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A12	**Seguridad de las operaciones**		**49%**
A12.1	**Procedimientos y responsabilidades operacionales**		**40%**
A12.1.1	Documentación de procedimientos operacionales	L3 - Definido	90%
A12.1.2	Gestión de cambios	L1 - Inicial	10%
A12.1.3	Gestión de capacidades	L1 - Inicial	10%
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	L2 - Repetible	50%
A12.2	**Protección contra el software malicioso (malware)**		**95%**
A12.2.1	Controles contra el código malicioso	L4 - Gestionado	95%
A12.3	**Copias de seguridad**		**95%**
A12.3.1	Copias de seguridad de la información	L4 - Gestionado	95%
A12.4	**Registros y supervisión**		**50%**
A12.4.1	Registro de eventos	L3 - Definido	90%
A12.4.2	Protección de la información del registro	L1 - Inicial	10%
A12.4.3	Registros de administración y operación	L1 - Inicial	10%
A12.4.4	Sincronización del reloj	L3 - Definido	90%
A12.5	**Control del software en explotación**		**10%**
A12.5.1	Instalación del software en explotación	L1 - Inicial	10%
A12.6	**Gestión de la vulnerabilidad técnica**		**50%**
A12.6.1	Gestión de las vulnerabilidades técnicas	L3 - Definido	90%
A12.6.2	Restricción en la instalación de software	L1 - Inicial	10%
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		**0%**
A12.7.1	Controles de auditoría de sistemas de información	L0 - Inexistente	0%
A13	**Seguridad de las comunicaciones**		**43%**
A13.1	**Gestión de la seguridad de las redes**		**63%**
A13.1.1	Controles de red	L4 - Gestionado	95%
A13.1.2	Seguridad de los servicios de red	L0 - Inexistente	0%
A13.1.3	Segregación en redes	L4 - Gestionado	95%
A13.2	**Intercambio de información**		**23%**
A13.2.1	Políticas y procedimientos de intercambio de información	L0 - Inexistente	0%
A13.2.2	Acuerdos de intercambio de información	L0 - Inexistente	0%
A13.2.3	Mensajería electrónica	L3 - Definido	90%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		**0%**
A14.1	**Requisitos de seguridad en los sistemas de información**		**0%**
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	L0 - Inexistente	0%
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	L0 - Inexistente	0%
A14.1.3	Protección de las transacciones de servicios de aplicaciones	L0 - Inexistente	0%
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		**0%**
A14.2.1	Política de desarrollo seguro	L0 - Inexistente	0%
A14.2.2	Procedimiento de control de cambios en sistemas	L0 - Inexistente	0%
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0 - Inexistente	0%
A14.2.4	Restricciones a los cambios en los paquetes de software	L0 - Inexistente	0%
A14.2.5	Principios de ingeniería de sistemas seguros	L0 - Inexistente	0%
A14.2.6	Entorno de desarrollo seguro	L0 - Inexistente	0%
A14.2.7	Externalización del desarrollo de software	L0 - Inexistente	0%
A14.2.8	Pruebas funcionales de seguridad de sistemas	L0 - Inexistente	0%
A14.2.9	Pruebas de aceptación de sistemas	L0 - Inexistente	0%
A14.3	**Datos de prueba**		**0%**
A14.3.1	Protección de los datos de prueba	L0 - Inexistente	0%
A15	**Relación con proveedores**		**0%**
A15.1	**Seguridad en las relaciones con proveedores**		**0%**
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	L0 - Inexistente	0%
A15.1.2	Requisitos de seguridad en contratos con terceros	L0 - Inexistente	0%
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	L0 - Inexistente	0%
A15.2	**Gestión de la provisión de servicios del proveedor**		**0%**
A15.2.1	Control y revisión de la provisión de servicios del proveedor	L0 - Inexistente	0%
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A16	**Gestión de incidentes de seguridad de la información**		**0%**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		**0%**
A16.1.1	Responsabilidades y procedimientos	L0 - Inexistente	0%
A16.1.2	Notificación de los eventos de seguridad de la información	L0 - Inexistente	0%
A16.1.3	Notificación de puntos débiles de la seguridad	L0 - Inexistente	0%
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	L0 - Inexistente	0%
A16.1.5	Respuesta a incidentes de seguridad de la información	L0 - Inexistente	0%
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	L0 - Inexistente	0%
A16.1.7	Recopilación de evidencias	L0 - Inexistente	0%
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		**0%**
A17.1	**Continuidad de la seguridad de la información**		**0%**
A17.1.1	Planificación de la continuidad de la seguridad de la información	L0 - Inexistente	0%
A17.1.2	Implementar la continuidad de la seguridad de la información	L0 - Inexistente	0%
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L0 - Inexistente	0%
A17.2	**Redundancias**		**0%**
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	L0 - Inexistente	0%
A18	**Cumplimiento**		**0%**
A18.1	**Cumplimiento de los requisitos legales y contractuales**		**0%**
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	L0 - Inexistente	0%
A18.1.2	Derechos de Propiedad Intelectual (DPI)	L0 - Inexistente	0%
A18.1.3	Protección de los registros de la organización	L0 - Inexistente	0%
A18.1.4	Protección y privacidad de la información de carácter personal	L0 - Inexistente	0%
A18.1.5	Regulación de los controles criptográficos	L0 - Inexistente	0%
A18.2	**Revisiones de la seguridad de la información**		**0%**
A18.2.1	Revisión independiente de la seguridad de la información	L0 - Inexistente	0%
A18.2.2	Cumplimiento de las políticas y normas de seguridad	L0 - Inexistente	0%
A18.2.3	Comprobación del cumplimiento técnico	L0 - Inexistente	0%

Anexo B. POLÍTICA DE SEGURIDAD

1. OBJETO.

El objeto de este documento es establecer la política de seguridad de la información en RecycleSA, así como su marco organizativo.

2. ALCANCE

Esta Política de Seguridad aplica a todo el ámbito organizativo de RecycleSA, a sus recursos humanos y técnicos y a la totalidad de los procesos, ya sean internos o externos vinculados a la organización a través de contratos o acuerdos con terceros.

3. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Son objetivos de la política de seguridad de la información:

a) Garantizar la seguridad de la información, proteger los activos o recursos de información.

b) Crear la estructura de organización de la seguridad de la RecycleSA.

c) Marcar las directrices, los objetivos y los principios básicos de seguridad de la información de la organización.

d) Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad de la información.

4. COMPROMISO

La Dirección de RecycleSA contempla la información como un activo vital para la organización, por lo que expresa su máximo compromiso y exigencia para su protección de acuerdo con su valor y sensibilidad, por lo que velará por el mantenimiento de su confidencialidad, integridad y disponibilidad independientemente de los medios en los que se encuentre.

Desde la dirección, se dará cumplimiento a todas las regulaciones, leyes y normativas vigentes relacionadas con Seguridad de la Información, igualmente se signarán los recursos requeridos para la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

Se realizará una evaluación periódicamente el estado general del Sistema de Gestión de Seguridad de la Información, por parte del Comité de Seguridad de la Información relativa a los principales riesgos identificados, haciéndose un seguimiento detallado a los correspondientes planes de acción.

5. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los principios que conforman la Política de Seguridad de la Información de RecycleSA son los siguientes:

- La información que posee RecycleSA, tiene un valor muy importante y, por lo tanto, es primordial protegerla. Toda la información se considerará confidencial hasta el momento en el que se haga pública por los canales oficiales.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.

- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tienen acceso a la información de la RecycleSA deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se puedan producir en ella.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importante el Reglamento General de Protección de Datos (RGPD)[14]

6. ESTRUCTURA ORGANIZATIVA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información afecta y es responsabilidad de todos los miembros de RecycleSA.

Para su correcta gestión se han establecido una estructura organizativa que comprende diversos de los comités, así como los roles necesarios junto con sus responsabilidades.

La siguiente figura muestra la estructura organizativa de RecycleSA.

Nivel	Órgano/Departamento	Aportación/Implicación	Miembros
Estratégico	Comité de Dirección	Visión estratégica Aportación de recursos	▪ CEO. ▪ Director Financiero. ▪ Director Servicios de Reciclaje de Acero. ▪ Director Servicios de Reciclaje de Aluminio. ▪ Director Tecnologías de la Información.
Táctico	Comité de Seguridad de la Información	Liderazgo Gestión del riesto Comunicación	▪ CEO. ▪ Director Financiero. ▪ Director Servicios de Reciclaje de Acero. ▪ Director Servicios de Reciclaje de Aluminio. ▪ Director Tecnologías de la Información. ▪ Responsable de Seguridad. ▪ Posibles invitados según temática.
Operativo	Responsable de Seguridad de la Información	Coordinación y Gestión Lenguaje común	▪ Responsable de Seguridad.
	Departamento de Tecnologías de la Información	Implanta en los SI los controles de seguridad	▪ Director de Tecnologías de la Información. ▪ Service Managers. ▪ Proveedores de servicio de TI.
	Recursos Humanos	Informa sobre los cambios de personal y aplica procedimientos disciplianarios	▪ Personal del departamento de Recursos Humanos.
	Legal	Colabora en definición de normas y políticas	▪ Personal del departamento de Legal.
	Personal general	Confidencialidad y uso adecuado de los recursos	▪ Personal de la organización ▪ Personal de proveedores de servicios con acces a información de la organización

Figura 1. Estructura organizativa de la Seguridad de la Información de RecycleSA

7. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información deben ser revisados a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.

Para ello, el Comité de Seguridad propondrá la realización de revisiones sobre la vigencia e implementación de la Política de Seguridad de la Información con el objetivo de garantizar que las prácticas en la RecycleSA reflejan adecuadamente sus disposiciones.

La revisión de las políticas de seguridad de la información debe tener en cuenta las *Revisiones por la Dirección*, por lo que se planificarán para su realización anual tras ésta.

8. OBLIGACIONES DEL PERSONAL

Todo el personal de la RecycleSA tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todos.

El canal de comunicación principal que utilizará el Comité de Seguridad para transmitir dicha información a todos los empleados de la RecycleSA será su Intranet.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

9. FORMACIÓN Y CONCIENCIACIÓN

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal y a todas las actividades de acuerdo al principio de seguridad integral. A estos efectos, la RecycleSA, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

El Comité de Seguridad de la Información aprobará una Política de formación y concienciación en el tratamiento seguro de la información con los siguientes objetivos:

a) Formación sobre la Protección de la información de carácter personal, orientada hacia los responsables de los ficheros y hacia los usuarios con privilegios sobre los datos

c) Formación genérica sobre Seguridad de la Información (aplicación de las normas ISO 27002/27001)

d) De prevención de amenazas. Todos los usuarios deben recibir (o tener disponible para consulta en la Intranet) una guía de seguridad que contenga pautas de concienciación sobre los riesgos del uso de la tecnología, cómo detectar una anomalía de seguridad o comportamiento sospechoso de un sistema y cómo reportar los incidentes de seguridad.

Anexo C. PROCEDIMIENTO DE AUDITORÍAS INTERNAS

1. OBJETO.

El presente documento recoge la metodología que debe llevarse a cabo para realizar la auditoría interna del SGSI de RecycleSA, según los requisitos que establece la norma ISO/IEC 27001:2013.

2. ALCANCE

Este procedimiento es de aplicación a todas las auditorías internas que se realicen en RecycleSA en el marco de los procesos de evaluación del desempeño del SGSI.

3. RESPONSABILIDADES

Los auditores internos juegan un papel fundamental en la gestión y control del SGSI, por lo que es fundamental garantizar su imparcialidad en el proceso de auditoría. Por ello el Comité de Seguridad de la información que se encargará de elegir el personal interno que se encargará de realizar estas auditorías deberá tener cuenta:

El Responsable de Seguridad deberá:

- Lanzar la auditoría interna.
- Determinar la viabilidad de la auditoría.
- Designar al auditor interno que se ocupará de llevar a cabo la auditoría. Si es necesario, se pueden designar varios auditores, ejerciendo uno de ellos de auditor jefe para coordinar el trabajo de auditoría.
- Proporcionar al auditor interno designado aquellos recursos (tanto materiales como de tiempo) que le sean necesarios para llevar a cabo esta actividad.
- Acreditar al auditor como una persona autorizada para tener acceso a las evidencias pertinentes.
- Evaluar el trabajo del auditor.
- En aquellas áreas auditadas en las que se hayan detectado no conformidades o acciones de mejora, informará al responsable para que lleve a cabo las acciones recomendadas por el auditor Interno y ratificadas por él mismo.

El Auditor Interno por su parte deberá:

- Cumplir con los requisitos definidos en este documento en el apartado 4.
- Llevar a cabo las actividades definidas en este documento en el apartado 5.

4. PERFIL AUDITORES INTERNOS

Los auditores internos juegan un papel fundamental en la gestión y control del SGSI, por lo que es fundamental garantizar su imparcialidad en el proceso de auditoría. Por ello Responsable de Seguridad de la información, que se encargará de elegir el personal interno que se encargará de realizar estas auditorías, deberá tener cuenta:

Requisitos

- Independencia.
- Es absolutamente necesario garantizar la independencia de los auditores internos, de manera que no deben tener ninguna responsabilidad sobre la implantación y gestión del SGSI que se auditará.
- Formación.

- Es necesaria la formación reglada de los auditores en los principios de auditoría y en la norma ISO/IEC 27001.
- Para facilitar los conocimientos necesarios se puede responsabilizar a un auditor con estudios y conocimientos de TI, de los procesos orientados a TI (control de acceso, criptografía, seguridad de las comunicaciones, etc.) frente a un auditor sin dichos conocimientos para responsabilizarse de los procesos más generales (políticas de seguridad, organización, seguridad de los recursos humanos, etc.).

Habilidades y Capacidades

- Se imparcial, sincero y honesto
- Ser discreto y comprender el concepto de confidencialidad
- Mantener la mente abierta para considerar las ideas y los punto de vista alternativos
- Ser diplomático y saber tratar con las personas
- Ser firme. Es muy importante, ya que durante la auditoría no debe negociar con el auditado sobre la inclusión o eliminación de una determinada no conformidad en el informe final ya que, de esta forma, se desvirtúa la eficiencia que puede tener la auditoría. Aunque se lleve a cabo de forma responsable y ética, algunas decisiones pueden no ser admitidas por las personas de la organización. Todo esto puede generar desacuerdos y confrontaciones que no deben llevar a la negociación para la aceptación del informe.
- Tener la alta capacidad de observación.
- Tener el instinto de ser consciente y comprender todas las situaciones.
- Es necesario que se adapte de forma fácil a todos los contextos.
- Estar orientado a conseguir los objetivos.
- Obtener conclusiones de razonamientos lógicos y analizar las distintas evidencias.
- Estar seguro de uno mismo.
- No contar con prejuicios que eliminen su objetividad.

5. ACTIVIDADES

El auditor Interno debe llevar a cabo las siguientes actividades:

1. **Planificación de la auditoría:** Se debe identificar a los responsables con quienes se deben llevar a cabo entrevistas. Establecer con ellos la fecha, hora y lugar de cada entrevista.
2. **Preparación documental:** Preparación de los documentos de trabajo.
3. **Revisión las auditorías previas:** Se debe comprobar:
   a. Que se están realizando con la periodicidad establecida.
   b. Que, en caso de que se hubieran detectado no conformidades, éstas han sido subsanadas.
4. **Auditoría del sistema de gestión:** Se debe auditar la documentación del SGSI para comprobar su cumplimiento con la ISO 27001. Identificar si esta norma ISO ha sido actualizada.
5. **Auditoría de los controles:** Se debe auditar los objetivos de control para comprobar su nivel de cumplimiento con la ISO 27002:2013. Identificar si esta norma ISO ha sido actualizada. Como parte de la auditoría de los controles se incluye la auditoria de cumplimiento de la legislación aplicable.
6. **Comprobación de que se cumplen los procedimientos:** Se debe verificar que se cumplen los procedimientos establecidos. Para ello se realizará un muestreo simple sobre algún

procedimiento y se obtendrá evidencia de su cumplimiento.

7. **Redacción del informe:** Conforme al modelo que se describe en el apartado 7 de este documento.
8. **Entrega del informe:** Entregar el informe de la auditoría interna al Responsable de Seguridad del SGSI.
9. **Oportunidades de mejora:** Reflejar qué oportunidades de mejora se han detectado y enumerar las actividades para llevarlas a cabo.

6. PLANIFICACIÓN

Las auditorías internas deberán realizarse una vez al año, preferentemente en el primer semestre de cada año, a no ser que la anterior auditoría interna haya recomendado un plazo inferior.

Para facilitar su ejecución por parte de dos auditores internos, con cualificaciones técnicas distintas, tal como se indica en el apartado 4 de este documento, se plantea su realización en dos fases diferenciadas:

- Fase 1. Primer trimestre. Auditoría de **procesos generales**.

  Se auditarán los controles correspondientes a procesos más generales, que corresponden a los siguientes dominios de la ISO/IEC 27002:2013:

  - 5 Políticas de seguridad de la información.
  - 6 Organización de la seguridad de la información.
  - 7 Seguridad de los recursos humanos.
  - 8 Gestión de activos.
  - 15 Relaciones de proveedores.
  - 16 Gestión de incidentes de seguridad de la información.
  - 17 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
  - 18 Cumplimiento.

- Fase 2. Segundo trimestre. Auditoría de **procesos orientados a IT.**

  Se auditarán los controles correspondientes a procesos orientados a IT y que requieren de conocimientos en esta materia del auditor designado. Es decir:

  - 9 Control de acceso.
  - 10 Criptografía.
  - 11 Seguridad física y medioambiental.
  - 12 Seguridad operacional.
  - 13 Seguridad de las comunicaciones.
  - 14 Adquisición, desarrollo y mantenimiento del sistema.

7. MODELO DE INFORME DE AUDITORÍA

El informe de auditoría debe incluir los siguientes elementos:

1. **Alcance:** Indicar el alcance del SGSI.
2. **Criterios considerados:** Indicar los estándares y legislación empleada como elementos de juicio así como las consideraciones para su medición.
3. **Equipo auditor:** Indicar los integrantes del equipo auditor y su perfil.
4. **Fecha de realización:** Indicar el periodo en el que se ha realizado la auditoría.
5. **Lugar de realización:** Indicar la ubicación o ubicaciones donde se ha llevado a cabo la auditoría.
6. **Idioma de la auditoría**: Indicar el idioma en el que se han llevado a cabo las entrevistas.
7. **Plan de auditoría**: Indicar la planificación que se estableció.
8. **Registros de auditoría:** Indicar qué documentación se ha utilizado para su análisis, así como el personal entrevistado.
9. **Resultado de la auditoría:** Indicar si el SGSI funciona como se espera, distinguiendo entre:
   - No conformidades: pueden ser no conformidades mayores (incumplimiento de requisitos de la norma ISO/IEC 27001:2013 que impedirían la certificación del SGSI de no ser resueltas) o no conformidades leves. Ambas se resuelven mediante acciones correctivas.
   - Posibles no conformidades: indican el riesgo de un potencial incumplimiento. Se resuelven mediante acciones preventivas.
   - Mejoras: para aquellos aspectos que no suponen incumplimiento, el auditor fijará un criterio mínimo aconsejable de nivel de cumplimiento y las acciones de mejora recomendadas para alcanzar dicho nivel.
10. **Planificación de la futura auditoría**: Indicarle al Responsable de Seguridad, basándose en la planificación de auditorías establecida y a la fecha de finalización de esta auditoría, en qué fecha debe llevarse a cabo la siguiente auditoría interna del SGSI.

Anexo D. GESTIÓN DE INDICADORES

La siguiente tabla muestra los indicadores que se han definido para medir la eficacia de los controles de seguridad implantados en RecycleSA.

A5	**Políticas de seguridad de la información**
A5.1	**Directrices de gestión de la seguridad de la información**
Indicador	**Revisiones de la política por parte de la dirección**
Control asociado	A5.1.2 Políticas para la seguridad de la información
Descripción	Revisión de las políticas por parte de la dirección
Frecuencia	Anual
Fórmula de medición	Número de Revisiones de la política por parte de la dirección
Unidad de medida	Número de revisioness anuales
Valor objetivo	1
Valor Umbral	1
A6	**Organización de la seguridad de la información**
A6.1	**Organización interna**
Indicador	**Asignación de roles**
Control asociado	A6.1.1 Roles y responsabilidades en seguridad de la información
Descripción	Verificación de que todos los roles y responsabilidades están asignados
Frecuencia	Anual
Fórmula de medición	Número de roles asignados / Número de roles definidos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
Indicador	**Segregación de tareas**
Control asociado	A6.1.2 Segregación de tareas
Descripción	Se revisian las tareas que están efectivamente segregadas
Frecuencia	Anual
Fórmula de medición	Número de tareas efectivamente segregadas / Total de tareas
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
Indicador	**Seguridad en los proyectos**
Control asociado	A6.1.5 Seguridad de la información en la gestión de proyectos
Descripción	Verificar si la seguridad se tiene en cuenta en los proyectos.
Frecuencia	Anual
Fórmula de medición	Número de proyectos que tienen en cuenta la seguridad / Numero total de Proyectos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	95%
A6.2	**Los dispositivos móviles y el teletrabajo**
Indicador	**Dispositivos móviles gestionados**
Control asociado	A6.2.2 Teletrabajo
Descripción	Determinar los dispositivos móviles efectivamente gestionados por la organización
Frecuencia	Anual
Fórmula de medición	Número de dispositivos móviles efectivamente gestionados /Número total de dispositivos móviles
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	85%

A7	**Seguridad relativa a los recursos humanos**
A7.1	**Antes del empleo**
Indicador	**Antecedentes nuevo personal investigados**
Control asociado	A7.1.1 Investigación de antecedentes
Descripción	Verificar que efectivamente se investigan los antecedentes del nuevo personal contratado.
Frecuencia	Anual
Fórmula de medición	Nuevo personal investigado/ Total nuevo personal
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
Indicador	**Clausulas de seguridad en nuevos contratos**
Control asociado	A7.1.2 Términos y condiciones del empleo
Descripción	Determinar si los contratos a nuevos usuarios reflejan las cuestiones de seguridad.
Frecuencia	Anual
Fórmula de medición	Numero de nuevos contratos con clausulas de seguridad / Total nuevos contratos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A7.2	**Durante el empleo**
Indicador	**Eficacia de los cursos de formación de seguridad de la información**
Control asociado	A7.2.2 Concienciación, educación y capacitación en seguridad de la información
Descripción	Determinar la eficacia de los cursos de formación referentes a la seguridad de la información
Frecuencia	Anual
Fórmula de medición	Suma de valoraciones de encuestas a cursos *10 / Total de encuestas
Unidad de medida	Porcentaje
Valor objetivo	80%
Valor Umbral	70%
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**
Indicador	**Comunicación de responsabilidades**
Control asociado	A7.3.1 Responsabilidades ante la finalización o cambio
Descripción	Determinar si al finalizar los contratos se comunican las responsabilidades a los empleados
Frecuencia	Anual
Fórmula de medición	Número de comunicaciones de responsabilides / Total de contratos finalizados
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A8	**Gestión de activos**
A8.1	**Responsabilidad sobre los activos**
Indicador	**Activos inventariados**
Control asociado	A8.1.1 Inventario de activos
Descripción	Determinar si los activos están claramente identificados
Frecuencia	Anual
Fórmula de medición	Númerto total de activos invenariados /Número total de activos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	90%
Indicador	**Propietarios de activos**
Control asociado	A8.1.2 Propiedad de los activos
Descripción	Determinar el propietario de los activos
Frecuencia	Anual
Fórmula de medición	Número total activos con propietario designado /Número total de activos inventariados
Unidad de medida	Porcentaje
Valor objetivo	90%
Valor Umbral	80%

Indicador	**Roturas de activos**
Control asociado	A8.1.3 Uso aceptable de los activos
Descripción	Verificar el uso aceptable de los activos
Frecuencia	Semestral
Fórmula de medición	Número de activos rotos /Número total de activos
Unidad de medida	Porcentaje
Valor objetivo	0%
Valor Umbral	5%
Indicador	**Activos no recuperados**
Control asociado	A8.1.4. Devolución de activos
Descripción	Determinar los activos que no se recuperan tras la salida del propietario
Frecuencia	Semestral
Fórmula de medición	Activos no recuperados / Activos debieron recuperarse
Unidad de medida	Porcentaje
Valor objetivo	0%
Valor Umbral	5%
A9	**Control de acceso**
A9.1	**Requisitos de negocio para el control de acceso**
Indicador	**Accessos no autorizados**
Control asociado	A9.1.2 Acceso a las redes y a los servicios de red
Descripción	Cuantificar accesos no autorizados
Frecuencia	Trimestral
Fórmula de medición	Cuenta Número de accesos no autorizados
Unidad de medida	Número de accesos no autorizados
Valor objetivo	0
Valor Umbral	1
A9.2	**Gestión de acceso de usuario**
Indicador	**Uso de cuentas genéricas con privilegios**
Control asociado	A9.2.3 Gestión de privilegios de acceso
Descripción	Minimizar el uso "no controlado" de cuentas con privilegios
Frecuencia	Semestral
Fórmula de medición	Número de cuentas genéricas con privilegios /Número de total de cuentas con privlegios
Unidad de medida	Porcentaje
Valor objetivo	0%
Valor Umbral	2%
Indicador	**Bajas comunicadas a IT**
Control asociado	A9.2.6 Retirada o reasignación de los derechos de acceso
Descripción	Determinar si se comunican las bajas de personal a IT para retirar derechos de acceso.
Frecuencia	Semestral
Fórmula de medición	Númerto total de bajas de empleados comunicadas a IT/Número Total de Bajas
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	90%
A9.3	**Responsabilidades del usuario**
Indicador	**Incidentes de autenticación**
Control asociado	A9.3.1 Uso de la información secreta de autenticación
Descripción	Determinar los incidentes debido a mal uso de información de contraseñas
Frecuencia	Anual
Fórmula de medición	Número de usuarios con incidentes de autenticación /Número total de usuarios
Unidad de medida	Porcentaje
Valor objetivo	0%
Valor Umbral	1%

A9.4	**Control de acceso a sistemas y aplicaciones**
Indicador	**Usuarios de aplicaciones con contraseñas no robustas**
Control asociado	A9.4.3 Sistema de gestión de contraseñas
Descripción	Determinar número de usuarios que acceden a aplicaciones con mecanismos que obligan a utilizar contraseñas no robustas
Frecuencia	Anual
Fórmula de medición	Total de usuarios que acceden a aplicaciones con contraseñas no robustas /Total usuarios
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A10	**Criptografía**
A10.1	**Controles criptográficos**
Indicador	**Revisiones políticas controles criptográficos**
Control asociado	A10.1.1 Política de uso de los controles criptográficos
Descripción	Determinar si se revisan periódicamente las políticas de controles criptográficos
Frecuencia	Anual
Fórmula de medición	Número de revisiones de las polítiicas de controles criptog´raficos
Unidad de medida	Número de revisiones
Valor objetivo	2
Valor Umbral	1
A11	**Seguridad física y del entorno**
A11.1	**Áreas seguras**
Indicador	**Control de accesos autorizados**
Control asociado	A11.1.2 Controles físicos de entrada
Descripción	Determinar accesos autorizados frente a total de accesos
Frecuencia	Trimestral
Fórmula de medición	Número de accesos autorizados /Número de accesos totales
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	85%
Indicador	**Revisión de sistemas anti-incendios**
Control asociado	A11.1.4 Protección contra las amenazas externas y ambientales
Descripción	Determinar si las revisiones de los sistemas anti-incencios se realizan periodicamente
Frecuencia	Anual
Fórmula de medición	Número de revisiones anuales
Unidad de medida	Número de revisiones
Valor objetivo	1
Valor Umbral	1
Indicador	**Control de Areas de carga y descarga**
Control asociado	A11.1.6 Áreas de carga y descarga
Descripción	Determinar el grado de control en las zonas de carga y descarga
Frecuencia	Anual
Fórmula de medición	Número Areas de carga y descarga con sistemas de control de acceso / Total de Areas de carga y descarga
Unidad de medida	Porcentaje
Valor objetivo	90%
Valor Umbral	80%

A11.2	Seguridad de los equipos
Indicador	Sistemas sensibles no protegidos
Control asociado	A11.2.1 Emplazamiento y protección de equipos
Descripción	Determinar los sistemas con informacón sensible no protegidos adecuadamente
Frecuencia	Anual
Fórmula de medición	Número de sistemas con información sensible fuera de areas seguras /Numero total de sistemas con información sensible
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	90%
Indicador	Eficacia de los sistemas de actualizaciónes de parches de seguridad
Control asociado	A11.2.4 Mantenimiento de los equipos
Descripción	Determinar la eficacia de los mecanismos de parcheado de sistemas.
Frecuencia	Mensaul
Fórmula de medición	Número de sistemas a último nivel de parches /Total de sistemas
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	90%
Indicador	Cifrado de dispositivos portátiles
Control asociado	A11.2.6 Seguridad de los equipos fuera de las instalaciones
Descripción	Determinar el grado de confidencialidad de la información en los dispositivos móviles.
Frecuencia	Mensual
Fórmula de medición	Número de dispositivos móviles cifrados /Total de dispositivos móviles
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	90%
Indicador	Retirada segura de equipos
Control asociado	A11.2.7 Reutilización o eliminación segura de equipos
Descripción	Determinar si elimina de forma segura la información de los equipos retirados.
Frecuencia	Semestral
Fórmula de medición	Número de equipos retirados con eliminación de datos segura /Número de equipos retirados
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A12	**Seguridad de las operaciones**
A12.1	Procedimientos y responsabilidades operacionales
Indicador	Sistemas productivos sin entorno desarrollo y pruebas
Control asociado	A12.1.4 Separación de los recursos de desarrollo, prueba y operación
Descripción	Cuantificar los sistemas productivos sin entorno de desarrollo y pruebas
Frecuencia	Anual
Fórmula de medición	Sistemas productivos sin entorno desarrollo y pruebas /Total de sistemas productivos
Unidad de medida	Porcentaje
Valor objetivo	10%
Valor Umbral	20%
A12.2	Protección contra el software malicioso (malware)
Indicador	Sistemas protegidos por antivirus
Control asociado	A12.2.1 Controles contra el código malicioso
Descripción	Cuantificar los sistemas protegidos por antivirus
Frecuencia	Mensual
Fórmula de medición	Sistemas con antivirus instalado y actualizado /Total Sistemas
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	95%

A12.3	**Copias de seguridad**
Indicador	**Fiabilidad de las copias de seguridad**
Control asociado	A12.3.1 Copias de seguridad de la información
Descripción	Determinar la fiabilidad de las copias de backup realizadas
Frecuencia	Semestral
Fórmula de medición	Número de restauraciones de backup exitosas /Número de restauraciones de backup
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	98%
A12.4	**Registros y supervisión**
Indicador	**Revisiones de eventos**
Control asociado	A12.4.1 Registro de eventos
Descripción	Verificar la revision periodica de los registros de eventos
Frecuencia	Trimestral
Fórmula de medición	Número de revisiones
Unidad de medida	Número de revisiones
Valor objetivo	1
Valor Umbral	1
A12.6	**Gestión de la vulnerabilidad técnica**
Indicador	
Control asociado	A122.6.1 Gestión de las vulnerabilidades técnicas
Descripción	Tiempo en parchear la mitad de los sistemas vulnerables
Frecuencia	Trimestral
Fórmula de medición	Tiempo de parcheo /(Número de sistemas vulnerables /2)
Unidad de medida	Tiempo / Número de sistemas
Valor objetivo	5 minutos / sistema
Valor Umbral	20 Minutos /Sistema
A12.7	**Consideraciones sobre la auditoria de sistemas de información**
Indicador	**Auditorias realizadas**
Control asociado	A12.7.1 Controles de auditoría de sistemas de información
Descripción	Verificar que se realizan las auditorias previstas
Frecuencia	Anaul
Fórmula de medición	Número de auditorias realizadas
Unidad de medida	Numero de auditorias
Valor objetivo	1
Valor Umbral	1
A13	**Seguridad de las comunicaciones**
A13.2	**Intercambio de información**
Indicador	**Servicios no cifrados**
Control asociado	A13.2.1 Políticas y procedimientos de intercambio de información
Descripción	Cuantificar los servicios que no cifran el intercambio de información
Frecuencia	Anual
Fórmula de medición	Servicios/Aplicaciones que cifran la información /Total Servicios aplicaciones
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**
A14.1	**Requisitos de seguridad en los sistemas de información**
Indicador	**Servicios publicados no cifrados**
Control asociado	A14.1.2 Asegurar los servicios de aplicaciones en redes públicas
Descripción	Cuantificar los servicios publicados en Internet que no cifran el intercambio de información
Frecuencia	Anual
Fórmula de medición	Servicios/Aplicaciones publicados que cifran la información /Total Servicios aplicaciones publicados en Internet
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**
Indicador	**Control de la seguridad del desarrollo software**
Control asociado	A14.2.7 Externalización del desarrollo de software
Descripción	Auditar la seguridad del software desarrollado
Frecuencia	Anual
Fórmula de medición	Número de auditorias de seguridad por software entregado
Unidad de medida	Auditorías / Software desarrollado
Valor objetivo	2
Valor Umbral	1
A15	**Relación con proveedores**
A15.1	**Seguridad en las relaciones con proveedores**
Indicador	**Control de la seguridad en los contratos con proveedores**
Control asociado	A15.1.2 Requisitos de seguridad en contratos con terceros
Descripción	Determinar si la seguridad de la información se tiene en cuenta en los contratos con proveedores
Frecuencia	Anual
Fórmula de medición	Número de contratos que incluyen clausulas de seguridad /Total contratos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A16	**Gestión de incidentes de seguridad de la información**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**
Indicador	**Utilización de canales de notificación de incidentes**
Control asociado	A16.1.2 Notificación de los eventos de seguridad de la información
Descripción	Determinar el conocimiento y utilización de los canales establecidos para la notificación de incidentes de seguridad
Frecuencia	Anual
Fórmula de medición	Número de incidentes de seguridad
Unidad de medida	Porcentaje
Valor objetivo	80%
Valor Umbral	70%
Indicador	**Eficacia de la respuesta a incidentes**
Control asociado	A16.1.5 Respuesta a incidentes de seguridad de la información
Descripción	Determinar la eficacia de los procedimientos establecidos en la respuesta ante incidentes
Frecuencia	Semestral
Fórmula de medición	Número de incidentes resueltos en menos de 4 horas /Número total de incidentes
Unidad de medida	Porcentaje
Valor objetivo	80%

Indicador	Evidencias recopiladas
Control asociado	A16.1.7 Recopilación de evidencias
Descripción	Cuantificar las evidencias recopiladas de los incidentes
Frecuencia	Semestral
Fórmula de medición	Número de incidentes con evidencias recopiladas /Número total de incidentes
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**
A17.1	**Continuidad de la seguridad de la información**
Indicador	**Sistemas con plan de continuidad**
Control asociado	A17.1.2 Implementar la continuidad de la seguridad de la información
Descripción	Determinar los sistemas con plan de continuidad operativo
Frecuencia	Anual
Fórmula de medición	Número de sistemas con plan de continuidad funcional /Número total de sistemas
Unidad de medida	Porcentaje
Valor objetivo	70%
Valor Umbral	60%
A17.2	**Redundancias**
Indicador	**Sistemas críticos redundados**
Control asociado	A17.2.1 Disponibilidad de los recursos de tratamiento de la información
Descripción	Determinar los sistemas criticos redundados
Frecuencia	Anual
Fórmula de medición	Número de sistemas críticos redundados /Total de sistemas críticos
Unidad de medida	Porcentaje
Valor objetivo	100%
Valor Umbral	80%
A18	**Cumplimiento**
A18.1	**Cumplimiento de los requisitos legales y contractuales**
Indicador	**Registros y supervisión**
Control asociado	A18.1.3 Protección de los registros de la organización
Descripción	Cuantificar la protección de los registros
Frecuencia	Anual
Fórmula de medición	Registros con incidentes /Total Registros
Unidad de medida	Porcentaje
Valor objetivo	0%
Valor Umbral	2%
A18.2	**Revisiones de la seguridad de la información**
Indicador	**Auditorias de seguridad**
Control asociado	A18.2.1 Revisión independiente de la seguridad de la información
Descripción	Auditorías realizadas sobre la seguridad de la información
Frecuencia	Anual
Fórmula de medición	Número de auditorías realizadas
Unidad de medida	Número de auditorias
Valor objetivo	2
Valor Umbral	1

Anexo F. PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

1. OBJETO.

El presente documento del SGSI recoge el procedimiento de revisión del SGSI por parte de la Dirección de RecycleSA, según los requisitos que establece la norma ISO/IEC 27001:2013.

2. PLANIFICACIÓN

Se realizará, al menos, una revisión anual que será llevada a cabo en fechas posteriores y próximas a la auditoría interna. De forma ordinaria esta revisión se realizará en el tercer trimestre de cada año.

3. ENTRADAS

Las entradas al proceso de revisión por la dirección son:

- Informe de revisiones anteriores, si las hubo.
- Posibles cambios relevantes en la organización que afecten al SGSI.
- Posibles cambios relevantes en las tecnologías implantadas en la organización.
- No conformidades en las auditorias previas.
- Informes de auditoría previos, ya sean internas o externas.
- Informes de administración de la seguridad.
- Informes relevantes de monitorización de la seguridad de la información, como antivirus, cortafuegos, disponibilidad de servicios, incidentes, vulnerabilidades, etc.
- Informes de sugerencias del personal de la organización y/o proveedores externos relativos a la seguridad de la información.
- Registros de incidentes de seguridad.
- Informe de Riesgos.

4. PROCESO DE REVISIÓN

El Responsable de Seguridad lanzará el proceso de revisión por la Dirección. La Dirección, representada en el Comité de Seguridad y guiada por el Responsable de Seguridad realizará las siguientes acciones de revisión:

a. REVISIÓN DE LAS ACCIONES DE SEGUIMIENTO DE REVISIONES ANTERIORES

En caso de existir revisiones anteriores del SGSI por la Dirección, se revisará el informe resultante y de cada línea de acción propuesta se verificará si ha sido realizada y los resultados obtenidos.

b. REVISIÓN DE CUALQUIER CAMBIO QUE PUDIESE AFECTAR AL SGSI

El Responsable de Seguridad, con anterioridad a la revisión por la Dirección, enviará un mensaje a los miembros del Comité de Seguridad, para que comuniquen cualquier cambio relevante (técnico u organizativo) que pudiese afectar al SGSI, como por ejemplo cambios de responsabilidades, nuevas tecnologías o herramientas en uso, etc. Estos cambios serán revisados por la Dirección.

c. REVISIÓN DE TENDENCIAS EN LA GESTIÓN DE LA SEGURIDAD

El Responsable de Seguridad, con anterioridad a la revisión por la Dirección, recopilará información sobre:

- No conformidades y acciones correctivas.
- Resultados de la monitorización: se revisará el estado de los indicadores del SGSI.
- Revisión de los resultados de las auditorías y revisiones del SGSI: se revisarán los siguientes informes:
- El informe de la última (si existe) revisión llevada a cabo por la Dirección.
- El informe de auditoría interna.
- Informes de administración de la seguridad u otros relativos a procesos de monitorización de la seguridad de la información que puedan considerarse relevantes (antivirus, cortafuegos, disponibilidad de servicios, incidentes, vulnerabilidades, etc.).

d. REVISIÓN DE COMENTARIOS DE PARTES INTERESADAS

El Responsable de Seguridad, con anterioridad a la revisión por la Dirección, recopilará información sobre comentarios o quejas, relacionadas con la seguridad de la información, de usuarios y/o proveedores externos, basándose en los registros de quejas existentes y el registro de incidentes de seguridad.

e. REVISIÓN DEL INFORME DE RIESGOS Y SITUACIÓN DEL PLAN DE TRATAMIENTO

Se revisará el Informe de Riesgos, el Programa de Implantación y la situación actual de las acciones.

f. REVISIÓN DE LAS OPORTUNIDADES DE MEJORA

Se revisarán, si existen, los últimos informes de auditoría externa (auditoría de seguimiento, certificación o re-certificación) o interna y, de cada recomendación propuesta, se verificará si ha sido realizada y los resultados.

El Responsable de Seguridad informará sobre las sugerencias de mejora que le hayan podido llegar durante el periodo previo a la revisión.

El Responsable de Seguridad, con anterioridad a la revisión por la Dirección, enviará un mensaje a los miembros del Comité de Seguridad para que sugieran cualquier posible mejora técnica u organizativa que, en su implicación diaria con los sistemas de información, hayan detectado que puedan ser útiles para mejorar el comportamiento y eficacia del SGSI.

5. RESULTADOS DE LA REVISIÓN

Como resultado de la revisión, se emitirá un informe de resultados, aprobado por la Dirección, que incluirá una lista de conclusiones y acciones relativas a la mejora continua del SGSI, como por ejemplo:

- Si se considera aceptable la eficacia del SGSI o si es preciso reforzar la eficacia de algún aspecto, a la vista de la revisión de indicadores, informes de administración, auditorías y comentarios de las partes interesadas.
- Si los niveles de riesgo evaluados en el último análisis de riesgos y el Programa de Implementación para tratarlos son adecuados a la realidad.

- Si es preciso reforzar el número de recursos, materiales y humanos, así como de servicios subcontratados a terceros dedicados al SGSI, para poder aumentar o mantener su eficacia.
- Si es preciso modificar el catálogo de indicadores.
- Cualquier otro resultado que se considere necesario.

6. SALIDAS

7. LAS SALIDAS DEL PROCESO DE REVISIÓN POR LA DIRECCIÓN SON:

- Informe de revisión.
- Evaluación del tratamiento de riesgos actualizado.
- Procedimientos actualizados.
- Catálogo de indicadores actualizado

Anexo G. GESTIÓN DE ROLES Y RESPONSABILIDADES

1. OBJETO.

La implantación con éxito de un SGSI requiere la definición clara de sobre quien cae la responsabilidad de cada uno de los aspectos que se definen en el mismo. Para ello se deben definir órganos necesarios y los roles adecuados en la organización.

El objeto de este documento es establecer la estructura interna de RecycleSA con respecto a las responsabilidades sobre la seguridad de la información.

2. COMITÉ DE DIRECCIÓN

a. RESPONSABILIDADES

Las responsabilidades del Comité de Dirección, en materia de Seguridad de la información, son las siguientes:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
- Nombrar a los miembros de un Comité de Seguridad de la Información y darles soporte, dotarlo de los recursos necesarios y establecer sus directrices de trabajo.
- Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.
- Determinar el umbral de riesgo aceptable en materia de seguridad.
- Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el Plan de seguridad de la información, que recoge los principales proyectos e iniciativas en la materia.
- Realizar el seguimiento del cuadro de mando de la seguridad de la información.

b. MIEMBROS

- CEO.
- Director Financiero.
- Director Servicios de Reciclaje de Acero.
- Director Servicios de Reciclaje de Aluminio.
- Director Tecnologías de la Información.
-

3. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)

a. RESPONSABILIDADES

Las responsabilidades del Comité de Seguridad de la Información de RecyleSA son las siguientes:

- Implantar las directrices del Comité de Dirección.
- Asignar roles y funciones en materia de seguridad.

- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).
- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.
- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

b. MIEMBROS

Los miembros permanentes del Comité de Seguridad son los siguientes:

- CEO.
- Director Financiero.
- Director Servicios de Reciclaje de Acero.
- Director Servicios de Reciclaje de Aluminio.
- Director Tecnologías de la Información.
- Responsable de Seguridad.

En función de la temática tratada se podrán incorporar miembros invitados, como podrían ser:

- Director de Legal.
- Director de Recursos Humanos.

4. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI)

a. RESPONSABILIDADES

Las funciones y responsabilidades que competen al Responsable de Seguridad de RecycleSA son las siguientes:

- Implantar las directrices del Comité de Seguridad de la Información de la compañía.
- Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información.
- Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el área de Organización/RR. HH., en el cual se recogerá quién asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.
- Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.
- Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención,

emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.

- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección. Elevar el mapa de riesgos y el Plan de seguridad de la información al CSI.
- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando. Una vez aprobado dicho plan y el presupuesto por el CSI, el RSI deberá gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.
- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.
- Velar por el cumplimiento legal, como el Reglamento General de Protección de Datos (RGPD), coordinando las actuaciones necesarias con las unidades responsables.
- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al CSI si corresponde.
- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.
- Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al CSI si corresponde.
- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El RSI debe analizar y mantener actualizado dicho cuadro de mando, presentándolo al CSI con la periodicidad que se establezca.

b. MIEMBROS

El responsable de Seguridad de la Información será designado por el Comité de Dirección de RecycleSA.

5. DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

a. RESPONSABILIDADES

Las responsabilidades del departamento de Tecnología de la información de RecycleSA; respecto a la seguridad de la información, son:

- Cumplir con las políticas, normas y procedimientos en materia de seguridad de la información. Colaborar con el RSI en su definición.
- Implantar en los sistemas de información los controles de seguridad prescritos, las acciones correctoras establecidas y gestionar las vulnerabilidades detectadas.
- Requerir la participación del RSI en nuevos proyectos de desarrollo o adaptación/implantación de productos de mercado, especialmente cuando puedan ser críticos en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio y trazabilidad, o puedan tener un impacto mediático importante.
- Requerir la participación del RSI en la implantación o gestión de los cambios de hardware y software.
- Garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos: creación, mantenimiento, conservación y destrucción, y en los procesos de gestión de hardware y software.

- Adoptar medidas para proteger la información según su clasificación por parte del responsable de la información.
- Colaborar con el RSI en la identificación de riesgos y la propuesta de soluciones, y colaborar en las revisiones o auditorías de seguridad que se lleven a cabo.

b. APLICA A

Todos los miembros del equipo de TI de RecycleSA deben realizar las funciones descritas anteriormente. Además, puesto que buena parte de los servicios de TI de RecycleSA se encuentran externalizados en proveedores de servicio, éstos deben asumir dichas funciones. Así pues, a efectos de la Seguridad de la Información, los miembros del departamento de TI son:

- Director de Tecnologías de la Información.
- Service Managers.
- Proveedores de servicio de TI.

6. DEPARTAMENTO DE RECURSOS HUMANOS

a. RESPONSABILIDADES

Las responsabilidades del personal del departamento de recursos humanos de RecycleSA, respecto a la Seguridad de la Información, son:

- Informar a las unidades gestoras de recursos de información sobre cambios / movimientos de personal para poder realizar una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría y/o funciones, cambios organizativos, etc.
- Trabajar conjuntamente con el RSI en el desarrollo de la política de seguridad de la información en los temas referentes al personal.
- Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo.

b. APLICA A

- Personal del departamento de Recursos Humanos de RecycleSA.

7. DEPARTAMENTO DE LEGAL

a. RESPONSABILIDADES

Las responsabilidades del personal del departamento de Legal de RecycleSA, respecto a la Seguridad de la Información, son:

- Colaborar con el RSI en la emisión de nuevas políticas y normas de seguridad y en la investigación y resolución de incidentes de seguridad cuando se puedan derivar acciones legales (reclamaciones de terceras partes, acciones contra un trabajador...).
- Colaborar con el RSI en la definición de cláusulas específicas de seguridad de la información, e incluirlas en los contratos con terceras partes y contratos de personal externo.
- Informar al RSI de nueva legislación o cambios en la legislación aplicable, que pudieran tener impacto sobre la seguridad de la información, dando soporte en su interpretación.

b. APLICA A

- Personal del Departamento de Legal de RecycleSA.

8. PERSONAL EN GENERAL

a. RESPONSABILIDADES

Todo el personal con acceso a la información de RecycleSA, incluyendo tanto al personal interno como a los trabajadores de su proveedores de servicio, tienen la obligación de:

- Mantener la confidencialidad de la información.
- Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados.
- Respetar las normas y procedimientos vigentes en materia de seguridad de la información, y velar por que terceras partes en prestación de servicios también la respeten.
- Utilizar adecuadamente las credenciales de acceso a los sistemas de información.
- Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación.
- Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.

b. APLICA A

- Personal de RecycleSA
- Personal de proveedores de servicios con acceso a información de RecycleSA.

Anexo H. METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología para el análisis de riesgos que se utilizará en la implantación del SGSI de RecycleSA es MAGERIT.

Según MAGERIT, el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se introducen los conceptos de "impacto y riesgo potenciales" entre los pasos 2 y 3. Estas valoraciones son "teóricas": en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo. La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

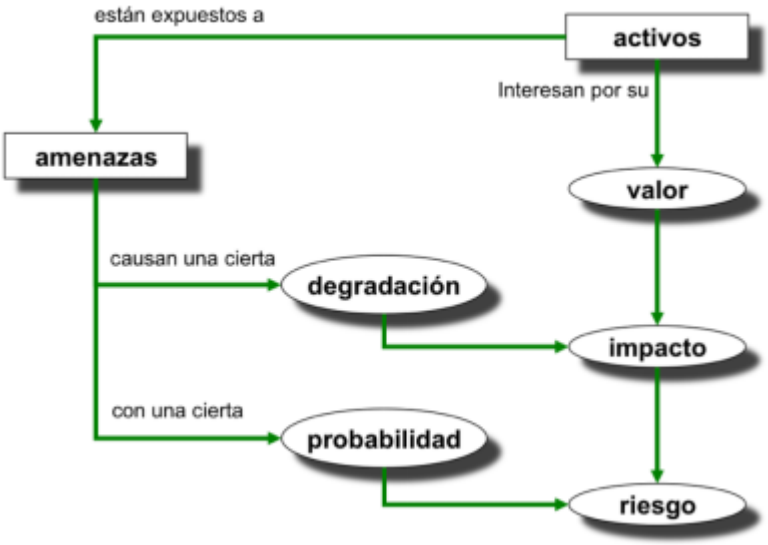

Figura 2. Elementos del análisis de riesgos potenciales

A continuación se describen los conceptos básicos y tareas a realizar en cada paso:

1. Determinación de activos

MAGERIT distingue entre

- Activos esenciales:
- Información que maneja el sistema de información
- Servicios que presta el sistema de información
- Otros activos relevantes, subordinados a los esenciales:
- Datos que materializan la información.

- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y
- servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados

De cada activo se deben calibrar sus diferentes dimensiones:

- **Confidencialidad.** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
- **Integridad.** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
- **Disponibilidad.** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
- **Autenticidad**. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
- **Trazabilidad.** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Una vez determinados los activos y sus dependencias, se deben valorar. En ese sentido MAGERIT considera que el valor nuclear suele estar en la información que el sistema maneja y en los servicios que se prestan (activos esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección esencial.

La valoración de los activos se pueden realizar de forma cualitativa o cuantitativa.

2. Determinación de amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo.

Una amenaza es una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Para ello hay que identificar a qué dimensiones del activo afecta la amenaza y su influencia en el valor del activo en dos sentidos:

- **Degradación.** Mide el daño causado por un incidente en el supuesto de que ocurriera.

  Se suele caracterizar como una fracción del valor del activo.

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Figura 3. Degradación del valor

- **Probabilidad.** Mide cuán probable o improbable es que se materialice la amenaza.

La probabilidad de la ocurrencia suele ser más compleja de determinar y expresar. Se suele modelar cualitativamente mediante una escala nominal:

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Figura 4. Probabilidad de ocurrencia.

3. Determinación de salvaguardas

Se definen las salvaguardas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal.

Las salvaguardas entran en el cálculo del riesgo de 2 formas:

- **Reduciendo la probabilidad de las amenazas**. Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.
- **Limitando el daño causado.** Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

4. Estimación del impacto residual.

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

5. Estimación del riesgo.

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Anexo I. PLANTILLA DECLARACIÓN DE APLICABILIDAD

Plantilla para la declaración de aplicabilidad.

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A5	**Políticas de seguridad de la información**								
A5.1	**Directrices de gestión de la seguridad de la información**								
A5.1.1	Políticas para la seguridad de la información								
A5.1.2	Revisión de las políticas para la seguridad de la información								
A6	**Organización de la seguridad de la información**								
A6.1	**Organización interna**								
A6.1.1	Roles y responsabilidades en seguridad de la información								
A6.1.2	Segregación de tareas								
A6.1.3	Contacto con las autoridades								
A6.1.4	Contacto con grupos de interés especial								
A6.1.5	Seguridad de la información en la gestión de proyectos								
A6.2	**Los dispositivos móviles y el teletrabajo**								
A6.2.1	Política de dispositivos móviles								
A6.2.2	Teletrabajo								
A7	**Seguridad relativa a los recursos humanos**								
A7.1	**Antes del empleo**								
A7.1.1	Investigación de antecedentes								
A7.1.2	Términos y condiciones del empleo								
A7.2	**Durante el empleo**								
A7.2.1	Responsabilidades de gestión								
A7.2.2	Concienciación, educación y capacitación en seguridad de la información								
A7.2.3	Proceso disciplinario								
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**								
A7.3.1	Responsabilidades ante la finalización o cambio								
A8	**Gestión de activos**								
A8.1	**Responsabilidad sobre los activos**								
A8.1.1	Inventario de activos								
A8.1.2	Propiedad de los activos								
A8.1.3	Uso aceptable de los activos								
A8.1.4	Devolución de activos								
A8.2	**Clasificación de la información**								
A8.2.1	Clasificación de la información								
A8.2.2	Etiquetado de la información								
A8.2.3	Manipulado de la información								
A8.3	**Manipulación de los soportes**								
A8.3.1	Gestión de soportes extraíbles								
A8.3.2	Eliminación de soportes								
A8.3.3	Soportes físicos en tránsito								
A9	**Control de acceso**								
A9.1	**Requisitos de negocio para el control de acceso**								
A9.1.1	Política de control de acceso								
A9.1.2	Acceso a las redes y a los servicios de red								
A9.2	**Gestión de acceso de usuario**								
A9.2.1	Registro y baja de usuario								
A9.2.2	Provisión de acceso de usuario								
A9.2.3	Gestión de privilegios de acceso								
A9.2.4	Gestión de la información secreta de autenticación de los usuarios								
A9.2.5	Revisión de los derechos de acceso de usuario								
A9.2.6	Retirada o reasignación de los derechos de acceso								
A9.3	**Responsabilidades del usuario**								
A9.3.1	Uso de la información secreta de autenticación								
A9.4	**Control de acceso a sistemas y aplicaciones**								
A9.4.1	Restricción del acceso a la información								
A9.4.2	Procedimientos seguros de inicio de sesión								
A9.4.3	Sistema de gestión de contraseñas								
A9.4.4	Uso de utilidades con privilegios del sistema								
A9.4.5	Control de acceso al código fuente de los programas								
A10	**Criptografía**								
A10.1	**Controles criptográficos**								
A10.1.1	Política de uso de los controles criptográficos								
A10.1.2	Gestión de claves								
A11	**Seguridad física y del entorno**								
A11.1	**Áreas seguras**								
A11.1.1	Perímetro de seguridad física								
A11.1.2	Controles físicos de entrada								
A11.1.3	Seguridad de oficinas, despachos y recursos								
A11.1.4	Protección contra las amenazas externas y ambientales								
A11.1.5	El trabajo en áreas seguras								
A11.1.6	Áreas de carga y descarga								
A11.2	**Seguridad de los equipos**								
A11.2.1	Emplazamiento y protección de equipos								
A11.2.2	Instalaciones de suministro								
A11.2.3	Seguridad del cableado								
A11.2.4	Mantenimiento de los equipos								
A11.2.5	Retirada de materiales propiedad de la empresa								
A11.2.6	Seguridad de los equipos fuera de las instalaciones								
A11.2.7	Reutilización o eliminación segura de equipos								
A11.2.8	Equipo de usuario desatendido								
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia								

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A12	**Seguridad de las operaciones**								
A12.1	**Procedimientos y responsabilidades operacionales**								
A12.1.1	Documentación de procedimientos operacionales								
A12.1.2	Gestión de cambios								
A12.1.3	Gestión de capacidades								
A12.1.4	Separación de los recursos de desarrollo, prueba y operación								
A12.2	**Protección contra el software malicioso (malware)**								
A12.2.1	Controles contra el código malicioso								
A12.3	**Copias de seguridad**								
A12.3.1	Copias de seguridad de la información								
A12.4	**Registros y supervisión**								
A12.4.1	Registro de eventos								
A12.4.2	Protección de la información del registro								
A12.4.3	Registros de administración y operación								
A12.4.4	Sincronización del reloj								
A12.5	**Control del software en explotación**								
A12.5.1	Instalación del software en explotación								
A12.6	**Gestión de la vulnerabilidad técnica**								
A12.6.1	Gestión de las vulnerabilidades técnicas								
A12.6.2	Restricción en la instalación de software								
A12.7	**Consideraciones sobre la auditoria de sistemas de información**								
A12.7.1	Controles de auditoría de sistemas de información								
A13	**Seguridad de las comunicaciones**								
A13.1	**Gestión de la seguridad de las redes**								
A13.1.1	Controles de red								
A13.1.2	Seguridad de los servicios de red								
A13.1.3	Segregación en redes								
A13.2	**Intercambio de información**								
A13.2.1	Políticas y procedimientos de intercambio de información								
A13.2.2	Acuerdos de intercambio de información								
A13.2.3	Mensajería electrónica								
A13.2.4	Acuerdos de confidencialidad o no revelación								
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**								
A14.1	**Requisitos de seguridad en los sistemas de información**								
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información								
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas								
A14.1.3	Protección de las transacciones de servicios de aplicaciones								
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**								
A14.2.1	Política de desarrollo seguro								
A14.2.2	Procedimiento de control de cambios en sistemas								
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo								
A14.2.4	Restricciones a los cambios en los paquetes de software								
A14.2.5	Principios de ingeniería de sistemas seguros								
A14.2.6	Entorno de desarrollo seguro								
A14.2.7	Externalización del desarrollo de software								
A14.2.8	Pruebas funcionales de seguridad de sistemas								
A14.2.9	Pruebas de aceptación de sistemas								
A14.3	**Datos de prueba**								
A14.3.1	Protección de los datos de prueba								
A15	**Relación con proveedores**								
A15.1	**Seguridad en las relaciones con proveedores**								
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores								
A15.1.2	Requisitos de seguridad en contratos con terceros								
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones								
A15.2	**Gestión de la provisión de servicios del proveedor**								
A15.2.1	Control y revisión de la provisión de servicios del proveedor								
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor								
A16	**Gestión de incidentes de seguridad de la información**								
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**								
A16.1.1	Responsabilidades y procedimientos								
A16.1.2	Notificación de los eventos de seguridad de la información								
A16.1.3	Notificación de puntos débiles de la seguridad								
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información								
A16.1.5	Respuesta a incidentes de seguridad de la información								
A16.1.6	Aprendizaje de los incidentes de seguridad de la información								
A16.1.7	Recopilación de evidencias								
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**								
A17.1	**Continuidad de la seguridad de la información**								
A17.1.1	Planificación de la continuidad de la seguridad de la información								
A17.1.2	Implementar la continuidad de la seguridad de la información								
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información								
A17.2	**Redundancias**								
A17.2.1	Disponibilidad de los recursos de tratamiento de la información								
A18	**Cumplimiento**								
A18.1	**Cumplimiento de los requisitos legales y contractuales**								
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales								
A18.1.2	Derechos de Propiedad Intelectual (DPI)								
A18.1.3	Protección de los registros de la organización								
A18.1.4	Protección y privacidad de la información de carácter personal								
A18.1.5	Regulación de los controles criptográficos								
A18.2	**Revisiones de la seguridad de la información**								
A18.2.1	Revisión independiente de la seguridad de la información								
A18.2.2	Cumplimiento de las políticas y normas de seguridad								
A18.2.3	Comprobación del cumplimiento técnico								

En la plantilla anterior, el origen del control se puede codificar de la siguiente manera:

Código	Orígen
R	Análisis de Riesgos
L	Legal o normativo
I	Requerimiento interno
C	Requerimiento Contractual

Anexo J. TABLA DE AMENAZAS MAGERIT

A continuación se muestra una tabla con las distintas amenazas y los grupos en los que la metodología Magerit las encuadra.

Grupo	Amenaza
[N] Desastres Naturales	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
[I] De origen industrial	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación mecánica
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios y suministros esenciales
	[I.10] Degradación de los soportes de almacenamiento de la información
	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.3] Errores de monitorización (log)
	[E.4] Errores de configuración
	[E.7] Deficiencias en la organización
	[E.8] Difusión de software dañino
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[E.14] Escapes de información
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[E.28] Indisponibilidad del personal
[A] Ataques Intencionados	[A.3] Manipulación de los registros de actividad (log)
	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.9] [Re-]encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[A.12] Análisis de tráfico
	[A.13] Repudio
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
	[A.22] Manipulación de programas
	[A.23] Manipulación de los equipos
	[A.24] Denegación de servicio
	[A.25] Robo
	[A.26] Ataque destructivo
	[A.27] Ocupación enemiga
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)

Anexo K. TABLA DE ANÁLISIS AMENAZAS/ACTIVOS

A continuación se muestra la tabla con el análisis que muestra cómo afecta cada amenaza identificada a los distintos activos de la organización.

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[N] Desastres Naturales	[N.1] Fuego	Instalaciones [L]	B				100%	
		Hardware [HW]	B				100%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				100%	
	[N.2] Daños por agua	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				75%	
	[N.*] Desastres naturales	Instalaciones [L]	MB				100%	
		Hardware [HW]	MB				100%	
		Soportes de información [M]	MB				100%	
		Equipamiento auxiliar [AUX]	MB				100%	
[I] De origen industrial	[I.1] Fuego	Instalaciones [L]	B				100%	
		Hardware [HW]	B				100%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				100%	
	[I.2] Daños por agua	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				75%	
		Equipamiento auxiliar [AUX]	B				75%	
	[I.*] Desastres industriales	Instalaciones [L]	B				100%	
		Hardware [HW]	B				100%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				100%	
	[I.3] Contaminación mecánica	Hardware [HW]	B				50%	
		Soportes de información [M]	MB				50%	
		Equipamiento auxiliar [AUX]	MB				50%	
	[I.4] Contaminación electromagnética	Hardware [HW]	MB				75%	
		Soportes de información [M]	MB				75%	
		Equipamiento auxiliar [AUX]	MB				75%	
	[I.5] Avería de origen físico o lógico	Hardware [HW]	B				50%	
		Aplicación/Software [SW]	B				50%	
		Soportes de información [M]	B				75%	
		Equipamiento auxiliar [AUX]	B				20%	
	[I.6] Corte del suministro eléctrico	Hardware [HW]	M				100%	
		Soportes de información [M]	M				100%	
		Equipamiento auxiliar [AUX]	M				100%	
	[I.7] Condiciones inadecuadas de temperatura o humedad	Hardware [HW]	MB				75%	
		Soportes de información [M]	MB				75%	
		Equipamiento auxiliar [AUX]	MB				50%	
	[I.8] Fallo de servicios de comunicaciones	Redes de comunicación [COM]	B				100%	
	[I.9] Interrupción de otros servicios y suministros esenciales	Equipamiento auxiliar [AUX]	M				100%	
	[I.10] Degradación de los soportes de almacenamiento de la	Soportes de información [M]	MB				100%	
	[I.11] Emanaciones electromagnéticas	Instalaciones [L]	MB				5%	
		Hardware [HW]	MB				75%	
		Soportes de información [M]	MB				75%	
		Equipamiento auxiliar [AUX]	MB				20%	

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	Aplicación/Software [SW]	A		5%	5%	5%	
		Datos/Información [D]	A		50%	5%	5%	
		Servicios [S]	A		50%	20%	5%	
		Soportes de información [M]	A		50%	50%	50%	
	[E.2] Errores del administrador	Hardware [HW]	A		5%	20%	50%	
		Aplicación/Software [SW]	A		75%	50%	75%	
		Datos/Información [D]	A		75%	50%	75%	
		Redes de comunicación [COM]	A		5%	50%	75%	
		Servicios [S]	A		75%	50%	75%	
		Soportes de información [M]	A		75%	50%	75%	
	[E.3] Errores de monitorización (log)	Datos/Información [D]	M			50%		75%
	[E.4] Errores de configuración	Datos/Información [D]	M			50%		
	[E.7] Deficiencias en la organización	Personal [P]	M				75%	
	[E.8] Difusión de software dañino	Aplicación/Software [SW]	M		75%	75%	75%	
	[E.9] Errores de [re-]encaminamiento	Aplicación/Software [SW]	M		50%			
		Redes de comunicación [COM]	M		50%			
		Servicios [S]	M		20%			
	[E.10] Errores de secuencia	Aplicación/Software [SW]	B			20%		
		Redes de comunicación [COM]	B			20%		
		Servicios [S]	B			20%		
	[E.14] Escapes de información	Datos/Información [D]	M		100%			
	[E.15] Alteración accidental de la información	Instalaciones [L]	B			5%		
		Aplicación/Software [SW]	B			20%		
		Datos/Información [D]	B			75%		
		Redes de comunicación [COM]	B			50%		
		Soportes de información [M]	B			50%		
		Servicios [S]	B			75%		
	[E.18] Destrucción de información	Instalaciones [L]	B				5%	
		Aplicación/Software [SW]	B				75%	
		Datos/Información [D]	B				100%	
		Redes de comunicación [COM]	B				20%	
		Servicios [S]	B				75%	
		Soportes de información [M]	B				75%	
	[E.19] Fugas de información	Instalaciones [L]	B		5%			
		Aplicación/Software [SW]	B		75%			
		Datos/Información [D]	B		100%			
		Redes de comunicación [COM]	B		50%			
		Servicios [S]	B		50%			
		Soportes de información [M]	B		75%			
		Personal [P]	B		75%			
	[E.20] Vulnerabilidades de los programas (software)	Aplicación/Software [SW]	A			20%	100%	
	[E.21] Errores de mantenimiento / actualización de	Aplicación/Software [SW]	A			50%	75%	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Hardware [HW]	A				75%	
		Soportes de información [M]	A				75%	
		Equipamiento auxiliar [AUX]	A				75%	
	[E.24] Caída del sistema por agotamiento de recursos	Hardware [HW]	B				100%	
		Redes de comunicación [COM]	B				100%	
		Servicios [S]	B				100%	
	[E.25] Pérdida de equipos	Hardware [HW]	M		100%		100%	
		Soportes de información [M]	M		100%		100%	
		Equipamiento auxiliar [AUX]	B		5%		100%	
	[E.28] Indisponibilidad del personal	Personal [P]	A				100%	

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	Datos/Información [D]	MB			100%		100%
	[A.4] Manipulación de la configuración	Datos/Información [D]	MB		75%	100%	75%	
	[A.5] Suplantación de la identidad del usuario	Aplicación/Software [SW]	B	75%	100%	5%		
		Datos/Información [D]	B	100%	100%	50%		
		Redes de comunicación [COM]	B	75%	75%	50%		
		Servicios [S]	B	75%	75%	50%		
	[A.6] Abuso de privilegios de acceso	Hardware [HW]	B		20%	50%	5%	
		Aplicación/Software [SW]	B		75%	50%	50%	
		Datos/Información [D]	B		100%	50%	50%	
		Redes de comunicación [COM]	B		75%	50%	50%	
		Servicios [S]	B		75%	50%	50%	
	[A.7] Uso no previsto	Instalaciones [L]	B		5%	20%	20%	
		Hardware [HW]	B		20%	20%	20%	
		Aplicación/Software [SW]	B		20%	20%	20%	
		Redes de comunicación [COM]	B		20%	20%	20%	
		Servicios [S]	B		20%	20%	20%	
		Soportes de información [M]	B		20%	20%	20%	
		Equipamiento auxiliar [AUX]	B		5%	20%	20%	
	[A.8] Difusión de software dañino	Aplicación/Software [SW]	B		75%	75%	75%	
	[A.9] [Re-]encaminamiento de mensajes	Aplicación/Software [SW]	MB		50%			
		Redes de comunicación [COM]	MB		50%			
		Servicios [S]	MB		50%			
	[A.10] Alteración de secuencia	Aplicación/Software [SW]	MB			20%		
		Redes de comunicación [COM]	MB			20%		
		Servicios [S]	MB			50%		
	[A.11] Acceso no autorizado	Instalaciones [L]	B		5%	20%		
		Hardware [HW]	B		5%	50%		
		Aplicación/Software [SW]	B		50%	50%		
		Datos/Información [D]	B		75%	75%		
		Redes de comunicación [COM]	B		50%	75%		
		Servicios [S]	B		50%	50%		
		Soportes de información [M]	B		100%	50%		
		Equipamiento auxiliar [AUX]	B		20%	20%		
	[A.12] Análisis de tráfico	Redes de comunicación [COM]	MB		100%			
	[A.13] Repudio	Datos/Información [D]	MB			5%		75%
		Servicios [S]	MB			5%		75%
	[A.14] Interceptación de información (escucha)	Redes de comunicación [COM]	MB		100%			
	[A.15] Modificación deliberada de la información	Instalaciones [L]	MB			5%		
		Aplicación/Software [SW]	MB			20%		
		Datos/Información [D]	MB			100%		
		Redes de comunicación [COM]	MB			20%		
		Servicios [S]	MB			50%		
		Soportes de información [M]	MB			50%		
	[A.18] Destrucción de información	Instalaciones [L]	MB				5%	
		Aplicación/Software [SW]	MB				75%	
		Datos/Información [D]	MB				100%	
		Servicios [S]	MB				75%	
		Soportes de información [M]	MB				5%	
	[A.19] Divulgación de información	Instalaciones [L]	B		20%			
		Aplicación/Software [SW]	B		75%			
		Datos/Información [D]	B		100%			
		Redes de comunicación [COM]	B		50%			
		Servicios [S]	B		75%			
		Soportes de información [M]	B		100%			
	[A.22] Manipulación de programas	Aplicación/Software [SW]	MB		75%	100%	100%	
	[A.23] Manipulación de los equipos	Hardware [HW]	MB		50%		100%	
		Soportes de información [M]	MB		75%		100%	
		Equipamiento auxiliar [AUX]	MB		5%		100%	
	[A.24] Denegación de servicio	Hardware [HW]	B				5%	
		Redes de comunicación [COM]	B				100%	
		Servicios [S]	B				100%	
	[A.25] Robo	Hardware [HW]	B		5%		100%	
		Soportes de información [M]	B		100%		100%	
		Equipamiento auxiliar [AUX]	MB		5%		100%	
	[A.26] Ataque destructivo	Instalaciones [L]	MB				100%	
		Hardware [HW]	MB				100%	
		Soportes de información [M]	MB				100%	
		Equipamiento auxiliar [AUX]	MB				100%	
	[A.27] Ocupación enemiga	Instalaciones [L]	MB		20%		100%	
	[A.28] Indisponibilidad del personal	Personal [P]	A				100%	
	[A.29] Extorsión	Personal [P]	MB		20%	20%	20%	
	[A.30] Ingeniería social (picaresca)	Personal [P]	M		20%	20%	20%	

Anexo L. Tabla de Análisis amenazas/activos tras ejecución de Proyectos.

A continuación se muestra la tabla con el análisis que muestra cómo afecta cada amenaza identificada a los distintos activos de la organización una vez se hayan realizado los proyectos propuestos.

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[N] Desastres Naturales	[N.1] Fuego	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				75%	
	[N.2] Daños por agua	Instalaciones [L]	B				75%	
		Hardware [HW]	B				20%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				75%	
	[N.*] Desastres naturales	Instalaciones [L]	MB				75%	
		Hardware [HW]	MB				75%	
		Soportes de información [M]	MB				75%	
		Equipamiento auxiliar [AUX]	MB				75%	
[I] De origen industrial	[I.1] Fuego	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				75%	
	[I.2] Daños por agua	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				75%	
		Equipamiento auxiliar [AUX]	B				75%	
	[I.*] Desastres industriales	Instalaciones [L]	B				75%	
		Hardware [HW]	B				75%	
		Soportes de información [M]	B				100%	
		Equipamiento auxiliar [AUX]	B				75%	
	[I.3] Contaminación mecánica	Hardware [HW]	B				50%	
		Soportes de información [M]	MB				50%	
		Equipamiento auxiliar [AUX]	MB				50%	
	[I.4] Contaminación electromagnética	Hardware [HW]	MB				50%	
		Soportes de información [M]	MB				50%	
		Equipamiento auxiliar [AUX]	MB				50%	
	[I.5] Avería de origen físico o lógico	Hardware [HW]	B				50%	
		Aplicación/Software [SW]	B				50%	
		Soportes de información [M]	B				75%	
		Equipamiento auxiliar [AUX]	B				20%	
	[I.6] Corte del suministro eléctrico	Hardware [HW]	M				75%	
		Soportes de información [M]	M				100%	
		Equipamiento auxiliar [AUX]	M				75%	
	[I.7] Condiciones inadecuadas de temperatura o humedad	Hardware [HW]	MB				50%	
		Soportes de información [M]	MB				50%	
		Equipamiento auxiliar [AUX]	MB				50%	
	[I.8] Fallo de servicios de comunicaciones	Redes de comunicación [COM]	B				75%	
	[I.9] Interrupción de otros servicios y suministros esenciales	Equipamiento auxiliar [AUX]	M				100%	
	[I.10] Degradación de los soportes de almacenamiento de la	Soportes de información [M]	MB				100%	
	[I.11] Emanaciones electromagnéticas	Instalaciones [L]	MB				5%	
		Hardware [HW]	MB				50%	
		Soportes de información [M]	MB				50%	
		Equipamiento auxiliar [AUX]	MB				20%	

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	Aplicación/Software [SW]	M		5%	5%	5%	
		Datos/Información [D]	M		50%	5%	5%	
		Servicios [S]	M		50%	20%	5%	
		Soportes de información [M]	M		50%	50%	50%	
	[E.2] Errores del administrador	Hardware [HW]	M		5%	20%	50%	
		Aplicación/Software [SW]	M		75%	50%	75%	
		Datos/Información [D]	M		75%	50%	75%	
		Redes de comunicación [COM]	M		5%	50%	75%	
		Servicios [S]	M		75%	50%	75%	
		Soportes de información [M]	M		75%	50%	75%	
	[E.3] Errores de monitorización (log)	Datos/Información [D]	M			50%		75%
	[E.4] Errores de configuración	Datos/Información [D]	M			50%		
	[E.7] Deficiencias en la organización	Personal [P]	M				75%	
	[E.8] Difusión de software dañino	Aplicación/Software [SW]	M		75%	75%	75%	
	[E.9] Errores de [re-]encaminamiento	Aplicación/Software [SW]	M		50%			
		Redes de comunicación [COM]	M		50%			
		Servicios [S]	M		20%			
	[E.10] Errores de secuencia	Aplicación/Software [SW]	B			20%		
		Redes de comunicación [COM]	B			20%		
		Servicios [S]	B			20%		
	[E.14] Escapes de información	Datos/Información [D]	B		100%			
	[E.15] Alteración accidental de la información	Instalaciones [L]	B			5%		
		Aplicación/Software [SW]	B			20%		
		Datos/Información [D]	B			75%		
		Redes de comunicación [COM]	B			50%		
		Soportes de información [M]	B			50%		
		Servicios [S]	B			75%		
	[E.18] Destrucción de información	Instalaciones [L]	B				5%	
		Aplicación/Software [SW]	B				75%	
		Datos/Información [D]	B				100%	
		Redes de comunicación [COM]	B				20%	
		Servicios [S]	B				75%	
		Soportes de información [M]	B				75%	
	[E.19] Fugas de información	Instalaciones [L]	B		5%			
		Aplicación/Software [SW]	MB		75%			
		Datos/Información [D]	B		100%			
		Redes de comunicación [COM]	B		50%			
		Servicios [S]	B		50%			
		Soportes de información [M]	B		75%			
		Personal [P]	B		75%			
	[E.20] Vulnerabilidades de los programas (software)	Aplicación/Software [SW]	M			20%	75%	
	[E.21] Errores de mantenimiento / actualización de	Aplicación/Software [SW]	A			50%	75%	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Hardware [HW]	A				75%	
		Soportes de información [M]	A				75%	
		Equipamiento auxiliar [AUX]	A				75%	
	[E.24] Caída del sistema por agotamiento de recursos	Hardware [HW]	MB				75%	
		Redes de comunicación [COM]	B				100%	
		Servicios [S]	MB				75%	
	[E.25] Pérdida de equipos	Hardware [HW]	B		75%		75%	
		Soportes de información [M]	B		100%		100%	
		Equipamiento auxiliar [AUX]	B		5%		100%	
	[E.28] Indisponibilidad del personal	Personal [P]	A				75%	

Grupo	Amenaza	Activo	Frecuencia	A	C	I	D	T
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	Datos/Información [D]	MB			100%		100%
	[A.4] Manipulación de la configuración	Datos/Información [D]	MB		75%	100%	75%	
	[A.5] Suplantación de la identidad del usuario	Aplicación/Software [SW]	B	75%	100%	5%		
		Datos/Información [D]	B	100%	100%	50%		
		Redes de comunicación [COM]	B	75%	75%	50%		
		Servicios [S]	B	75%	75%	50%		
	[A.6] Abuso de privilegios de acceso	Hardware [HW]	B		20%	50%	5%	
		Aplicación/Software [SW]	B		75%	50%	50%	
		Datos/Información [D]	B		100%	50%	50%	
		Redes de comunicación [COM]	B		75%	50%	50%	
		Servicios [S]	B		75%	50%	50%	
	[A.7] Uso no previsto	Instalaciones [L]	B		5%	20%	20%	
		Hardware [HW]	B		20%	20%	20%	
		Aplicación/Software [SW]	B		20%	20%	20%	
		Redes de comunicación [COM]	B		20%	20%	20%	
		Servicios [S]	B		20%	20%	20%	
		Soportes de información [M]	B		20%	20%	20%	
		Equipamiento auxiliar [AUX]	B		5%	20%	20%	
	[A.8] Difusión de software dañino	Aplicación/Software [SW]	B		75%	75%	75%	
	[A.9] [Re-]encaminamiento de mensajes	Aplicación/Software [SW]	MB		50%			
		Redes de comunicación [COM]	MB		50%			
		Servicios [S]	MB		50%			
	[A.10] Alteración de secuencia	Aplicación/Software [SW]	MB			20%		
		Redes de comunicación [COM]	MB			20%		
		Servicios [S]	MB			50%		
	[A.11] Acceso no autorizado	Instalaciones [L]	B		5%	20%		
		Hardware [HW]	B		5%	50%		
		Aplicación/Software [SW]	MB		50%	50%		
		Datos/Información [D]	MB		75%	75%		
		Redes de comunicación [COM]	MB		50%	75%		
		Servicios [S]	MB		50%	50%		
		Soportes de información [M]	B		100%	50%		
		Equipamiento auxiliar [AUX]	B		20%	20%		
	[A.12] Análisis de tráfico	Redes de comunicación [COM]	MB		100%			
	[A.13] Repudio	Datos/Información [D]	MB			5%		75%
		Servicios [S]	MB			5%		75%
	[A.14] Interceptación de información (escucha)	Redes de comunicación [COM]	MB		100%			
	[A.15] Modificación deliberada de la información	Instalaciones [L]	MB			5%		
		Aplicación/Software [SW]	MB			20%		
		Datos/Información [D]	MB			100%		
		Redes de comunicación [COM]	MB			20%		
		Servicios [S]	MB			50%		
		Soportes de información [M]	MB			50%		
	[A.18] Destrucción de información	Instalaciones [L]	MB				5%	
		Aplicación/Software [SW]	MB				75%	
		Datos/Información [D]	MB				75%	
		Servicios [S]	MB				75%	
		Soportes de información [M]	MB				5%	
	[A.19] Divulgación de información	Instalaciones [L]	B		20%			
		Aplicación/Software [SW]	MB		75%			
		Datos/Información [D]	B		100%			
		Redes de comunicación [COM]	B		50%			
		Servicios [S]	MB		75%			
		Soportes de información [M]	B		100%			
	[A.22] Manipulación de programas	Aplicación/Software [SW]	MB		75%	100%	75%	
	[A.23] Manipulación de los equipos	Hardware [HW]	MB		50%		75%	
		Soportes de información [M]	MB		75%		100%	
		Equipamiento auxiliar [AUX]	MB		5%		100%	
	[A.24] Denegación de servicio	Hardware [HW]	MB				5%	
		Redes de comunicación [COM]	B				100%	
		Servicios [S]	B				75%	
	[A.25] Robo	Hardware [HW]	B		5%		75%	
		Soportes de información [M]	B		100%		100%	
		Equipamiento auxiliar [AUX]	MB		5%		100%	
	[A.26] Ataque destructivo	Instalaciones [L]	MB				75%	
		Hardware [HW]	MB				75%	
		Soportes de información [M]	MB				100%	
		Equipamiento auxiliar [AUX]	MB				100%	
	[A.27] Ocupación enemiga	Instalaciones [L]	MB		20%		75%	
	[A.28] Indisponibilidad del personal	Personal [P]	A				75%	
	[A.29] Extorsión	Personal [P]	MB		20%	20%	20%	
	[A.30] Ingeniería social (picaresca)	Personal [P]	M		20%	20%	20%	

Anexo M. EFECTIVIDAD DE LOS CONTROLES ISO/IEC 27002:213 TRAS IMPLANTACIÓN DE PROYECTOS

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A5	**Políticas de seguridad de la información**		**10%**
A5.1	**Directrices de gestión de la seguridad de la información**		**10%**
A5.1.1	Políticas para la seguridad de la información	L1 - Inicial	10%
A5.1.2	Revisión de las políticas para la seguridad de la información	L1 - Inicial	10%
A6	**Organización de la seguridad de la información**		**64%**
A6.1	**Organización interna**		**38,00%**
A6.1.1	Roles y responsabilidades en seguridad de la información	L1 - Inicial	10%
A6.1.2	Segregación de tareas	L0 - Inexistente	0%
A6.1.3	Contacto con las autoridades	L0 - Inexistente	0%
A6.1.4	Contacto con grupos de interés especial	L3 - Definido	90%
A6.1.5	Seguridad de la información en la gestión de proyectos	L3 - Definido	90%
A6.2	**Los dispositivos móviles y el teletrabajo**		**90%**
A6.2.1	Política de dispositivos móviles	L3 - Definido	90%
A6.2.2	Teletrabajo	L3 - Definido	90%
A7	**Seguridad relativa a los recursos humanos**		**0%**
A7.1	**Antes del empleo**		**0%**
A7.1.1	Investigación de antecedentes	L0 - Inexistente	0%
A7.1.2	Términos y condiciones del empleo	L0 - Inexistente	0%
A7.2	**Durante el empleo**		**0%**
A7.2.1	Responsabilidades de gestión	L0 - Inexistente	0%
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	L0 - Inexistente	0%
A7.2.3	Proceso disciplinario	L0 - Inexistente	0%
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		**0%**
A7.3.1	Responsabilidades ante la finalización o cambio	L0 - Inexistente	0%
A8	**Gestión de activos**		**13%**
A8.1	**Responsabilidad sobre los activos**		**38%**
A8.1.1	Inventario de activos	L3 - Definido	90%
A8.1.2	Propiedad de los activos	L1 - Inicial	10%
A8.1.3	Uso aceptable de los activos	L0 - Inexistente	0%
A8.1.4	Devolución de activos	L2 - Repetible	50%
A8.2	**Clasificación de la información**		**0%**
A8.2.1	Clasificación de la información	L0 - Inexistente	0%
A8.2.2	Etiquetado de la información	L0 - Inexistente	0%
A8.2.3	Manipulado de la información	L0 - Inexistente	0%
A8.3	**Manipulación de los soportes**		**0%**
A8.3.1	Gestión de soportes extraíbles	L0 - Inexistente	0%
A8.3.2	Eliminación de soportes	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A9	**Control de acceso**		**90,00%**
A9.1	**Requisitos de negocio para el control de acceso**		**90%**
A9.1.1	Política de control de acceso	L3 - Definido	90%
A9.1.2	Acceso a las redes y a los servicios de red	L3 - Definido	90%
A9.2	**Gestión de acceso de usuario**		**90%**
A9.2.1	Registro y baja de usuario	L3 - Definido	90%
A9.2.2	Provisión de acceso de usuario	L3 - Definido	90%
A9.2.3	Gestión de privilegios de acceso	L3 - Definido	90%
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	L3 - Definido	90%
A9.2.5	Revisión de los derechos de acceso de usuario	L3 - Definido	90%
A9.2.6	Retirada o reasignación de los derechos de acceso	L3 - Definido	90%
A9.3	**Responsabilidades del usuario**		**90%**
A9.3.1	Uso de la información secreta de autenticación	L3 - Definido	90%
A9.4	**Control de acceso a sistemas y aplicaciones**		**90%**
A9.4.1	Restricción del acceso a la información	L3 - Definido	90%
A9.4.2	Procedimientos seguros de inicio de sesión	L3 - Definido	90%
A9.4.3	Sistema de gestión de contraseñas	L3 - Definido	90%
A9.4.4	Uso de utilidades con privilegios del sistema	L3 - Definido	90%
A9.4.5	Control de acceso al código fuente de los programas	No Aplica	#N/A
A10	**Criptografía**		**0%**
A10.1	**Controles criptográficos**		**0%**
A10.1.1	Política de uso de los controles criptográficos	L0 - Inexistente	0%
A10.1.2	Gestión de claves	L0 - Inexistente	0%
A11	**Seguridad física y del entorno**		**4%**
A11.1	**Áreas seguras**		**0%**
A11.1.1	Perímetro de seguridad física	L0 - Inexistente	0%
A11.1.2	Controles físicos de entrada	L0 - Inexistente	0%
A11.1.3	Seguridad de oficinas, despachos y recursos	L0 - Inexistente	0%
A11.1.4	Protección contra las amenazas externas y ambientales	L0 - Inexistente	0%
A11.1.5	El trabajo en áreas seguras	L0 - Inexistente	0%
A11.1.6	Áreas de carga y descarga	L0 - Inexistente	0%
A11.2	**Seguridad de los equipos**		**12%**
A11.2.1	Emplazamiento y protección de equipos	L1 - Inicial	10%
A11.2.2	Instalaciones de suministro	L0 - Inexistente	0%
A11.2.3	Seguridad del cableado	L0 - Inexistente	0%
A11.2.4	Mantenimiento de los equipos	L0 - Inexistente	0%
A11.2.5	Retirada de materiales propiedad de la empresa	L0 - Inexistente	0%
A11.2.6	Seguridad de los equipos fuera de las instalaciones	L3 - Definido	90%
A11.2.7	Reutilización o eliminación segura de equipos	L0 - Inexistente	0%
A11.2.8	Equipo de usuario desatendido	L1 - Inicial	10%
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A12	**Seguridad de las operaciones**		**54%**
A12.1	**Procedimientos y responsabilidades operacionales**		**40%**
A12.1.1	Documentación de procedimientos operacionales	L3 - Definido	90%
A12.1.2	Gestión de cambios	L1 - Inicial	10%
A12.1.3	Gestión de capacidades	L1 - Inicial	10%
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	L2 - Repetible	50%
A12.2	**Protección contra el software malicioso (malware)**		**95%**
A12.2.1	Controles contra el código malicioso	L4 - Gestionado	95%
A12.3	**Copias de seguridad**		**95%**
A12.3.1	Copias de seguridad de la información	L4 - Gestionado	95%
A12.4	**Registros y supervisión**		**50%**
A12.4.1	Registro de eventos	L3 - Definido	90%
A12.4.2	Protección de la información del registro	L1 - Inicial	10%
A12.4.3	Registros de administración y operación	L1 - Inicial	10%
A12.4.4	Sincronización del reloj	L3 - Definido	90%
A12.5	**Control del software en explotación**		**10%**
A12.5.1	Instalación del software en explotación	L1 - Inicial	10%
A12.6	**Gestión de la vulnerabilidad técnica**		**90%**
A12.6.1	Gestión de las vulnerabilidades técnicas	L3 - Definido	90%
A12.6.2	Restricción en la instalación de software	L3 - Definido	90%
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		**0%**
A12.7.1	Controles de auditoría de sistemas de información	L0 - Inexistente	0%
A13	**Seguridad de las comunicaciones**		**43%**
A13.1	**Gestión de la seguridad de las redes**		**63%**
A13.1.1	Controles de red	L4 - Gestionado	95%
A13.1.2	Seguridad de los servicios de red	L0 - Inexistente	0%
A13.1.3	Segregación en redes	L4 - Gestionado	95%
A13.2	**Intercambio de información**		**23%**
A13.2.1	Políticas y procedimientos de intercambio de información	L0 - Inexistente	0%
A13.2.2	Acuerdos de intercambio de información	L0 - Inexistente	0%
A13.2.3	Mensajería electrónica	L3 - Definido	90%
A13.2.4	Acuerdos de confidencialidad o no revelación	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		**0%**
A14.1	**Requisitos de seguridad en los sistemas de información**		**0%**
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	L0 - Inexistente	0%
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	L0 - Inexistente	0%
A14.1.3	Protección de las transacciones de servicios de aplicaciones	L0 - Inexistente	0%
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		**0%**
A14.2.1	Política de desarrollo seguro	L0 - Inexistente	0%
A14.2.2	Procedimiento de control de cambios en sistemas	L0 - Inexistente	0%
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0 - Inexistente	0%
A14.2.4	Restricciones a los cambios en los paquetes de software	L0 - Inexistente	0%
A14.2.5	Principios de ingeniería de sistemas seguros	L0 - Inexistente	0%
A14.2.6	Entorno de desarrollo seguro	L0 - Inexistente	0%
A14.2.7	Externalización del desarrollo de software	L0 - Inexistente	0%
A14.2.8	Pruebas funcionales de seguridad de sistemas	L0 - Inexistente	0%
A14.2.9	Pruebas de aceptación de sistemas	L0 - Inexistente	0%
A14.3	**Datos de prueba**		**0%**
A14.3.1	Protección de los datos de prueba	L0 - Inexistente	0%
A15	**Relación con proveedores**		**0%**
A15.1	**Seguridad en las relaciones con proveedores**		**0%**
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	L0 - Inexistente	0%
A15.1.2	Requisitos de seguridad en contratos con terceros	L0 - Inexistente	0%
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	L0 - Inexistente	0%
A15.2	**Gestión de la provisión de servicios del proveedor**		**0%**
A15.2.1	Control y revisión de la provisión de servicios del proveedor	L0 - Inexistente	0%
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	L0 - Inexistente	0%

Sección	Controles de Seguridad de la Información	Estado	Efectividad
A16	**Gestión de incidentes de seguridad de la información**		**90%**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		**90%**
A16.1.1	Responsabilidades y procedimientos	L3 - Definido	90%
A16.1.2	Notificación de los eventos de seguridad de la información	L3 - Definido	90%
A16.1.3	Notificación de puntos débiles de la seguridad	L3 - Definido	90%
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	L3 - Definido	90%
A16.1.5	Respuesta a incidentes de seguridad de la información	L3 - Definido	90%
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	L3 - Definido	90%
A16.1.7	Recopilación de evidencias	L3 - Definido	90%
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		**90%**
A17.1	**Continuidad de la seguridad de la información**		**90%**
A17.1.1	Planificación de la continuidad de la seguridad de la información	L3 - Definido	90%
A17.1.2	Implementar la continuidad de la seguridad de la información	L3 - Definido	90%
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L3 - Definido	90%
A17.2	**Redundancias**		**90%**
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	L3 - Definido	90%
A18	**Cumplimiento**		**0%**
A18.1	**Cumplimiento de los requisitos legales y contractuales**		**0%**
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	L0 - Inexistente	0%
A18.1.2	Derechos de Propiedad Intelectual (DPI)	L0 - Inexistente	0%
A18.1.3	Protección de los registros de la organización	L0 - Inexistente	0%
A18.1.4	Protección y privacidad de la información de carácter personal	L0 - Inexistente	0%
A18.1.5	Regulación de los controles criptográficos	L0 - Inexistente	0%
A18.2	**Revisiones de la seguridad de la información**		**0%**
A18.2.1	Revisión independiente de la seguridad de la información	L0 - Inexistente	0%
A18.2.2	Cumplimiento de las políticas y normas de seguridad	L0 - Inexistente	0%
A18.2.3	Comprobación del cumplimiento técnico	L0 - Inexistente	0%

Anexo N. DECLARACIÓN APLICABILIDAD

A continuación se muestra la declaración de aplicabilidad de los controles definidos en el anexo A de la ISO/IEC 27001:2013.

Junto con cada control, en la tabla se indica si aplica dicho control en RecycleSA, la justificación que explica su no aplicación, el estado de madurez, el origen del control y una descripción del mismo.

El origen del control se codifica siguiendo lo establecido en la siguiente tabla:

Código	Orígen
R	Análisis de Riesgos
L	Legal o normativo
I	Requerimiento interno
C	Requerimiento Contractual

La tabla con la declaración de aplicabilidad resultante es la siguiente:

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A5	**Políticas de seguridad de la información**								
A5.1	**Directrices de gestión de la seguridad de la información**								
A5.1.1	Políticas para la seguridad de la información	SI		Implantada		✓	✓		Se tienen que definir las políticas de seguridad de la información que sean aprobadas por la dirección y comunicadas a todos los trabajadores.
A5.1.2	Revisión de las políticas para la seguridad de la información	SI		Implantada		✓	✓		Las políticas de seguridad deben ser revisadas con cierta frecuencia o cuando ocurran cambios significativos.
A6	**Organización de la seguridad de la información**								
A6.1	**Organización interna**								
A6.1.1	Roles y responsabilidades en seguridad de la información	SI		Implantada			✓		Deben definirse y asignarse todas las responsabilidades relativas a la seguridad de la información.
A6.1.2	Segregación de tareas	SI		No implantada		✓	✓		Las funciones y tareas se deben segregar para reducir las modificaciones no autorizadas, no intencionadas o usos indebidos
A6.1.3	Contacto con las autoridades	SI		No implantada		✓	✓		Se deben mantener los contactos apropiados con las autoridades pertinentes en los casos necesarios.
A6.1.4	Contacto con grupos de interés especial	SI		Implantada		✓	✓		Se deben mantener contactos con grupos de interés especial para la mejora del conocimiento
A6.1.5	Seguridad de la información en la gestión de proyectos	SI		Implantada			✓		Se tiene que integrar para identificar los riesgos en el marco de cada proyecto.
A6.2	**Los dispositivos móviles y el teletrabajo**								
A6.2.1	Política de dispositivos móviles	SI		Implantada					Adoptar política de seguridad de dispositivos móviles para asegurar que no comprometen la seguridad de la información de la empresa.
A6.2.2	Teletrabajo	SI		Implantada					Se deben implementar política y medios técnicos para proteger la información accedida desde fuera del centro de trabajo.
A7	**Seguridad relativa a los recursos humanos**								
A7.1	**Antes del empleo**								
A7.1.1	Investigación de antecedentes	SI		No implantada			✓		Se deben comprobar los antecedentes de las nuevas incorporaciones de acuerdo a la ley.
A7.1.2	Términos y condiciones del empleo	SI		No implantada			✓	✓	Se deben establecer los términos y condiciones del contrato en lo que respecta a seguridad de la información para protegerla.
A7.2	**Durante el empleo**								
A7.2.1	Responsabilidades de gestión	SI		No implantada			✓		La dirección debe exigir cumplir las normas de seguridad a contratistas y empleados.
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI		No implantada			✓		Los empleados y contratistas deben recibir la formación adecuada.
A7.2.3	Proceso disciplinario	SI		No implantada			✓	✓	Debe existir un proceso disciplinario formal que recoja las acciones a tomar en caso de que se haya provocado una brecha de seguridad que sirva de formula preventiva.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**								
A7.3.1	Responsabilidades ante la finalización o cambio	SI		No implantada	✓	✓	✓	✓	Se deben definir, comunicar y cumplir las responsabilidades una vez finalizado el contrato o el cambio para proteger los intereses de la empresa.

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A8	**Gestión de activos**								
A8.1	**Responsabilidad sobre los activos**								
A8.1.1	Inventario de activos	SI		Implantada	✔		✔		Los activos deben estar claramente identificados y debería crearse y mantenerse un inventario de los mismos para identificar las medidas de protección adecuadas y su responsabilidad.
A8.1.2	Propiedad de los activos	SI		Implantada	✔		✔		Todos los activos del inventario deberían tener un propietario.
A8.1.3	Uso aceptable de los activos	SI		No implantada	✔		✔	✔	Se deben identificar, documentar e implementar las reglas de uso aceptable de los activos.
A8.1.4	Devolución de activos	SI		Implantada			✔	✔	Todos los empleados y terceros deben entregar todos los activos.
A8.2	**Clasificación de la información**								
A8.2.1	Clasificación de la información	SI		No implantada			✔		La información debe ser clasificada según la importancia con objeto de que reciba un adecuado nivel de protección.
A8.2.2	Etiquetado de la información	SI		No implantada			✔		Se debe desarrollar e implantar un método de etiquetado de la información.
A8.2.3	Manipulado de la información	SI		No implantada			✔		Se debe desarrollar e implantar un conjunto adecuado de procedimientos para la manipulación de la información.
A8.3	**Manipulación de los soportes**								
A8.3.1	Gestión de soportes extraíbles	SI		Implantada	✔		✔		Se deben implantar los procedimientos para la gestión de soportes extraíbles según el esquema de clasificación adoptado.
A8.3.2	Eliminación de soportes	SI		Implantada	✔		✔		Los soportes deben eliminarse de forma segura para evitar fugas de información.
A8.3.3	Soportes físicos en tránsito	**NO**	La organización no transporta soporte físicos fuera de sus límites físicos	No Aplica					
A9	**Control de acceso**								
A9.1	**Requisitos de negocio para el control de acceso**								
A9.1.1	Política de control de acceso	SI		Implantada	✔	✔	✔		Se debe implementar una política de control de acceso para limitar el mismo a los recursos y a la información, basada en los requisitos de negoricio y la seguridad de la información.
A9.1.2	Acceso a las redes y a los servicios de red	SI		Implantada	✔		✔		Solo se debe proporcionar acceso a las redes y servicios a los usuarios autorizados.
A9.2	**Gestión de acceso de usuario**								
A9.2.1	Registro y baja de usuario	SI		Implantada	✔		✔		Se debe implantar un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A9.2.2	Provisión de acceso de usuario	SI		Implantada	✔		✔		Se debe implantar un procedimiento que haga posible la asignación de derechos de acceso.
A9.2.3	Gestión de privilegios de acceso	SI		Implantada	✔		✔		La asignación y el uso de privilegios debe estar restringida y controlada.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI		Implantada	✔	✔	✔		La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A9.2.5	Revisión de los derechos de acceso de usuario	SI		Implantada	✔	✔			Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
A9.2.6	Retirada o reasignación de los derechos de acceso	SI		Implantada	✔				Los derechos de acceso a la información y a sus recursos deben ser retirados al finalizar la relación.
A9.3	**Responsabilidades del usuario**								
A9.3.1	Uso de la información secreta de autenticación	SI		Implantada	✔		✔		Se debe requerir a los usuarios el uso de la información secreta de autenticación para que sean responsables de salvaguardar la información.
A9.4	**Control de acceso a sistemas y aplicaciones**								
A9.4.1	Restricción del acceso a la información	SI		Implantada	✔		✔		Se debe restringir el acceso a la información y a las funciones de las aplicaciones para prevenir el acceso no autorizado.
A9.4.2	Procedimientos seguros de inicio de sesión	SI		Implantada		✔	✔		Se debe controlar el acceso a los sistemas de forma controlada mediante inicio de sesión.
A9.4.3	Sistema de gestión de contraseñas	SI		Implantada	✔				Los procesos de gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A9.4.4	Uso de utilidades con privilegios del sistema	SI		Implantada	✔		✔		Se debe controlar el uso de utilidades que pueden ser capaces de invalidar los sistemas con accesos privilegiados.
A9.4.5	Control de acceso al código fuente de los programas	**NO**	La organización no desarrolla aplicaciones	No Aplica					
A10	**Criptografía**								
A10.1	**Controles criptográficos**								
A10.1.1	Política de uso de los controles criptográficos	SI		No implantada	✔	✔	✔		Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.
A10.1.2	Gestión de claves	SI		No implantada		✔	✔		Se debe desarrollar e implantar una política sobre el ciclo de
A11	**Seguridad física y del entorno**								
A11.1	**Áreas seguras**								
A11.1.1	Perímetro de seguridad física	SI		No implantada			✔		Se deben utilizar sistemas para proteger el perímetro de seguridad para proteger áreas que contienen información sensible.
A11.1.2	Controles físicos de entrada	SI		No implantada			✔		Las áreas seguras deben estar protegidas mediante controles de entrada adecuados.
A11.1.3	Seguridad de oficinas, despachos y recursos	SI		No implantada			✔		Se debe aplicar métodos de seguridad física para estos entornos.
A11.1.4	Protección contra las amenazas externas y ambientales	SI		No implantada			✔		Se debe implementar protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A11.1.5	El trabajo en áreas seguras	SI		No implantada			✔		Se debe implementar procedimientos de trabajos en áreas seguras como el centro de datos.
A11.1.6	Áreas de carga y descarga	SI		No implantada			✔		Se deben controlar las áreas de carga y descarga para prevenir accesos no autorizados.

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A11.2	**Seguridad de los equipos**								
A11.2.1	Emplazamiento y protección de equipos	SI		Implantada	✔		✔		Los equipos se deben proteger de forma que se reduzcan los riesgos de pérdida, daño o robo.
A11.2.2	Instalaciones de suministro	SI		No implantada			✔		Los equipos deberán estar protegidos contra fallos de alimentación.
A11.2.3	Seguridad del cableado	SI		No implantada	✔		✔		El cableado eléctrico y de telecomunicaciones deberá estar protegido frente intercepciones, interferencias o daños.
A11.2.4	Mantenimiento de los equipos	SI		No implantada	✔		✔		Se debe implantar un correcto mantenimiento sobre los equipos y sistemas.
A11.2.5	Retirada de materiales propiedad de la empresa	SI		No implantada		✔	✔		Sin autorización no se deben sacar los equipos y sistemas de las instalaciones de la empresa.
A11.2.6	Seguridad de los equipos fuera de las instalaciones	SI		Implantada	✔	✔	✔		Se debe aplicar medidas de seguridad para los equipos situados fuera de las instalaciones.
A11.2.7	Reutilización o eliminación segura de equipos	SI		No implantada	✔		✔		Se debe comprobar que todos los soportes con información sensible de elimine de manera segura.
A11.2.8	Equipo de usuario desatendido	SI		Implantada	✔				Los usuarios deben asegurarse que el equipo queda bloqueado cuando esté desatendido.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI		No implantada	✔				Se debe mantener el puesto de trabajo libre de información
A12	**Seguridad de las operaciones**								
A12.1	**Procedimientos y responsabilidades operacionales**								
A12.1.1	Documentación de procedimientos operacionales	SI		Implantada	✔		✔		Se deben documentar y mantener la documentación de las operaciones y ponerla a disposición de los usuarios que la necesiten.
A12.1.2	Gestión de cambios	SI		Implantada	✔		✔		Los cambios que afecten a la seguridad de la información deben ser controlados.
A12.1.3	Gestión de capacidades	SI		Implantada			✔		Se debe supervisar y ajustar la utilización de los recursos a la demanda de capacidad presente y de proyectos futuros.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	SI		Implantada	✔	✔	✔		Se deben separar estos entornos para evitar riesgos de acceso no autorizados o cambios.
A12.2	**Protección contra el software malicioso (malware)**								
A12.2.1	Controles contra el código malicioso	SI		Implantada	✔		✔		Se deben implantar sistemas de control contra malware en los sistemas.
A12.3	**Copias de seguridad**								
A12.3.1	Copias de seguridad de la información	SI		Implantada	✔	✔	✔	✔	Se deben realizar copias de seguridad de la información crítica con la política de seguridad acordada
A12.4	**Registros y supervisión**								
A12.4.1	Registro de eventos	SI		Implantada		✔	✔		Se deben registras los eventos de los sistemas, protegerlos y revisarlos periódicamente.
A12.4.2	Protección de la información del registro	SI		Implantada	✔	✔			Los dispositivos de registro y la información afín deben ser correctamente protegida.
A12.4.3	Registros de administración y operación	SI		Implantada	✔	✔			Se deben registrar, proteger y revisar los registros de administración de los sistemas.
A12.4.4	Sincronización del reloj	SI		Implantada		✔	✔		Los relojes de todos los sistemas de la empresa deben estar sincronizados desde una fuente única y precisa.
A12.5	**Control del software en explotación**								
A12.5.1	Instalación del software en explotación	SI		Implantada	✔	✔	✔		Se deben implementar procedimientos para controlar la instalación de software en explotación.
A12.6	**Gestión de la vulnerabilidad técnica**								
A12.6.1	Gestión de las vulnerabilidades técnicas	SI		Implantada	✔	✔	✔		Se debe obtener información de las vulnerabilidades técnicas de los sistemas, evaluarlas y adoptar medidas de seguridad
A12.6.2	Restricción en la instalación de software	SI		Implantada	✔	✔	✔		Se deben aplicar reglas que rijan la instalación de software
A12.7	**Consideraciones sobre la auditoria de sistemas de información**								
A12.7.1	Controles de auditoría de sistemas de información	SI		No implantada			✔		Se deberán planificar y ejecutar las auditorias pactadas en la política de seguridad.
A13	**Seguridad de las comunicaciones**								
A13.1	**Gestión de la seguridad de las redes**								
A13.1.1	Controles de red	SI		Implantada	✔	✔	✔		Se deben implantar sistemas para gestionar, controlar y proteger la red de la empresa.
A13.1.2	Seguridad de los servicios de red	SI		No implantada			✔		Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.
A13.1.3	Segregación en redes	SI		Implantada	✔				Los grupos de servicios de información, sistemas y usuarios deben estar segregados en redes distintas.
A13.2	**Intercambio de información**								
A13.2.1	Políticas y procedimientos de intercambio de información	SI		No implantada			✔		Se deben implantar políticas que protejan la información cuando sea trasferida.
A13.2.2	Acuerdos de intercambio de información	SI		No implantada			✔	✔	Se deben establecer acuerdos para el intercambio seguro de información con terceros.
A13.2.3	Mensajería electrónica	SI		Implantada	✔		✔	✔	La información objeto de mensajería electrónica debe estar adecuadamente protegida.
A13.2.4	Acuerdos de confidencialidad o no revelación	SI		Implantada		✔	✔	✔	Se deben implementar y revisar acuerdos de no revelación de la información con terceros.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**								
A14.1	**Requisitos de seguridad en los sistemas de información**								
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI		No implantada	✔		✔		Los nuevos sistemas implementados deben cumplir los requisitos de seguridad de la información.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI		No implantada		✔	✔		Se debe proteger la información que se transmite a través de redes públicas.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	SI		No implantada		✔	✔		Se debe proteger las transacciones de servicios de aplicaciones.

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**								
A14.2.1	Política de desarrollo seguro	SI		No implantada			✔	✔	Se deben establecer y aplicar normas para el desarrollo seguro de las aplicaciones de la empresa.
A14.2.2	Procedimiento de control de cambios en sistemas	SI		No implantada	✔		✔		La implantación de cambios debe controlarse a lo largo del ciclo de vida mediante procedimientos formales.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI		No implantada			✔		Cuando se realicen cambios en los Sistemas Operativos las aplicaciones de negocio críticas deben ser revisadas y probadas.
A14.2.4	Restricciones a los cambios en los paquetes de software	SI		No implantada			✔		Por norma no se permiten modificaciones en los paquetes software
A14.2.5	Principios de ingeniería de sistemas seguros	SI		No implantada			✔		Se deberían establecer, documentar, mantener y aplicarse principios de ingeniería seguros a todos los sistemas de información de la empresa.
A14.2.6	Entorno de desarrollo seguro	SI		No implantada		✔	✔		Se deben proteger adecuadamente los entornos de desarrollo seguro.
A14.2.7	Externalización del desarrollo de software	SI		No implantada			✔	✔	El desarrollo del software externalizado debería ser supervisoado y controlado por la organización.
A14.2.8	Pruebas funcionales de seguridad de sistemas	SI		No implantada			✔		Se deben llevar a cabo pruebas funciones durante el desarrollo de aplicaciones.
A14.2.9	Pruebas de aceptación de sistemas	SI		No implantada			✔		Se deben establecer baterías de pruebas de aceptación y criterios relacionados para nuevos sistemas que pasen a producción.
A14.3	**Datos de prueba**								
A14.3.1	Protección de los datos de prueba	SI		No implantada		✔	✔		Los datos de prueba se deben seleccionar con cuidado y deberían ser protegidos y controlados.
A15	**Relación con proveedores**								
A15.1	**Seguridad en las relaciones con proveedores**								
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI		No implantada	✔		✔		Se deben acordar las políticas de acceso de los proveedores a los sistemas de información de la empresa y a los activos.
A15.1.2	Requisitos de seguridad en contratos con terceros	SI		No implantada			✔		Se deben establecer y acordar con cada proveedor los requisitos relacionados con la seguridad.
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI		No implantada			✔		La cadena de suministros acordada con los proveedores debe incluir requisitos ante los riesgos relacionados con las TIC.
A15.2	**Gestión de la provisión de servicios del proveedor**								
A15.2.1	Control y revisión de la provisión de servicios del proveedor	SI		No implantada			✔		Se debe controlar, revisar y auditar los servicios de proveedor.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	SI		No implantada			✔		Se deben gestionar los cambios en la provisión del servicio proporcionado por lo profesores teniendo en cuenta la criticidad del sistema.
A16	**Gestión de incidentes de seguridad de la información**								
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**								
A16.1.1	Responsabilidades y procedimientos	SI		Implantada		✔	✔		Se deben establecer responsabilidades y procesos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes.
A16.1.2	Notificación de los eventos de seguridad de la información	SI		Implantada		✔	✔		Los eventos de seguridad de la información se deberán notificar por los canales de gestión adecuados lo antes posible.
A16.1.3	Notificación de puntos débiles de la seguridad	SI		Implantada			✔		Todos los usuarios deben notificar cualquier punto que afecte a la seguridad de la información.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI		Implantada			✔		Los eventos de seguridad de la información deben ser evaluados y clasificados apropiadamente.
A16.1.5	Respuesta a incidentes de seguridad de la información	SI		Implantada	✔		✔		Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI		Implantada	✔		✔		El conocimiento obtenido de los incidentes de seguridad deberá ser utilizado para reducir la probabilidad de ocurrencia a futuro.
A16.1.7	Recopilación de evidencias	SI		Implantada		✔	✔		Se deben definir y aplicar procedimientos para la aplicación, recogida, adquisición y preservación de información que pueda servir de evidencia.
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**								
A17.1	**Continuidad de la seguridad de la información**								
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI		Implantada	✔	✔	✔		Se debe determinar las necesidades de continuidad de negocio para la gestión de la seguridad de la información en situaciones adversas.
A17.1.2	Implementar la continuidad de la seguridad de la información	SI		Implantada	✔	✔	✔		Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información en situaciones adversas .
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI		Implantada			✔		Se deben controlar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces.
A17.2	**Redundancias**								
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI		Implantada	✔		✔		Los recursos que tratan la seguridad de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de seguridad.

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A18	**Cumplimiento**								
A18.1	**Cumplimiento de los requisitos legales y contractuales**								
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI		No implantada		✓	✓		Todos los requisitos pertinentes y el enfoque de la empresa para cumplirlos se deben definir de forma explícita documentarse y mantenerse actualizados para cada sistema de información de la organización
A18.1.2	Derechos de Propiedad Intelectual (DPI)	SI		No implantada		✓	✓	✓	Se deben implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legales respecto a los derechos de propiedad intelectual.
A18.1.3	Protección de los registros de la organización	SI		No implantada			✓		Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizado.
A18.1.4	Protección y privacidad de la información de carácter personal	SI		No implantada		✓	✓		Se debe garantizar la protección y la privacidad de los datos según la regulación vigente.
A18.1.5	Regulación de los controles criptográficos	SI		No implantada		✓	✓		Se deben utilizar los controles criptográficos según las leyes y regulaciones de aplicación.
A18.2	**Revisiones de la seguridad de la información**								
A18.2.1	Revisión independiente de la seguridad de la información	SI		No implantada			✓		La seguridad de la información de la empresa debe someterse a una revisión independiente a intervalos regulares o siempre que se realicen cambios significativos.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI		No implantada			✓		La dirección de la empresa debe asegurarse que todos los procedimientos relativos a la seguridad se realizan correctamente con el fin de cumplir el cumplimiento legal y normativo.
A18.2.3	Comprobación del cumplimiento técnico	SI		No implantada			✓		Se debe comprobar periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Anexo O. CUMPLIMIENTO REQUERIMIENTOS ISO/IEC 27001:2013

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
4	**Contexto de la organización**		
4.1	Comprensión de la organización y de su contexto	OK	La organización tiene identificada y documentada las cuestiones externas e internas pertinentes
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	NC-	No están documentados todos los requisitos legales y contractuales.
4.3	Determinación del alcance del SGSI	OK	El alcance está definido en el documento de Contexto, Requerimientos y alcance del SGSI
4.4	SGSI	OK	El SGSI está implementado y los los procesos de mejora continua definidos
5	**Liderazgo**		
4.1	Liderazgo y compromiso	OK	La alta dirección está plenamente comprometida con el sistema de gestion de la seguridad.
5.2	Política	OK	La politica de seguridad está plenamente definida, es acorde a lo establecido aen la norma y es accesible a toda la organización.
5.3	Roles, responsabilidades y autoridades en la organización	OK	Los roles y responsabilidades están asignados y comunicados en la organización.
6	**Planificación**		
6.1	Acciones para tratar los riesgos y oportunidades	NC-	No están documentados los crierios para llevar a cabo las apreciaciones de riesgo.
6.2	Objetivos de seguridad de la información y planificación para su consecución	OK	Los objetivos objetivos de la seguridad de la informacion son coherentes y medibles, y son comunicados y actualizados adecuadamente.
7	**Soporte**		
7.1	Recursos	OK	Aunque limitados, la alta dirección proporciona recursos suficientes para la implantación, mantenimiento y mejora continual del sistema de gestión
7.2	Competencia	NC-	No están documentadas las evidencias de competencias de todos los actores del sistema de gestión de información
7.3	Concienciación	OK	Se imparten cursos de concienciación en seguridad de la información a toda la organización
7.4	Comunicación	OK	Están definidos y documentados los procedimientos para las comunicaciones internas y externas
7.5	Información documentada	NC+	No está documentada toda la información requerida: Requerimientos legales, regulatorios y contractuales, política de seguridad para proveedores y algunos procedimientos operativos de gestión de TI.
8	**Operación**		
8.1	Planificación y control operacional	NC+	No se planifican y controlan acciones para el tratamiento de riesgos.
8.2	Apreciación de los riesgos de seguridad de la información	NC-	No hay evidencias de de los resultados de apreciación del riesgo.
8.3	Tratamiento de los riesgos de seguridad de la información	NC+	NO hay evidencia de información documentada de los resultados del tratamiento de los riesgos de seguridad
9	**Evaluación del desempeño**		
9.1	Seguimiento, medición, análisis y evaluación	NC+	No están documentadas evidencias de seguimiento, medición, análisis y evaluación del desempeño del sistema de gestión.
9.2	Auditoría interna	OK	Se planifican y realizan las auditorías internas conforme a lo establecido por la norma.
9.3	Revisión por la dirección	OK	La Alta Dirección revisa el sistema de gestión de seguridad de la información.
10	**Mejora**		
10.1	No conformidad y acciones correctivas	OK	Las no conformidades se analizan y generan las acciones correctivas adecuadas.
10.2	Mejora continua	OK	Se han definido los procesos necesarios para la mejora continua del sistema de gestión de la seguridad de la información.

Anexo P. CUMPLIMIENTO CONTROLES

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	SI	NC+	Aunque se ha definido la Política de Seguridad y algunas políticas espécificas, faltan otras políticas, alguna de ellas obligatorias como la política de seguridad de proveedores y
A5.1.2	Revisión de las políticas para la seguridad de la información	SI	OK	Revisiones definidas en la Política de Seguridad
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	SI	NC-	Las responsabilidades se encuentran definidas conforme a la Política de Seguridad definida, pero no han recibido la formacion adecuada a sus responsabilidades en seguridad.
A6.1.2	Segregación de tareas	SI	NC+	Aunque existen grupos de trabajo difeenciados, existen tareas que autoriza y realiza la misma pesona. No hay definida una política para la segregación de tareas.
A6.1.3	Contacto con las autoridades	SI	NC+	No esixten procedimientos documentados que especifiquen cuando y con qué autoridades se debería contactar.
A6.1.4	Contacto con grupos de interés especial	SI	OK	Se mantienen contactos con proveedores de servicios de seguridad.. Suscripción a diversos boletines de seguridad.
A6.1.5	Seguridad de la información en la gestión de proyectos	SI	OK	La seguridad se tiene en cuenta en al implantación de todos los proyectos.
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles	SI	OK	Definición de política. Cifrado de portátiles. Implantación de solución MDM para la gestión de dispositivos móviles.
A6.2.2	Teletrabajo	SI	OK	Definición de política. Utilización de solución VPN para acceso remoto seguro.
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	SI	NC+	No se realiza ningún tipo de comprbación de referencias ni confirmación de cualificaciones académicas.
A7.1.2	Términos y condiciones del empleo	SI	NC+	En los contratos no se incluyen clausulas relativas a la seguridad de la información, más alla de una simple cláusuala de deber de confidencialidad.
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	SI	NC-	No se notifican a las contratas los requereimientos de la política de seguridad
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	NC-	Planificada formación a empleados. Pero no se verifica que los contratistas tengan la formación adecuada en seguridad
A7.2.3	Proceso disciplinario	SI	NC+	NO existe proceso disciplanario formal para el incumplimiento de medidas de seguridad.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio	SI	NC+	No se ha establecido procedimiento para comunicar las respensabilidades que se mantienen tras la baja de de usuarios y/o contratistas.
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos	SI	OK	Existe inventario de activos
A8.1.2	Propiedad de los activos	SI	NC-	NO se encuentra documentado el propietario de diversos activos
A8.1.3	Uso aceptable de los activos	SI	NC+	No se ha definido política para el uso aceptable de los diferentes activos.
A8.1.4	Devolución de activos	SI	OK	Existe procedimiento para la devolución de los activos de los usuarios
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	SI	NC+	No se realiza clasificación de la información que pemita protegerla adecuadametne en función de su importancia
A8.2.2	Etiquetado de la información	SI	NC+	NO se etiqueta la información
A8.2.3	Manipulado de la información	SI	NC+	NO existen procedimientos para la maniulación de la información
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles	SI	NC+	No existen procedimientos para la gestión de soportes extraibles
A8.3.2	Eliminación de soportes	SI	NC+	No existen procedimientos para la eliminación segura de soportes extraibles
A8.3.3	Soportes físicos en tránsito	**NO**		

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A9	**Control de acceso**			
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	SI	OK	Políitca de control de acceso definida e implantada
A9.1.2	Acceso a las redes y a los servicios de red	SI	OK	Todos los accesos a las redes y servicios deben ser solicitados y autorizados
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	SI	OK	Existe procedimiento de altas y bajas
A9.2.2	Provisión de acceso de usuario	SI	OK	Existe procedimiento para asignación de derechos
A9.2.3	Gestión de privilegios de acceso	SI	OK	Se gestiona la asignación de privilegios en función de las necesades de uso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI	OK	Procesos definidos en el proyeto de política y auditoría de control de acesos
A9.2.5	Revisión de los derechos de acceso de usuario	SI	OK	Definida en la política de control de accesos
A9.2.6	Retirada o reasignación de los derechos de acceso	SI	OK	Definida en la política de control de accesos
A9.3	**Responsabilidades del usuario**			
A9.3.1	Uso de la información secreta de autenticación	SI	OK	Definida en la polítca de control de accesos y concienciados los usuarios en los planes de formación
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	SI	OK	Todo acceso requiere autenticación previa
A9.4.2	Procedimientos seguros de inicio de sesión	SI	OK	Se utilizan medios de autenticación seguros de los fabricantes de los productos: Directorio activo, SAP,..
A9.4.3	Sistema de gestión de contraseñas	SI	OK	Definindas las olíticas de contraseñas y aplicadas en el Directorio Activo y resto fabricantes
A9.4.4	Uso de utilidades con privilegios del sistema	SI	OK	Definida política e identificadas las cuentas
A9.4.5	Control de acceso al código fuente de los programas	**NO**		
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos	SI	NC+	No existe política sobre controles criptográficos
A10.1.2	Gestión de claves	SI	NC+	No exite política sobre el ciclo de vida de claves.
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	SI	NC+	No hay definidos perímetros de seguridad física ni procedimientos formales de acceso a las salas técnicas.
A11.1.2	Controles físicos de entrada	SI	NC+	No hay definidas areas seguras ni controles de acceso a dichas áreas
A11.1.3	Seguridad de oficinas, despachos y recursos	SI	NC+	No existen directrices para asegurar las oficinas y despachos
A11.1.4	Protección contra las amenazas externas y ambientales	SI	NC+	No existen directrices, relativas a la seguridad de la información, para protección ante estas amenazas
A11.1.5	El trabajo en áreas seguras	SI	NC+	No se han definido areas seguras. No ha procedimientos para trabajar en salas técnicas
A11.1.6	Áreas de carga y descarga	SI	NC+	No hay procedimientos específicos, relativos a la seguridad de la información, para areas de carga y descarga
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	SI	NC+	No existen politicas ni procedimientos específicos para el emplazamiento y protección de los equipos
A11.2.2	Instalaciones de suministro	SI	NC+	No existen procedimientos para evaluar y/o inspeccionar regularmente las instalaciones de suministro
A11.2.3	Seguridad del cableado	SI	NC+	No existen procedimientos ni directrices para la seguridad del cableado.
A11.2.4	Mantenimiento de los equipos	SI	NC+	No existe procedimientos formales ni registros para el mantenidimiento de los equipos
A11.2.5	Retirada de materiales propiedad de la empresa	SI	NC+	NO existen procedimientos para la autorización de retirada de materiales de las oficinas
A11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	OK	Concienciación de usuarios mediante planes de formación. Cifrado de equipos.
A11.2.7	Reutilización o eliminación segura de equipos	SI	NC+	No existen procedimientos definidos para la eliminación segura de los equipos
A11.2.8	Equipo de usuario desatendido	SI	OK	Políticas de Directorio Activo. Formación de usuarios.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	NC+	Política de puesto de trabajo despejado no definida
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales	SI	OK	Los procedimientos operativos se encuentran documentados y desponbiles
A12.1.2	Gestión de cambios	SI	OK	Se realiza proceso de gestiónde cambios en base a ITIL
A12.1.3	Gestión de capacidades	SI	OK	Se realiza proceso de gestión de capacidades en base a ITIL
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	SI	OK	Existen entornos de desarrollo, pruebas y operación difrenciados y con accesos difrenciados.
A12.2	**Protección contra el software malicioso (malware)**			
A12.2.1	Controles contra el código malicioso	SI	OK	Software de gestión de antivirus implantado y gestionado.
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	SI	OK	Políticas de backup implantadas para toda la infraestructura

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A12.4	**Registros y supervisión**			
A12.4.1	Registro de eventos	SI	OK	Plataforma SIEM implantada y gestionada
A12.4.2	Protección de la información del registro	SI	OK	Se realiza copia de seguridad de la información de registro
A12.4.3	Registros de administración y operación	SI	OK	Se registran y auditan las activaidades de los administradores y operadores de los sistemas
A12.4.4	Sincronización del reloj	SI	OK	Sincronización de infraestructura mediante fuentes de tiempo
A12.5	**Control del software en explotación**			
A12.5.1	Instalación del software en explotación	SI	OK	Restricción de privilegios en PCs. Herramienta SCCM para el inventario automático de software
A12.6	**Gestión de la vulnerabilidad técnica**			
A12.6.1	Gestión de las vulnerabilidades técnicas	SI	OK	Parcheado automático mediante SCCM en puestos de trabajo. Parcheado manual en servidores
A12.6.2	Restricción en la instalación de software	SI	OK	Usuarios de PCs no son adminstradores de sus máquinas
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información	SI	NC+	NO existen políticias ni procedimientos de auditoria definidos.
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	SI	OK	Se utilizan Firewalls, proxys, IPS, antivirus
A13.1.2	Seguridad de los servicios de red	SI	OK	Se utilizan Firewalls, proxys, IPS, antivirus
A13.1.3	Segregación en redes	SI	OK	VLANS específicas para usuarios, impresras, wifi, servidores, DMZ, etc.
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A13.2.2	Acuerdos de intercambio de información	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A13.2.3	Mensajería electrónica	SI	OK	El servicio de correo se basa en Office 365 y está debidamente protegido mediante autenticación y cifrado
A13.2.4	Acuerdos de confidencialidad o no revelación	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	NC+	No hay procedimiento formal para validar los requisitos de seguridad de los nuevos proyectos o sistemas
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI	NC+	No se ha definido el nivel de protección necesario para la información que se transmita por redes públicas
A14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	NC+	No se han definido controles para la protección de transacciones de servicios de aplicaciones
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	SI	NC+	No se han definido normas para el desarrollo seguro de las aplicaciones
A14.2.2	Procedimiento de control de cambios en sistemas	SI	NC+	No se han establecido procedimientos formales para la gestión de cambios en los sistemas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	NC+	No se han definido procedimientos formales para la revisión
A14.2.4	Restricciones a los cambios en los paquetes de software	SI	NC+	No se han documentdo normas para la limitación de la modificación de los paquetes de software
A14.2.5	Principios de ingeniería de sistemas seguros	SI	NC+	No existe documento que reflejen los principios de ingeniería de sistemas seguros
A14.2.6	Entorno de desarrollo seguro	SI	NC+	No se ha documentado los requisitos de seguridad de los entornos de desarrollo
A14.2.7	Externalización del desarrollo de software	SI	NC+	No exige a alos proveedores de desarrollo la presentación de la realización de pruebas de seguridad
A14.2.8	Pruebas funcionales de seguridad de sistemas	SI	NC+	No se realizan pruebas de seguridad funcional durante el desarrollo
A14.2.9	Pruebas de aceptación de sistemas	SI	NC+	No se establecen por norma pruebas de aceptación y criterios formales de los nuevos desarrollos
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba	SI	NC+	No se realiza selección de datos de prueba utilizando criterios de seguridad
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	NC+	No hay definida política de seguridad para proveedores
A15.1.2	Requisitos de seguridad en contratos con terceros	SI	NC+	No hay definida política de seguridad para proveedores
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	NC+	No hay definida política de seguridad para proveedores
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	NC+	No hay definida política de seguridad para proveedores
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	SI	NC+	No hay definida política de seguridad para proveedores

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
A16.1.1	Responsabilidades y procedimientos	SI	OK	Responsabilidades definidas en los procedimientos de gestión de incidentes de seguridad
A16.1.2	Notificación de los eventos de seguridad de la información	SI	OK	Se utilizan los canales de información definidos en los procedimientos
A16.1.3	Notificación de puntos débiles de la seguridad	SI	OK	Todos los empleados han sido formados en la necesiad de informar sobre las debilidades de la seguridad
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI	OK	Se siguen los procedimienos de gestión de incidente de seguridad definidos
A16.1.5	Respuesta a incidentes de seguridad de la información	SI	OK	Se siguen los procedimienos de gestión de incidente de seguridad definidos
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	OK	Se constata que se evalúan posteriormente los incidentes de seguridad
A16.1.7	Recopilación de evidencias	SI	OK	Se siguen los procedimienos de gestión de incidente de seguridad definidos
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI	OK	Definido Plan de continuidad de negocio
A17.1.2	Implementar la continuidad de la seguridad de la información	SI	OK	Plan de continuidad de negocio implantado y mantenido
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	OK	Plan de continuidad de negocio revisado periodicamente
A17.2	**Redundancias**			
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI	OK	Definidos e implantados según el plan de continuidad de negocio
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	NC+	No están documentados los requerimientos legales, regulatorios y contractuales
A18.1.2	Derechos de Propiedad Intelectual (DPI)	SI	NC+	No hay procedimientos para garantizar el cumplimiento de los requisitos legales
A18.1.3	Protección de los registros de la organización	SI	NC+	No están documentados y categroizados los registros de la organización
A18.1.4	Protección y privacidad de la información de carácter personal	SI	NC+	No hay definida una política de privacidad y protección de los datos de carácter personal
A18.1.5	Regulación de los controles criptográficos	SI	NC+	No hay evidencias de controles criptograficos
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información	SI	NC+	No se realizan auditorías externoas
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	NC+	No se verifica por la dirección que los procedimientos de seguridad se realizan correctametne
A18.2.3	Comprobación del cumplimiento técnico	SI	NC+	No se realizan pruebas de instrusión ni, chequeos completos de vulnerabilidades

Anexo Q. INFORME DE AUDITORÍA

Informe auditoría interna

Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001: 2013

RecycleSA

Control de Versiones		
0.0	25/07/209	Borrador
1.0	30/07/2019	Informe final

Datos Auditoría	
Organización auditada	RecycleSA
Lugar	Oficinas España- Sede 2
Fecha	Julio 2019
Idioma	Español

Equipo de auditoría	
JBA	Auditor responsable y procesos generales
CGR	Auditor procesos orientados IT

1. INTRODUCCIÓN

Este informe de auditoría interna pretende determinar el grado de cumplimiento del Sistema de Gestión de Seguridad de RecycleSA con la norma ISO/IEC 27001:2013.

Es el resultado de la primera auditoría interna del SGSI de RecycleSA que se realiza como parte del plan de auditoría establecido por la organización para la implantación y mejora de su SGSI.

2. ALCANCE

El Plan Director de Seguridad que se desea implantar en RecycleSA pretende adecuar a la norma ISO/IEC 27001:2013 todos los procesos y procedimientos, tanto organizativos como técnicos, relacionados con los Sistemas de Información de la organización.

Esta auditoría abarca todos los Sistemas de Información que incluye el SGSI de RecycleSA, que son:

- Sistemas relativos a los procesos productivos de RecycleSA: Servicios de reciclaje.
- Servicios financieros.
- Recursos Humanos.
- Legal.
- Seguridad y Medio Ambiente.
- Desarrollo de negocio.
- Tecnologías de la información.

La auditoría se realiza sobre todos los dominios y controles que establece la norma ISO/IEC 27001:2013.

3. CRITERIOS

Esta auditoría sigue los criterios establecidos por:

- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27002:2013

4. PLAN DE AUDITORÍA:

La auditoría de cumplimento se ha realizado conforme a la siguiente planificación:

- Fase 1. Primer trimestre 2019. Auditoría de **procesos generales**.

  Se auditan los controles correspondientes a procesos más generales, que corresponden a los siguientes dominios de la ISO/IEC 27002:2013:

  - 5 Políticas de seguridad de la información.
  - 6 Organización de la seguridad de la información.
  - 7 Seguridad de los recursos humanos.
  - 8 Gestión de activos.
  - 15 Relaciones de proveedores.
  - 16 Gestión de incidentes de seguridad de la información.
  - 17 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
  - 18 Cumplimiento.

- Fase 2. Segundo trimestre 2019. Auditoría de **procesos orientados a IT.**

  Se auditan los controles correspondientes a procesos orientados a IT y que requieren de conocimientos en esta materia del auditor designado. Es decir:

  - 9 Control de acceso.
  - 10 Criptografía.
  - 11 Seguridad física y medioambiental.
  - 12 Seguridad operacional.
  - 13 Seguridad de las comunicaciones.
  - 14 Adquisición, desarrollo y mantenimiento del sistema.

5. REGISTROS DE AUDITORÍA:

a. DOCUMENTACIÓN CONSULTADA

Para la realización de esta auditoría se ha consultando la siguiente documentación

Documentos	Políticas	Procedimientos
. ▪ Contexto, requerimientos y alcance SGSI ▪ Declaración de aplicabilidad ▪ Roles y responsabilidades de Seguridad ▪ Inventario de activos ▪ Plan de continuidad de negocio ▪ Análisis de Riesgos	▪ Política de Seguridad ▪ Política de control de acceso. ▪ Política de seguridad de dispositivos móviles. ▪ Política de uso aceptable de los activos ▪ Política de contraseñas ▪	▪ Procedimiento de auditorías internas ▪ Procedimientos de operación de TI ▪ Procedimiento de gestión de incidentes ▪ Procedimientos de continuidad de negocio ▪ Procedimiento de altas y bajas de usuario. ▪ Procedimiento de asignación y retirada de privilegios.

b. PERSONAL ENTREVISTADO

El siguiente personal ha sido entrevistado durante la auditoría de cumplimiento:

- Responsable de Seguridad.
- Responsable Servicio de reciclaje acero.
- Responsable Servicios de reciclaje aluminio.
- Responsable Departamento Legal.
- Responsable Recursos Humanos.
- Responsable TI.
- IT Service Manager Infraestructura, puesto de trabajo.
- IT Service Manager Movilidad, web corporativas y gestión documental.

6. RESULTADO DE LA AUDITORÍA:

A continuación se muestran los hallazgos de auditoría detectados tanto para los requerimientos de la ISO/IEC 27001:2013 como para los distintos controles. Se contemplan dos tipos de hallazgos:

- **No Confirmad Mayor**: Incumplimiento de un requisito normativo que vulnera o pone en serio riesgo la integridad del Sistema de Gestión
- **No Conformidad Menor**: Desviación mínima en relación a los requisitos normativos que no afecta a la eficiencia e integridad del Sistema de Gestión

a. REQUERIMIENTOS ISO/IEC 27001:2013

No conformidades mayores

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
7	**Soporte**		
7.5	Información documentada	NC+	No está documentada toda la información requerida: Requerimientos legales, regulatorios y contractuales, política de seguridad para proveedores y algunos procedimientos operativos de gestión de TI.
8	**Operación**		
8.1	Planificación y control operacional	NC+	No se planifican y controlan acciones para el tratamiento de riesgos.
8.3	Tratamiento de los riesgos de seguridad de la información	NC+	NO hay evidencia de información documentada de los resultados del tratamiento de los riesgos de seguridad
9	**Evaluación del desempeño**		
9.1	Seguimiento, medición, análisis y evaluación	NC+	No están documentadas evidencias de seguimiento, medición, análisis y evaluación del desempeño del sistema de gestión.

No conformidades menores

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
4	**Contexto de la organización**		
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	NC-	No están documentados todos los requisitos legales y contractuales.
6	**Planificación**		
6.1	Acciones para tratar los riesgos y oportunidades	NC-	No están documentados los crierios para llevar a cabo las apreciaciones de riesgo.
7	**Soporte**		
7.2	Competencia	NC-	No están documentadas las evidencias de competencias de todos los actores del sistema de gestión de información
8	**Operación**		
8.2	Apreciación de los riesgos de seguridad de la información	NC-	No hay evidencias de de los resultados de apreciación del riesgo.

b. CONTROLES

No conformidades mayores

Las NO Conformidades mayores detectadas se muestran en la siguiente tabla

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	SI	NC+	Aunque se ha definido la Política de Seguridad y algunas políticas espécificas, faltan otras políticas, alguna de ellas obligatorias como la política de seguridad de proveedores y
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.2	Segregación de tareas	SI	NC+	Aunque existen grupos de trabajo difeenciados, existen tareas que autoriza y realiza la misma pesona. No hay definida una política para la segregación de tareas.
A6.1.3	Contacto con las autoridades	SI	NC+	No esixten procedimientos documentados que especifiquen cuando y con qué autoridades se debería contactar.
A6.2	**Los dispositivos móviles y el teletrabajo**			
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	SI	NC+	No se realiza ningún tipo de comprbación de referencias ni confirmación de cualificaciones académicas.
A7.1.2	Términos y condiciones del empleo	SI	NC+	En los contratos no se incluyen clausulas relativas a la seguridad de la información, más alla de una simple cláusuala de deber de confidencialidad.
A7.2	**Durante el empleo**			
A7.2.3	Proceso disciplinario	SI	NC+	NO existe proceso disciplanario formal para el incumplimiento de medidas de seguridad.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio	SI	NC+	No se ha establecido procedimiento para comunicar las respensabilidades que se mantienen tras la baja de de usuarios y/o contratistas.
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.3	Uso aceptable de los activos	SI	NC+	No se ha definido política para el uso aceptable de los diferentes activos.
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	SI	NC+	No se realiza clasificación de la información que pemita protegerla adecuadametne en función de su importancia
A8.2.2	Etiquetado de la información	SI	NC+	NO se etiqueta la información
A8.2.3	Manipulado de la información	SI	NC+	NO existen procedimientos para la maniulación de la información
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles	SI	NC+	No existen procedimientos para la gestión de soportes extraibles
A8.3.2	Eliminación de soportes	SI	NC+	No existen procedimientos para la eliminación segura de soportes extraibles
A8.3.3	Soportes físicos en tránsito	**NO**		
A9	**Control de acceso**			
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.5	Control de acceso al código fuente de los programas	**NO**		
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos	SI	NC+	No existe política sobre controles criptográficos
A10.1.2	Gestión de claves	SI	NC+	No exite política sobre el ciclo de vida de claves.

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	SI	NC+	No hay definidos perímetros de seguridad física ni procedimientos formales de acceso a las salas técnicas.
A11.1.2	Controles físicos de entrada	SI	NC+	No hay definidas areas seguras ni controles de acceso a dichas áreas
A11.1.3	Seguridad de oficinas, despachos y recursos	SI	NC+	No existen directrices para asegurar las oficinas y despachos
A11.1.4	Protección contra las amenazas externas y ambientales	SI	NC+	No existen directrices, relativas a la seguridad de la información, para protección ante estas amenazas
A11.1.5	El trabajo en áreas seguras	SI	NC+	No se han definido areas seguras. No ha procedimientos para trabajar en salas técnicas
A11.1.6	Áreas de carga y descarga	SI	NC+	No hay procedimientos específicos, relativos a la seguridad de la información, para areas de carga y descarga
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	SI	NC+	No existen politicas ni procedimientos específicos para el emplazamiento y protección de los equipos
A11.2.2	Instalaciones de suministro	SI	NC+	No existen procedimientos para evaluar y/o inspeccionar regularmente las instalaciones de suministro
A11.2.3	Seguridad del cableado	SI	NC+	No existen procedimientos ni directrices para la seguridad del cableado.
A11.2.4	Mantenimiento de los equipos	SI	NC+	No existe procedimientos formales ni registros para el mantenidimiento de los equipos
A11.2.5	Retirada de materiales propiedad de la empresa	SI	NC+	NO existen procedimientos para la autorización de retirada de materiales de las oficinas
A11.2.7	Reutilización o eliminación segura de equipos	SI	NC+	No existen procedimientos definidos para la eliminación segura de los equipos
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	NC+	Política de puesto de trabajo despejado no definida
A12	**Seguridad de las operaciones**			
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información	SI	NC+	NO existen políticias ni procedimientos de auditoria definidos.
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A13.2.2	Acuerdos de intercambio de información	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A13.2.4	Acuerdos de confidencialidad o no revelación	SI	NC+	No hay politicas definidas ni procedimientos para el intercambio de información en las comunicaciones
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	NC+	No hay procedimiento formal para validar los requisitos de seguridad de los nuevos proyectos o sistemas
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI	NC+	No se ha definido el nivel de protección necesario para la información que se transmita por redes públicas
A14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	NC+	No se han definido controles para la protección de transacciones de servicios de aplicaciones
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	SI	NC+	No se han definido normas para el desarrollo seguro de las aplicaciones
A14.2.2	Procedimiento de control de cambios en sistemas	SI	NC+	No se han establecido procedimientos formales para la gestión de cambios en los sistemas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	NC+	No se han definido procedimientos formales para la revisión
A14.2.4	Restricciones a los cambios en los paquetes de software	SI	NC+	No se han documentdo normas para la limitación de la modificación de los paquetes de software
A14.2.5	Principios de ingeniería de sistemas seguros	SI	NC+	No existe documento que reflejen los principios de ingeniería de sistemas seguros
A14.2.6	Entorno de desarrollo seguro	SI	NC+	No se ha documentado los requisitos de seguridad de los entornos de desarrollo
A14.2.7	Externalización del desarrollo de software	SI	NC+	No exige a alos proveedores de desarrollo la presentación de la realización de pruebas de seguridad
A14.2.8	Pruebas funcionales de seguridad de sistemas	SI	NC+	No se realizan pruebas de seguridad funcional durante el desarrollo
A14.2.9	Pruebas de aceptación de sistemas	SI	NC+	No se establecen por norma pruebas de aceptación y criterios formales de los nuevos desarrollos
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba	SI	NC+	No se realiza selección de datos de prueba utilizando criterios de seguridad

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	NC+	No hay definida política de seguridad para proveedores
A15.1.2	Requisitos de seguridad en contratos con terceros	SI	NC+	No hay definida política de seguridad para proveedores
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	NC+	No hay definida política de seguridad para proveedores
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	NC+	No hay definida política de seguridad para proveedores
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	SI	NC+	No hay definida política de seguridad para proveedores
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	NC+	No están documentados los requerimientos legales, regulatorios y contractuales
A18.1.2	Derechos de Propiedad Intelectual (DPI)	SI	NC+	No hay procedimientos para garantizar el cumplimiento de los requisitos legales
A18.1.3	Protección de los registros de la organización	SI	NC+	No están documentados y categroizados los registros de la organización
A18.1.4	Protección y privacidad de la información de carácter personal	SI	NC+	No hay definida una política de privacidad y protección de los datos de carácter personal
A18.1.5	Regulación de los controles criptográficos	SI	NC+	No hay evidencias de controles criptograficos
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información	SI	NC+	No se realizan auditorías externoas
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	NC+	No se verifica por la dirección que los procedimientos de seguridad se realizan correctametne
A18.2.3	Comprobación del cumplimiento técnico	SI	NC+	No se realizan pruebas de instrusión ni, chequeos completos de vulnerabilidades

No conformidades menores

Las NO Conformidades Menores detectadas se muestran en la siguiente tabla

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	SI	NC-	Las responsabilidades se encuentran definidas conforme a la Política de Seguridad definida, pero no han recibido la formacion adecuada a sus responsabilidades en seguridad.
A7	**Seguridad relativa a los recursos humanos**			
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	SI	NC-	No se notifican a las contratas los requerimientos de la política de seguridad
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	NC-	Planificada formación a empleados. Pero no se verifica que los contratistas tengan la formación adecuada en seguridad
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.2	Propiedad de los activos	SI	NC-	NO se encuentra documentado el propietario de diversos activos

7. OPORTUNIDADES DE MEJORA

El análisis realizado ha permitido identificar importantes aéreas de mejora del SGSI, entre las que se pueden destacar:

- Definir e implementar la política de seguridad de proveedores. Es un documento obligatorio de la ISO/IEC 27001:2013. Su definición y desarrollo permitirá cumplir con los controles relativos al dominio *A15.Relación con proveedores* actualmente inexistentes.
- Definir e implementar procedimientos para la correcta gestión de la seguridad desde el punto de vista de los recursos humanos. Su definición y desarrollo permitirá que el SGSI cumpla con los controles relativos al *dominio A7. Seguridad relativa a los recursos humanos*.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información: recursos humanos, TI, etc.
- Identificar las distintas áreas físicas y clasificarlas en función de sus necesidades en cuanto a la seguridad. Definir procedimientos de identificación y acceso en base a la clasificación realizada.
- Definir e implementar procedimientos para la autorización de retirada de materiales de las oficinas.

8. PLANIFICACIÓN DE LA FUTURA AUDITORÍA

Se aconseja seguir plan de auditoría definido en RecycleSA y realizar una nueva auditoría interna en el primer semestre del año 2.020.

El periodo de tiempo hasta esa nueva auditoría se debe utilizar para definir nuevos proyectos orientados a la mejora del SGSI, y en concreto a las oportunidades de mejora identificadas en el punto anterior.

Se aconseja priorizar y definir dichos proyectos de mejora para su implantación en un espacio temporal que permita evaluar su impacto en el SGSI en la siguiente auditoría de cumplimiento.

9. CONCLUSIONES

El Sistema de Gestión de Seguridad auditado, se encuentra bien definido en los aspectos más relevantes que establece la norma ISO/IEC 27001:2013: definición clara del contexto del SGSI, liderazgo, definición de roles y responsabilidades, definición de políticas, operación, etc.

En ese sentido, el SGSI tiene implantados buena parte de los controles que la norma específica.

Sin embargo, adolece de importantes carencias en el desarrollo de las políticas y controles en algunos aspectos, como son las relativas a los recursos humanos y a los proveedores.

Igualmente es necesario procedimentar y aplicar el desarrollo de evidencias documentales de algunos aspectos, como los requerimientos legales, contractuales y regulatorios, así como los relativos al análisis y tratamientos de los riesgos y la evaluación del desempeño del sistema de gestión.

Es por ello que la organización, en el marco de la mejora continua del SGSI, debe hacer esfuerzos para el desarrollo e implantación de dichas políticas y controles, que se identifican como oportunidades de mejora en este documento.